EC-Council

N|DE™
Network Defense Essentials

Network Defense Essentials

Professional Series

https://t.me/learningnets

Network Defense Essentials

Version 1

https://t.me/learningnets

EC-Council

Copyright © 2021 by EC-Council. All rights reserved. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but may not be reproduced for publication without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, write to EC-Council, addressed "Attention: EC-Council," at the address below:

EC-Council New Mexico
101C Sun Ave NE
Albuquerque, NM 87109

Information contained in this publication has been obtained by EC-Council from sources believed to be reliable. EC-Council takes reasonable measures to ensure that the content is current and accurate; however, because of the possibility of human or mechanical error, we do not guarantee the accuracy, adequacy, or completeness of any information and are not responsible for any errors or omissions nor for the accuracy of the results obtained from use of such information.

The courseware is a result of extensive research and contributions from subject-matter experts from all over the world. Due credits for all such contributions and references are given in the courseware in the research endnotes. We are committed to protecting intellectual property rights. If you are a copyright owner (an exclusive licensee or their agent) and you believe that any part of the courseware constitutes an infringement of copyright, or a breach of an agreed license or contract, you may notify us at **legal@eccouncil.org**. In the event of a justified complaint, EC-Council will remove the material in question and make necessary rectifications.

The courseware may contain references to other information resources and security solutions, but such references should not be considered as an endorsement of or recommendation by EC-Council.

Readers are encouraged to report errors, omissions, and inaccuracies to EC-Council at **legal@eccouncil.org**. If you have any issues, please contact us at **support@eccouncil.org**.

NOTICE TO THE READER

EC-Council does not warrant or guarantee any of the products, methodologies, or frameworks described herein nor does it perform any independent analysis in connection with any of the product information contained herein. EC-Council does not assume, and expressly disclaims, any obligation to obtain and include information other than that provided to it by the manufacturer. The reader is expressly warned to consider and adopt all safety precautions that might be indicated by the activities described herein and to avoid all potential hazards. By following the instruction contained herein, the reader willingly assumes all risks in connection with such instructions. EC-Council makes no representations or warranties of any kind, including but not limited to the warranties of fitness for particular purpose or merchantability, nor are any such representations implied with respect to the material set forth herein, and EC-Council takes no responsibility with respect to such material. EC-Council shall not be liable for any special, consequential, or exemplary damages resulting, in whole or in part, from the reader's use of or reliance upon this material.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

Foreword

The computer network has become more and more complex over the past few years and so has the threats to its security. The impact of security breaches on organizations vary from monetary loss, reputation damage, waning customer loyalty, diminishing investor confidence, to legal consequences. It does not matter if an organization installs the state of the art security software solutions or if it spends thousands of dollars on the security mechanisms; the fact remains that no organization is completely secure. Organizations need a security specialist who can help mitigate the security threats.

Network security plays a vital role in most of the organizations. It is the process of preventing and detecting unauthorized use of an organization's networking infrastructure. It protects networks and their services from unauthorized modification, destruction, or disclosure. Network security assures that a network performs its critical functions securely without any harmful side effects. Security awareness and well-structured training can help find the weaknesses of a network and keep network administrators abreast of the latest threats and techniques by gaining a better understanding of risk exposure as well as the newest countermeasures.

The Network Defense Essentials (NDE) program covers the fundamental concepts of network security. It equips students with the skills required to identify the increasing network security threats that reflect on the organization's security posture and implement general security controls to protect the underlying networking infrastructure from unauthorized access, modification, destruction, or disclosure.

This program gives a holistic overview of the key components of network security. The course is designed for those interested in learning the various fundamentals of network security and aspire to pursue a career in network security.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

About EC-Council

The International Council of Electronic Commerce Consultants, better known as EC-Council, was founded in late 2001 to address the need for well-educated and certified information security and e-business practitioners. EC-Council is a global, member-based organization composed of industry and subject matter experts working together to set the standards and raise the bar in information security certification and education.

EC-Council first developed the Certified Ethical Hacker (C|EH) program with the goal of teaching the methodologies, tools, and techniques used by hackers. Leveraging the collective knowledge of hundreds of subject-matter experts, the CEH program has rapidly gained popularity around the world and is now delivered in more than 145 countries by more than 950 authorized training centers. It is considered as the benchmark for many government entities and major corporations around the globe.

EC-Council, through its impressive network of professionals and huge industry following, has also developed a range of other leading programs in information security and e-business. EC-Council certifications are viewed as the essential certifications needed when standard configuration and security policy courses fall short. Providing a true, hands-on, tactical approach to security, individuals armed with the knowledge disseminated by EC-Council programs are tightening security networks around the world and beating hackers at their own game.

Other EC-Council Programs

Security Awareness: Certified Secure Computer User

The purpose of the CSCU training program is to provide students with the necessary knowledge and skills to protect their information assets. This class will immerse students in an interactive learning environment where they will acquire fundamental understanding of various computer and network security threats such as identity theft, credit card fraud, online banking phishing scams, viruses and backdoors, email hoaxes, sexual predators and other online threats, loss of confidential information, hacking attacks, and social engineering. More importantly, the skills learnt from the class help students take the necessary steps to mitigate their security exposure.

Network Defense: Certified Network Defender

Students enrolled in the Certified Network Defender course will gain a detailed understanding of network defense and develop their hands-on expertise to perform in real-life network defense situations. They will gain the depth of technical knowledge required to actively design a secure network within your organization. This course provides a fundamental understanding of the true nature of data transfer, network technologies, and software technologies so that students may understand how networks operate, how automation software behaves, and how to analyze networks and their defense.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

Students will learn how to protect, detect, and respond to the network attacks as well as learning about network defense fundamentals, the application of network security controls, protocols, perimeter appliances, secure IDS, VPN, and firewall configuration. Students will also learn the intricacies of network traffic signature, analysis, and vulnerability scanning, which will help in designing improved network security policies and successful incident response plans. These skills will help organizations foster resiliency and operational continuity during attacks.

Ethical Hacking: Certified Ethical Hacker

The Certified Ethical Hacker (CEH) credential is the most trusted ethical hacking certification and accomplishment recommended by employers globally. It is the most desired information security certification and represents one of the fastest-growing cyber credentials required by critical infrastructure and essential service providers. Since the introduction of CEH in 2003, it is recognized as a standard within the information security community. CEH continues to introduce the latest hacking techniques and the most advanced hacking tools and exploits used by hackers and information security professionals today. The Five Phases of Ethical Hacking and the original core mission of CEH remain valid and relevant today: "To beat a hacker, you need to think like a hacker."

CEH provides an in-depth understanding of ethical hacking phases, various attack vectors, and preventative countermeasures. It will teach you how hackers think and act maliciously so that you will be better positioned to set up your security infrastructure and defend future attacks. Understanding system weaknesses and vulnerabilities help organizations strengthen their system security controls to minimize the risk of an incident.

CEH was built to incorporate a hands-on environment and systematic process across every ethical hacking domain and methodology, giving you the opportunity to work towards proving the required knowledge and skills needed to perform the job of an ethical hacker. You will be exposed to an entirely different posture towards the responsibilities and measures required to be secure.

Penetration Testing: Certified Penetration Testing Professional

CPENT certification requires you to demonstrate the application of advanced penetration testing techniques such as advanced Windows attacks, IOT systems attacks, advanced binaries exploitation, exploits writing, bypassing a filtered network, Operational Technology (OT) pen testing, accessing hidden networks with pivoting and double pivoting, privilege escalation, and evading defense mechanisms.

EC-Council's CPENT standardizes the knowledge base for penetration testing professionals by incorporating best practices followed by experienced experts in the field. The objective of the CPENT is to ensure that each professional follows a strict code of ethics, is exposed to the best practices in the domain of penetration testing and aware of all the compliance requirements required by the industry.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

Unlike a normal security certification, the CPENT credential provides an assurance that security professionals possess skills to analyze the security posture of a network exhaustively and recommend corrective measures authoritatively. For many years EC-Council has been certifying IT Security Professionals around the globe to ensure these professionals are proficient in network security defense mechanisms. EC-Council's credentials vouch for their professionalism and expertise thereby making these professionals more sought after by organizations and consulting firms globally.

Computer Forensics: Computer Hacking Forensic Investigator

Computer Hacking Forensic Investigator (CHFI) is a comprehensive course covering major forensic investigation scenarios. It enables students to acquire crucial hands-on experience with various forensic investigation techniques. Students learn how to utilize standard forensic tools to successfully carry out a computer forensic investigation, preparing them to better aid in the prosecution of perpetrators.

EC-Council's CHFI certifies individuals in the specific security discipline of computer forensics from a vendor-neutral perspective. The CHFI certification bolsters the applied knowledge of law enforcement personnel, system administrators, security officers, defense and military personnel, legal professionals, bankers, security professionals, and anyone who is concerned about the integrity of network infrastructures.

Incident Handling: EC-Council Certified Incident Handler

EC-Council's Certified Incident Handler (E|CIH) program has been designed and developed in collaboration with cybersecurity and incident handling and response practitioners across the globe. It is a comprehensive specialist-level program that imparts knowledge and skills that organizations need to effectively handle post breach consequences by reducing the impact of the incident, from both a financial and a reputational perspective.

E|CIH is a method-driven program that uses a holistic approach to cover vast concepts concerning organizational incident handling and response from preparing and planning the incident handling response process to recovering organizational assets after a security incident. These concepts are essential for handling and responding to security incidents to protect organizations from future threats or attacks.

Management: Certified Chief Information Security Officer

The Certified Chief Information Security Officer (CCISO) program was developed by EC-Council to fill a knowledge gap in the information security industry. Most information security certifications focus on specific tools or practitioner capabilities. When the CCISO program was

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

developed, no certification existed to recognize the knowledge, skills, and aptitudes required for an experienced information security professional to perform the duties of a CISO effectively and competently. In fact, at that time, many questions existed about what a CISO really was and the value this role adds to an organization.

The CCISO Body of Knowledge helps to define the role of the CISO and clearly outline the contributions this person makes in an organization. EC-Council enhances this information through training opportunities conducted as instructor-led or self-study modules to ensure candidates have a complete understanding of the role. EC-Council evaluates the knowledge of CCISO candidates with a rigorous exam that tests their competence across five domains with which a seasoned security leader should be familiar.

Application Security: Certified Application Security Engineer

The Certified Application Security Engineer (CASE) credential is developed in partnership with large application and software development experts globally. The CASE credential tests the critical security skills and knowledge required throughout a typical software development life cycle (SDLC), focusing on the importance of the implementation of secure methodologies and practices in today's insecure operating environment.

The CASE certified training program is developed concurrently to prepare software professionals with the necessary capabilities that are expected by employers and academia globally. It is designed to be a hands-on, comprehensive application security course that will help software professionals create secure applications. The training program encompasses security activities involved in all phases of the Software Development Lifecycle (SDLC): planning, creating, testing, and deploying an application.

Unlike other application security trainings, CASE goes beyond just the guidelines on secure coding practices and includes secure requirement gathering, robust application design, and handling security issues in post development phases of application development. This makes CASE one of the most comprehensive certifications on the market today. It is desired by software application engineers, analysts, testers globally, and respected by hiring authorities.

Incident Handling: Certified Threat Intelligence Analyst

Certified Threat Intelligence Analyst (C|TIA) is designed and developed in collaboration with cybersecurity and threat intelligence experts across the globe to help organizations identify and mitigate business risks by converting unknown internal and external threats into known threats. It is a comprehensive, specialist-level program that teaches a structured approach for building effective threat intelligence.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

In the ever-changing threat landscape, C|TIA is an essential Threat Intelligence training program for those who deal with cyber threats on a daily basis. Organizations today demand a professional-level cybersecurity threat intelligence analyst who can extract the intelligence from data by implementing various advanced strategies. Such professional-level Threat Intelligence training programs can only be achieved when the core of the curricula maps with and is compliant to government and industry published threat intelligence frameworks.

Incident Handling: Certified SOC Analyst

The Certified SOC Analyst (CSA) program is the first step to joining a security operations center (SOC). It is engineered for current and aspiring Tier I and Tier II SOC analysts to achieve proficiency in performing entry-level and intermediate-level operations.

CSA is a training and credentialing program that helps the candidate acquire trending and in-demand technical skills through instruction by some of the most experienced trainers in the industry. The program focuses on creating new career opportunities through extensive, meticulous knowledge with enhanced level capabilities for dynamically contributing to a SOC team. Being an intense 3-day program, it thoroughly covers the fundamentals of SOC operations, before relaying the knowledge of log management and correlation, SIEM deployment, advanced incident detection, and incident response. Additionally, the candidate will learn to manage various SOC processes and collaborate with CSIRT at the time of need.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

NDE Exam Information

NDE Exam Details	
Exam Title	**Network Defense Essentials (NDE)**
Exam Code	**112-51**
Availability	**EC-Council Exam Portal** (please visit **https://www.eccexam.com**)
Duration	**2 Hours**
Questions	**75**
Passing Score	**70%**

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

Table of Contents

Module 01: Network Security Fundamentals **1**

Fundamentals of Network Security 3

Network Security Protocols 17

Module 02: Identification, Authentication, and Authorization **41**

Access Control Principles, Terminologies, and Models 43

Identity and Access Management (IAM) Concepts 55

Module 03: Network Security Controls - Administrative Controls **71**

Regulatory Frameworks, Laws, and Acts 73

Design and Develop Security Policies 112

Conduct Different Types of Security and Awareness Training 128

Module 04: Network Security Controls - Physical Controls **139**

Importance of Physical Security 141

Physical Security Controls 146

Workplace Security 175

Environmental Controls 185

Module 05: Network Security Controls - Technical Controls **195**

Types of Network Segmentation 197

Types of Firewalls and their Role 219

Types of IDS/IPS and their Role 263

Types of Honeypots 324

Types of Proxy Servers and their Benefits 333

Fundamentals of VPN and its importance in Network Security 360

Security Incident and Event Management (SIEM) 421

User Behavior Analytics (UBA) 429

Antivirus/Anti-malware Software 433

Module 06: Virtualization and Cloud Computing **439**

Virtualization Essential Concepts and OS Virtualization Security 442

Cloud Computing Fundamentals 483

Insights of Cloud Security and Best Practices 512

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

Module 07: Wireless Network Security **547**
Wireless Network Fundamentals 549
Wireless Network Encryption Mechanisms 576
Types of Wireless Network Authentication Methods 592
Implement Wireless Network Security Measures 597

Module 08: Mobile Device Security **621**
Mobile Device Connection Methods 623
Mobile Device Management Concepts 629
Common Mobile Usage Policies in Enterprises 636
Security Risks and Guidelines Associated with Enterprises Mobile Usage Policies 651
Implement Enterprise-level Mobile Security Management Solutions 658
Implement General Security Guidelines and Best Practices on Mobile Platforms 676

Module 09: IoT Device Security **687**
IoT Devices, Application Areas, and Communication Models 689
Security in IoT-enabled Environments 707

Module 10: Cryptography and PKI **723**
Cryptographic Techniques 725
Cryptographic Algorithms 736
Cryptography Tools 751
Public Key Infrastructure (PKI) 758

Module 11: Data Security **771**
Data Security and its Importance 773
Security Controls for Data Encryption 782
Data Backup and Retention 805
Data Loss Prevention Concepts 856

Module 12: Network Traffic Monitoring **865**
Need and Advantages of Network Traffic Monitoring 867
Determine Baseline Traffic Signatures for Normal and Suspicious Network Traffic 872
Perform Network Monitoring for Suspicious Traffic 880

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

Glossary **903**
References **923**

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

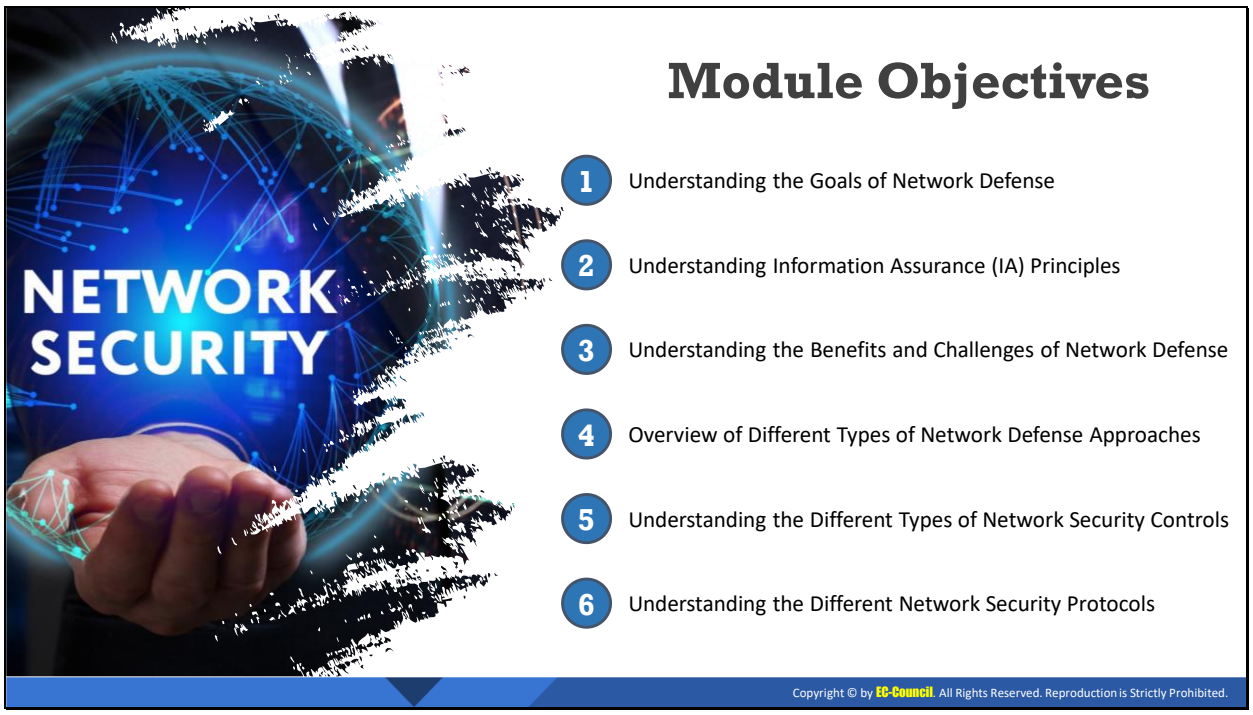
EC-Council

N|DE
Network Defense Essentials

Module 01

Network Security Fundamentals

https://t.me/learningnets



Module Objectives

With the increase in the usage of emerging technology, it has become increasingly important to secure information and data being processed online. As the Internet and computer networks are continually growing, network security has become a challenging task for organizations. Every organization requires a stable and efficient network security architecture that protects their critical assets and information systems from evolving threats.

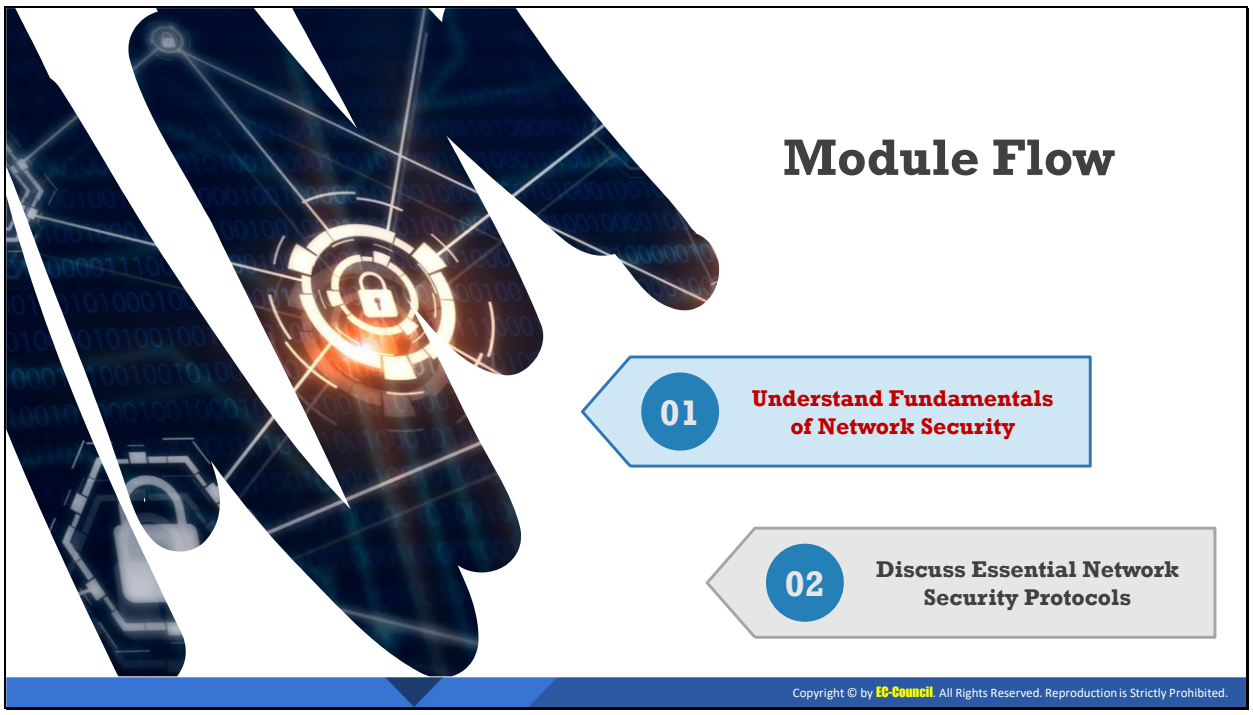
This module starts with an overview on network security and network defense. It provides insight into the different types of network defense approaches. Later, the module discusses the types of network security controls and ends with a brief discussion on network security protocols.

At the end of this module, you will be able to do the following:

- Understand the goals of network defense
- Describe the information assurance principles
- Describe the types of network defense approaches
- Understand the benefits and challenges of network defense
- Explain the different types of network security controls
- Explain the different network security protocols

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

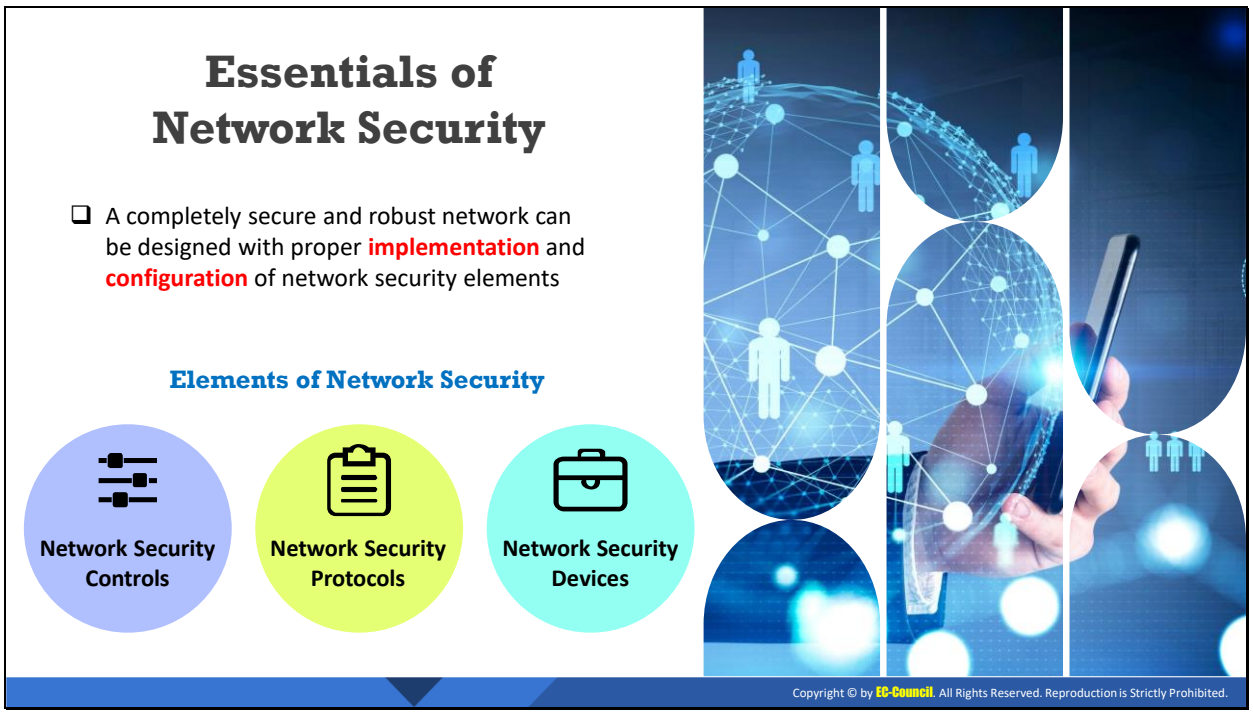


Understand Fundamentals of Network Security

Network security helps organizations in implementing necessary preventative measures to protect their IT infrastructure from misuse, unauthorized access, information disclosure, unauthorized access or modification of data in transit, destruction, etc., thereby providing a secure environment for the users, computers, and programs to perform their regular functions.

This section discusses the goal of network defense, information assurance principles, network defense benefits and challenges, types of network defense approaches and types of network security controls.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Essentials of Network Security

A completely secure and robust network can be designed with proper implementation and configuration of network security elements.

Network security relies on three main security elements:

- **Network Security Controls**

  Network security controls are the security features that should be appropriately configured and implemented to ensure network security. These are the cornerstones of any systematic discipline of security. These security controls work together to allow or restrict the access to organization's resources based on identity management.

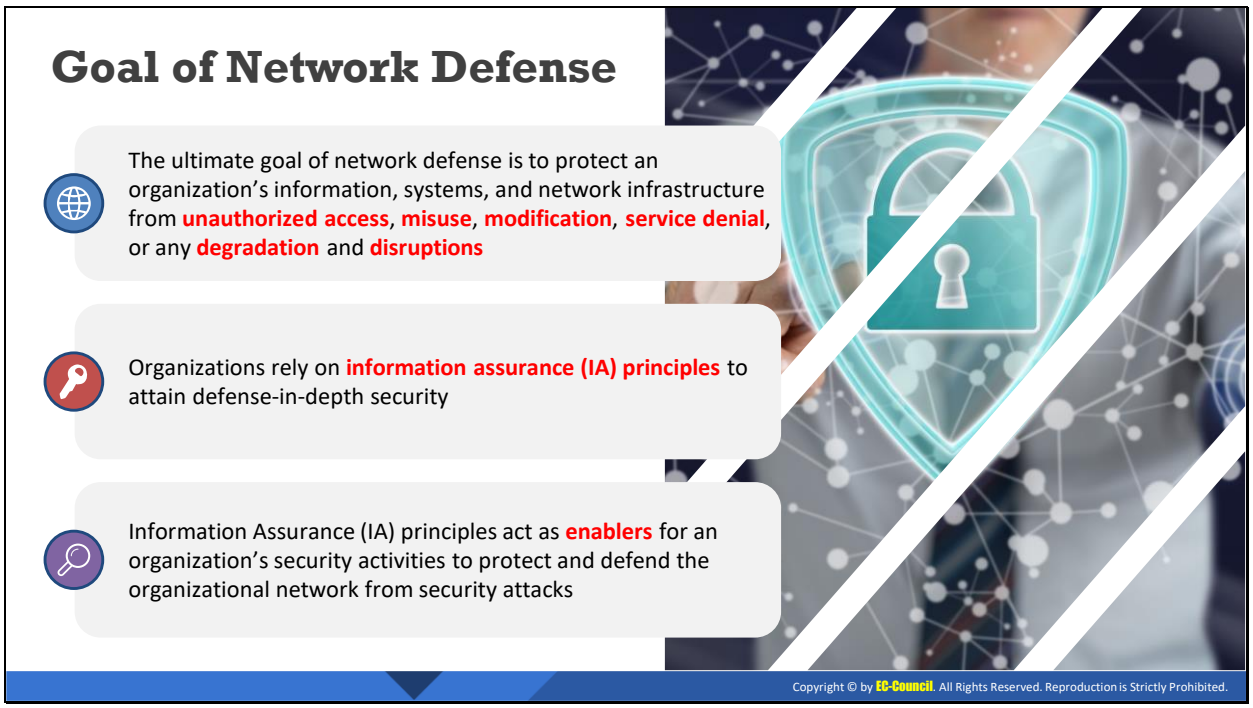
- **Network Security Protocols**

  Network security protocols implement security related operations to ensure the security and integrity of data in transit. The network security protocols ensure the security of the data passing through the network. They implement methods that restrict unauthorized users from accessing the network. The security protocols use encryption and cryptographic techniques to maintain the security of messages passing through the network.

- **Network Security Devices**

  Network security appliances are devices that are deployed to protect computer networks from unwanted traffic and threats. These devices can be categorized into active devices, passive devices, and preventative devices. It also consists of Unified Threat Management (UTM) which combines features of all the devices.

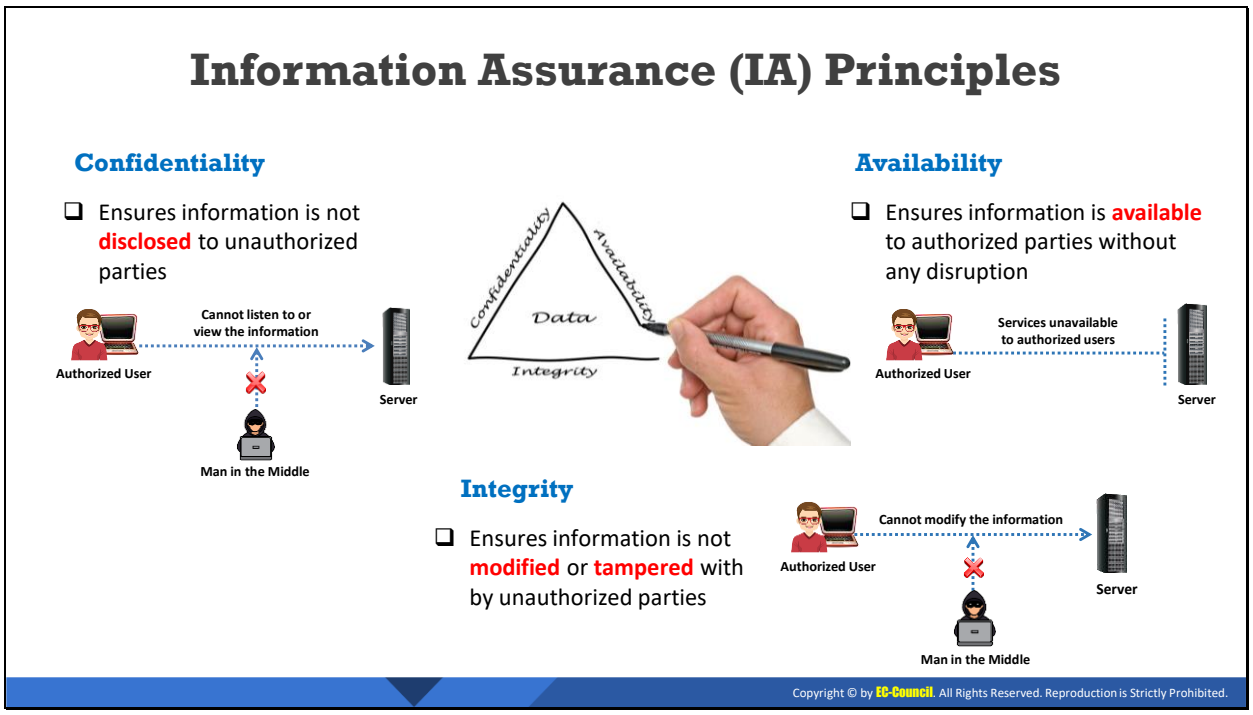
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

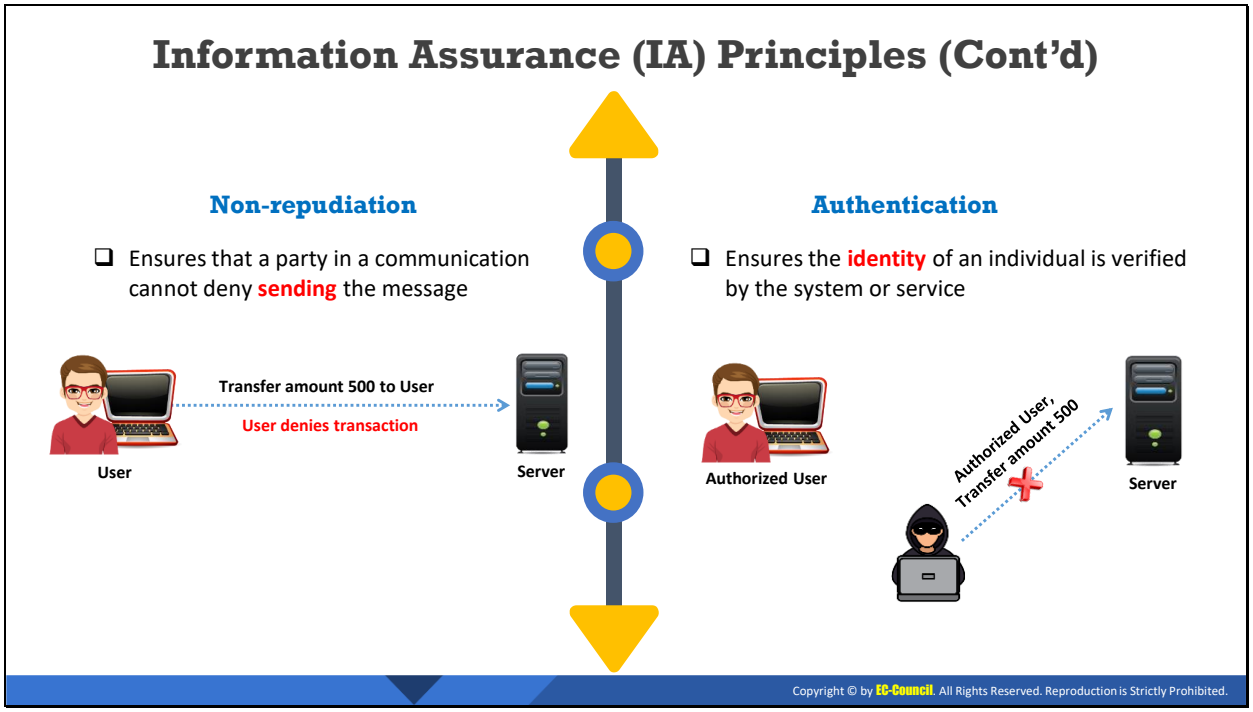


Goal of Network Defense

Different types of unauthorized or illegal activities may include interrupting, damaging, exploiting, or restricting access to networks or computing resources and stealing data and information from them. The implementation of numerous security measures, by itself, does not guarantee network security. For example, many organizations assume that deploying a firewall, or multiple firewalls, on the network is sufficient to protect their infrastructure from a variety of threats. However, attackers can bypass such security measures to gain access to systems. Thus, it is important to ensure comprehensive network defense to prevent and mitigate various types of threats. The goal of comprehensive network defense is to deploy continual and defense-in-depth security, which involves predicting, protecting, monitoring, analyzing, detecting, and responding to unauthorized activities such as unauthorized access, misuse, modification, service denial, and any degradation or disruption in the network, and to guarantee the overall security of the network. Organizations rely on information assurance (IA) principles to attain defense-in-depth security.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets





Information Assurance (IA) Principles

Information assurance (IA) principles act as enablers for an organization's security activities to protect and defend its network from security attacks. They facilitate the adoption of appropriate countermeasures and response actions upon a threat alert or detection. Therefore, network operators must use IA principles to identify data that is sensitive, and to counter events that may have security implications for the network. IA principles assist them in

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

identifying network security vulnerabilities, monitoring the network for any intrusion attempts or malicious activity, and defending the network by mitigating vulnerabilities.

Network defense activities should address the following IA principles to achieve defense-in-depth network security:

- **Confidentiality:** Confidentiality permits only authorized users to access, use or copy information. Authentication is crucial for confidentiality. If an unauthorized user accesses protected information, it implies that a breach of confidentiality has occurred.

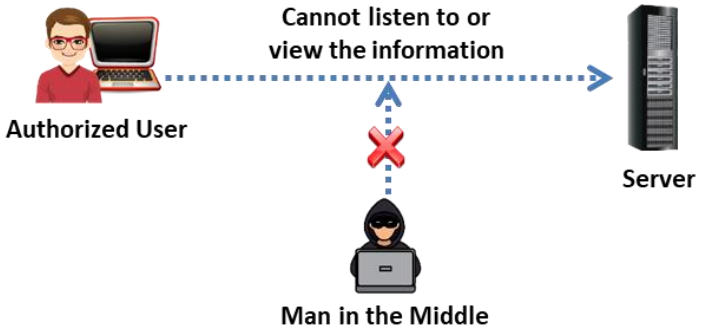


Figure 1.1: Confidentiality

- **Integrity:** Integrity protects data and does not allow modification, deletion, or corruption of data without proper authorization. This information assurance principle also relies on authentication to function properly.

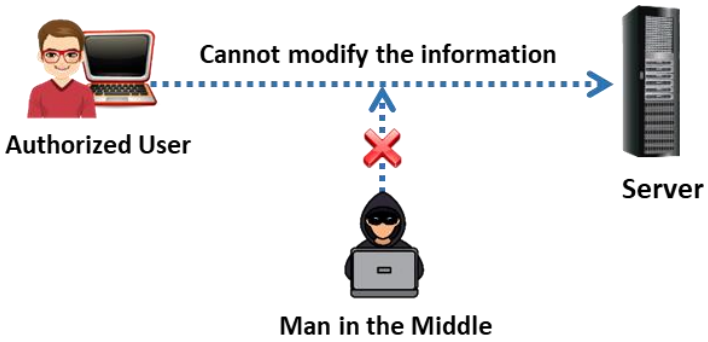


Figure 1.2: Integrity

- **Availability:** Availability is the process of protecting information systems or networks that store sensitive data, to make them available for the end users whenever they request access.

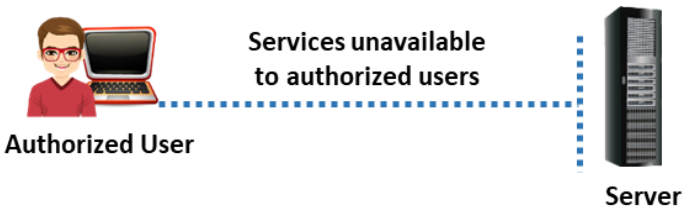


Figure 1.3: Availability

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **Non-repudiation:** Non-repudiation is a service that validates the integrity of a digital signature's transmission, starting from where it originated to where it arrived. Non-repudiation grants access to protected information by validating that the digital signature is from the intended party.

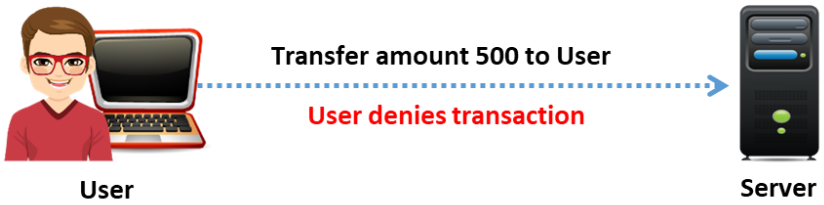


Figure 1.4: Non-repudiation

- **Authentication:** Authentication is a process of authorizing users with the credentials provided, by comparing them to those in a database of authorized users on an authentication server, to grant access to the network. It guarantees that the files or data passing through the network is safe.

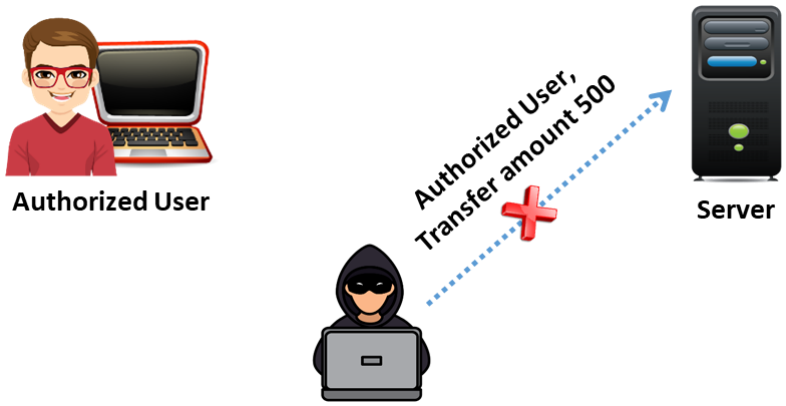
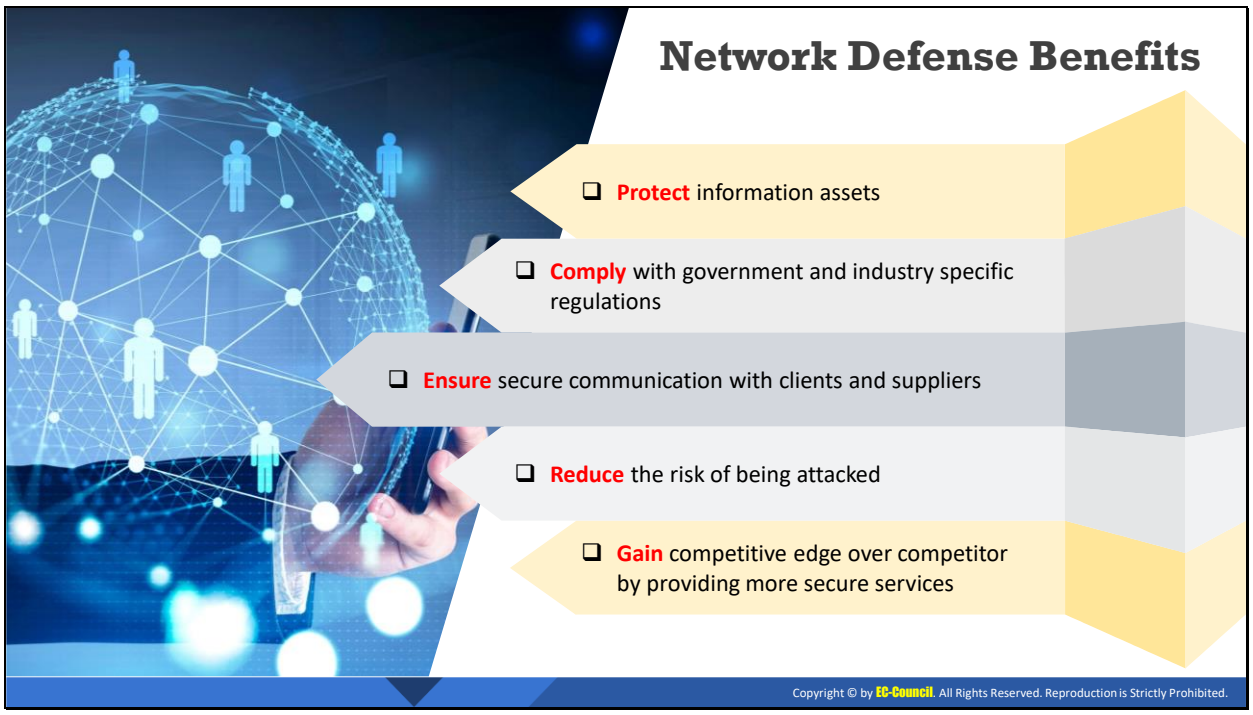


Figure 1.5: Authentication

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



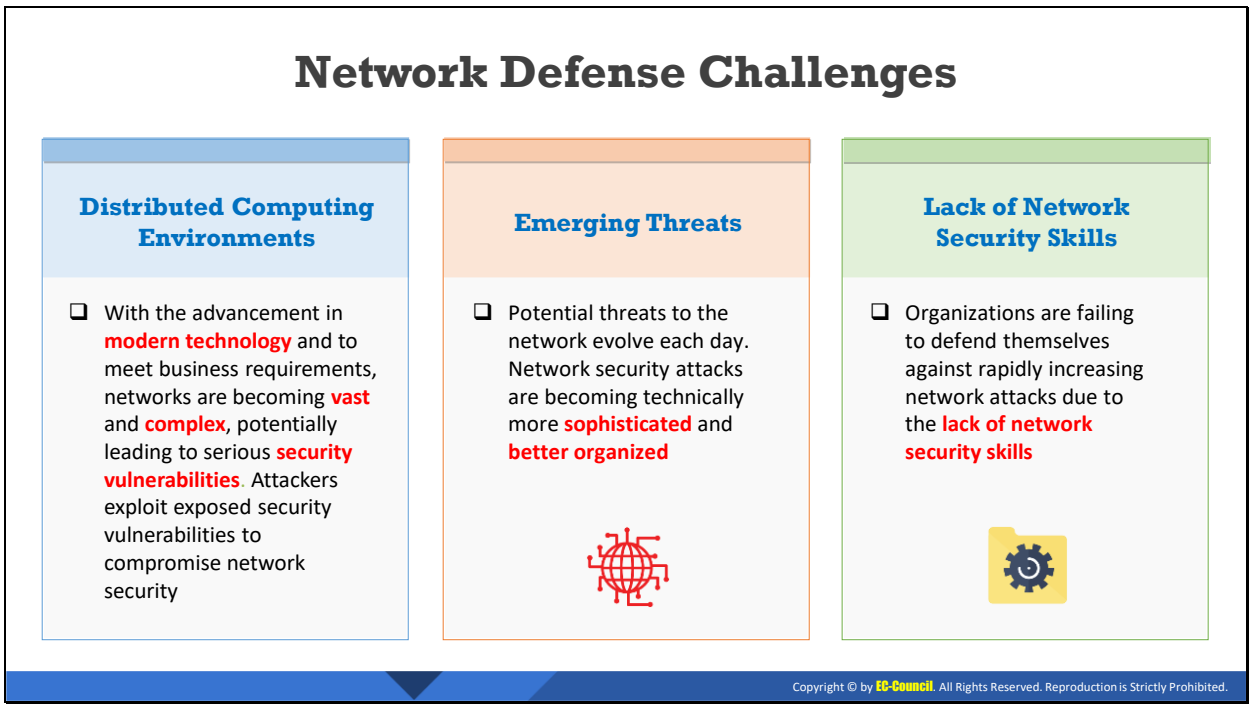
Network Defense Benefits

Network security is crucial for all organizations, irrespective of size. It safeguards systems, files, data, and personal information and protects these from unauthorized access.

In addition to ensuring protection against hacking attempts and virus attacks, network security provides the following indirect advantages and benefits.

- **Increased Profits**: Keeping computer networks secure is critical for any organization. With the deployment of comprehensive network defense, the organization can prevent threats, attacks, and vulnerabilities, which could otherwise cause significant loss. Thus, network security indirectly supports the organization in terms of profits. It also allows organizations to gain a competitive edge by providing more secure services.
- **Improved Productivity**: Network security can also help in improving the productivity of an organization. For example, it prevents employees from spending time on unproductive activities over the Internet such as browsing adult content, gaming, and gossip during office hours. These activities can be restricted with safe browsing techniques, consequently improving productivity.
- **Enhanced Compliance**: Network security helps organizations avoid penalties for lack of compliance. The real-time monitoring of data flows helps organizations enhance their compliance posture.
- **Client Confidence**: The knowledge that an organization's systems and data are protected and safe enhances clients' confidence and trust in the organization. This may translate into future purchases of other service offerings from the organization.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



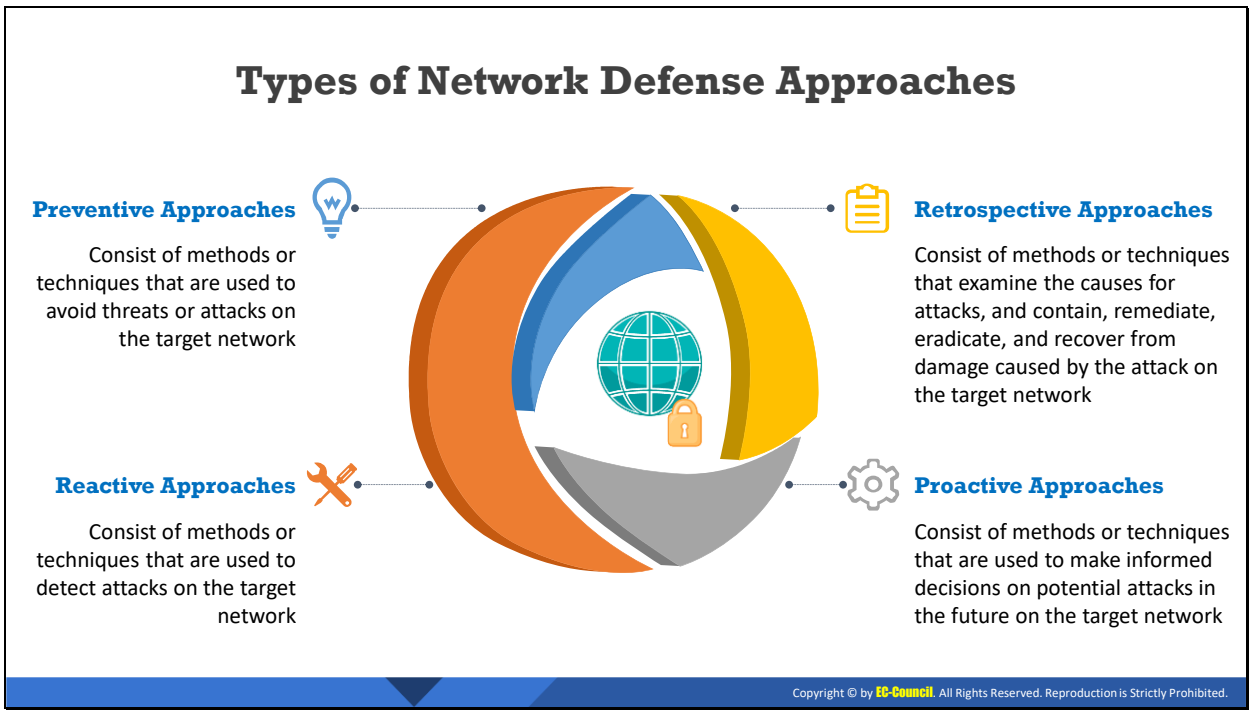
Network Defense Challenges

- **Distributed computing environments:** With the advancement in modern technology and to meet business requirements, networks are becoming vast and complex, potentially with serious security vulnerabilities. Attackers exploit exposed security vulnerabilities to compromise network security.
- **Emerging threats:** Potential threats to the network evolve on a daily basis. Network security attacks are becoming technically more sophisticated and better organized.
- **Lack of network security skills:** Organizations are failing to defend themselves against rapidly increasing network attacks owing to the lack of network security skills.

In addition to the broad categories of challenges discussed in the above, a network defender may face the following challenges in maintaining the security of a network:

- Protecting the network from attacks via the Internet
- Protecting public servers such as web, e-mail, and DNS servers
- Containing damage when a network or system is compromised
- Preventing internal attacks against the network
- Protecting highly important and sensitive information such as customer databases, financial records, and trade secrets
- Developing guidelines for network defenders to handle the network in a secure manner
- Enabling intrusion detection and logging capabilities

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Types of Network Defense Approaches

There are four main classifications of security defense techniques used for identification and prevention of threats and attacks in the network.

- **Preventive Approach:** The preventive approach essentially consists of methods or techniques that can easily prevent threats or attacks in the target network.

  The preventive approaches mainly used in networks are as follows:

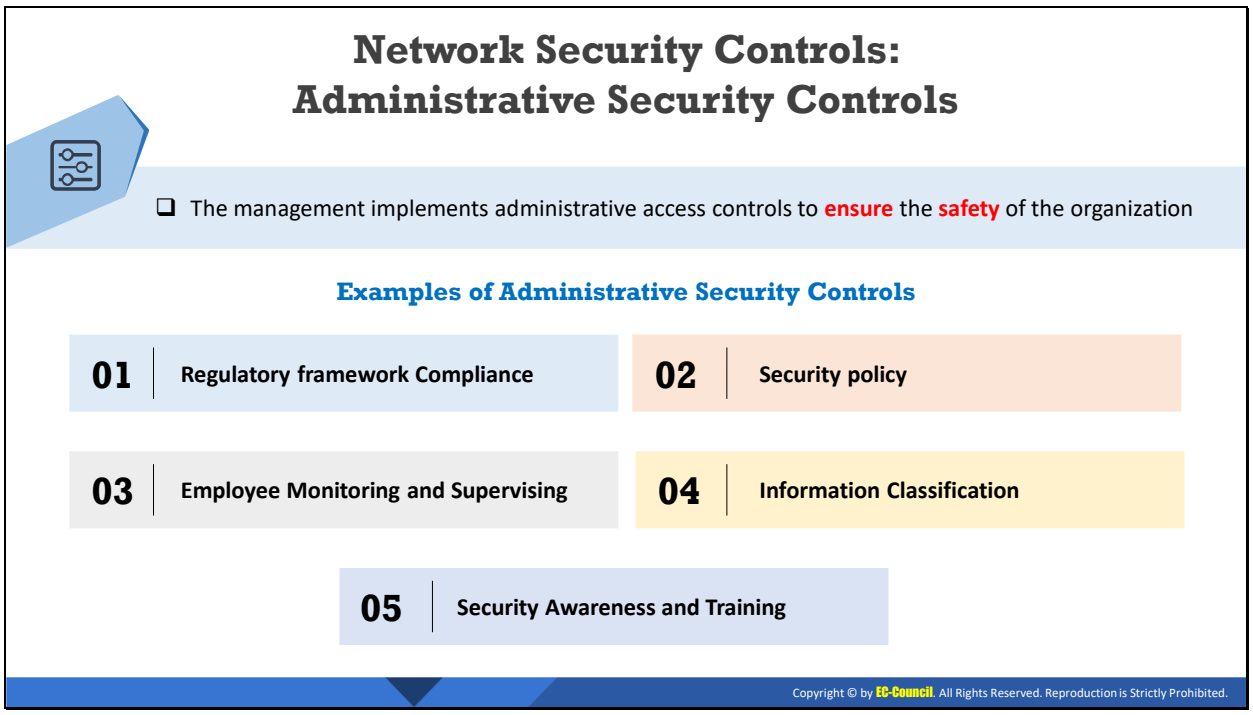
  - Access control mechanisms such as a firewall.
  - Admission control mechanisms such as NAC and NAP.
  - Cryptographic applications such as IPSec and SSL.
  - Biometric techniques such as speech or facial recognition.
- **Reactive Approach:** The reactive approach is complementary to the preventive approach. This approach addresses attacks and threats that the preventative approach may have failed to avert, such as DoS and DDoS attacks. It is necessary to implement both preventive and reactive approaches to ensure the security of the network. Reactive approaches include security monitoring methods such as IDS, SIMS, TRS, and IPS.
- **Retrospective Approach:** The retrospective approach examines the causes for attacks in the network. These include:
  - Fault finding mechanisms such as protocol analyzers and traffic monitors.
  - Security forensics techniques such as CSIRT and CERT.
  - Post-mortem analysis mechanism including risk and legal assessments.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **Proactive Approach:** The proactive approach consists of methods or techniques that are used to inform decision making for countering future attacks on the target network. Threat intelligence and risk assessment are examples of methods that can be used to assess probable future threats on the organization. The methods in this approach facilitate in the implementation of preemptive security actions and measures against potential incidents.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Network Security Controls

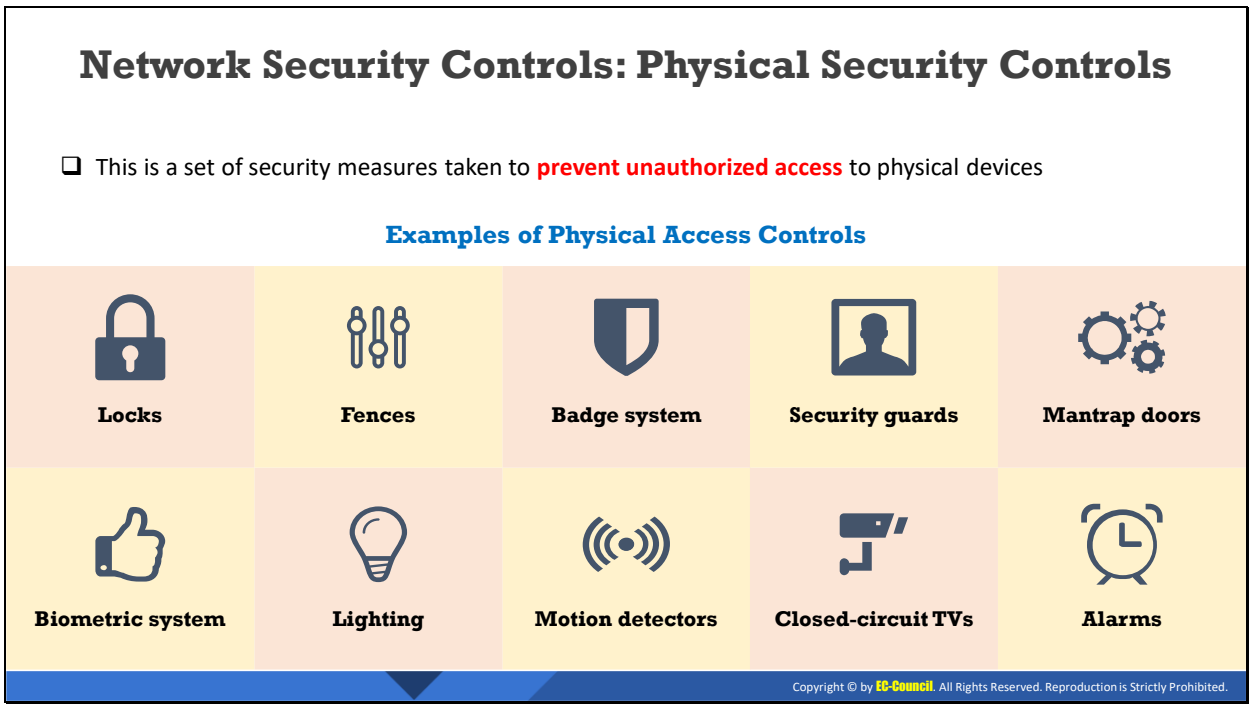
Administrative Security Controls

Administrative security controls are management limitations, operational and accountability procedures, and other controls that ensure the security of an organization. The procedures prescribed in administrative security control ensure the authorization and authentication of personnel at all levels.

Components of an administrative security control includes:

- Regulatory framework compliance
- Security policy
- Employee monitoring and supervising
- Information classification
- Separation of duties
- Principle of least privileges
- Security awareness and training

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Physical Security Controls

Appropriate physical security controls can reduce the chances of attacks and risks in an organization. Physical security controls provide physical protection of the information, buildings, and all other physical assets of an organization.

Physical security controls are categorized into:

- **Prevention Controls**

  These are used to prevent unwanted or unauthorized access to resources. They include access controls such as fences, locks, biometrics, and mantraps.

- **Deterrence Controls**

  These are used to discourage the violation of security policies. They include access controls such as security guards and warning signs.

- **Detection Controls**

  These are used to detect unauthorized access attempts. They include access controls such as CCTV and alarms.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Examples of Physical Access Controls:

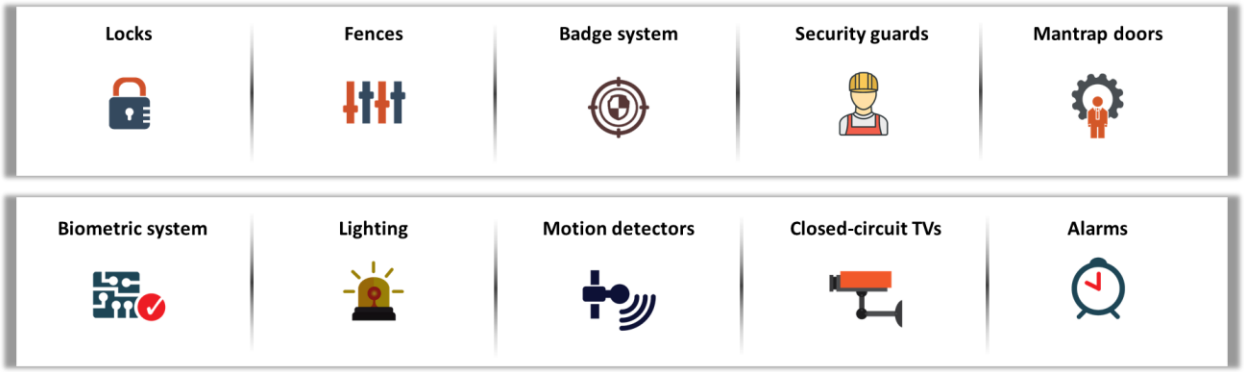
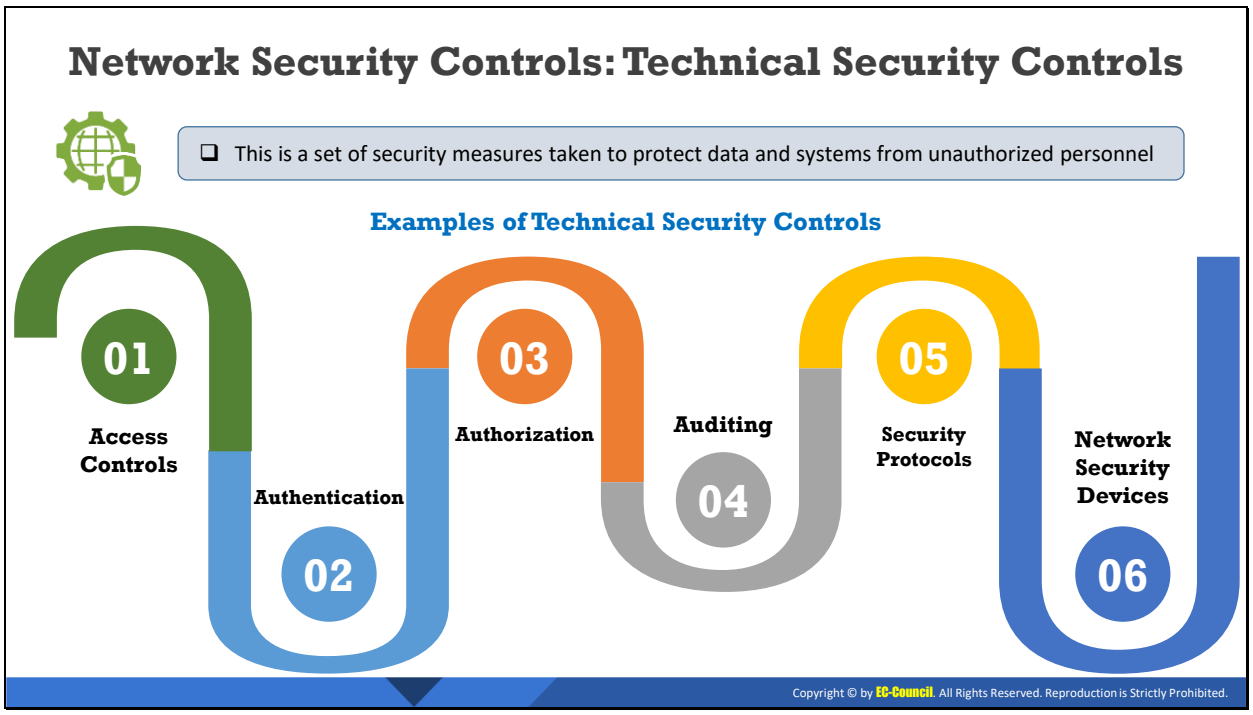


Figure 1.6: Physical Security Controls

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



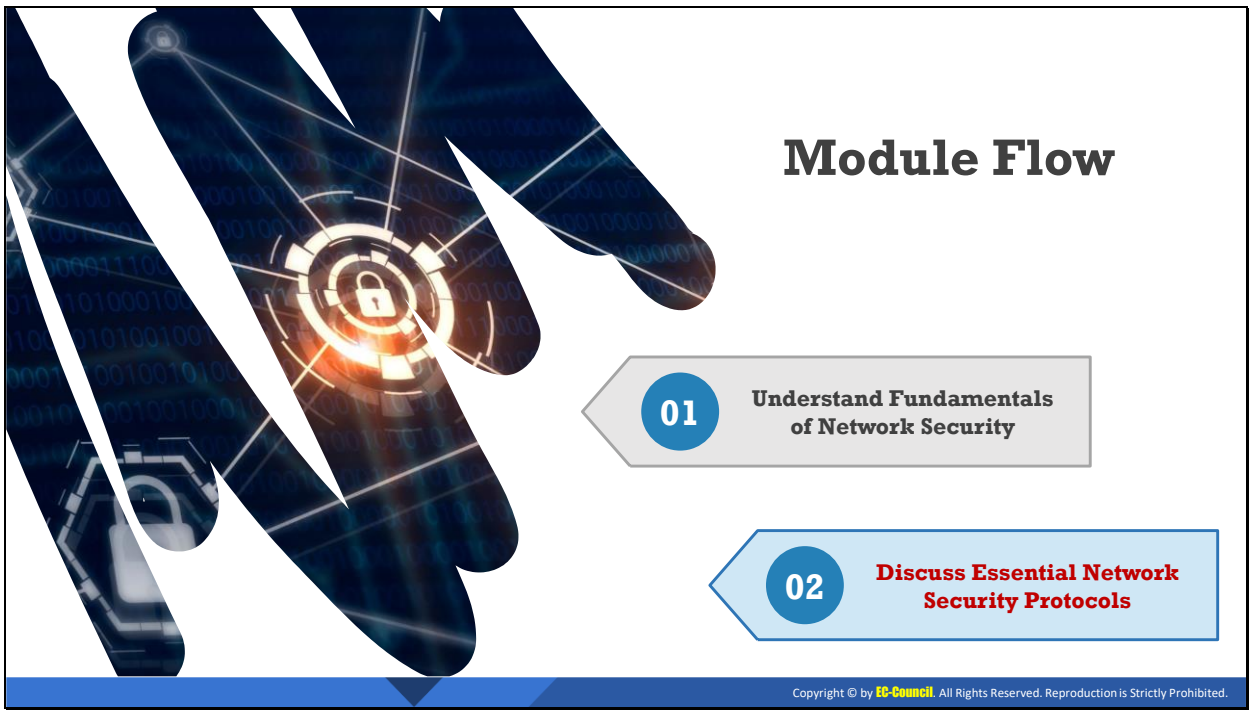
Technical Security Controls

Technical security controls are used for restricting access to devices in an organization to protect the integrity of sensitive data.

The components of technical security controls include:

- **System access controls:** System access controls are used for the restriction of access to data according to sensitivity of data, clearance level of users, user rights, and permissions.
- **Network access controls:** Network access controls offer various access control mechanisms for network devices like routers and switches.
- **Authentication and authorization:** Authentication and authorization ensure that only users with appropriate privileges can access the system or network resources.
- **Encryption and Protocols:** Encryption and protocols protect the information passing through the network and preserve the privacy and reliability of the data.
- **Network Security Devices:** Network security devices such as firewall and IDS are used to filter and detect malicious traffic, thus protecting the organization from threats.
- **Auditing:** Auditing refers to the tracking and examining of the activities of network devices in a network. This mechanism helps in identifying weaknesses in the network.

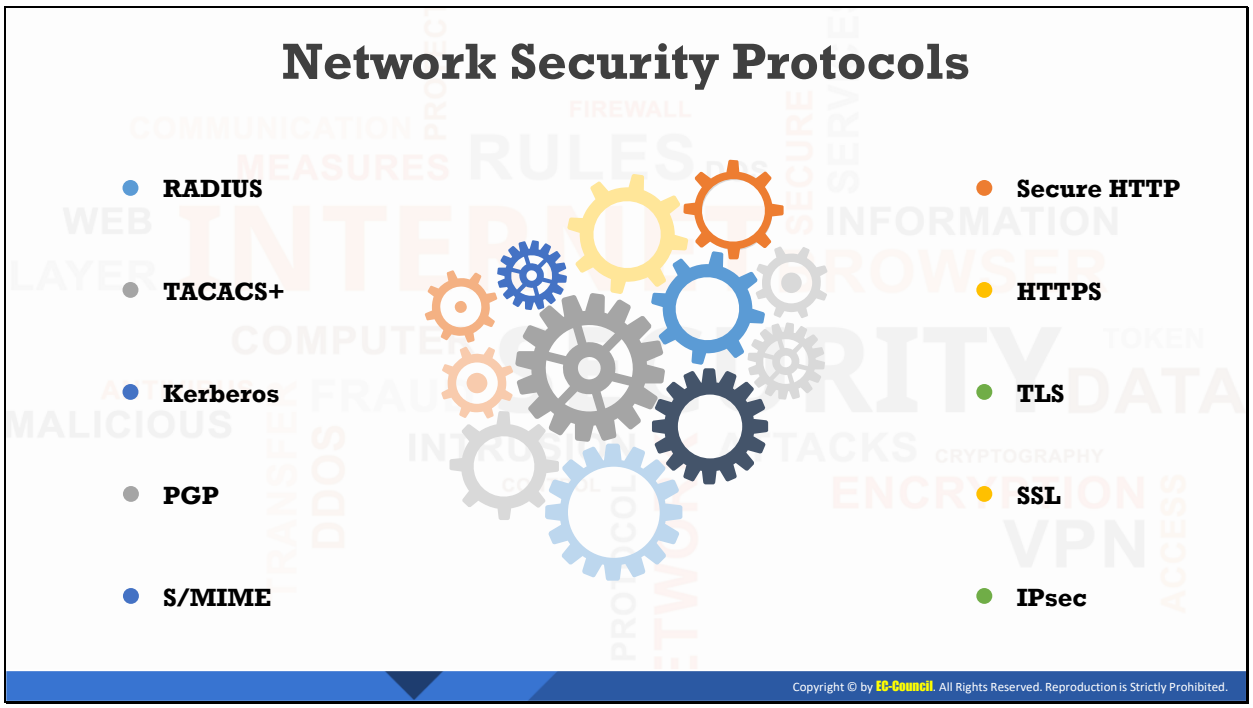
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Discuss Essential Network Security Protocols

The objective of this section is to explain the various essential network security protocols that work at the network, transport, and application layers. Details of Remote Access Dial-In User Service (RADIUS), TACAS terminal access controller access control system plus (TACACS+), Kerberos, Pretty good privacy (PGP), S/MIME, HyperText Transfer Protocol Secure (HTTPS), Transport Layer Security (TLS), Secure Sockets Layer (SSL), and Internet protocol Security (IPSec) protocols will be discussed in this section.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Network Security Protocols

There are various security protocols that work at the network, transport, and application layers. These protocols help organizations to enhance the security of their data and communication against different types of attacks.

- The security protocols that work at the **transport layer** are as follows:
  - **Transport Layer Security (TLS):** The TLS protocol provides security and dependability of data between two communicating parties.
  - **Secure Sockets Layer (SSL):** The SSL protocol provides security to the communication between a client and a server.
- The security protocols that work at the **network layer** are as follows:
  - **Internet Protocol Security (IPsec):** The IPSec protocol authenticates the packets during the transmission of data.
- The security protocols that work at the **application layer** are as follows:
  - **Pretty Good Privacy (PGP) protocol:** The PGP protocol provides cryptographic privacy and authentication for network communication and enhances the security of emails.
  - **S/MIME protocol:** Commonly known as Secure/Multi-Purpose Internet mail Extension. The S/MIME protocol provides security to e-mails.
  - **Secure HTTP:** Secure HTTP provides security to the data traversing through the world wide web.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **Hyper Text Transfer Protocol Secure (HTTPS):** The HTTPS protocol is widely used across the Internet to secure network communication.
- **Kerberos:** Kerberos is a client-server model that is implemented for authenticating requests in computer networks.
- **RADIUS**: The RADIUS protocol provides centralized authentication, authorization, and accounting (AAA) for remote-access servers to communicate with a central server.
- **TACACS**+: TACACS+ provides authentication, authorization, and accounting (AAA) services for network communication.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

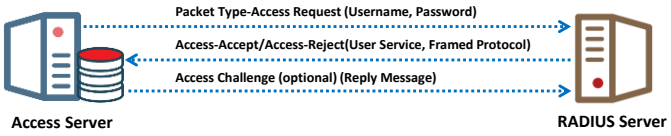
https://t.me/learningnets

Remote Authentication Dial-in User Service (RADIUS)

- Remote authentication dial-in user service (RADIUS) is an **authentication protocol** which provides centralized authentication, authorization, and accounting (AAA) for remote access servers to communicate with a central server

Authentication Steps in RADIUS

1) A client initiates a connection by sending the **access-request packet** to the server
2) The server receives the access request from the client and compares the credentials with the ones stored in the database. If the provided information matches, then it sends the **access-accept message** along with the **access-challenge** to the client for additional authentication, else it sends back an **accept-reject** message
3) Client sends the **accounting-request** to the server to specify the accounting information for a connection that was accepted

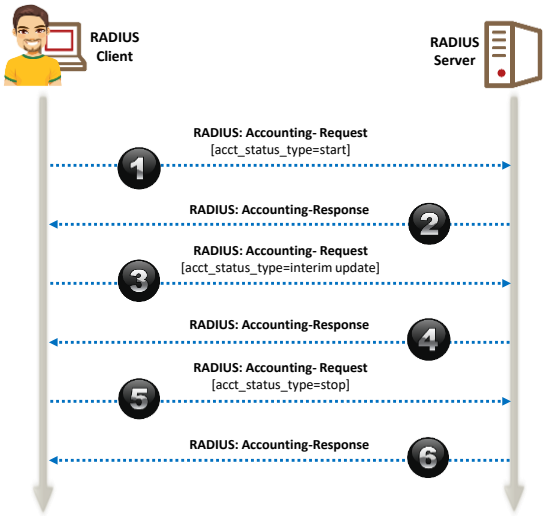


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Remote Authentication Dial-in User Service (RADIUS) (Cont'd)

Radius Accounting Steps

- Client sends the **accounting-request** to the server to specify the accounting information for a connection that was accepted
- The server receives this message and sends back the **accounting-response message** which states the successful establishment of the network



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Remote Authentication Dial-in User Service (RADIUS)

RADIUS stands for remote authentication dial-in user service. It was developed by Livingston Enterprises as a networking protocol, which provides centralized authentication, authorization, and accounting (AAA) for remote access servers to communicate with a central server. RADIUS has a client-server model, which works on the application layer of the OSI model by using UDP or TCP as a transport protocol. The RADIUS protocol is the de-facto standard for remote user authentication and is documented in RFC 2865 and RFC 2866.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

Authentication Steps in RADIUS:

- A client initiates a connection by sending an access-request packet to the server.
- The server receives the access request from the client and compares their credentials with those stored in the database. If the provided information matches, then the server sends an access-accept message along with the access-challenge to the client for additional authentication; else, it sends an access-reject message.
- The client sends an accounting-request to the server to specify the accounting information for a connection that was accepted.

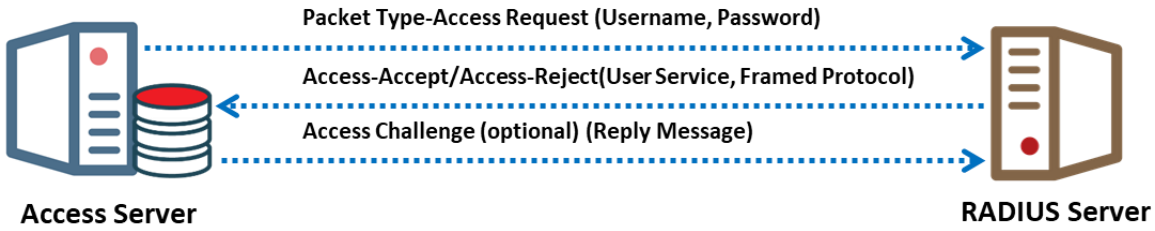


Figure 1.7: Authentication Steps in RADIUS

Radius Accounting Steps:

- The client sends an accounting-request to the server to specify the accounting information for a connection that was accepted.
- The server receives this message and sends back an accounting-response message, which states the successful establishment of the network.

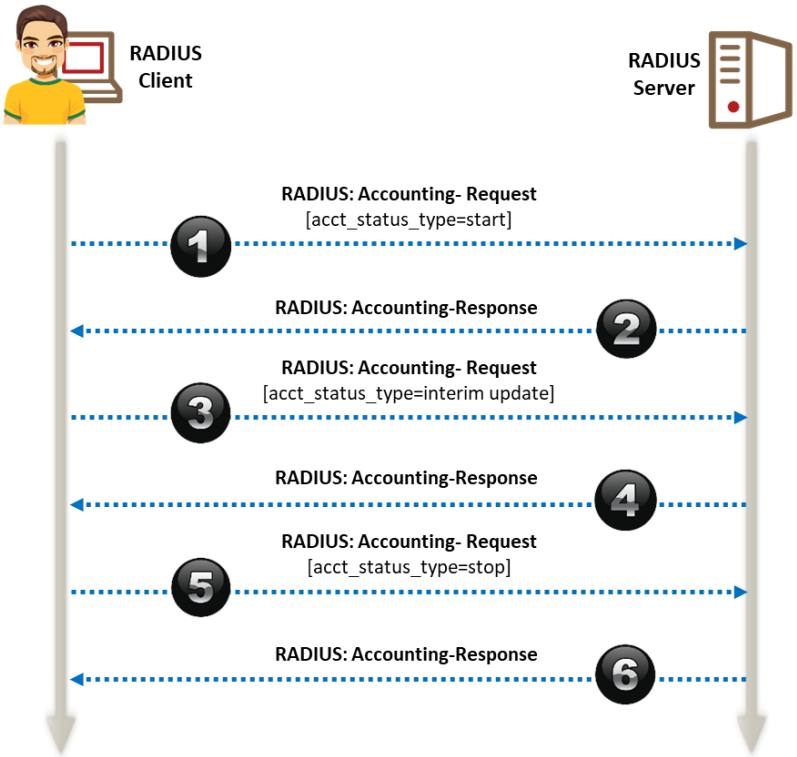


Figure 1.8: Radius Accounting Steps

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

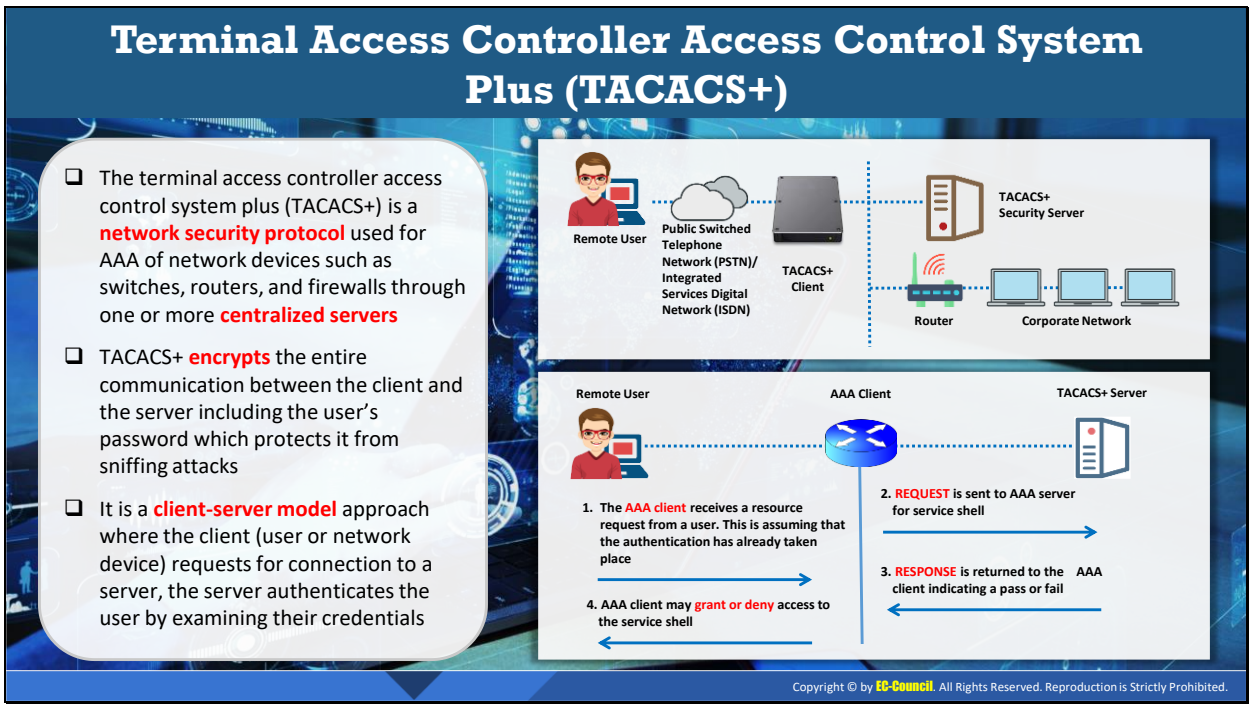
The RADIUS protocol is an AAA protocol that works on mobile as well as local networks. It uses the password authentication protocol (PAP), the challenge handshake authentication protocol (CHAP), or extensible authentication protocol (EAP) in order to authenticate the users communicating with servers. The components of a RADIUS AAA protocol are:

- Access clients
- Access servers
- RADIUS proxies
- RADIUS servers
- User account databases

RADIUS messages are sent as UDP messages and allow only one RADIUS message in the UDP payload section of the RADIUS packet. RADIUS messages consist of a RADIUS header and other RADIUS attributes.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Terminal Access Controller Access Control System Plus (TACACS+)

The Terminal Access Controller Access-Control System Plus (TACACS+) is a protocol developed by Cisco. It is derived from the TACACS protocol and performs AAA separately, unlike RADIUS. It is primarily used for device administration.

TACACS+ encrypts the entire communication between the client and server, including the user's password, which protects it from sniffing attacks. It is a client-server model approach in which the client (user or network device) requests for connection to a server and the server authenticates the user by examining their credentials.

Authentication of TACACS+

Consider the following example of authentication where a laptop user is connecting to a network-attached storage (NAS, router). The TACACS+ authentication involves the following steps:

- **Step 1**: A user initiates the connection for authentication
- **Step 2**: The router and the user exchange authentication parameters
- **Step 3**: The router sends the parameters to the server for authentication
- **Step 4**: The server responds with the REPLY message based on the provided information

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

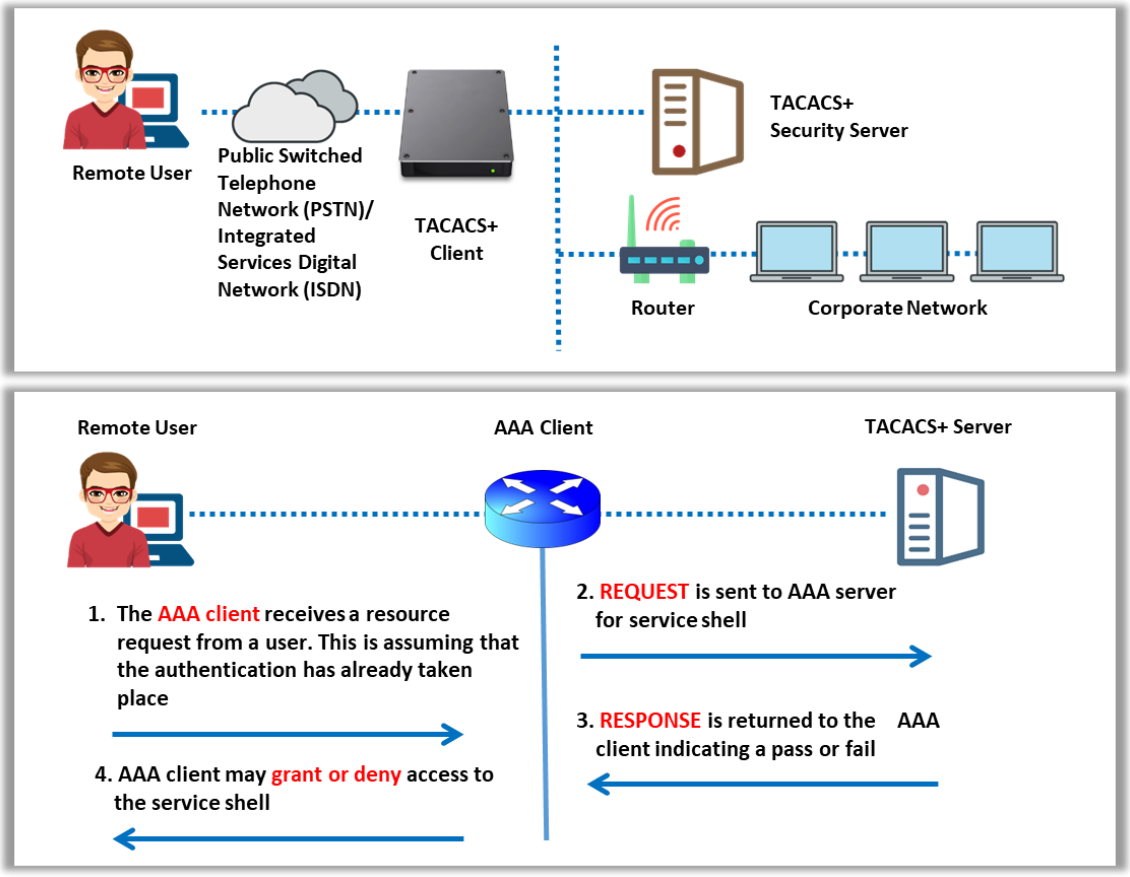


Figure 1.9: Authentication of TACACS+

Difference between RADIUS and TACACS+

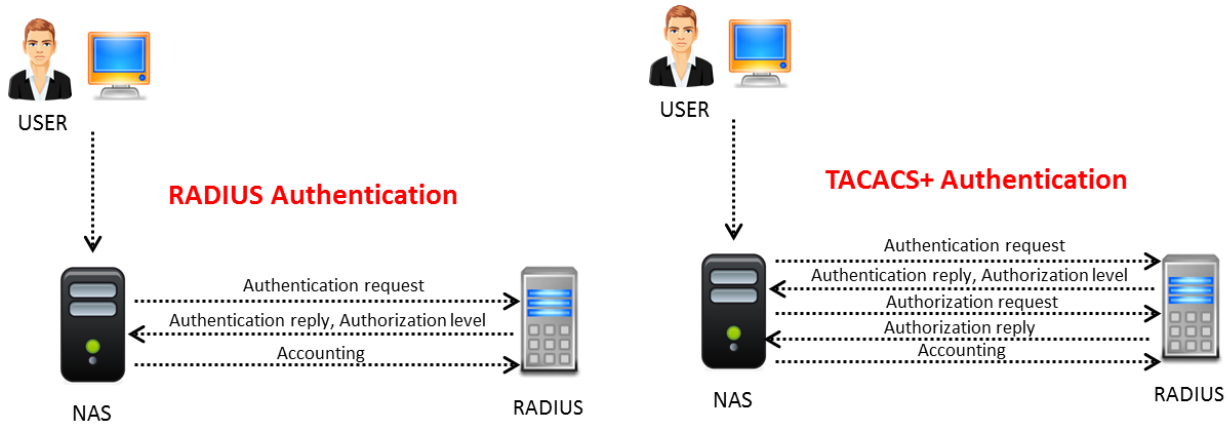


Figure 1.10: Schematic Showing the Different Between RADIUS and TACACS+ Protocols

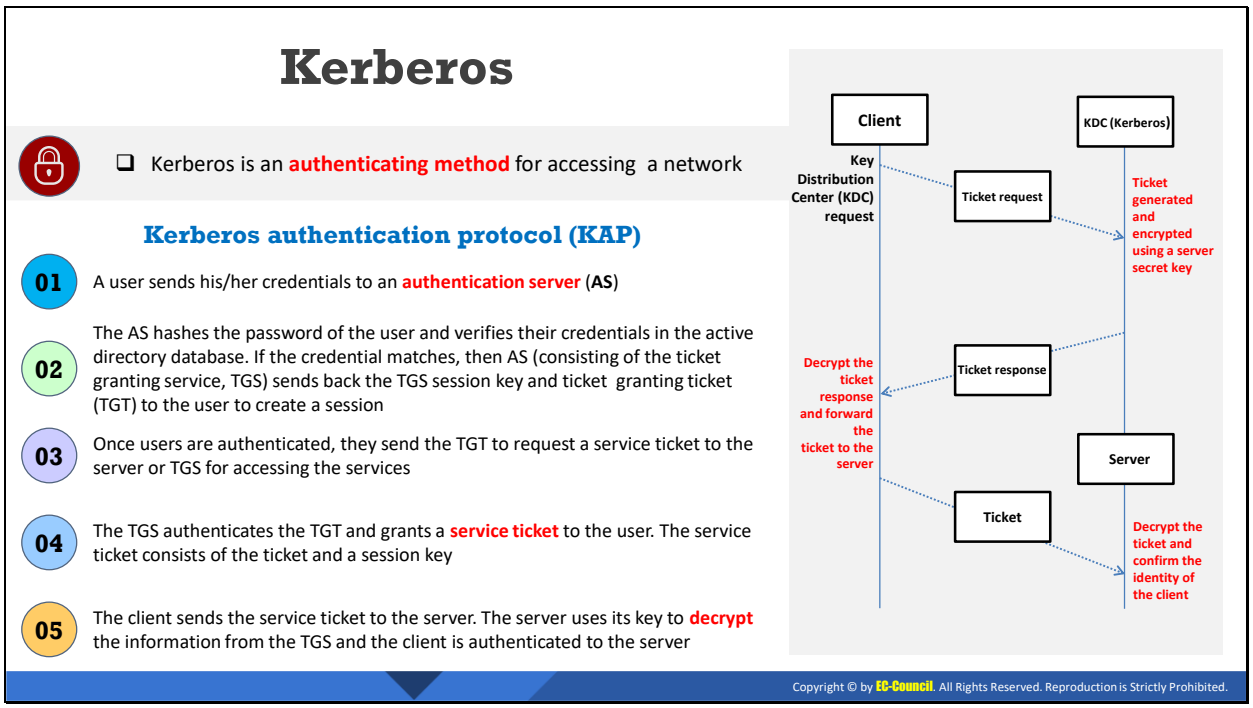
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

RADIUS	TACACS+
Combines authentication and authorization	Separates all three elements of AAA, thus making it more flexible
Encrypts only the password	Encrypts the username and password
Requires each network device to contain authorization configuration	Central management for authorization configuration
UDP- Connectionless UDP ports 1645/1646, 1812/1813	TCP- Connection oriented TCP port 49

Table 1.1: Difference between RADIUS and TACACS+

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Kerberos

Kerberos is a network authentication protocol that is implemented for authenticating requests in computer networks. It is based on the client-server model, which uses an encryption technology and a "ticket" mechanism to prove the identity of a user on a non-secure network. Kerberos protocol messages protect the network from replay attacks and eavesdropping. It commonly uses public-key cryptography while authenticating users attempting to access the server.

The Kerberos protocol consists of the following steps:

- **Step 1**: A user sends his/her credentials to the authentication server.
- **Step 2**: The authentication server hashes the password of the user and verifies the credentials with those in the active directory database. If the credential matches, then the authentication server (consisting of the ticket granting service (TGS)) sends back the TGS session key and ticket granting ticket (TGT) to the user to create a session.
- **Step 3**: Once users are authenticated, they send the TGT to request a service ticket to the server or TGS for accessing the services
- **Step 4**: The TGS authenticates the TGT and grants a service ticket to the user, which consists of a ticket and a session key.
- **Step 5**: The client sends the service ticket to the server. The server uses its key to decrypt the information from the TGS and the client is authenticated to the server.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

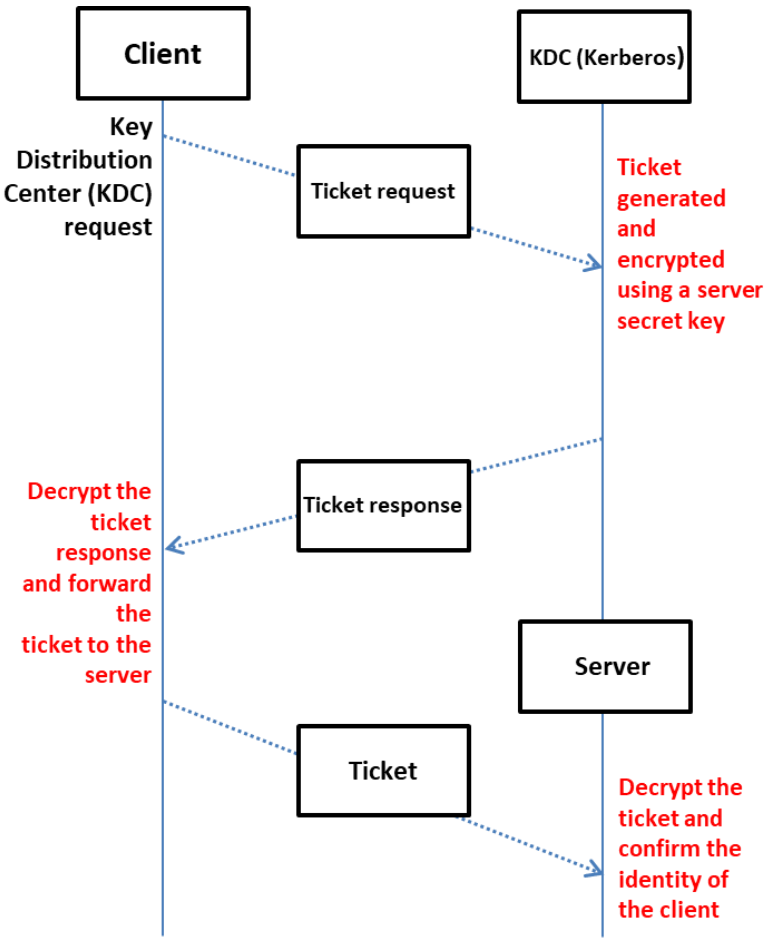
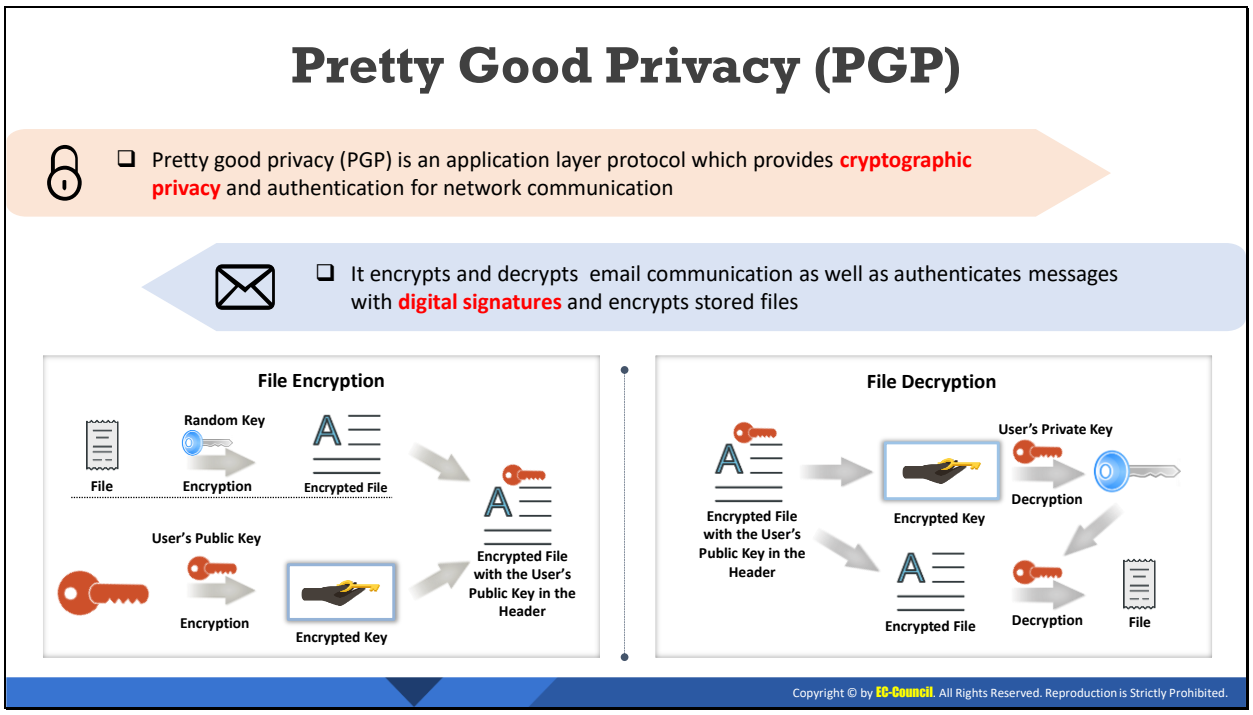


Figure 1.11: Kerberos Protocol Steps

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Pretty Good Privacy (PGP)

Pretty good privacy (PGP) is an application layer protocol which provides cryptographic privacy and authentication for network communication. Pretty good privacy (PGP) is an encryption and decryption computer program that is used for providing confidentiality and validation during communication. PGP enhances the security of emails.

How Does PGP Work?

Every user has a public encryption key and a private key. Messages are sent to another user after encrypting them using the public key. The receiver decrypts the message using their private key. PGP compresses the message, resulting in an increase in the security of the message in the network. PGP creates a session key which is used only once. It encrypts the message using the session key along with the encryption algorithm. The session key is encrypted by the recipient's public key. The public key encrypted session key is sent to the recipient along with the encrypted message.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

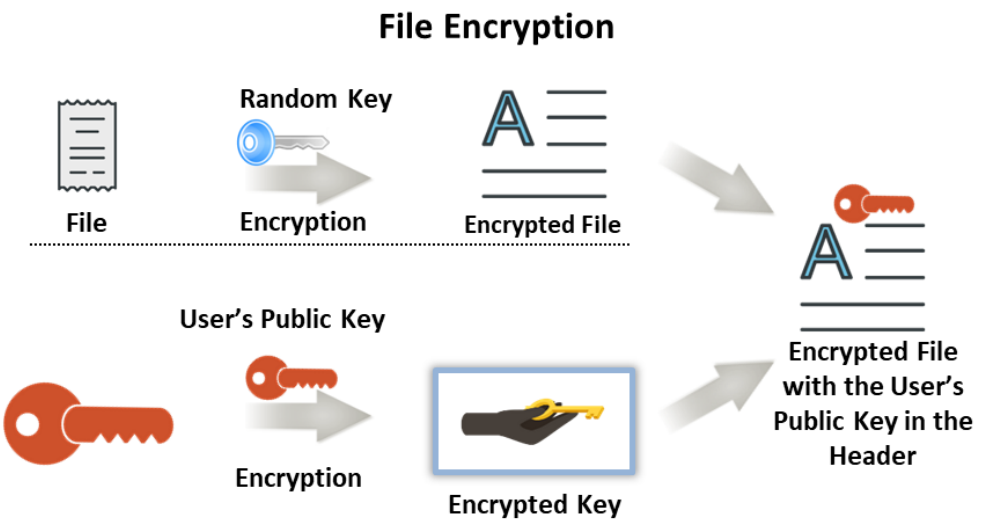


Figure 1.12: File Encryption using PGP

A recipient uses their private key to decrypt the session key and to decrypt the entire message.

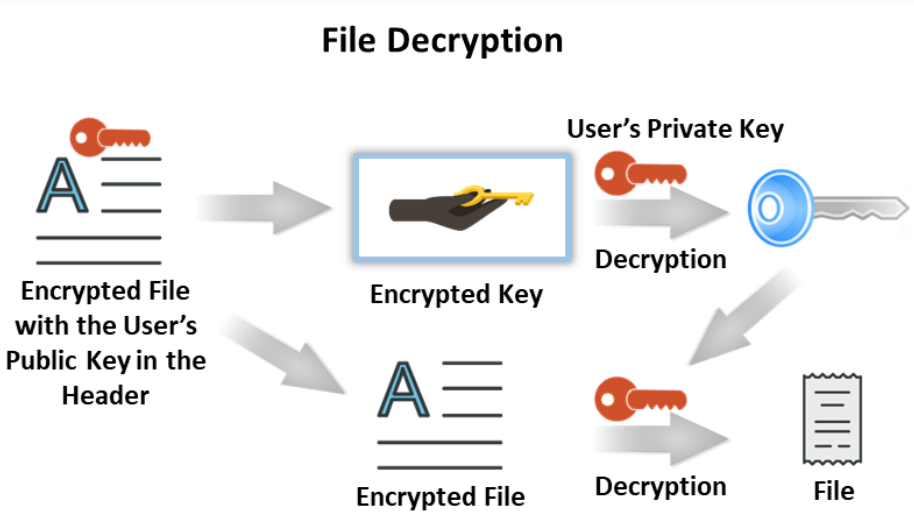


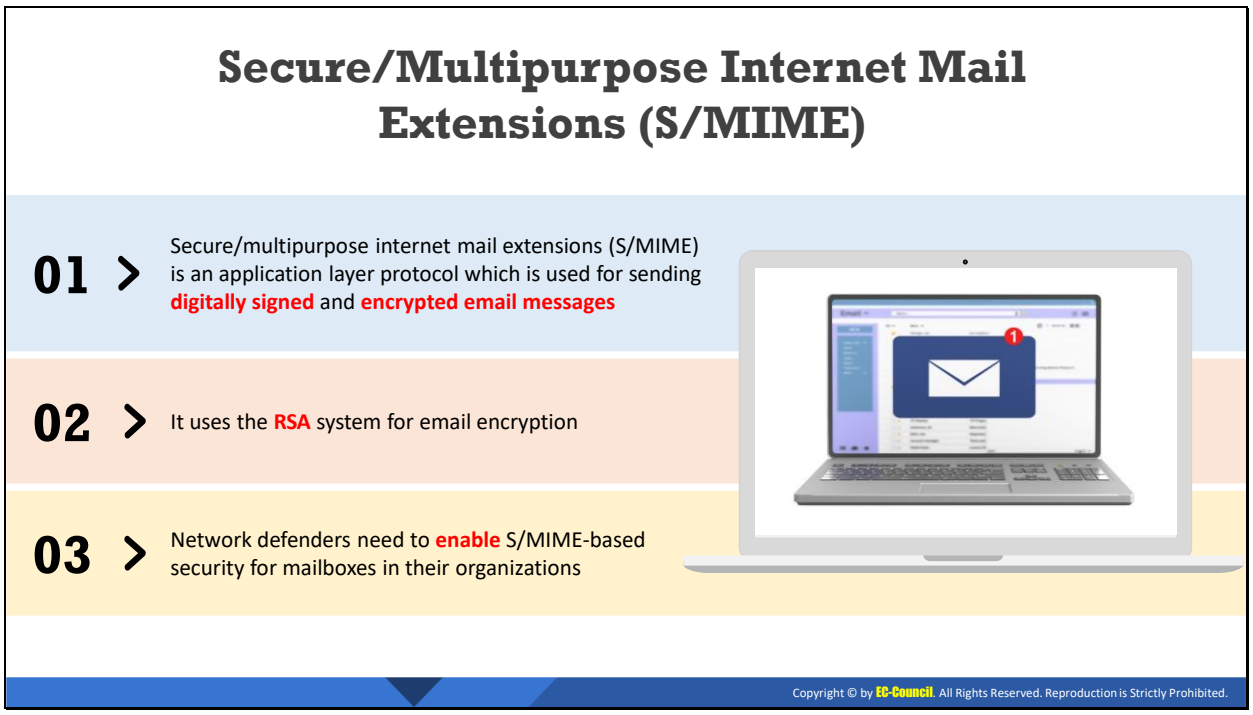
Figure 1.13: File Decryption

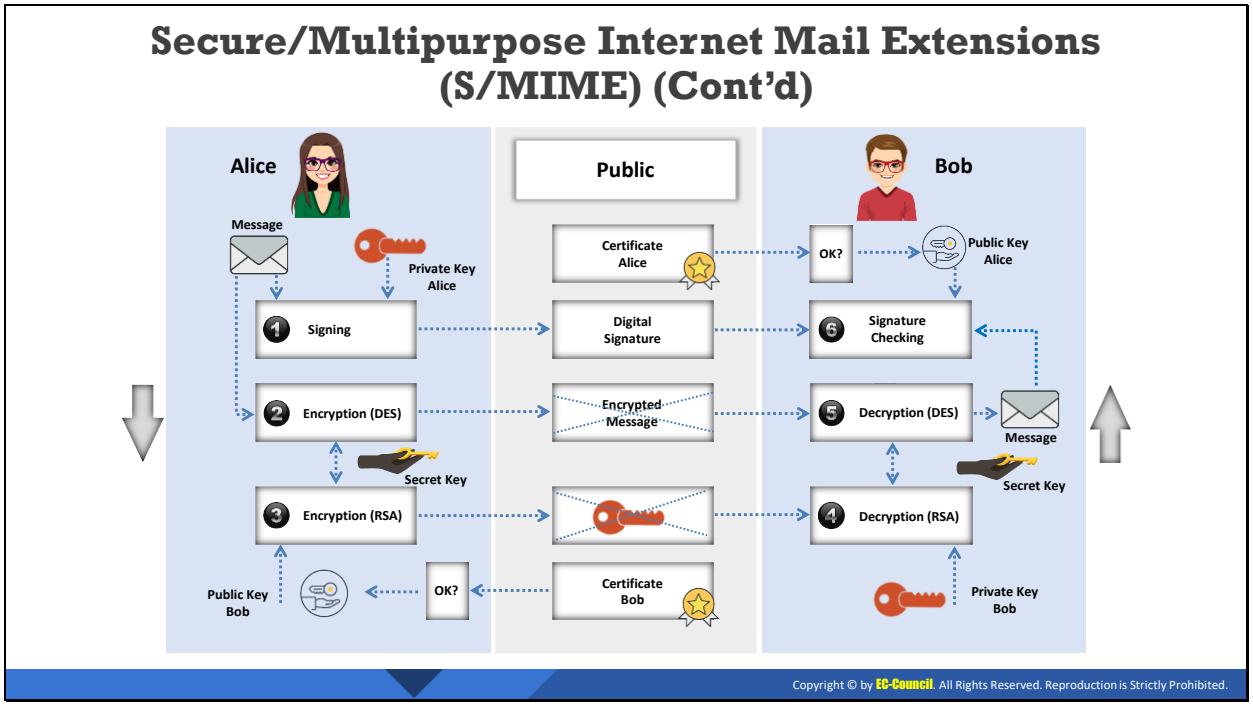
There are two versions of PGP:

- RSA Algorithm
- Diffie-Hellman Algorithm

PGP creates a hash code from the user's name and signature to encrypt the sender's private key. The receiver uses the sender's public key to decrypt the hash code.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets





Secure/Multipurpose Internet Mail Extensions (S/MIME)

Secure/multipurpose internet mail extensions (S/MIME) is used for sending digitally signed and encrypted messages. It allows you to encrypt email messages and digitally sign them to ensure confidentiality, integrity, and non-repudiation for messages.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

It provides cryptographic security services such as:

- Authentication
- Message integrity
- Non-repudiation
- Privacy
- Data security

S/MIME ensures e-mail security and has been included in the latest versions of different web browsers. It uses the RSA encryption method and provides details regarding the encryption and digital signatures in the message.

An S/MIME protocol needs to ensure that it gains a certificate from the CA or from a public CA. The protocol uses different private keys for signature and for encryption.

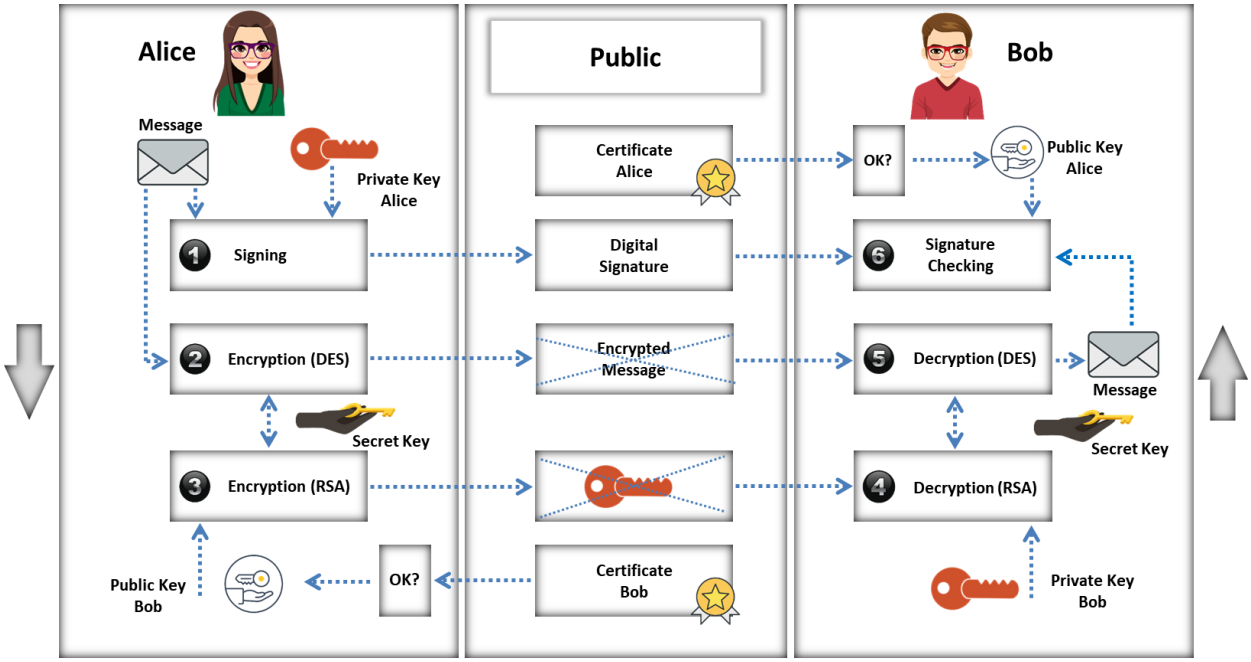
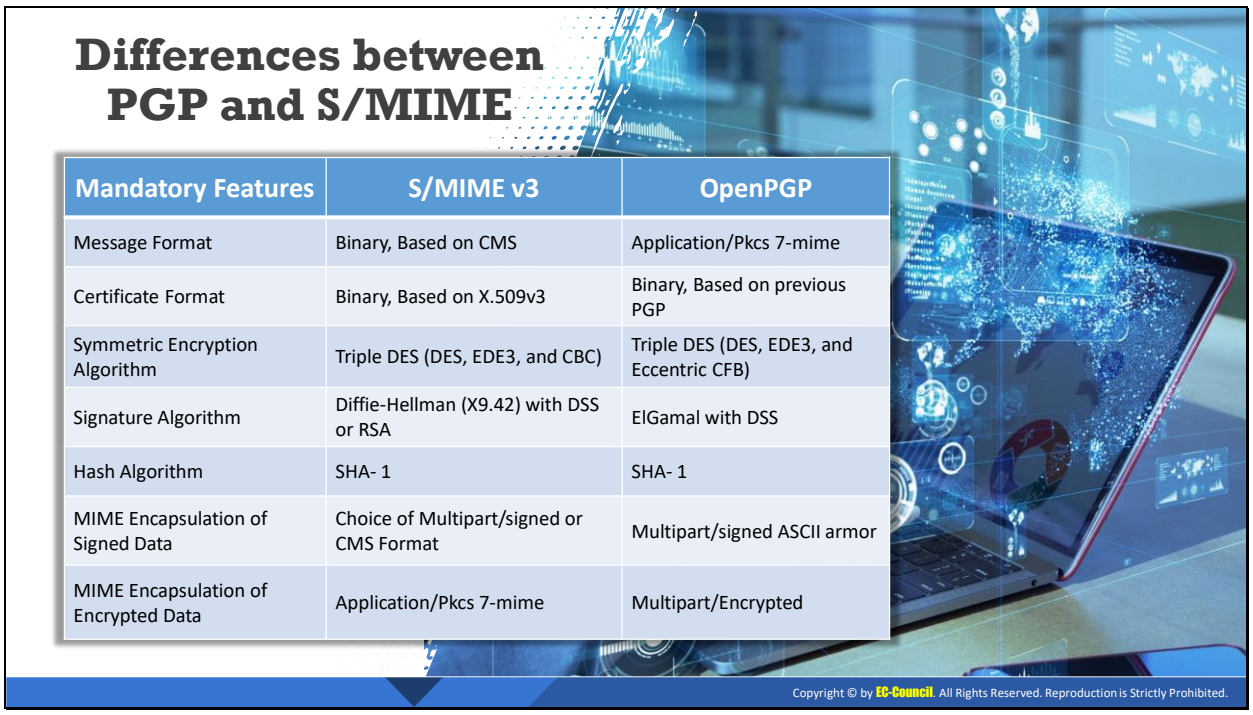


Figure 1.14: Working of S/MIME

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

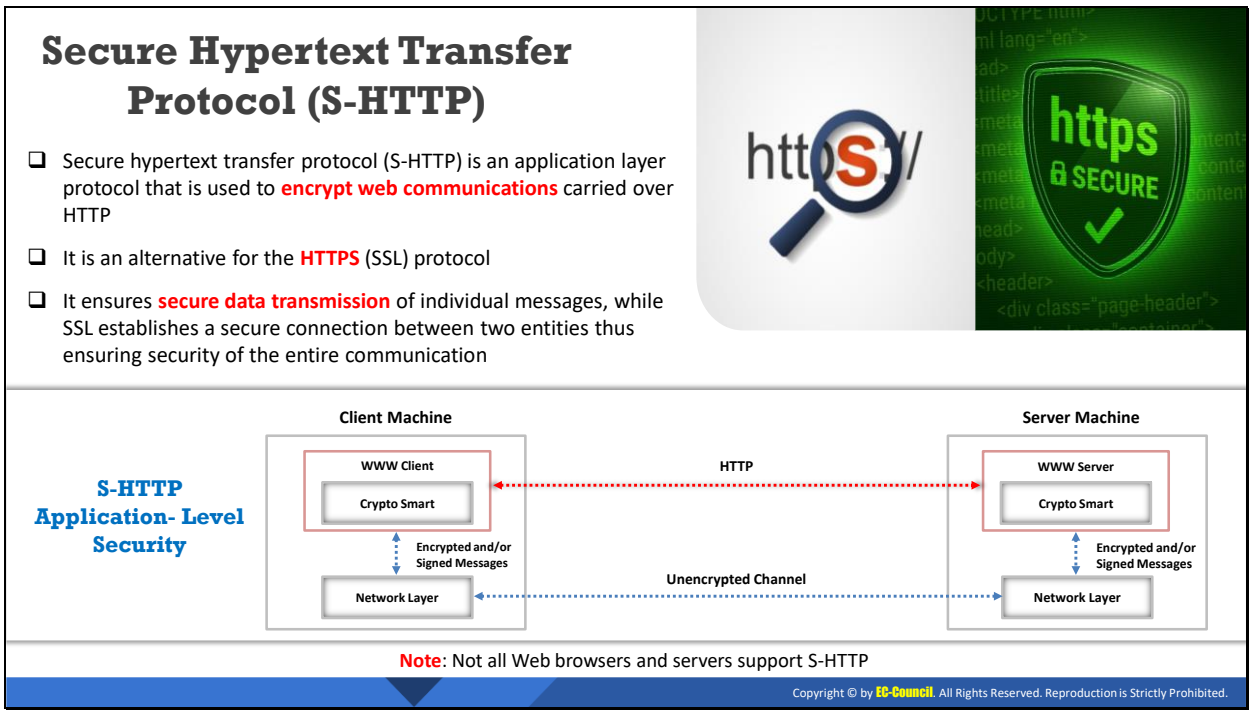


Differences between PGP and S/MIME

Mandatory Features	S/MIME v3	OpenPGP
Message Format	Binary, Based on CMS	Application/Pkcs 7-mime
Certificate Format	Binary, Based on X.509v3	Binary, Based on previous PGP
Symmetric Encryption Algorithm	Triple DES (DES, EDE3, and CBC)	Triple DES (DES, EDE3, and Eccentric CFB)
Signature Algorithm	Diffie-Hellman (X9.42) with DSS or RSA	ElGamal with DSS
Hash Algorithm	SHA- 1	SHA- 1
MIME Encapsulation of Signed Data	Choice of Multipart/signed or CMS Format	Multipart/signed ASCII armor
MIME Encapsulation of Encrypted Data	Application/Pkcs 7-mime	Multipart/Encrypted

Table 1.2: Differences between PGP and S/MIME

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Secure Hypertext Transfer Protocol (S-HTTP)

The Secure Hypertext Transfer Protocol (S-HTTP) ensures secured data exchange on the world wide web. It is an alternative to HTTPS (SSL). It implements application-level security that offers encryption and digital signatures on the message. S-HTTP verifies the user by using a certificate and provides many cryptographic algorithms and modes of operations. It also ensures secure data transmission for individual messages, while SSL establishes a secure connection between two entities, thus ensuring the security of the entire communication. S-HTTP uses the client-server protocol to determine the security conditions for an instance of client-server communication. It allows the client to send a certificate to authenticate a user. There are many web servers that support the S-HTTP protocol, which allows them to communicate without requiring any encryption.

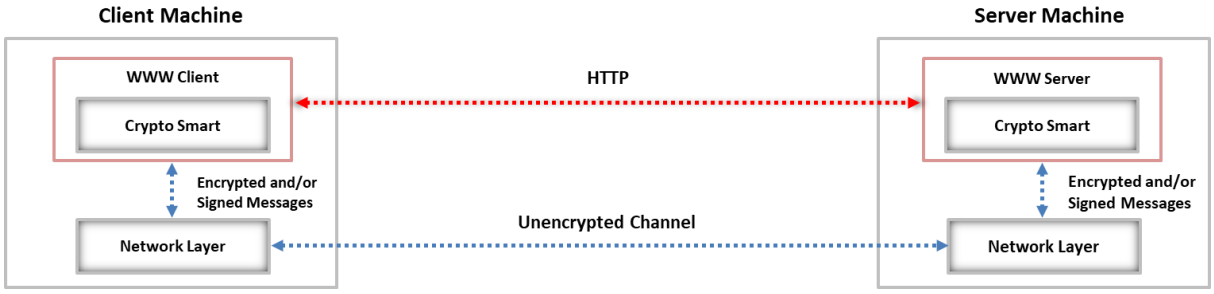
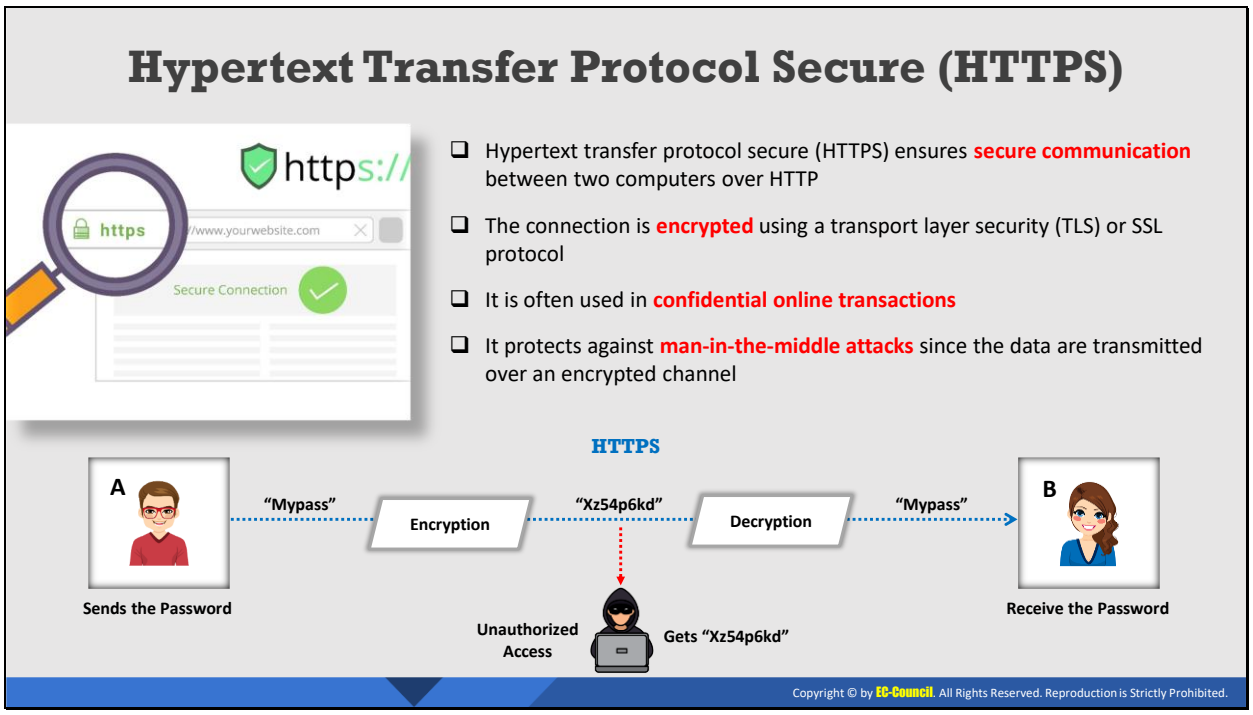


Figure 1.15: S-HTTP Application-Level Security

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Hypertext Transfer Protocol Secure (HTTPS)

The hypertext transfer protocol secure (HTTPS) is a protocol used for ensuring secure communication in the network. It uses protocols such as TLS and SSL to ensure secure transmission of data. HTTPS confirms the verification of websites and preserves the confidentiality and reliability of the messages passed over the internet.

It protects against man-in-the-middle attacks since the data are transmitted over an encrypted channel.

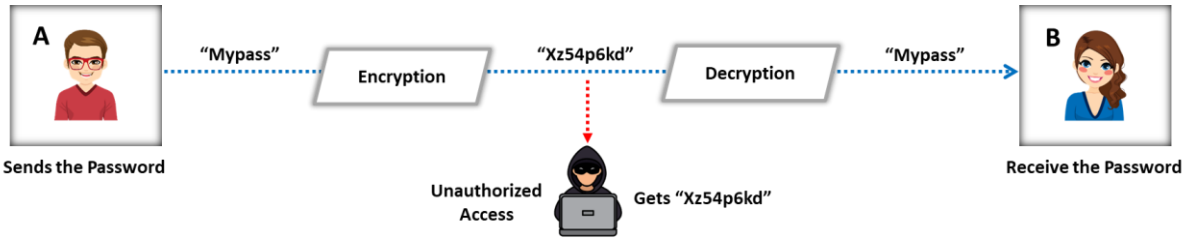
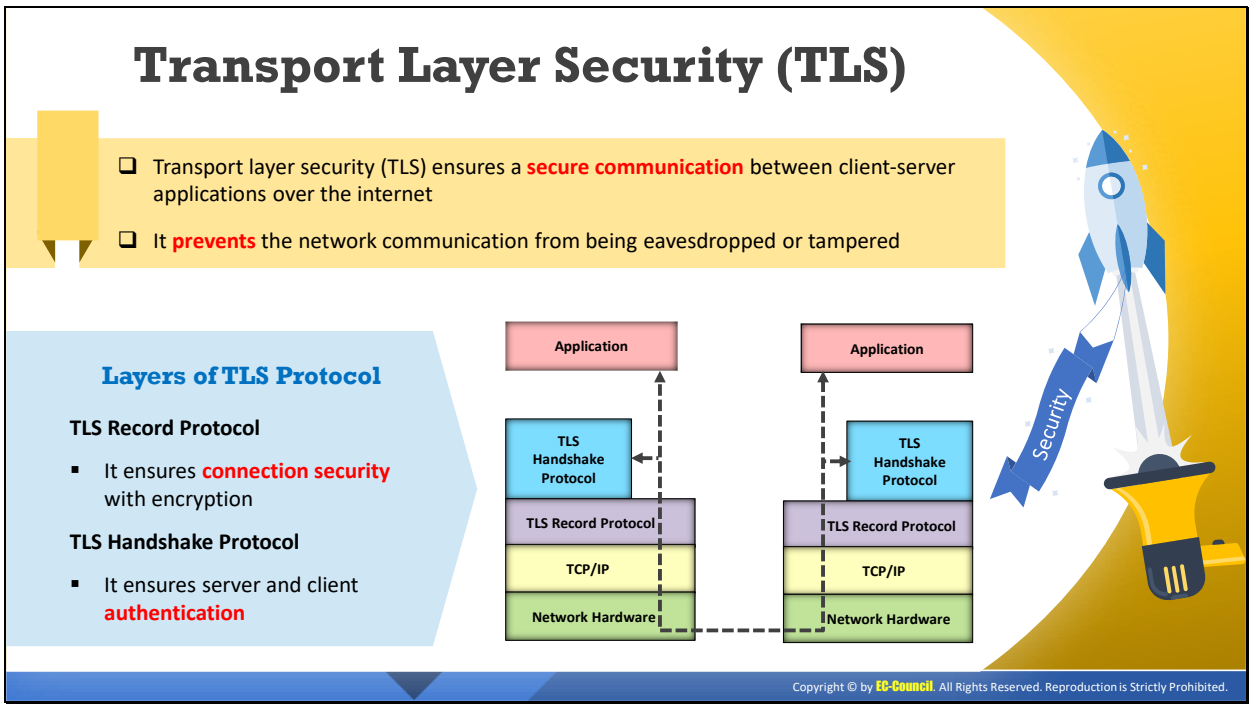


Figure 1.16: HTTPS Protection from MiTM Attack

HTTPS mainly uses SSL in order to protect any website, thus making it easier for users to access the website. SSL has the following advantages:

- It encrypts the confidential information during exchange of data.
- It maintains a record of the details of the certificate owner.
- A CA checks the owner of the certificate while issuing it.
- It is often used in confidential online transactions.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Transport Layer Security (TLS)

The transport layer security (TLS) provides a secure communication of data in addition to the confidentiality and reliability between the communicating parties.

The following are the properties of a secure TLS connection:

- It ensures confidentiality and reliability of data during communication between a client and a server using symmetric cryptography.
- It authenticates communication applications using public key cryptography.
- The authentication codes can maintain the reliability of the data.
- TLS consists of two protocols:
  - **TLS record protocol**: This protocol provides security using the encryption method.
  - **TLS handshake protocol**: This protocol provides security by performing an authentication of a client and a server before communication.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

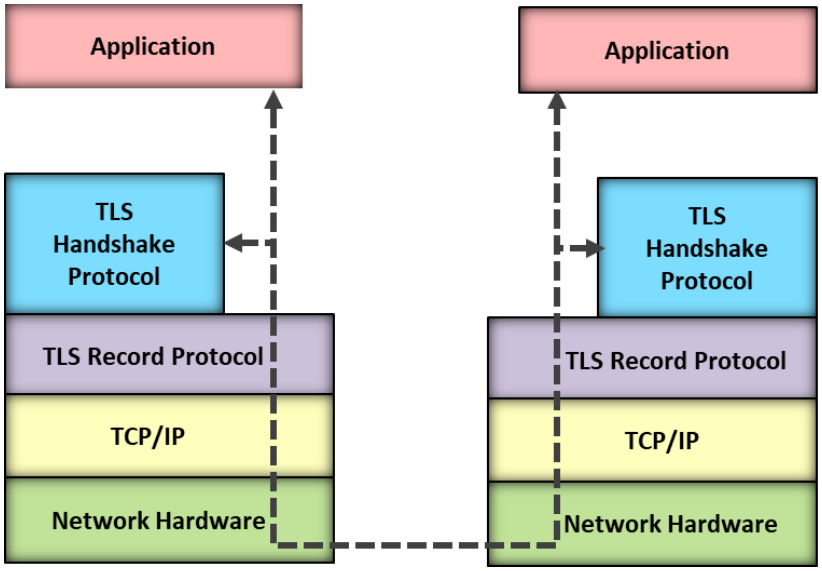
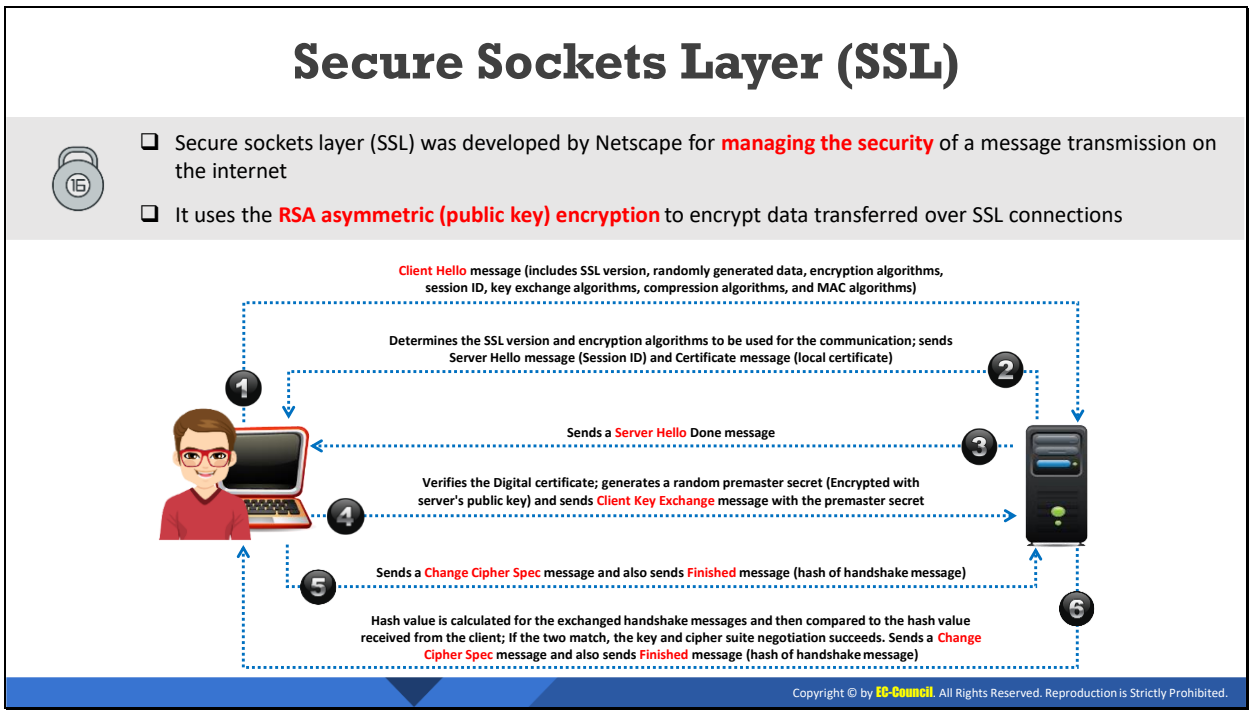


Figure 1.17: Layers of TLS Protocol

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Secure Sockets Layer (SSL)

The secure sockets layer (SSL) is a protocol used for providing a secure authentication mechanism between two communicating applications such as a client and a server. SSL requires a reliable transport protocol, such as TCP, for data transmission and reception.

Any application-layer protocol that is higher than SSL, such as HTTP, FTP, and telnet, can form a transparent layer over the SSL. SSL acts as an arbitrator between the encryption algorithm and session key. It also verifies the destination server prior to the transmission and reception of data. SSL encrypts the complete data of the application protocol to ensure security.

The SSL protocol also offers "**channel security**" via three basic properties:

- **Private channel**: All the messages are encrypted after a simple handshake is used to define a secret key.
- **Authenticated channel:** The server endpoint of the conversation is always encrypted, whereas the client endpoint is optionally authenticated.
- **Reliable channel:** Message transfer undergoes an integrity check.

SSL uses both asymmetric and symmetric authentication mechanisms. Public key encryption verifies the identities of the server, the client, or both. Once the authentication is completed, the client and the server can create symmetric keys allowing them to communicate and transfer data rapidly. An SSL session is responsible for carrying out the SSL handshake protocol for organizing the states of the server and clients, thus ensuring the consistency of the protocol.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

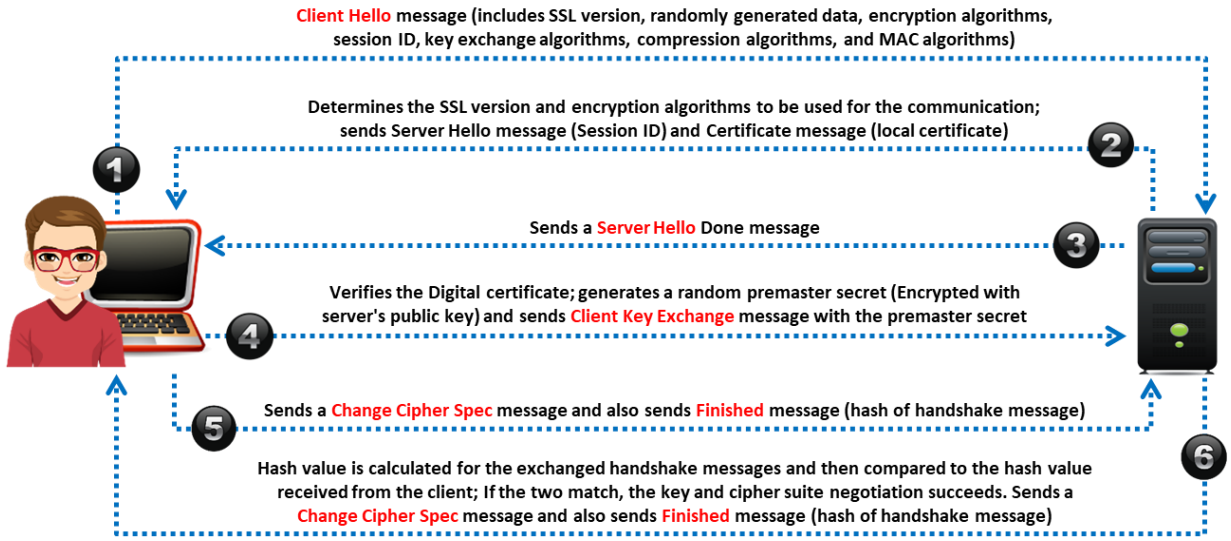
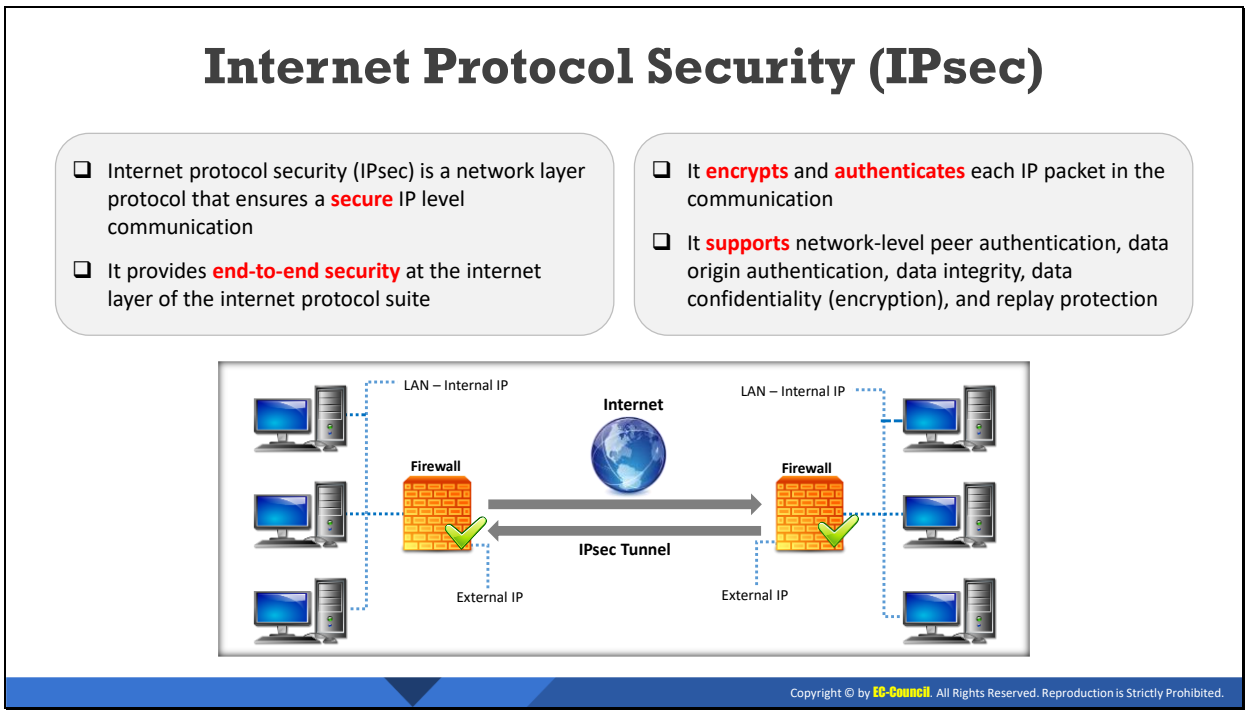


Figure 1.18: Working of SSL

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Internet Protocol Security (IPsec)

The Internet Protocol Security (IPsec) ensures secure communications over the IP network. It works at the network layer of the communication model and utilizes cryptographic security services to ensure secure communication. It allows the authentication of IP packets during communication. IPsec is applied in virtual private networks and remote user access. It is used between a pair of hosts, a pair of security gateways, or a security gateway and a host. It consists of two security services, namely, an authentication header (AH) and an encapsulating security payload (ESP). The AH allows the authentication of the sender, whereas the ESP allows the authentication of the sender as well as data encryption.

It provides secure communication for network-level peer authentication, data origin authentication and ensures data integrity, data confidentiality (encryption), and replay protection.

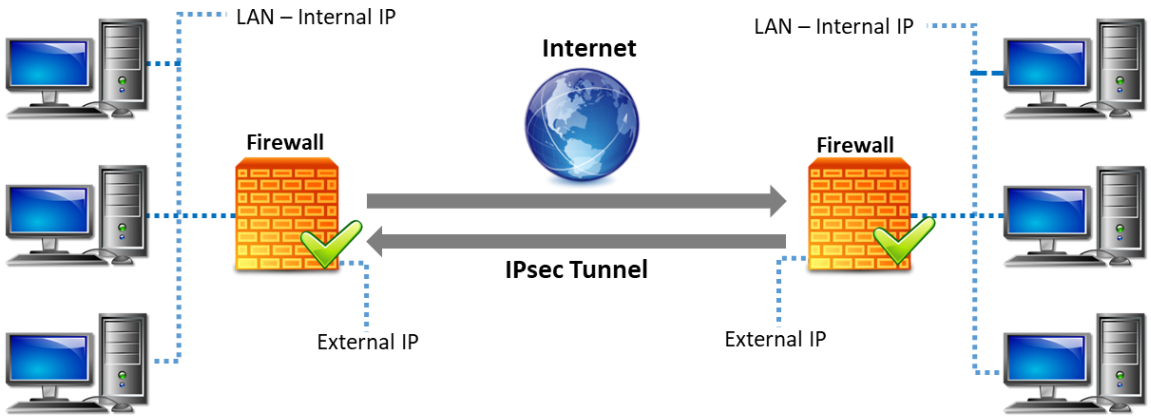
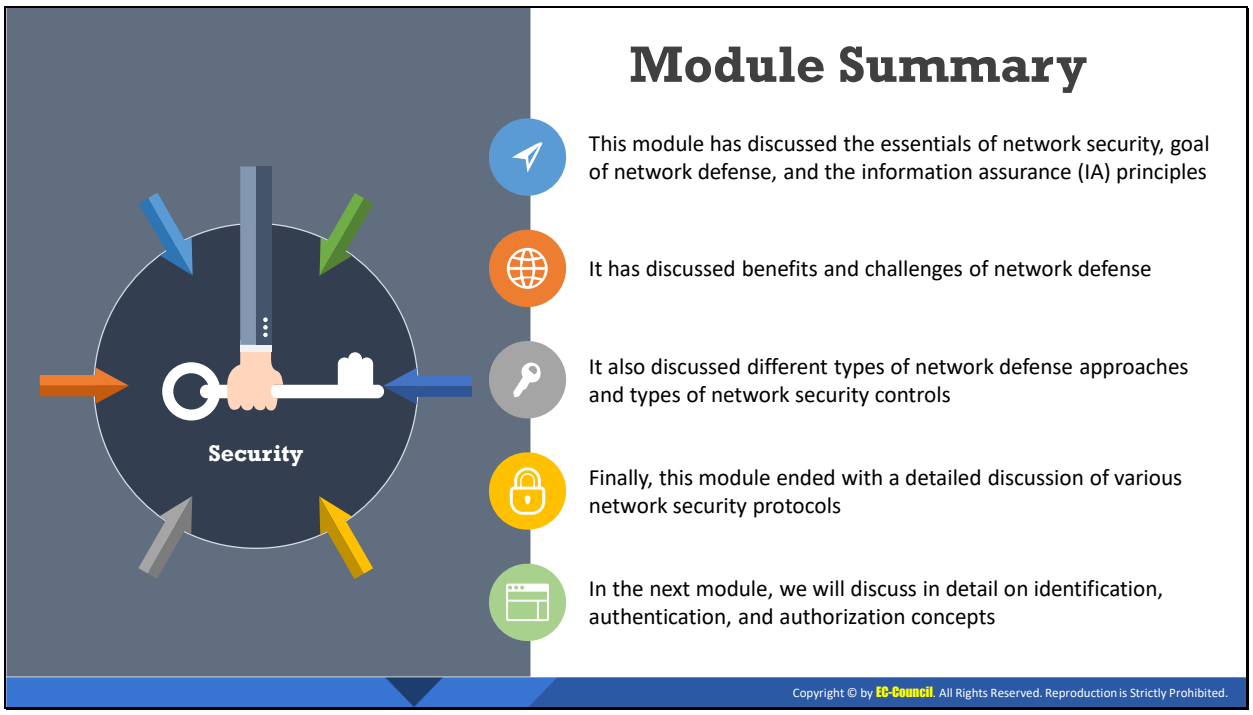


Figure 1.19: Working of IPsec

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Module Summary

This module discussed the essentials of network security, goal of network defense, and information assurance (IA) principles. It has discussed the benefits and challenges of network defense. It also discussed different types of network defense approaches and types of network security controls. Finally, this module presented a detailed discussion of various network security protocols.

In the next module, we will discuss identification, authentication, and authorization concepts in detail.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

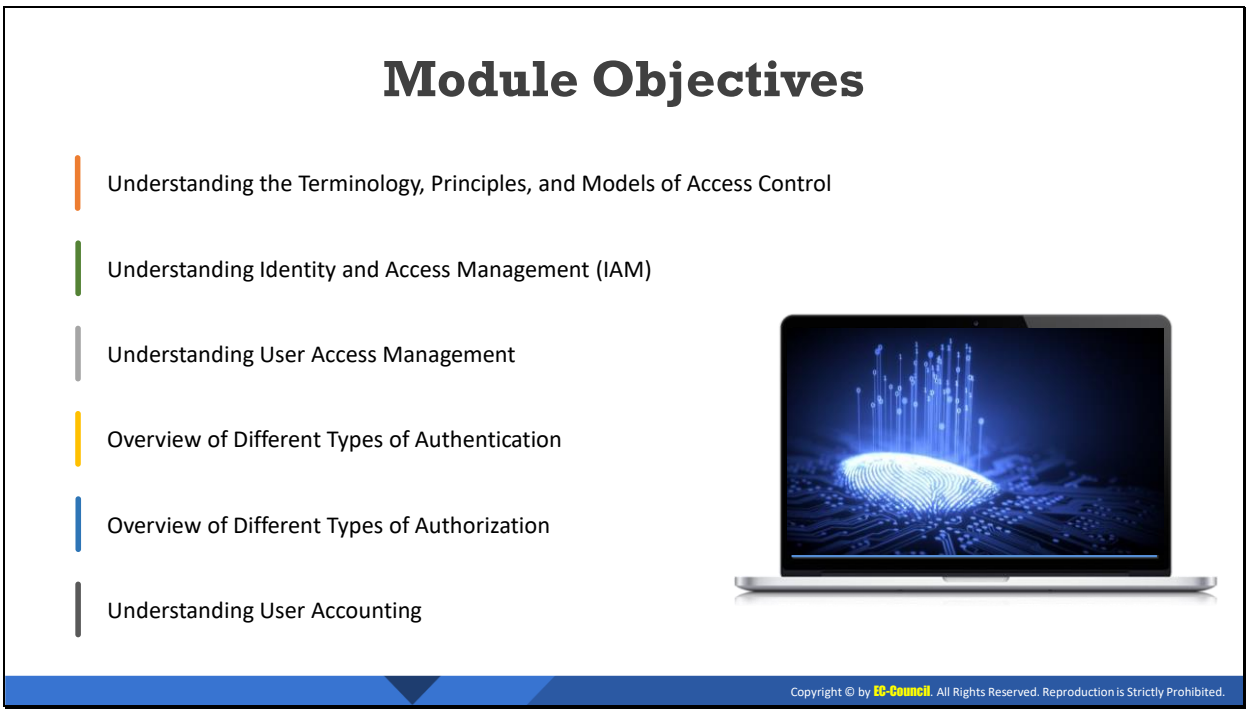
EC-Council

N|DE™
Network Defense Essentials

Module 02

Identification, Authentication, and Authorization

https://t.me/learningnets



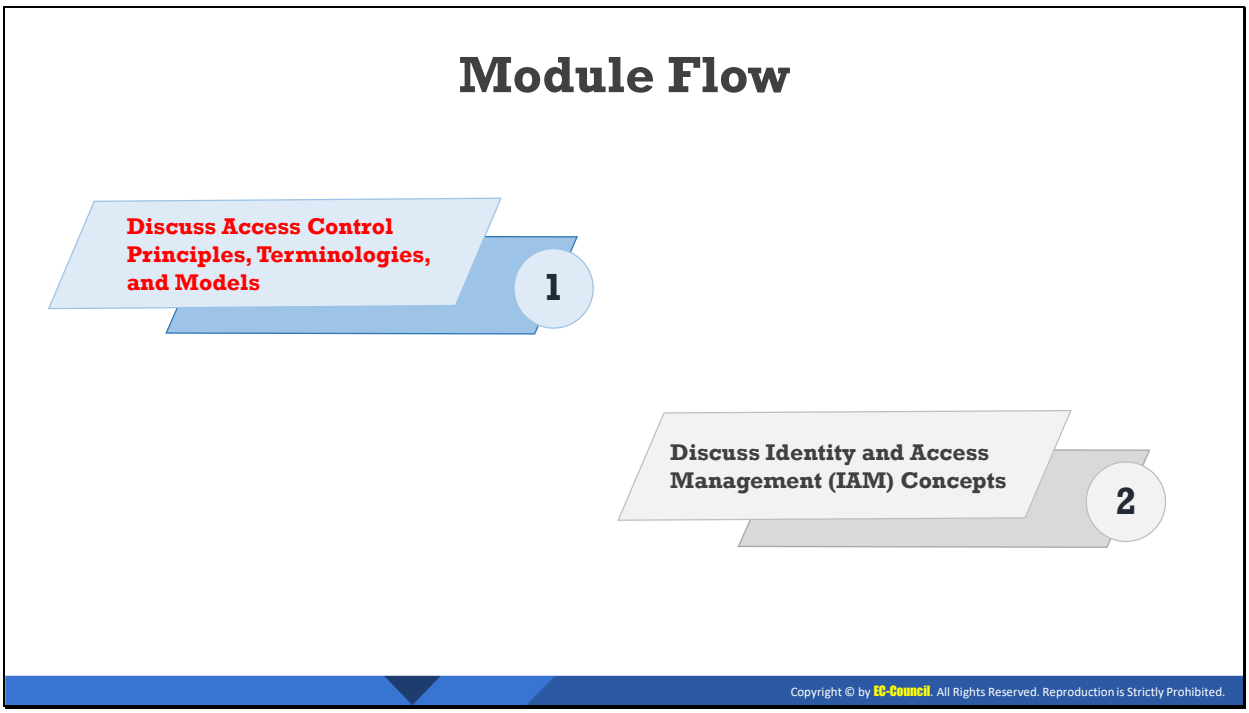
Module Objectives

The most serious risk that organizations are facing today is unauthorized access to sensitive data. To control such data breaches, organizations require strong identification, authentication, and authorization mechanisms to effectively manage access to critical assets and sensitive data. This module provides an overview of various methods and techniques used for the identification, authentication, and authorization of users accessing critical assets and resources.

At the end of this module, you will be able to do the following:

- Understand the terminology, principles, and models of access control
- Describe identity and access management (IAM)
- Understand user access management
- Explain the different types of authentication
- Explain the different types of authorization
- Understand user accounting

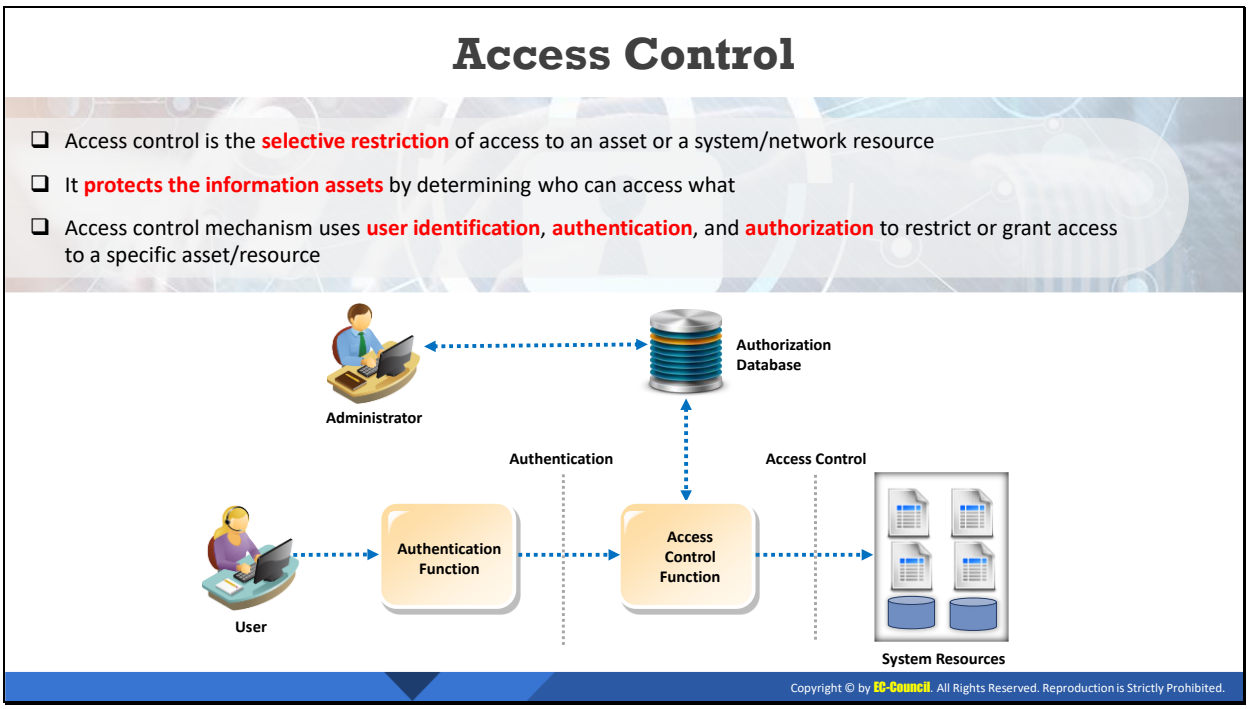
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Discuss Access Control Principles, Terminologies, and Models

The objective of this section is to explain the concept of access control by introducing the principles of access control, the terminologies used, and the different models that describe how access control helps in controlling the access of users to specific resources in a network.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Access Control

Access control is a method of limiting the access of an organization's resources for the users. A crucial aspect of implementing an access control is to maintain the integrity, confidentiality, and availability of the information.

An access control function uses identification, authentication, and mechanisms to identify, authenticate, and authorize the user requesting access to a specific resource. The access permissions determine the approvals or permissions provided to a user for accessing a system and other resources.

The general steps involved in the access control mechanism are as follows:

- **Step 1**: A user provides their credentials/identification while logging into the system.
- **Step 2**: The system validates the user with the database on the basis of the provided credentials/identification such as a password, fingerprint, etc.
- **Step 3**: Once the identification is successful, the system provides the user access to use the system.
- **Step 4**: The system then allows the user to perform only those operations or access only those resources for which the user has been authorized.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

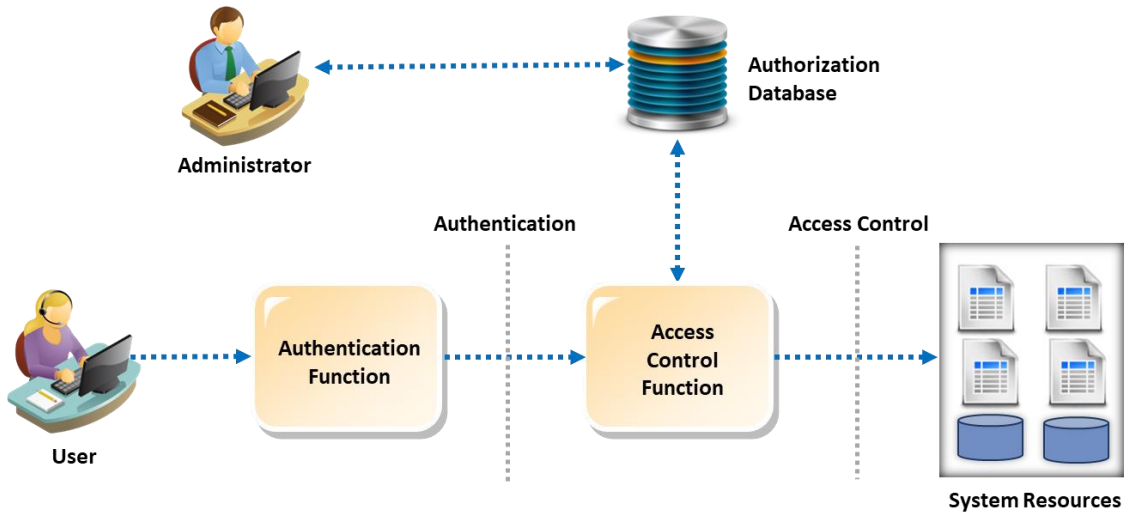
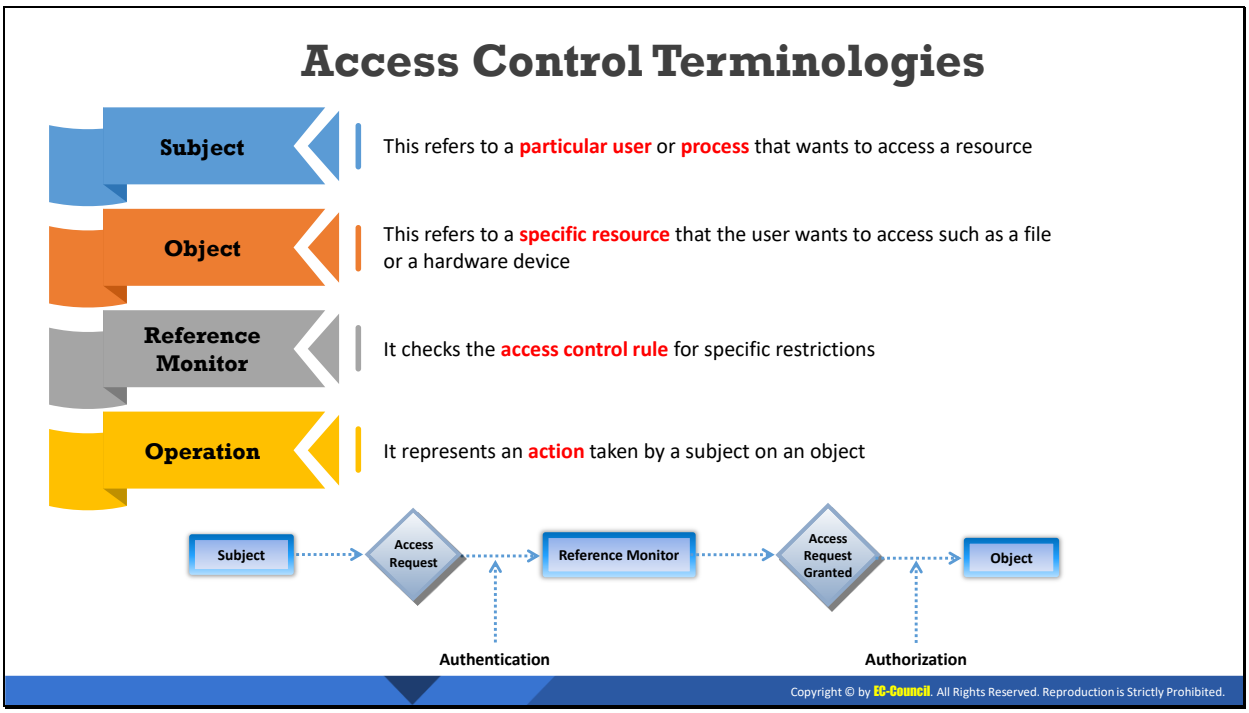


Figure 2.1: Access Control Mechanism

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Access Control Terminologies

The following terminologies are used to define the access control on specific resources:

- **Subject:** A subject can be defined as a user or a process that attempts to access the objects. The subjects are those entities that perform certain actions on the system.
- **Object:** An object is an explicit resource on which an access restriction is imposed. The access controls implemented on the objects further control the actions performed by the user. Examples of an object are a file or a hardware device.
- **Reference Monitor:** A reference monitor monitors the restrictions imposed on the basis of certain access control rules. It implements a set of rules on the ability of the subject to perform certain actions on the object.
- **Operation:** An operation is an action performed by a subject on an object. A user trying to delete a file is an example of an operation. Here, the user is the subject, the action of deleting refers to the operation, and the file is the object.

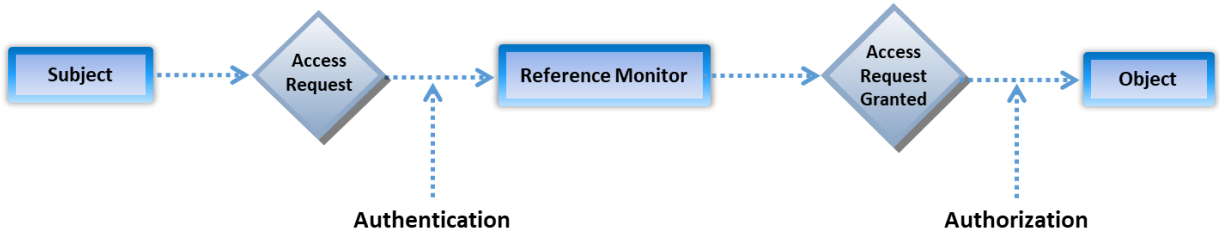
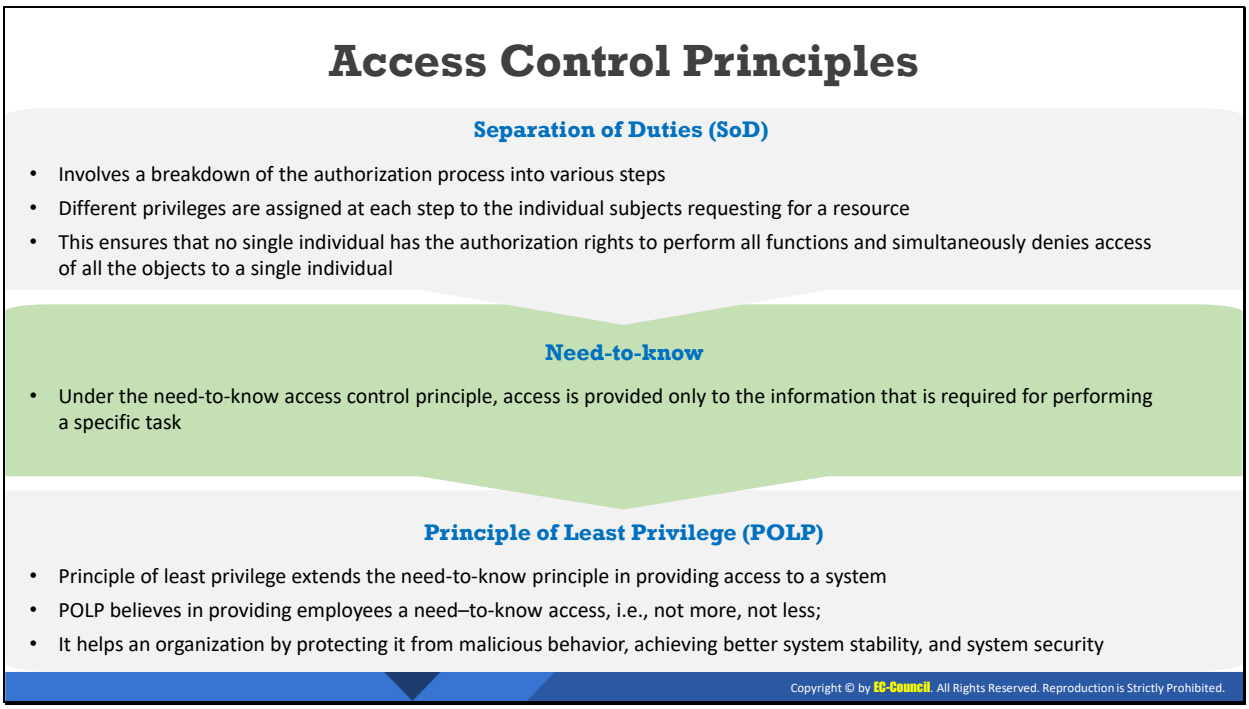


Figure 2.2: Access Control Terminologies

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Access Control Principles

The principles of access control describe the access permission levels of users in detail. By implementing an access control process, the security of processes and resources can be ensured. The process of access control should be based on the following principles.

- **Separation of Duties (SoD)**

  SoD involves a breakdown of the authorization process into various steps. Different privileges are assigned at each step to individual subjects requesting for a resource. This ensures that no single individual has the authorization rights to perform all functions; simultaneously, a single individual cannot gain access to all the objects. This division ensures that a single person is not responsible for a larger process. An example is the granting of web-server administrator rights to only configure a web server, without granting administrative rights to other servers.

- **Need-to-know**

  Under the need-to-know access control principle, access is provided only to the information that is required for performing a specific task.

- **Principle of Least Privilege (POLP)**

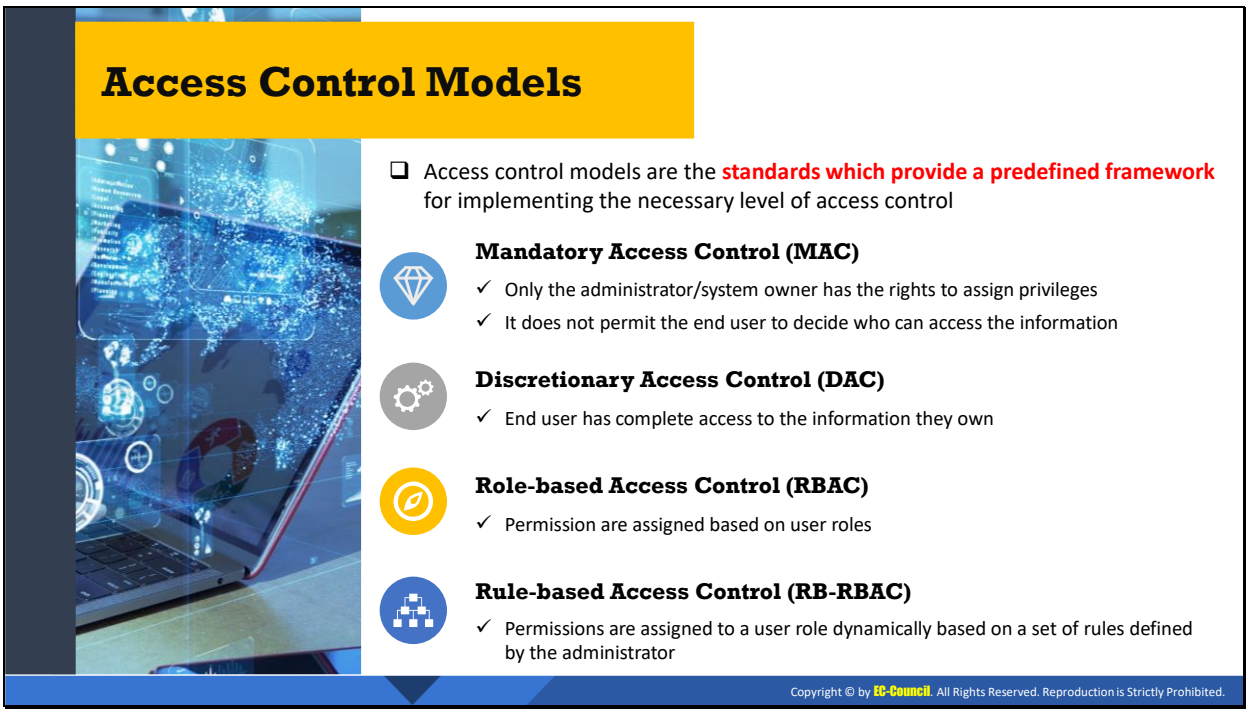
  The principle of least privilege (POLP) extends the need-to-know principle in providing access to a system. In other words, POLP entails providing employees exactly the need-to-know level of access, i.e., not more and not less. It helps an organization by protecting it from malicious behavior as well as improving system stability and system security.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Least privilege provides access permissions to only those users who need the access and resources. The permissions granted depend on the roles and responsibilities of the user requesting the access. There are two underlying principles involved in POLP: low rights and low risks. On the basis of these principles, a user needs to complete a task using a limited number of resources in a limited amount of time provided to them. This approach reduces the probability of unauthorized access to system resources.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Access Control Models

Access control models are the standards which provide a predefined framework for implementing the necessary level of access control. Access control models specify how a subject can access an object.

- **Mandatory Access Control**

  The mandatory access control (MAC) determines the usage and access policies for the users. A user can access a resource only if they have the access rights to that resource. MAC is applied in the case of data that has been marked as highly confidential. The administrators impose MAC depending on the operating system and the security kernel. It does not permit the end-user to decide who can access the information.

  The following are the advantages and disadvantages of MAC:

  - It provides a high level of security since the network defenders determine the access controls.
  - The MAC policies minimize the chances of errors.
  - Depending on the MAC, an operating system marks and labels the incoming data, thereby creating an external application control policy.

  Examples of MAC include Security-Enhanced Linux (SELinux) and Trusted Solaris.

- **Discretionary Access Control**

  Discretionary access control **(DAC)** determines the access control taken by any possessor of an object in order to decide the access control of a subject on that object.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

DAC is alternatively named as a **need-to-know** access model. The decision taken by the owner depends on the following measures:

- **File and data ownership**: Determines the access policies of the user
- **Access rights and permissions**: Involves the possessor setting the access privileges to other subjects

An owner can provide or deny access to any particular user or a group of users. The attributes of a DAC include the following:

- The owner of an object can transfer the ownership to another user.
- The access control prevents multiple unauthorized attempts to access an object.
- The DAC prevents unauthorized users from viewing details like the filesize, filename, directory path, etc.
- The DAC uses access control lists in order to identify and authorize users.

Disadvantage: A DAC requires maintenance of the access control list and access permissions for the users. Examples of DAC include UNIX, Linux, and Windows access control.

- **Role-Based Access Control**

  In a role-based access control **(RBAC)**, the access permissions are available based on the access policies determined by the system. The access permissions are beyond the user control which implies that users cannot amend the access policies created by the system. The rules for determining the role-based access controls are as follows:

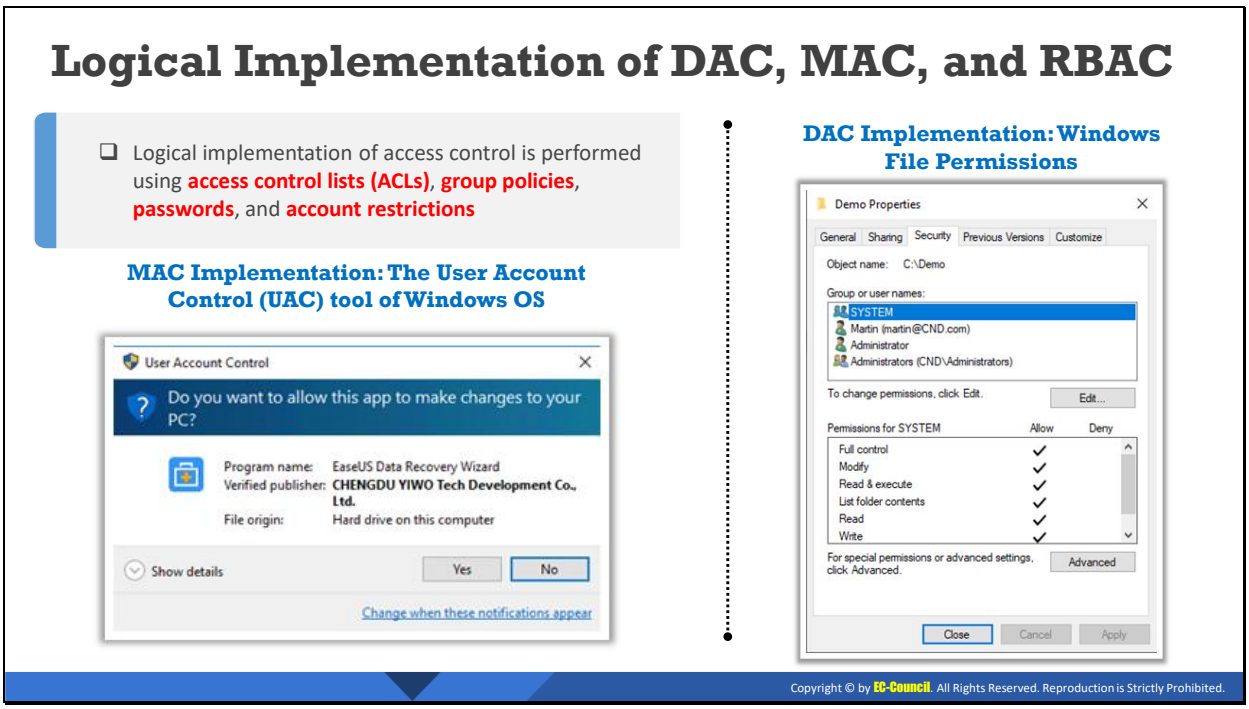
  - **Role assignment**: A certain role is required to be assigned to a user which enables them to perform a transaction.
  - **Role authorization**: A user needs to perform a role authorization in order to achieve a particular role.
  - **Transaction authorization**: Transaction authorization allows the users to execute only those transactions for which they have been authorized.

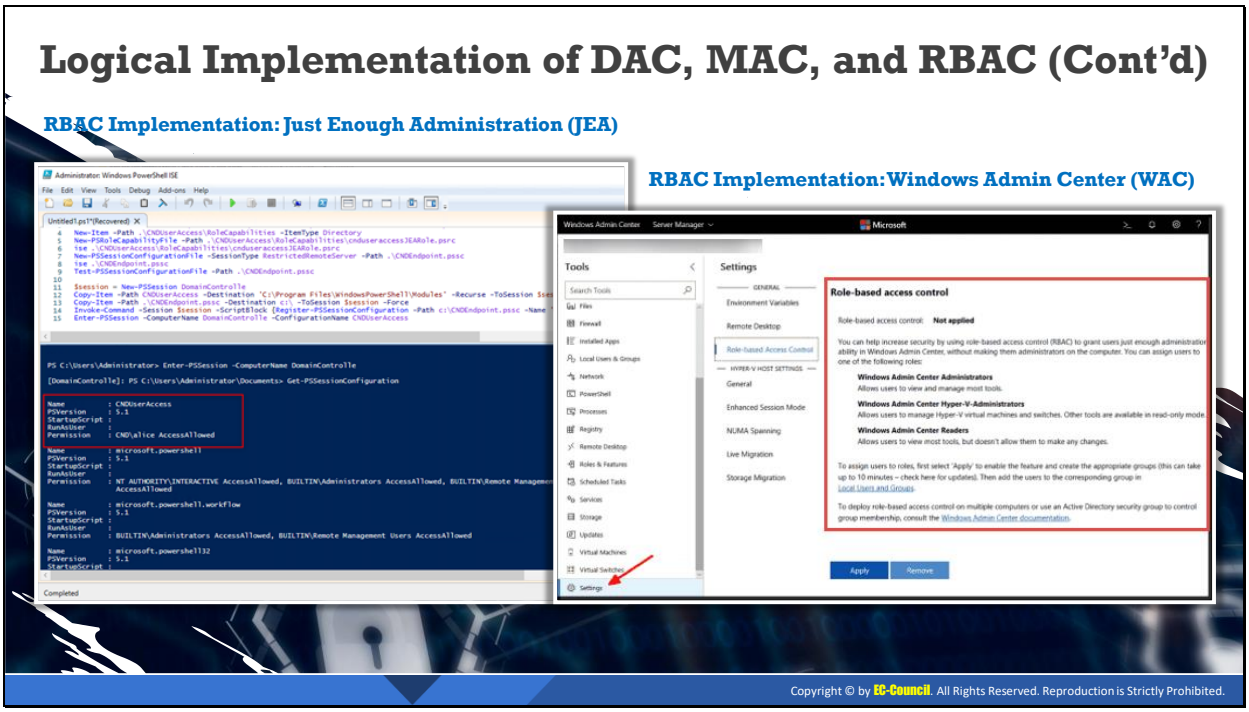
- **Rule-based Access Control (RB-RBAC)**

  Permissions are assigned to a user role dynamically based on a set of rules defined by the administrator.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets





Logical Implementation of DAC, MAC, and RBAC

In the Windows operating system (OS), the User Account Control (UAC) feature implements the MAC security model. It restricts the installation of any application software only through administrator authorizations. In other words, users without administrative privileges are restricted to install any application on the system.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

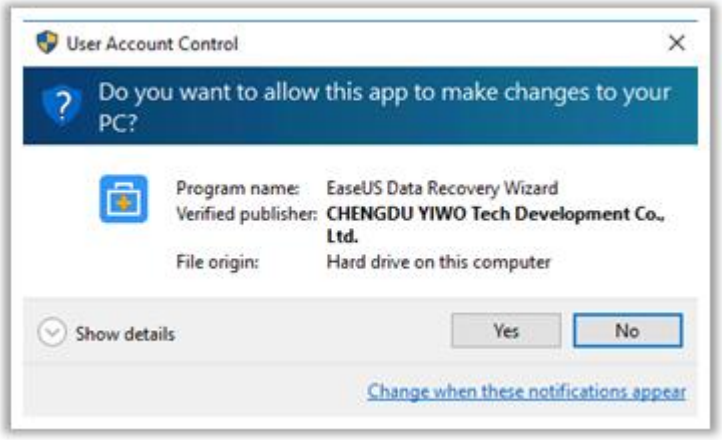


Figure 2.3: Mac Implementation: The User Account Control tool of Windows OS

Logical Implementation of DAC: Windows File Permissions

In the Windows OS, DAC is implemented for assigning file permissions to specific groups/users. Permissions to access files and folders on a system, to access files that exist on an old account of a user, or to edit system files are all controlled using DAC.

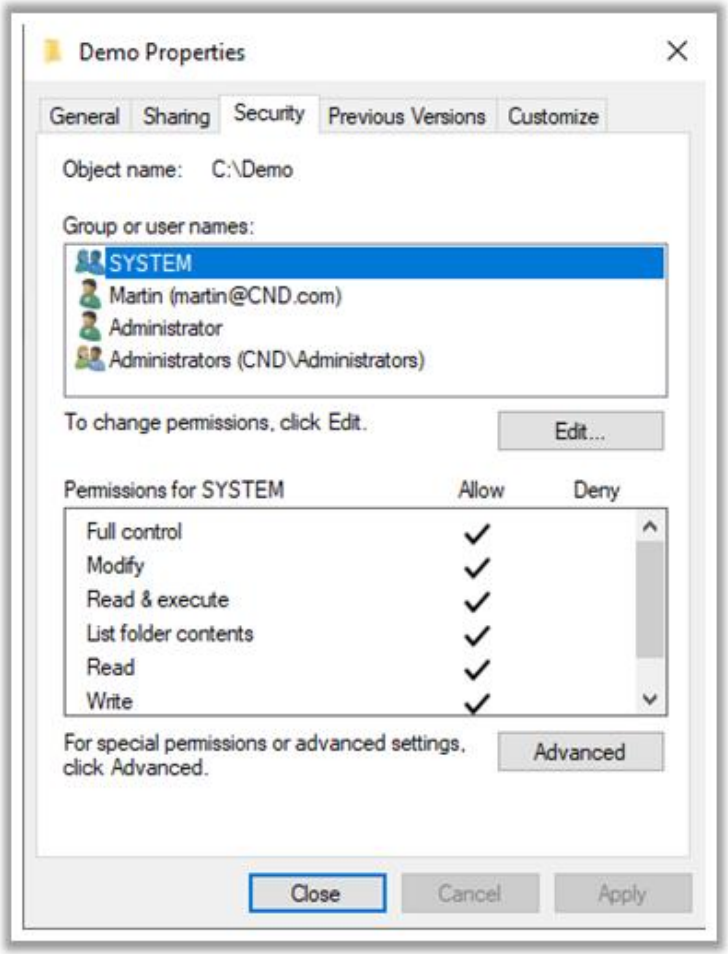


Figure 2.4: DAC Implementation: Windows File Permissions

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Logical Implementation of RBAC: Just Enough Administration (JEA)

The Just Enough Administration (JEA) management framework in Windows implements RBAC to restrict the rights of IT administrators in remote PowerShell sessions. Using JEA, fine-grained access control can be implemented for non-administrators to run specific commands, scripts, and executables.

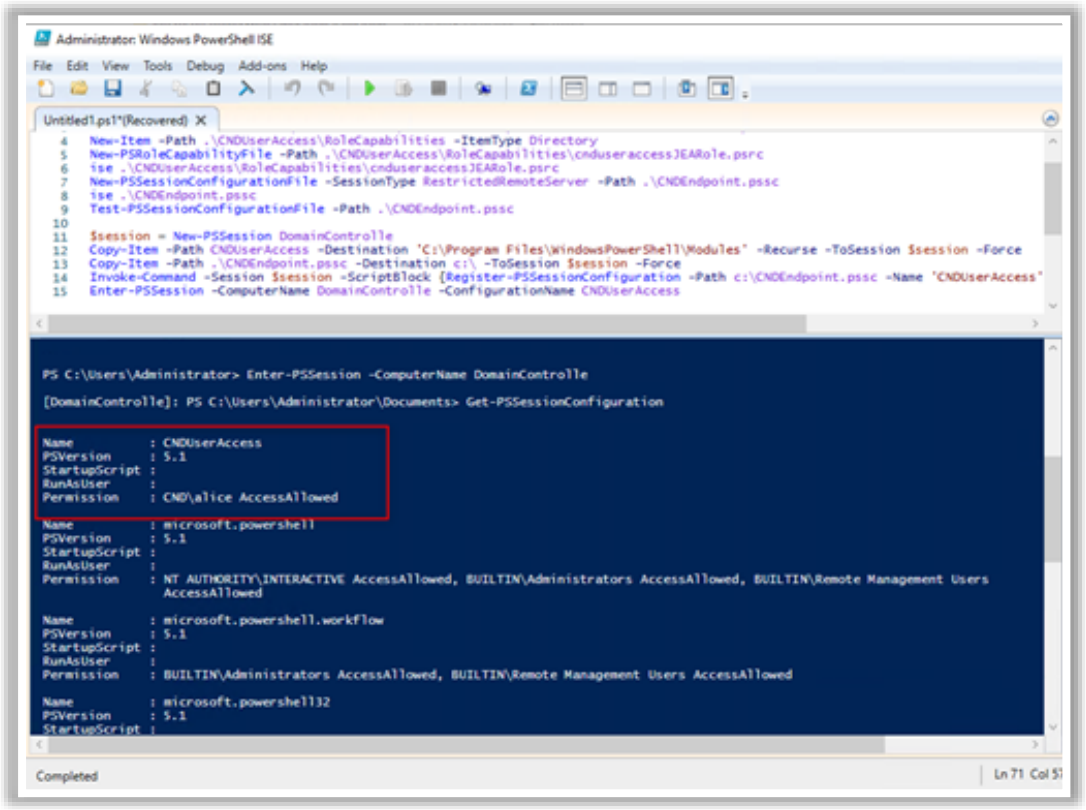


Figure 2.5: RBAC Implementation: Just Enough Administration (JEA)

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Logical Implementation of RBAC: Windows Admin Center (WAC)

Windows Admin Center (WAC) is a tool that helps configure RBAC for managing a server. The concept of a role is based on JEA, which enables granting the required rights to non-administrators.

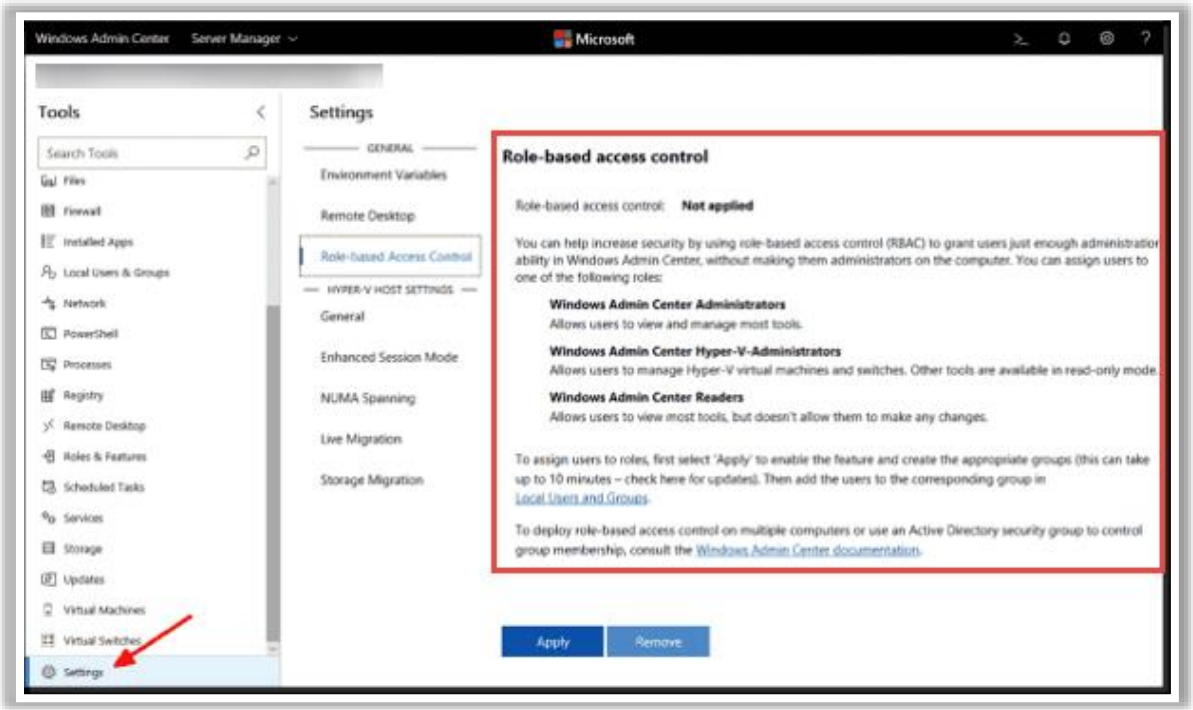
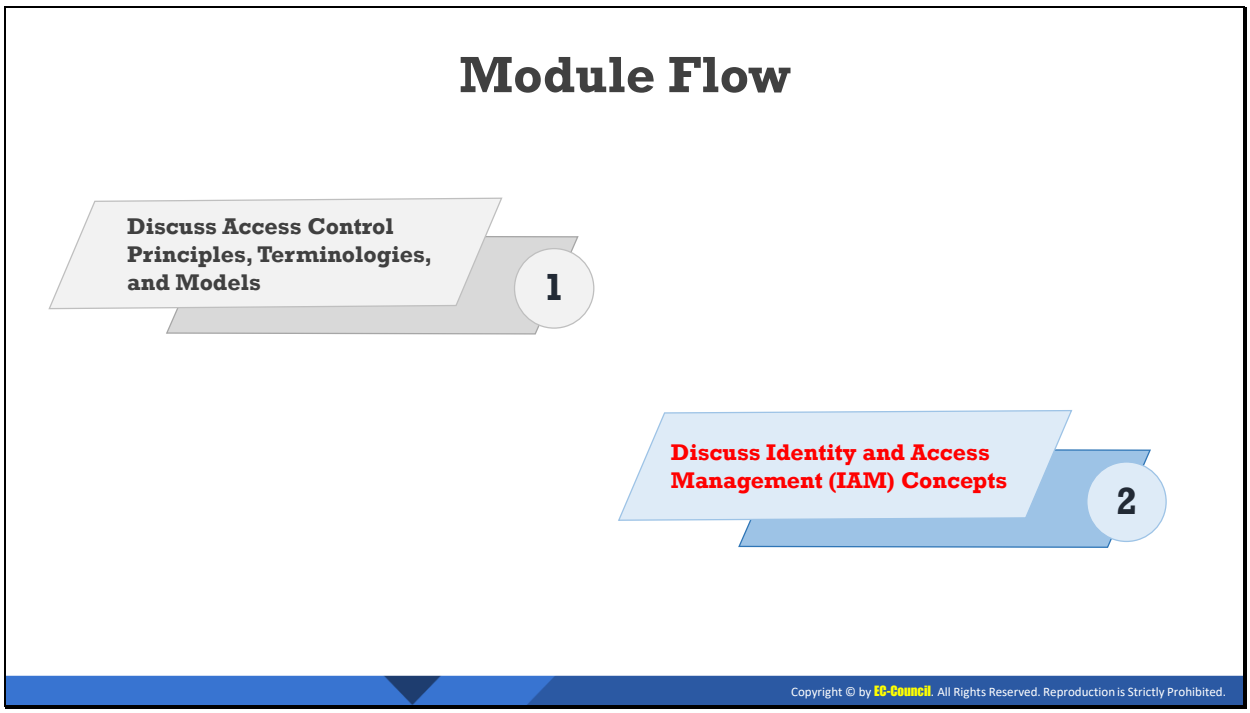


Figure 2.6: RBAC Implementation: Windows Admin Center (WAC)

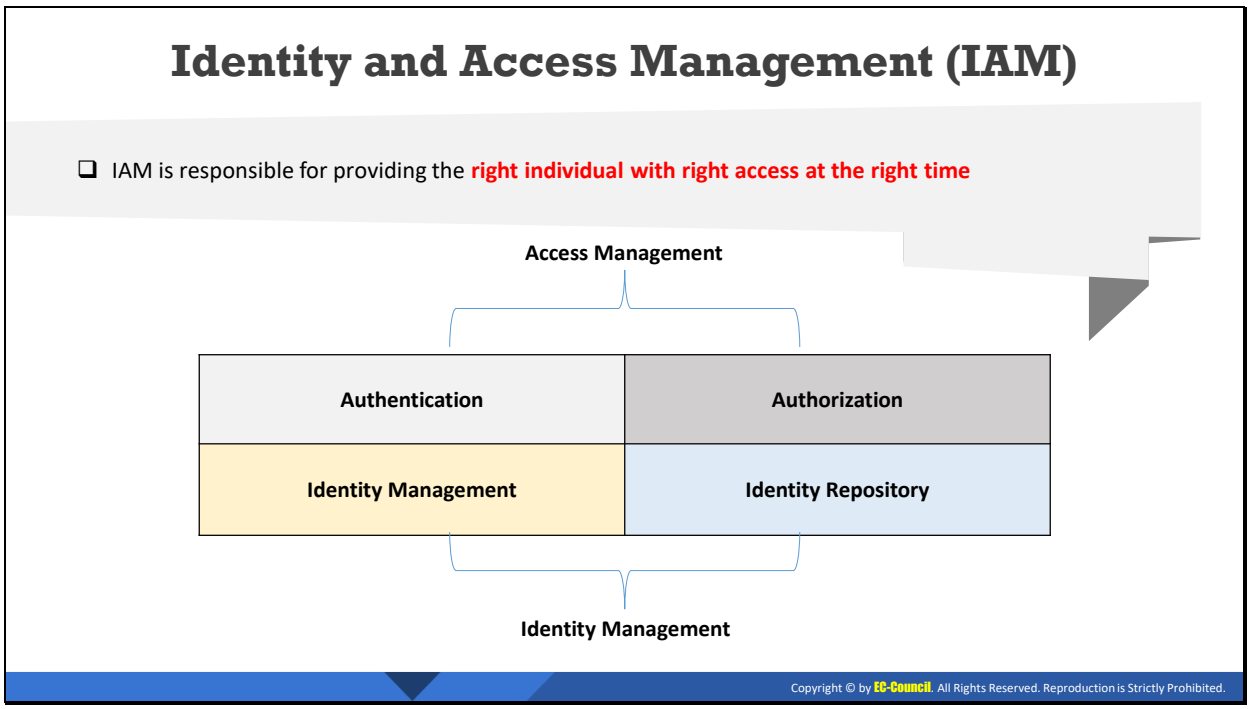
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

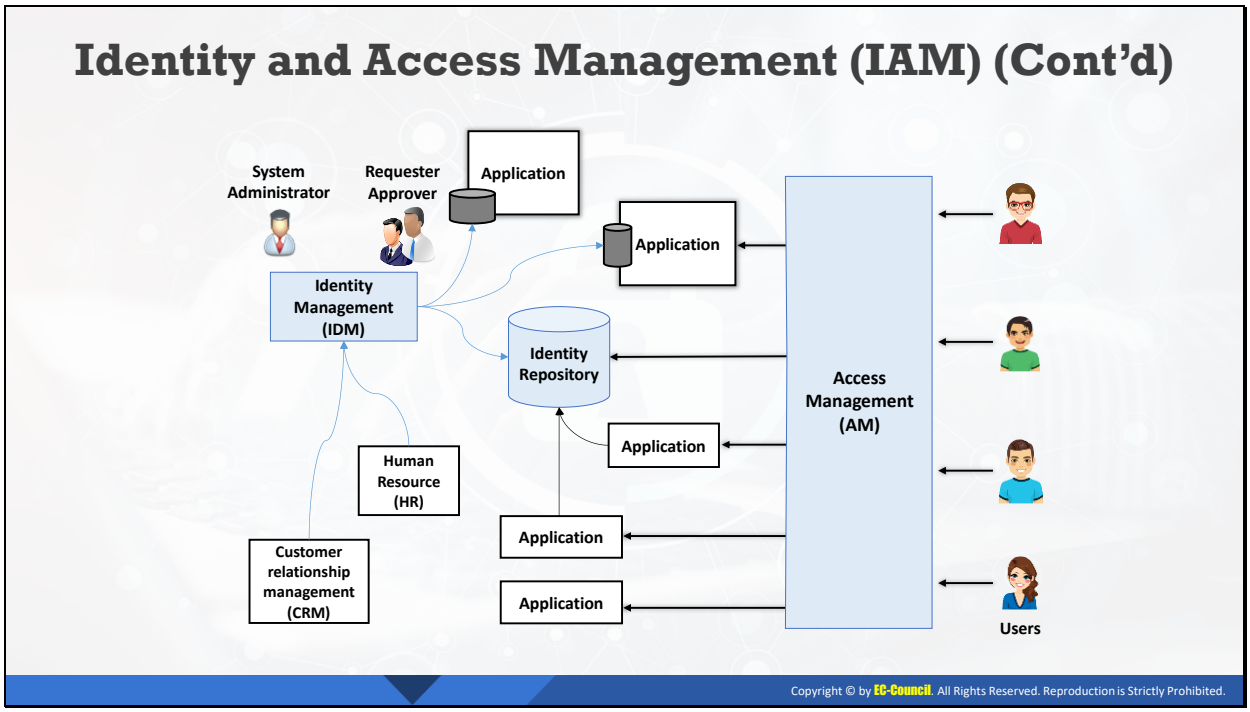


Discuss Identity and Access Management (IAM) Concepts

In an enterprise security, Identity and Access Management (IAM) plays an important role. It ensures that only authorized users have access to the network resources. The objective of this section is to explain the role of IAM and the security terminologies associated with it.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets





Identity and Access Management (IAM)

Identity and access management (IAM) is responsible for providing the right individual with the right access at the right time. It offers a role-based access control to the customers or employees of an organization for accessing critical information within the enterprise. It comprises of business processes, policies, and technologies that allow monitoring electronic or digital identities. IAM products provide the system administrators with tools and technologies for regulating user access (i.e., creating, managing, and removing access) to systems or

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

networks based on the roles of individual users within the enterprise. Organizations generally prefer an all-in-one authentication implementation which can be extended to identity a federation. This is because the identity federation includes IAM with a single sign-on (SSO) and a centralized active directory (AD) account for a secured management.

Organizations should ensure the correctness of data for the proper functioning of the IAM framework. An IAM framework can be divided into four areas, namely, authentication, authorization, user management, and central user repository/identity repository. All the IAM components are grouped under these four areas.

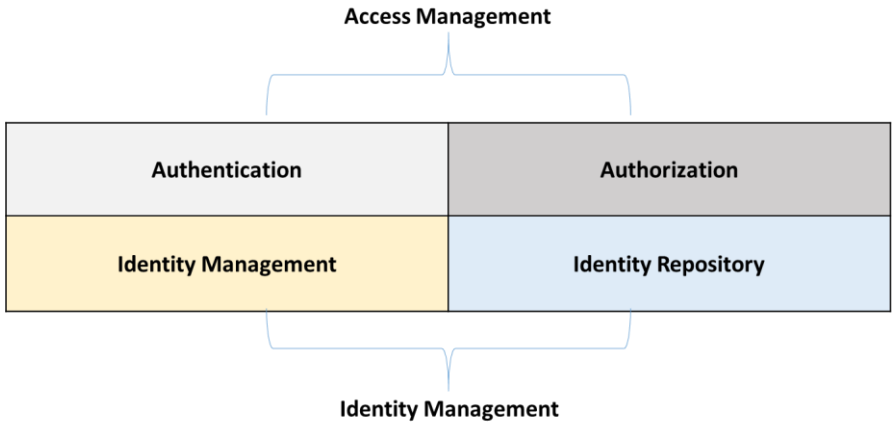


Figure 2.7: IAM Classification

Working of an IAM:

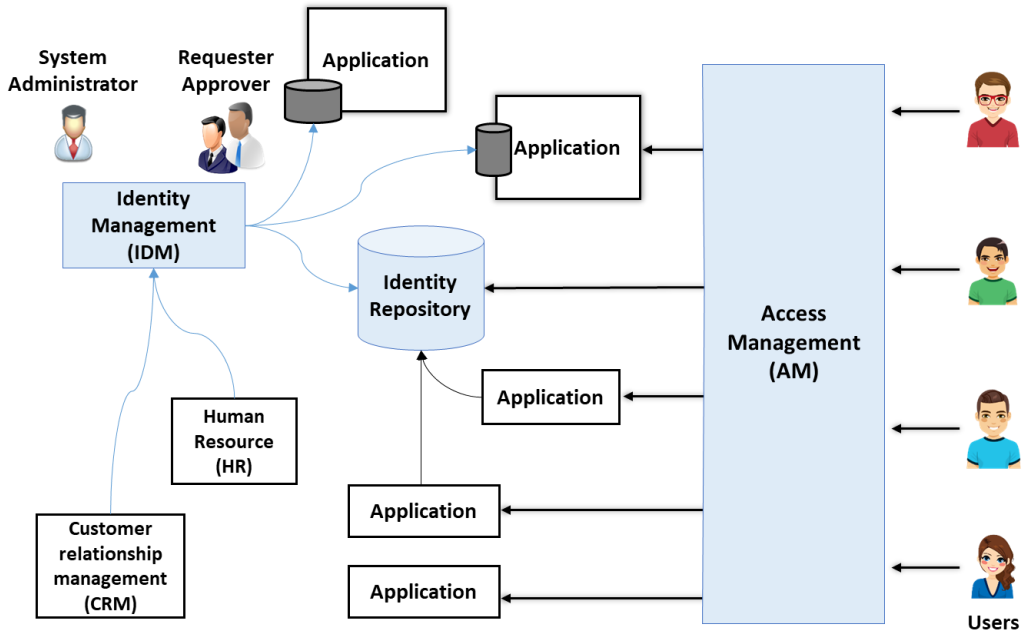
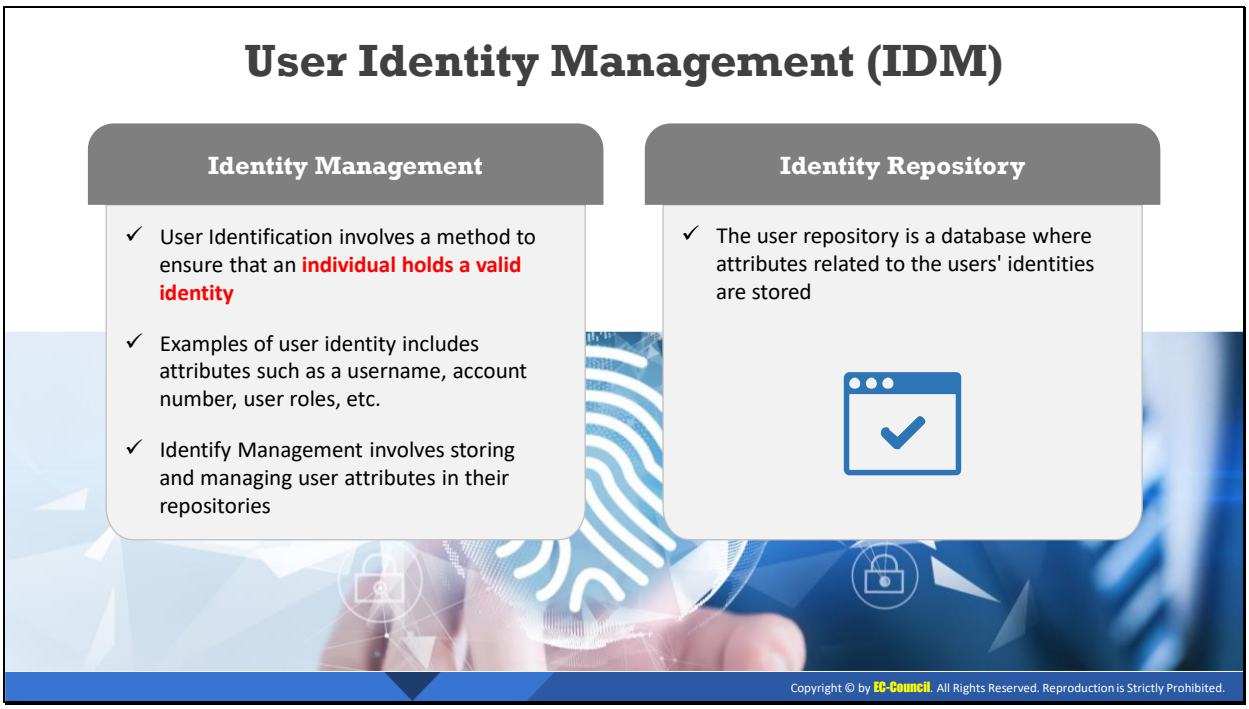


Figure 2.8: Working of IAM

The key responsibility of the identity management (IDM) framework is to manage the shared identity repository that is being accessed by the applications and the access management system.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

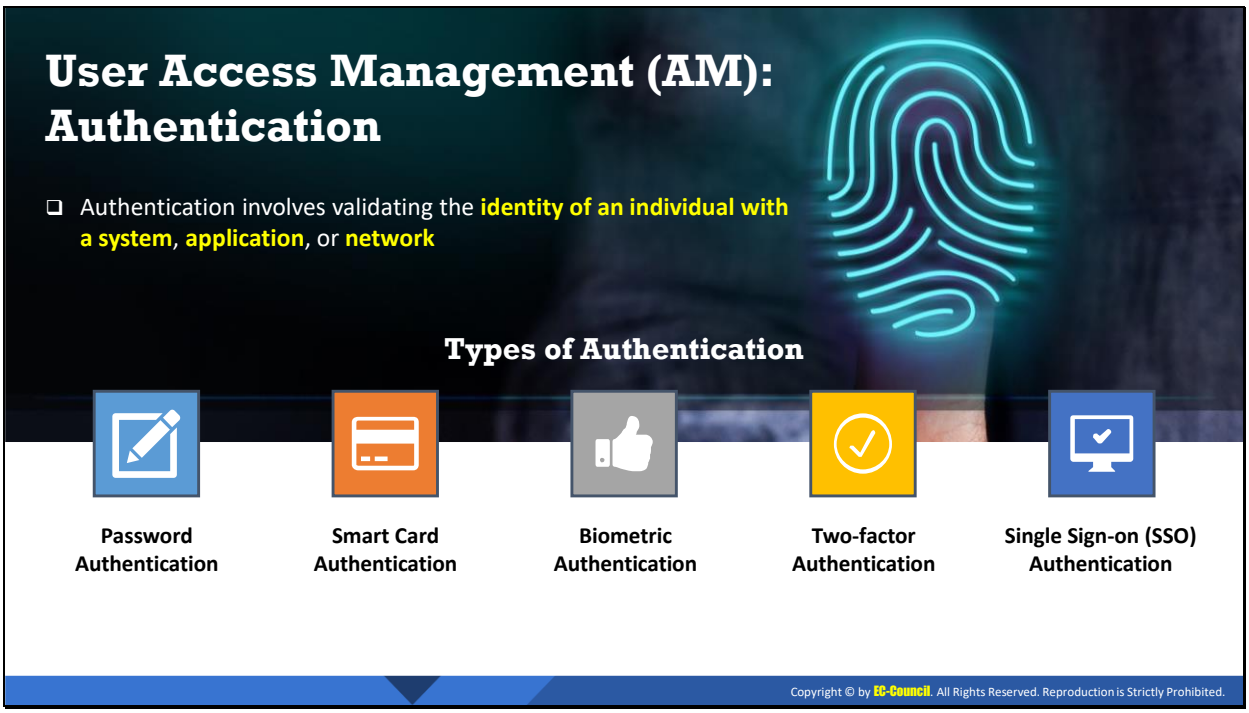


User Identity Management (IDM)

Identification deals with confirming the identity of a user, process, or device accessing the network. User identification is the most commonly used technique for authenticating the users in the network and applications. Users have a unique user ID which helps in their identification. Identify Management involves storing and managing user attributes in their repositories. Here, the user repository is a database where attributes related to the users' identities are stored.

The authentication process includes verifying a user ID and a password. Users are required to provide both the credentials in order to gain access to the network. The network administrators provide access controls such as the username, account number, etc. and permissions to various other services depending on the user IDs.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



User Access Management (AM): Authentication

Authentication involves verifying the credentials provided by a user while attempting to connect to a network. Both wired and wireless networks perform authentication of users before allowing them to access the resources in the network. A typical user authentication consists of a user ID and a password. Other forms of authentication include authenticating a website using a digital certificate and comparing the product and the label associated with it. The factors associated with the process of authentication are as follows:

- **Something you know**: The user should know the information such as usernames, passwords, etc., while trying to log into a system or a network.
- **Something you have:** The user should hold information such as a one-time password token, employee ID cards, etc., while trying to log into a system or a network.
- **Something you are:** The user should use their biometric characteristics such as a retina scan, fingerprint scan, etc., while trying to log into a system or a network.

The commonly used authentication methods are as follows:

- Password Authentication
- Smart Card Authentication
- Biometric Authentication
- Two-factor Authentication
- Single Sign-on (SSO) Authentication

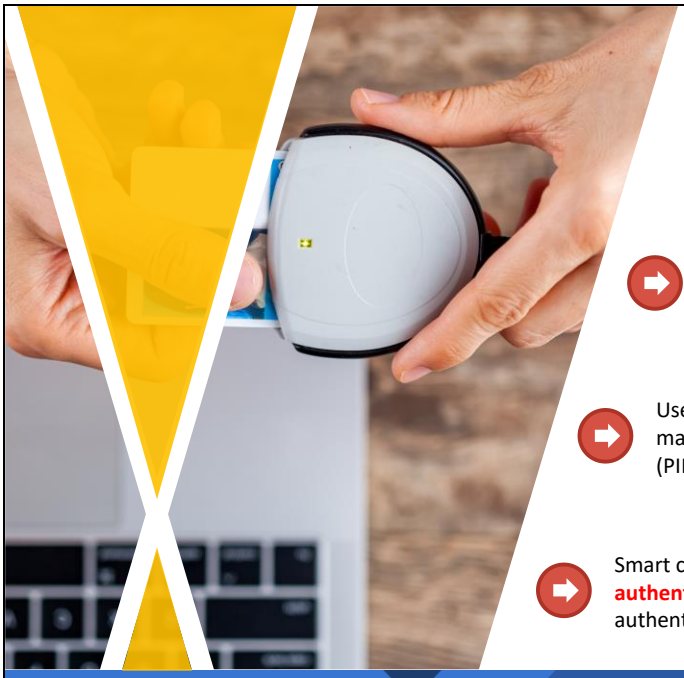
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Types of Authentication

Password Authentication

- Password Authentication uses a **combination** of a username and a password to authenticate the network users
- The password is checked against a **database** and the user is given access if it matches
- Password authentication can be vulnerable to **password cracking attacks** such as brute force or dictionary attacks

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Authentication (Cont'd)

Smart Card Authentication

- Smart card is a small **computer chip device** that holds a users' personal information required to authenticate them
- Users have to insert their smart cards into the card reader machines and enter their **personal identification number** (PIN) to authenticate themselves
- Smart card authentication is a **cryptography-based authentication** and provides stronger security than password authentication

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Types of Authentication (Cont'd)

Biometric Authentication

Biometrics refers to the **identification of individuals** based on their physical characteristics

Biometric Identification Techniques

Fingerprint Scanning

Compares two fingerprints for verification and identification on the basis of the patterns on the finger

Retinal Scanning

Analyzes the layer of blood vessels at the back of their eyes to identify a person

Iris Scanning

Analyzes the colored part of the eye suspended behind the cornea

Vein Structure Recognition

Analyzes thickness and location of veins to identify a person

Face Recognition

Uses facial features to identify or verify a person

Voice Recognition

Uses voice patterns to identify or verify a person

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Authentication (Cont'd)

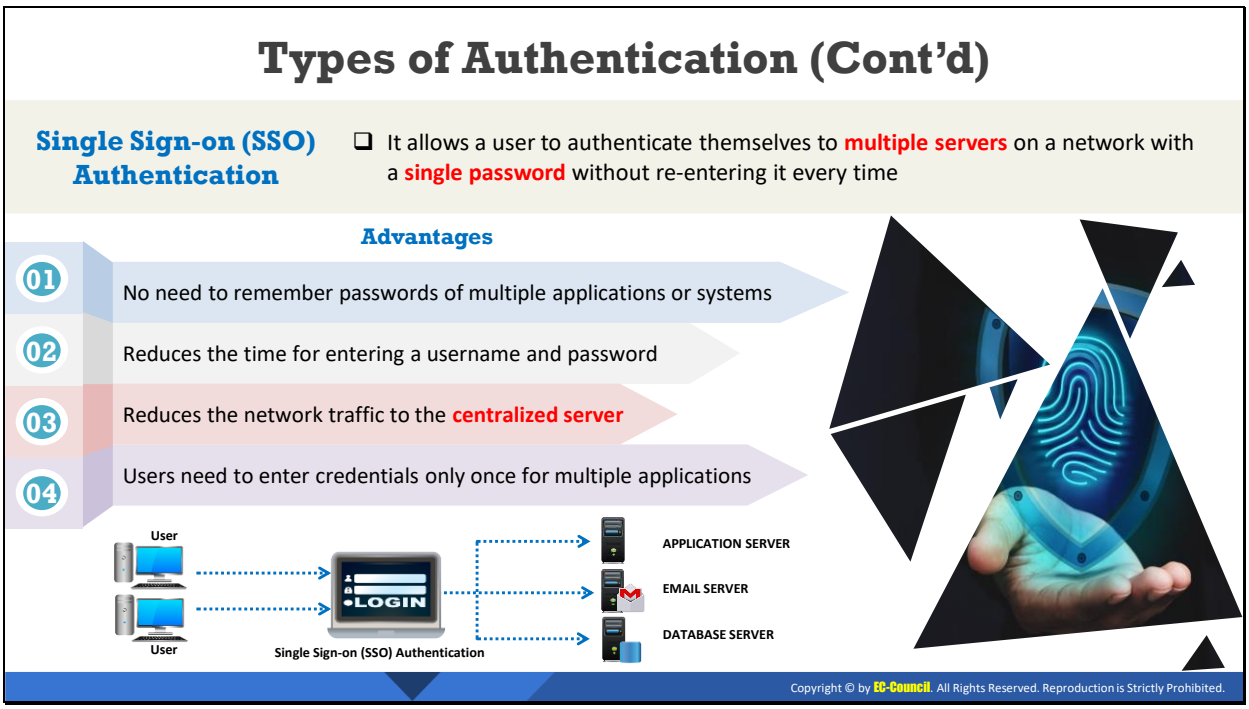
Two-factor Authentication

1. Two-factor authentication involves using two different authentication factors out of three (something you know, something your have, and something you are) to verify the **identity of an individual** in order to enhance the **security in authentication systems**
2. **Combinations of two-factor authentication:** password and smart card/token, password and biometrics, password and one-time password (OTP), smart card/token and biometrics, etc.
3. "Something you are" is the best companion of two-factor authentication as it is considered as the **hardest to forge** or **spoof**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Types of Authentication

- **Password Authentication**

  In password authentication, users are required to provide usernames and the passwords to prove their identity to a system, application, or a network. These are then matched against a list of authorized users in the database/Windows AD. Once matched, the users can access the system.

  The user password should follow standard password creation practices, including a mixture of alphabets, numbers, and special characters and having a length greater than 8 characters (since small passwords are easy to guess).

  Password authentication is vulnerable to brute force attacks or dictionary attacks, e.g., a person trying possible combinations of characters to guess the password or capture packets using a "packet sniffer" while sending data across the network as plain text.

- **Smart Card Authentication**

  Organizations use smart card technology to ensure strong authentication. Smart cards can store password files, authentication tokens, one-time password files, biometric templates, etc. This technology is used with another authentication token, thus providing multifactor authentication. This enables efficient logical access security. This technology is applied in VPN authentication, email and data encryption, electronic signatures, secure wireless logon, and biometric authentication.

  A smart card consists of a small computer chip that stores personal information of the user for identification. These cards are inserted into a machine for authentication, and a personal identification number (PIN) is input for processing the authentication information on the card. Smart cards also help in storing public and private keys.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Smart card authentication is a cryptography-based authentication technique and provides stronger security than password authentication. The main advantage of using a smart card is that it eliminates the risk of credential theft from a computer because credentials are stored in the card's chip. However, only a limited amount of information can be stored in the card's microchip.

Advantages of smart cards:

- **Highly secure technology:** The smart card technology uses efficient encryption and authentication methods, thus increasing the security of the card.
- **Easy to carry:** Smart cards are easy to carry and a user simply needs to know the PIN of the card.
- **Reduced chances of deception by users:** A smart card enables users to store information such as their fingerprint and other biometric details, thereby allowing organizations to recognize their employees.

Disadvantages of smart cards:

- **Easily lost:** Since smart cards are small in size, the chances of losing them are very high.
- **Security issues:** Losing a smart card puts its owner's information and identity at great risk.
- **High cost of production**: As smart cards have microchips and other encryption technologies; their production cost is high.

- **Biometric Authentication**

Biometrics is a technology which identifies human characteristics for authenticating people. The most commonly used biometrics are fingerprint scanner, retina scanner, facial recognition, DNA, and voice recognition.

Biometric authentication involves the following steps:

- The reader scans the biometric data
- A software converts the scanned information into a digital form and compares it against the biometric data stored in the database
- If both data match, then it confirms the authenticity of the user and allows permission.

The different types of identification techniques used in biometrics are as follows:

- **Fingerprint scanning:** Compares two fingerprints for verification and identification on the basis of the patterns on the finger. The patterns depend on the ridges and minutia points that differentiate each user's fingerprints.
- **Retinal scanning:** Compares and identifies a user on the basis of the distinctive patterns of the retina blood vessels.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- **Iris scanning:** Compares and identifies the images of the iris of one or both eyes of a user. The iris pattern differs from one person to another.
- **Vein structure recognition**: Compares and identifies the patterns produced by a user's veins. Each person has a different pattern depending on the flow of blood.
- **Face recognition:** Compares and identifies a person on the basis of the facial features from an image or a video source.
- **Voice recognition:** Compares and identifies a person on the basis of the voice patterns or speech patterns.

Advantages of biometrics:

- It is difficult to tamper with biometric data, in contrast to passwords or usernames. They cannot be shared or stolen using social engineering techniques. Biometric authentication requires the presence of the user, which reduces the chances unauthorized access.

Disadvantages of biometrics:

- It is difficult to change the biometric factors if this information has been compromised.
- Retinal scan and vein structure scanning can create privacy issues. Both retinal scan and vein structure scan information may inadvertently disclose a medical condition.

- **Two-factor Authentication**

Two-factor authentication is a process where a system confirms the user identification in two steps. The users could use a physical entity such as a security token as one of the credentials and the other credential can include security codes.

Two-factor authentication depends on three factors:

- Something you have
- Something you know
- Something you are

The factor "Something you are" is the best companion of two-factor authentication as it is considered as the hardest to forge or spoof.

Example: A bank card – A user is required to swipe the bank card and enter a PIN while accessing the bank card. Here, the bank card is the physical entity and the PIN is the security code.

The advantage of the two-factor authentication includes decreasing the chances of identity theft and phishing. However, there are certain drawbacks of this two-step process. There are situations where the user will have to wait for the organization to issue the physical token to the user. The delay in receiving the token results in the users waiting for a long time to access their private data.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

Identity evaluation depends on knowledge, possession, and inherent factors. Out of these, inherent factors are difficult to change as they depend on the characteristics of a human being.

There are many combinations available in the two-factor authentication process. The most commonly found combinations are:

- Password and smart card
- Password and biometrics
- Password and one-time password (OTP)
- Smart card and biometrics

Two-factor authentications performed without using tokens are called tokenless authentication. They can be implemented quickly across the network.

- **Single Sign-on (SSO) Authentication**

As the name suggests, it allows the users to access multiple applications using a single username and password. The SSO stores the credentials of a user in an SSO policy server. An example of SSO is Google applications. Users can access all Google applications using a single user name and password combination. Consider Google as a central service. This central service creates a cookie for all users logging in for the first time in any of the applications present in the central service. When the user attempts to access other applications of the central service, it eliminates the need for the user to enter the credentials again due to the cookie which has already been created. The system checks the credentials using the created cookie.

Figure 2.9: Single Sign-On (SSO) Authentication

Advantages of SSO:

- Reduces the chances of reauthentication, thereby increasing the productivity.
- Removes the chances of phishing.
- Provides a better management of applications owing to a centralized database.
- Assists with the account lifecycle. Provisioning and deprovisioning of accounts is simplified by the availability of a single source of truth.
- No need to remember passwords of multiple applications or systems.
- Reduces the time for entering a username and password.

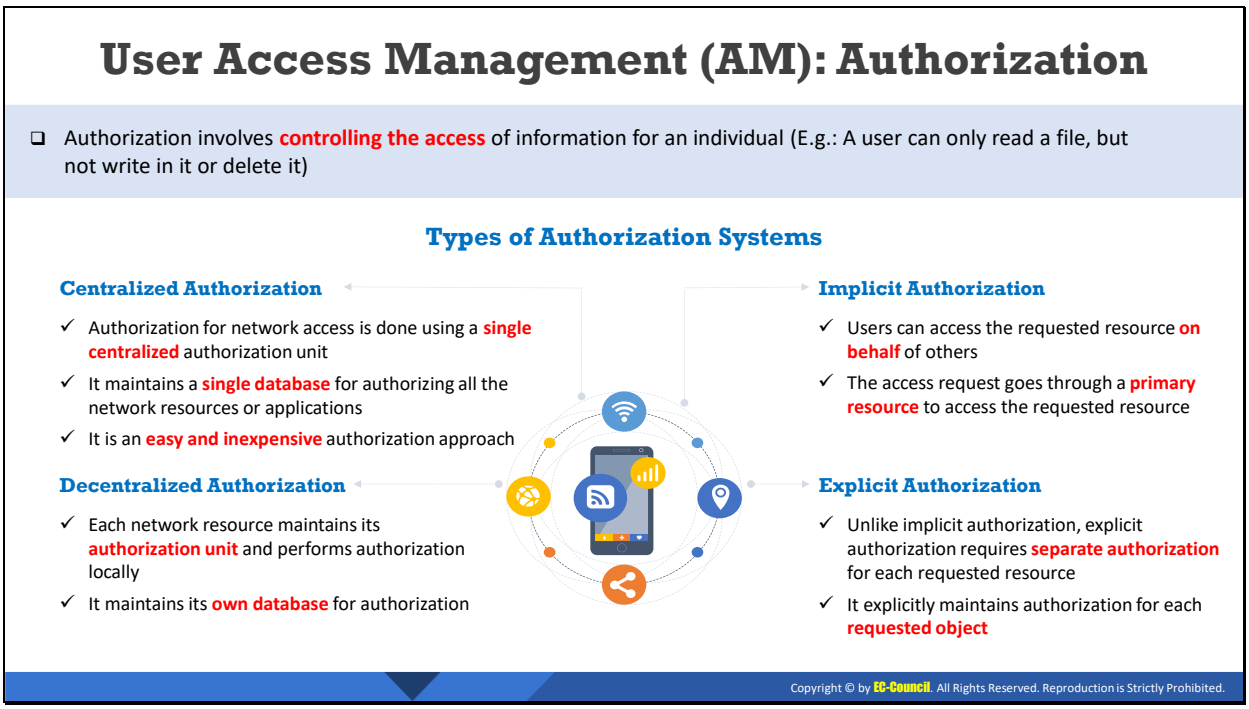
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Disadvantages of SSO:

- Losing credentials has a high impact as all the applications of the central service become unavailable.
- There are many vulnerability issues related with the authentication for all the applications.
- It is an issue in multiuser computers and requires the implementation of certain security policies to ensure security.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



User Access Management (AM): Authorization

Authorization refers to the process of providing permission to access the resources or perform an action on the network. s can decide the user privileges and access permissions of users on a multiuser system. The mechanism of authorization can allow the administrator to create access permissions for users as well as verify the access permissions created for each user.

Authorization can take different forms based on the needs of the organization.

- **Centralized Authorization**

  The need for centralized authentication came into existence when it became difficult to implement the authorization process individually for each resource. It uses a central authorization database that allows or denies access to the users and the decision on the access depends on the policies created by the centralized units. This enables an easy authorization for users accessing different platforms. Centralized authorization units are easy to handle and have low costs. A single database provides access to all applications, thereby enabling an efficient security. A centralized database also provides an easy and inexpensive method of adding, modifying, and deleting the applications from the centralized unit.

- **Decentralized Authorization**

  A decentralized authorization maintains a separate database for each resource. The database contains the details of all users who are permitted to access a particular resource. The decentralized authorization process enables users to provide access to other users as well. This increases the level of flexibility of the users in using the decentralized method. However, certain issues related to the decentralized authorization include cascading and cyclic authorizations.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **Implicit Authorization**

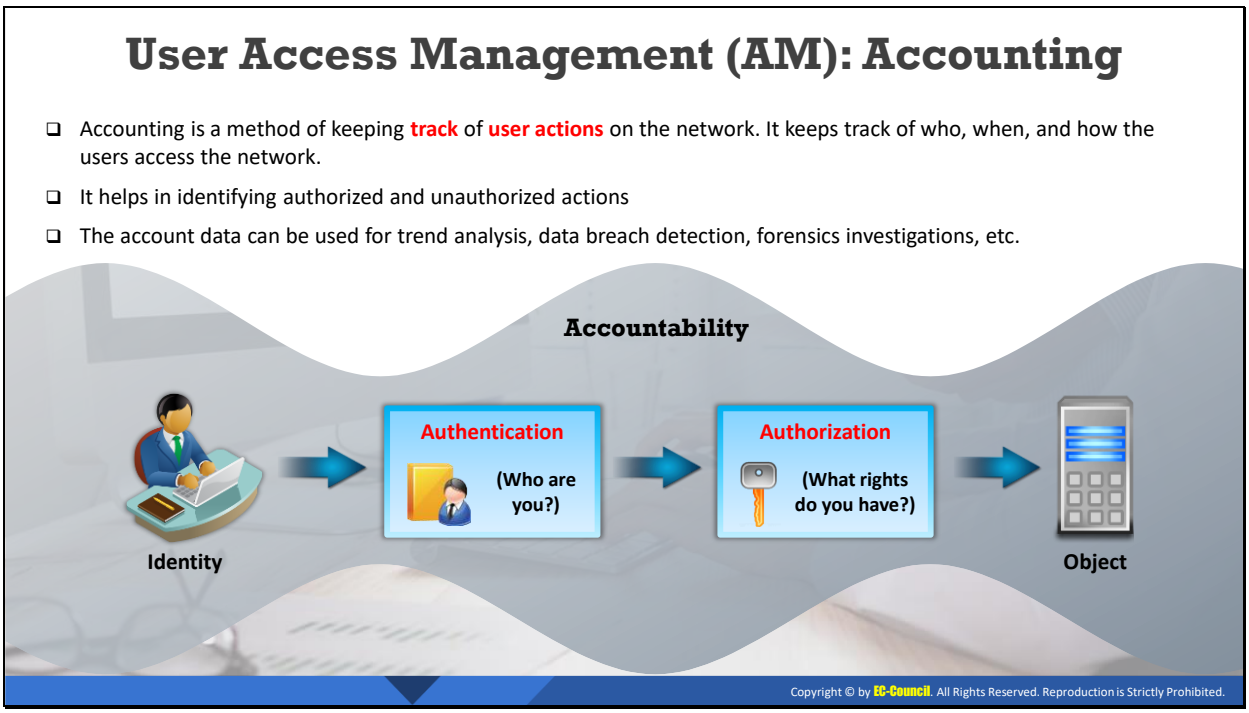
  Implicit authorization provides access to the resources indirectly. A task is possible after a user receives authorization for a primary resource through which access to the requested resource is possible. For example, a user requesting a web page has permission to access the main page as well as all pages linked to the main page. Hence, the user is gaining an indirect access to the other links and documents attached to the main page. The implicit authorization provides a level of higher granularity.

- **Explicit Authorization**

  An explicit authorization maintains separate authorization details for each resource request. This technique is simpler than the implicit technique. However, it takes up a large amount of storage space for storing all authorization details.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



User Access Management (AM): Accounting

User accounting involves tracking the actions performed by a user on a network. It keeps track of who, when, and how the users access the network. This includes verifying the files accessed by the user and functions such as alteration or modification of the files or data. It helps in identifying authorized and unauthorized actions. The account data can be used for trend analysis, data breach detection, forensics investigations, etc.

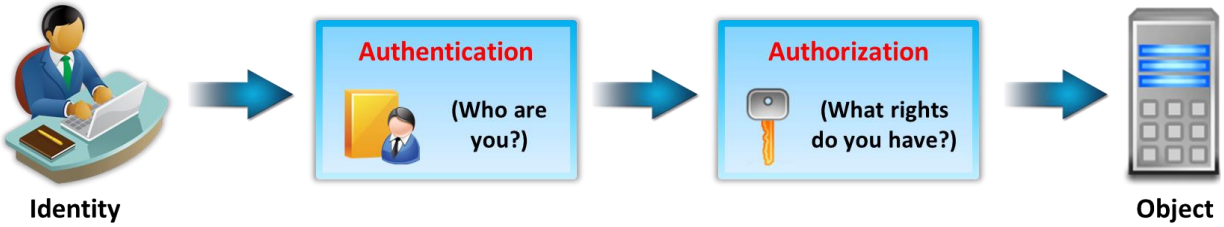
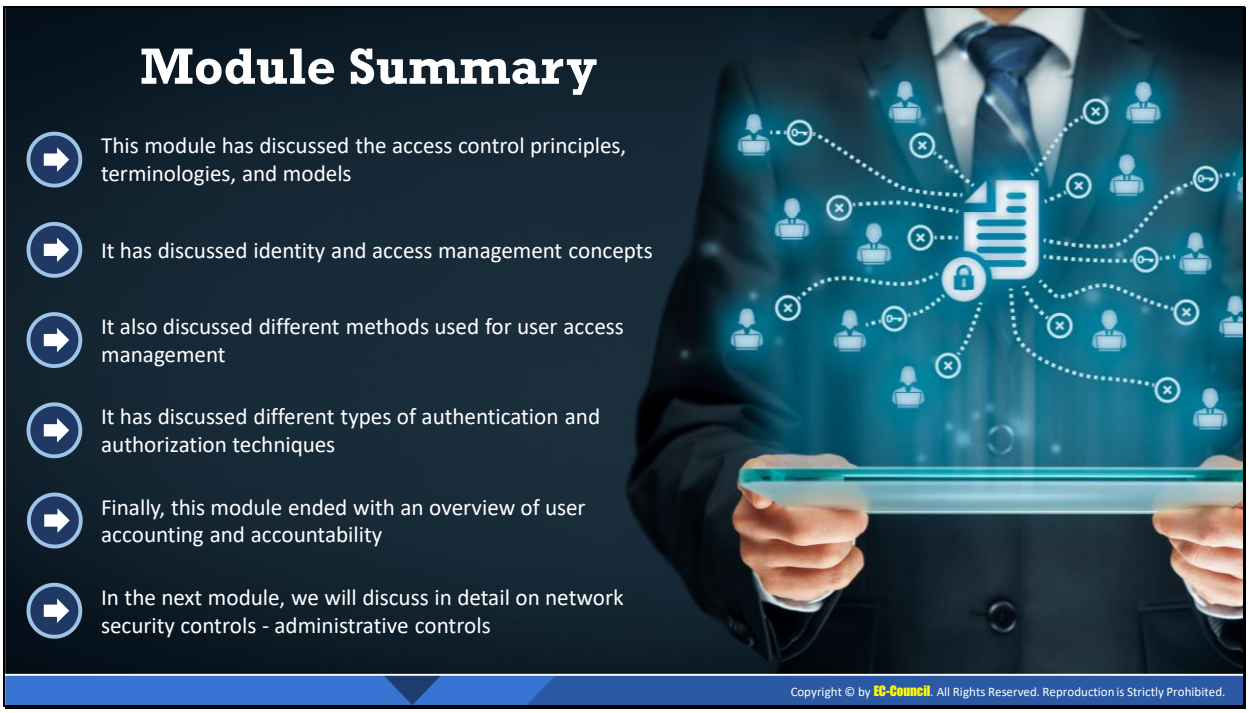


Figure 2.10: User Accounting

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Module Summary

This module discussed access control principles, terminologies, and models. Further, it discussed concepts related to identity and access management. It also discussed different methods used for user access management. Moreover, this module explained different types of authentication and authorization techniques. Finally, this module presented an overview of user accounting and accountability.

In the next module, we will discuss in detail network security controls; more specifically, the next module discusses administrative controls.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

EC-Council

N|DE
Network Defense Essentials

Module 03

Network Security Controls - Administrative Controls

https://t.me/learningnets

Module Objectives

Compliance, policies, and governance are integral to an information security program for any organization. An organization needs to comply with certain regulatory standards to run its businesses. At the same time, it must also have strong security policies and governance in order to fulfill regulatory standards. The current module addresses this administrative aspect of an organization's network security.

At the end of this module, you will be able to do the following:

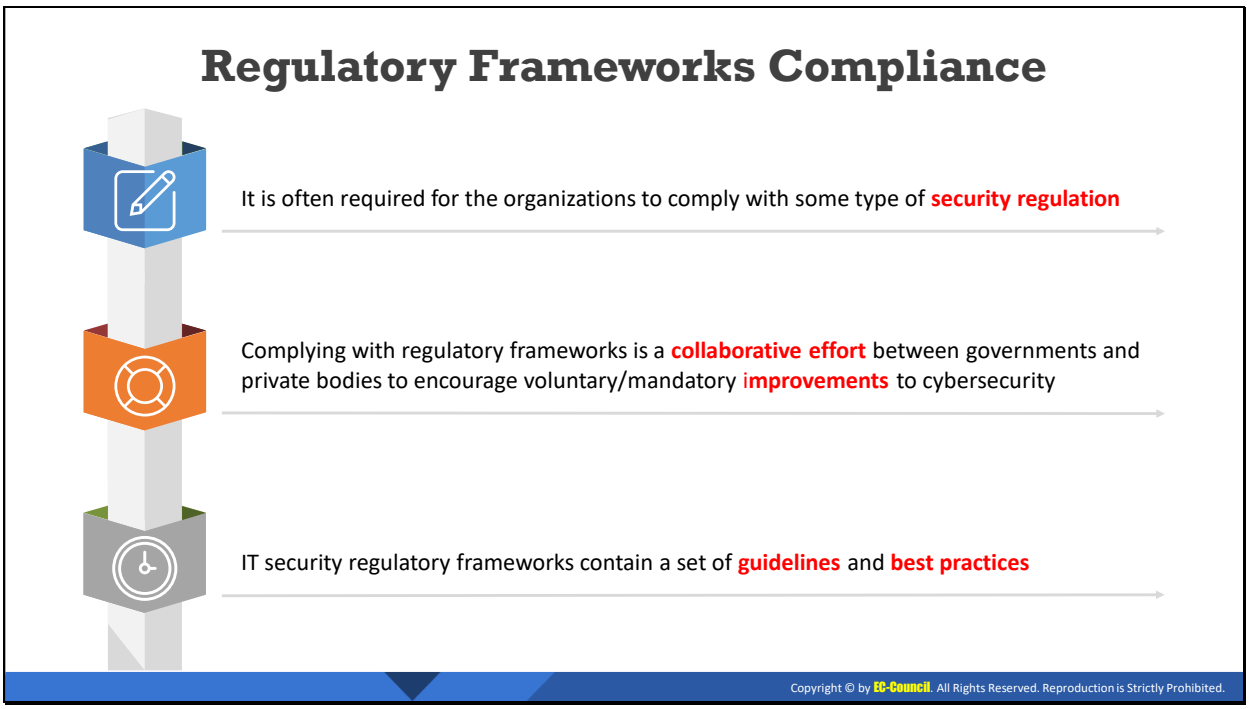
- Understand various regulatory frameworks, laws, and acts
- Understand why organizations need compliance
- Describe the need for and characteristics of good security policy
- Explain how to design and develop security policies
- Understand the different types of security policies
- Understand the different types of security and awareness training

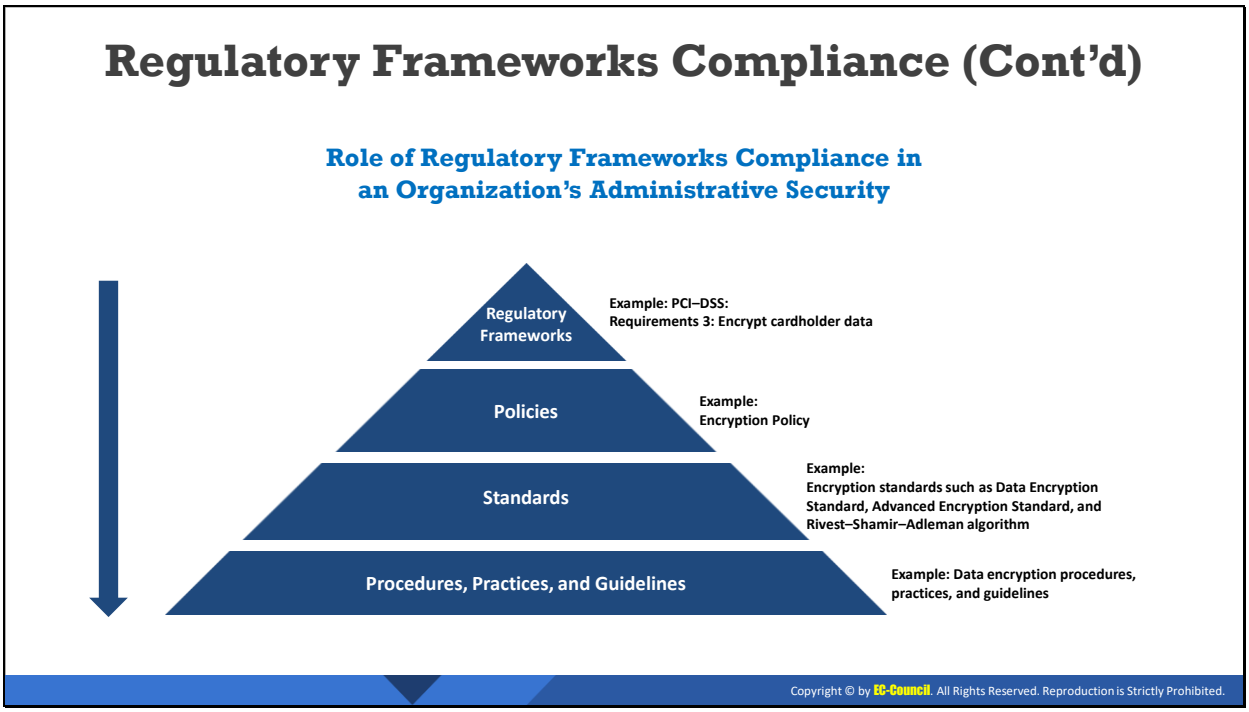
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Discuss Various Regulatory Frameworks, Laws, and Acts

This section explains the need for compliance and how to comply with a regulatory framework. This section also explains the various regulatory frameworks, laws, and acts. It describes frameworks, laws, and acts such as the Payment Card Industry Data Security Standard (PCI–DSS), Health Insurance Portability and Accountability Act (HIPAA), General Data Protection Regulation (GDPR), Sarbanes–Oxley Act (SOX), Gramm–Leach–Bliley Act (GLBA), ISO Information Security Standards, Digital Millennium Copyright Act (DMCA), and Federal Information Security Management Act (FISMA).

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets





Regulatory Frameworks Compliance

Regulatory framework compliance is a set of guidelines and best practices established in order for organizations to follow and, thus, meet their regulatory needs, enhance processes, improve protection, and accomplish any other objectives based on the industry and data types maintained. It is often required for the organizations to comply with some type of security regulation. Complying with regulatory frameworks is a collaborative effort between governments and private bodies to encourage voluntary/mandatory improvements to

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

cybersecurity. Regulatory compliance prevents organizations from incurring large fines or being victim to data breaches. Most organizations comply with more than one regulatory framework. Deciding which framework, policies, and controls are best compatible with an organization's compliance goals is a difficult task. At the same time, regulatory framework compliance has an evolving nature because organizational environments are always in flux. Generally, these guidelines are leveraged by

- Internal auditors and other stakeholders who assess the controls an organization requires;
- External auditors who assess the controls an organization requires; and
- Others/third parties (private/governments) such as key customers and investors who assess risk before collaborating with an organization.

IT security regulatory frameworks contain a set of guidelines and best practices. IT security regulatory frameworks inform businesses that they need to follow these guidelines and best practices to meet regulatory requirements, improve security, and achieve certain business objectives.

To ensure cybersecurity, organizations must implement the following standards to meet regulatory framework compliance:

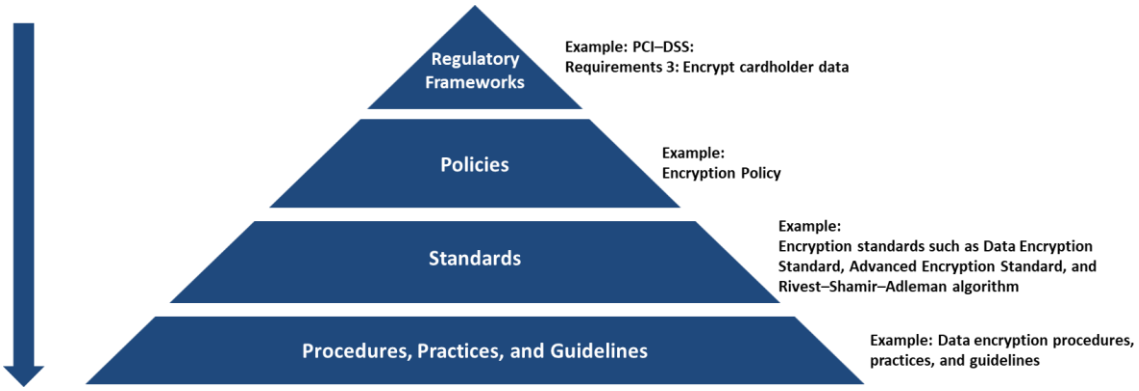


Figure 3.1: Role of Regulatory Frameworks Compliance in an Organization's Administrative Network Security

Regulatory Frameworks: Under a framework, an organization must document its policies, standards as well as procedures, practices, and guidelines. Each of these aspects have different purposes; hence, they cannot be combined into one document. Examples of regulatory frameworks include the Payment Card Industry—Data Security Standard (PCI–DSS) Requirement 3: Protect stored cardholder data.

- **Policies**

  Policies are high-level statements dealing with the administrative network security of an organization. These are leveraged by an organization's senior management. Organizations require at least one policy in place. A policy is viewed as a business mandate and has a top-down management. Some examples of policy include email and encryption policies. They generally outline the

  - Security roles and responsibilities,

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- Scope of information to be secured,
- Description of the required controls for securing information, and
- References to standards and guidelines that support the policies.

- **Standards**

  Standards comprise specific low-level mandatory controls or controls related to the implementation of a specific technology useful for enforcing and supporting policies and ensuring consistent businesses security. As noted earlier, this includes password policy such as password standards for password complexity, or encryption policy, which include standards such as data encryption standard (DES), advanced encryption standard (AES), and Rivest–Shamir–Adleman algorithms.

- **Procedures, Practices, and Guidelines**

  Procedures or standard operating procedures (SOP) comprise step-wise instructions useful for implementing the controls that are defined by multiple policies, standards, and guidelines such as a procedure for secure Windows installation or data encryption procedure, practices, and guidelines.

  Guidelines comprise recommendations, but non-mandatory controls, as well as general statements, administrative instructions, or best practices useful for supporting standards or acting as a reference when no standards in place. Guidelines and best practices are interchangeable. These changes are environment-dependent and must be reviewed more often than standards and policies. For example, a standard may state that a password should be eight characters or more, while a supporting guideline may state that it is also a best practice to follow password expiration and data encryption guidelines.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

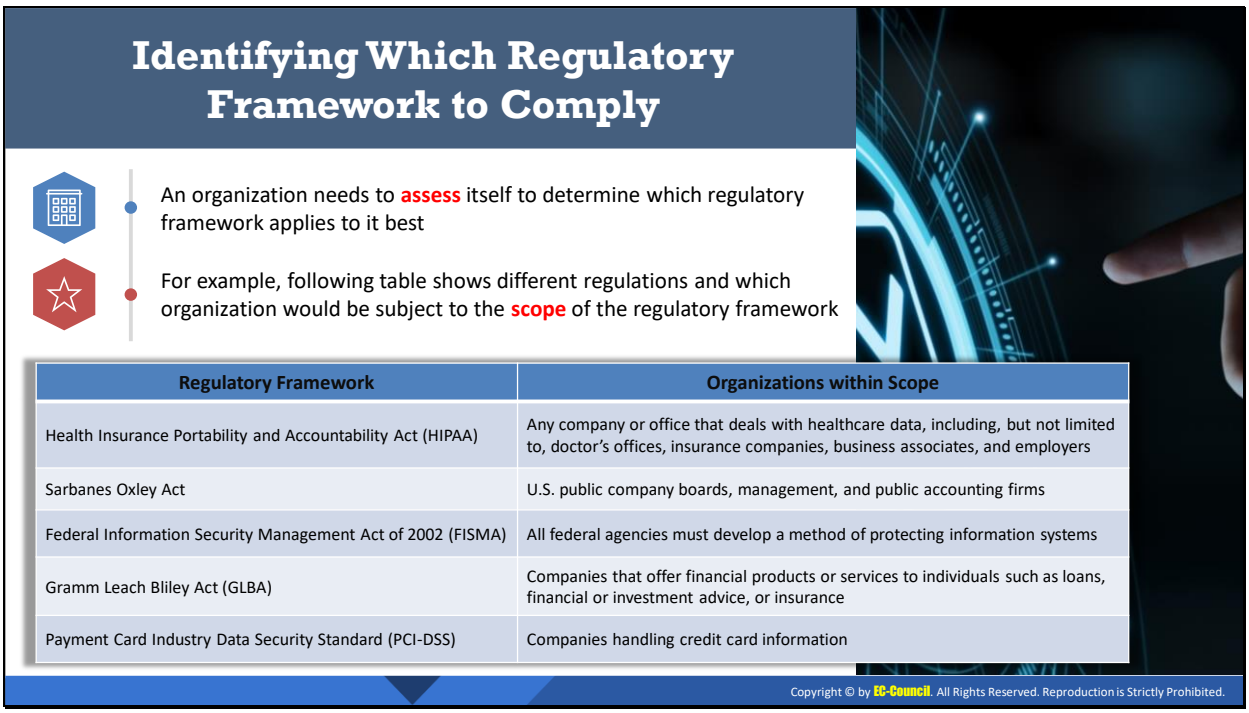
https://t.me/learningnets

Why Organizations Need Compliance

Information security compliance should be a requirement than a choice for organizations, since the money, time, and efforts invested in the compliance is worth more than the cost of risks. The advantages that regulatory framework compliance brings for an organization include:

- **Improved Security:** IT security regulations and standards improve the overall security of an organization by meeting baseline regulatory requirements. These baseline requirements ensure consistent data security.
- **Minimized Losses:** Improved security can prevent security breaches, which otherwise can lead to losses, repair costs, legal fees, or hefty fines.
- **Maintenance of Trust:** Data breaches cause companies to lose their reputation and trust from customers. Compliances makes customers trust an organization with the belief that their information is safe.
- **Increased Control:** An organization's security increases with increased controls such as preventing employees from committing mistakes, implementing strong credential systems and encryption systems, or monitoring outside threats.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Identifying Which Regulatory Framework to Comply

An organization must perform a self-assessment to ascertain the regulatory frameworks that best applies to it. This compliance assessment involves identifying gaps between the existing control environment and an organization's requirements. However, this is a challenging task wherein an organization should fully understand its needs and function to understand which controls suit its size and complexity. When assessing compliance, an organization must consider the following:

- Financial institution letters;
- National Institute of Standards and Technology publications;
- Industry implementation guidance and recommendations—for example, international standards such as ISO 27002 or the National Institute of Standards and Technology Framework for cybersecurity enhancement; and
- Notice the cybercrimes, new exploits, and new trends to ascertain the possibility of a large-scope breach.

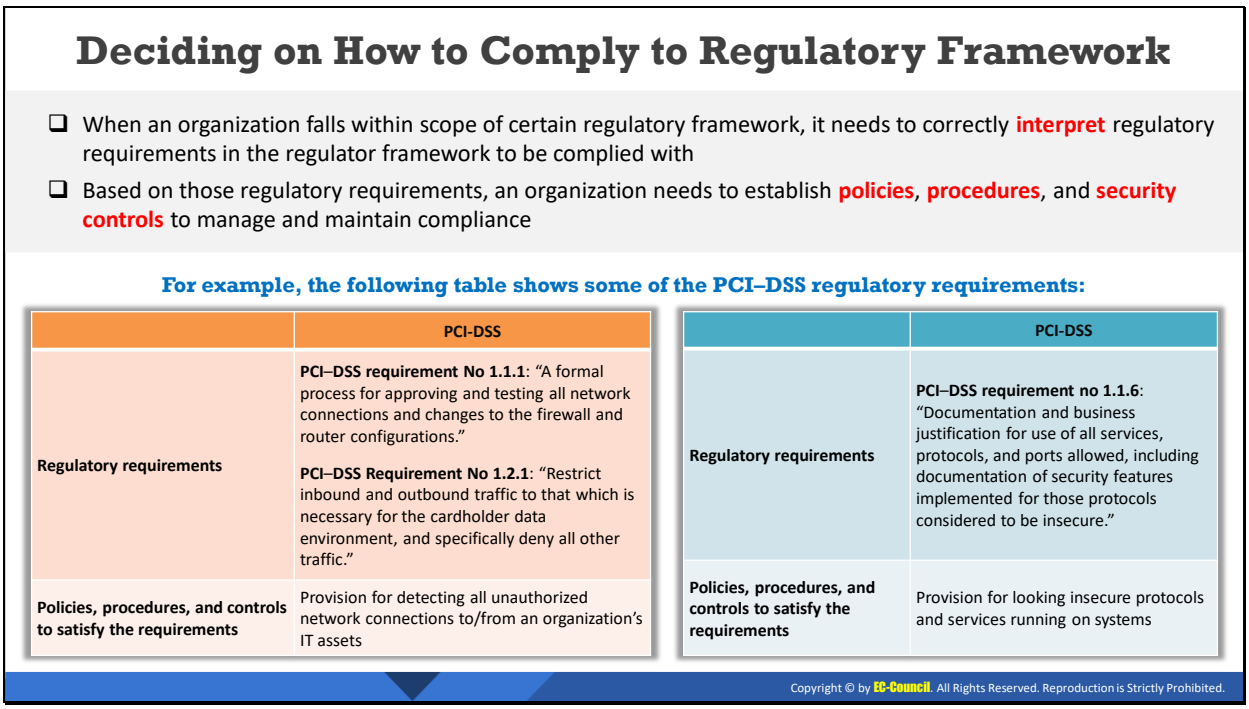
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

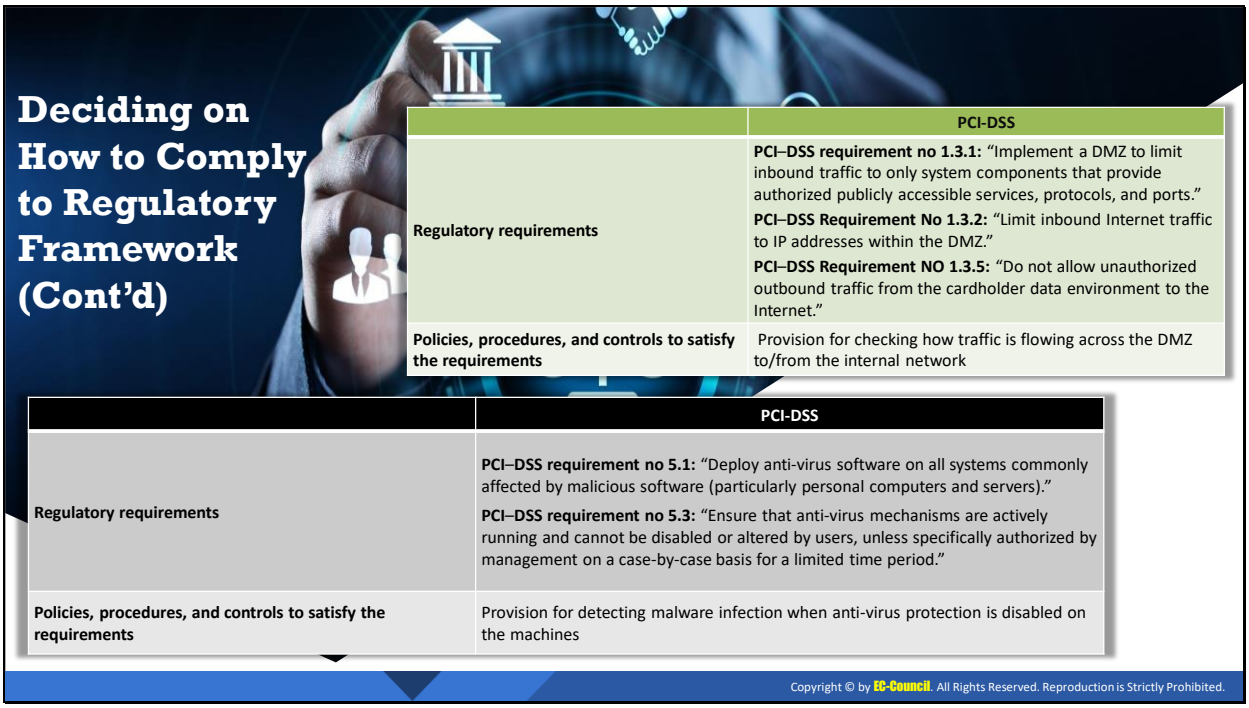
For example, following table shows different regulations and which organization would be subject to the scope of the regulatory framework.

Regulatory Framework	Organizations within Scope
Health Insurance Portability and Accountability Act (HIPAA)	Any company or office that deals with healthcare data, including, but not limited to, doctor's offices, insurance companies, business associates, and employers
Sarbanes Oxley Act	U.S. public company boards, management, and public accounting firms
Federal Information Security Management Act of 2002 (FISMA)	All federal agencies must develop a method of protecting information systems
Gramm Leach Bliley Act (GLBA)	Companies that offer financial products or services to individuals such as loans, financial or investment advice, or insurance
Payment Card Industry Data Security Standard (PCI-DSS)	Companies handling credit card information

Table 3.1: Different Regulatory Framework and Organizations within the Scope of Regulatory Framework

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets





Deciding on How to Comply to Regulatory Framework

An organization needs to correctly interpret its regulatory requirements once it has confirmed its framework. Then, it must analyze and interpret the collected information to determine how the collected information is relevant to an organization's services. Next, discuss and sort all an organization's internal/external personnel ambiguities, uncertainties, and problems faced during the interpretation of the identified compliance information. Assess and determine the order for suitable compliance requirements such as important implications and risks of possible

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

breaches. Separate/group the compliance requirements that are perceived as, first, important and central; then, only important; and finally, pertinent, but incidental, for an organization's operations.

Based on the regulatory requirements, an organization needs to establish proper policies, procedures, and security controls to organize its information security. For example, the following table shows some of the PCI–DSS regulatory requirements.

	PCI-DSS
Regulatory requirements	**PCI–DSS requirement No 1.1.1**: "*A formal process for approving and testing all network connections and changes to the firewall and router configurations.*" **PCI–DSS Requirement No 1.2.1**: "*Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.*"
Policies, procedures, and controls to satisfy the requirements	Provision for detecting all unauthorized network connections to/from an organization's IT assets

Table 3.2: PCI–DSS Requirement No 1.1.1 and 1.2.1

	PCI-DSS
Regulatory requirements	**PCI–DSS requirement no 1.1.6**: *"Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure."*
Policies, procedures, and controls to satisfy the requirements	Provision for looking insecure protocols and services running on systems

Table 3.3: PCI–DSS Requirements No 1.1.6

	PCI-DSS
Regulatory requirements	**PCI–DSS requirement no 1.3.1:** *"Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports."* **PCI–DSS Requirement No 1.3.2:** *"Limit inbound Internet traffic to IP addresses within the DMZ."* **PCI–DSS Requirement NO 1.3.5:** *"Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet."*

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

Policies, procedures, and controls to satisfy the requirements	Provision for checking how traffic is flowing across the DMZ to/from the internal network

Table 3.4: PCI–DSS Requirement No 1.3.1, 1.3.2, 1.3.5

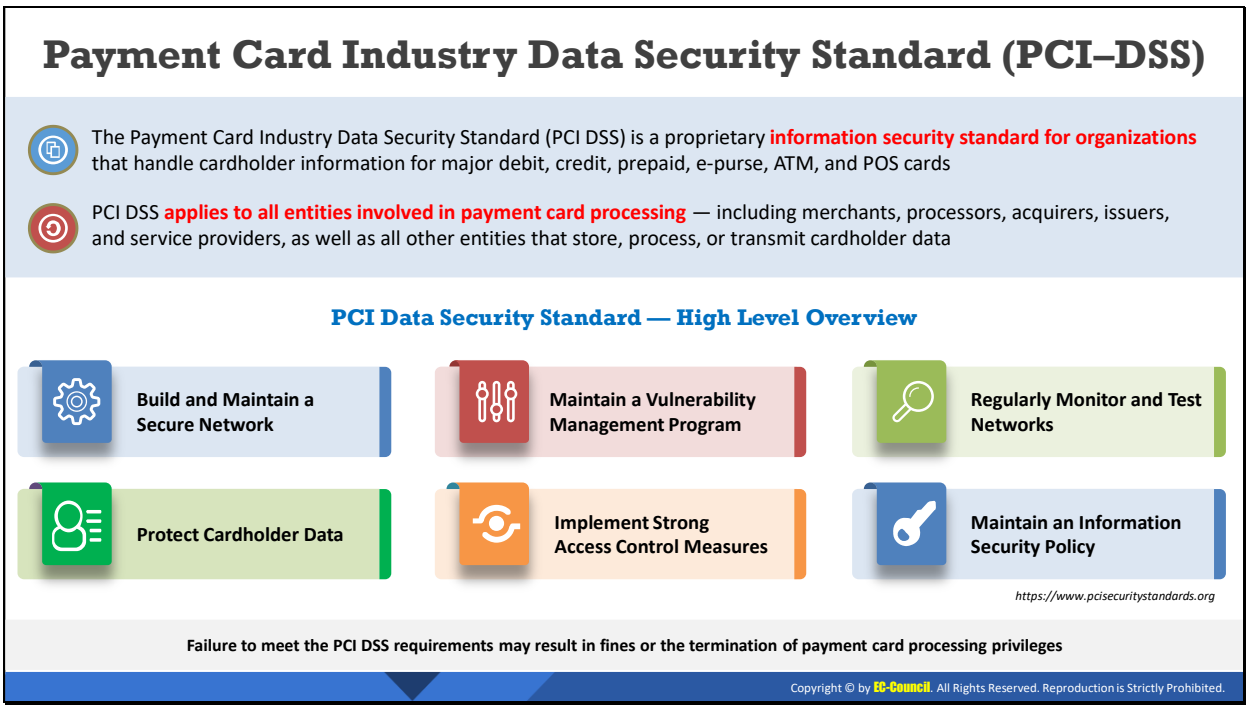
	PCI-DSS
Regulatory requirements	**PCI–DSS requirement no 5.1:** *"Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers)."* **PCI–DSS requirement no 5.3:** *"Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period."*
Policies, procedures, and controls to satisfy the requirements	Provision for detecting malware infection when anti-virus protection is disabled on the machines

Table 3.5: PCI–DSS Requirement No 5.1 and 5.3

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Regulatory Frameworks, Laws, and Acts

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Payment Card Industry Data Security Standard (PCI DSS)

Source: *https://www.pcisecuritystandards.org*

The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards. This standard offers robust and comprehensive standards and supporting materials to enhance payment card data security. These materials include a framework of specifications, tools, measurements, and support resources to help organizations ensure the safe handling of cardholder information. PCI DSS applies to all entities involved in payment card processing, including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process, or transmit cardholder data. PCI DSS comprises a minimum set of requirements for protecting cardholder data. The Payment Card Industry (PCI) Security Standards Council has developed and maintains a high-level overview of PCI DSS requirements.

PCI Data Security Standard – High Level Overview	
Build and Maintain a Secure Network	▪ Install and maintain a firewall configuration to protect cardholder data ▪ Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	▪ Protect stored cardholder data ▪ Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability	▪ Use and regularly update anti-virus software or programs

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

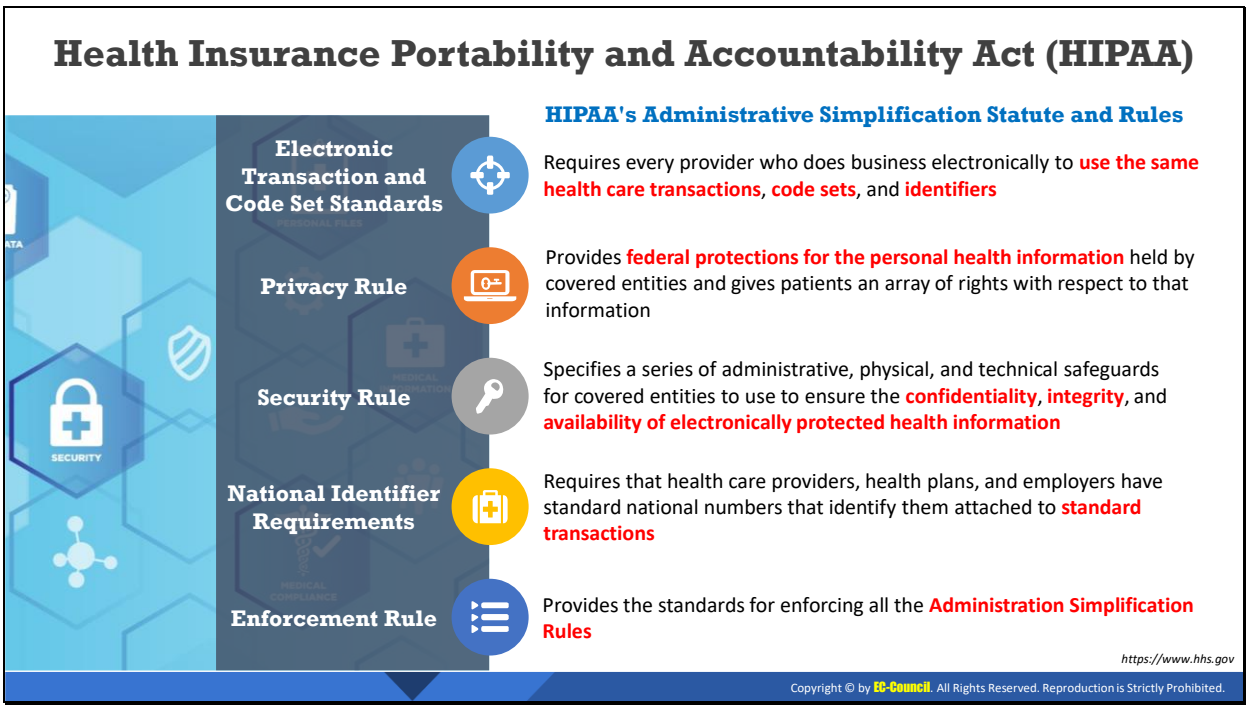
Management Program	▪ Develop and maintain secure systems and applications
Implement Strong Access Control Measures	▪ Restrict access to cardholder data by business need to know ▪ Assign a unique ID to each person with computer access ▪ Restrict physical access to cardholder data
Regularly Monitor and Test Networks	▪ Track and monitor all access to network resources and cardholder data ▪ Regularly test security systems and processes
Maintain an Information Security Policy	▪ Maintain a policy that addresses information security for all personnel

Table 3.6: Table Showing the PCI Data Security Standard—High-Level Overview

Failure to meet PCI DSS requirements may result in fines or the termination of payment-card processing privileges.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Health Insurance Portability and Accountability Act (HIPAA)

Source: *https://www.hhs.gov*

The HIPAA Privacy Rule provides federal protections for the individually identifiable health information held by covered entities and their business associates and gives patients an array of rights to that information. At the same time, the Privacy Rule permits the disclosure of health information needed for patient care and other necessary purposes.

The Security Rule specifies a series of administrative, physical, and technical safeguards for covered entities and their business associates to use to ensure the confidentiality, integrity, and availability of electronically protected health information.

The office of civil rights implemented HIPAA's Administrative Simplification Statute and Rules, as discussed below:

- **Electronic Transactions and Code Set Standards**

  Transactions are electronic exchanges involving the transfer of information between two parties for specific purposes. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) designated certain types of organizations as covered entities, including health plans, health care clearinghouses, and certain health care providers. In the HIPAA regulations, the Secretary of Health and Human Services (HHS) adopted certain standard transactions for the Electronic Data Interchange (EDI) of health care data. These transactions are claims and encounter information, payment and remittance advice, claim status, eligibility, enrollment and disenrollment, referrals and authorizations, coordination of benefits, and premium payment. Under HIPAA, if a covered entity electronically conducts one of the adopted transactions, they must use the adopted standard—either from ASC, X12N, or NCPDP (for certain pharmacy

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

transactions). Covered entities must adhere to the content and format requirements of each transaction. Every provider who does business electronically must use the same health care transactions, code sets, and identifiers.

- **Privacy Rule**

  The HIPAA Privacy Rule establishes national standards to protect people's medical records and other personal health information and applies to health plans, health care clearinghouses, and health care providers that conduct certain health care transactions electronically. The rule requires appropriate safeguards to protect the privacy of personal health information. It sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The rule also gives patients' rights over their health information, including the right to examine and obtain a copy of their health records and to request corrections.

- **Security Rule**

  The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronically protected health information.

- **Employer Identifier Standard**

  The HIPAA requires that each employer has a standard national number that identifies them on standard transactions.

- **National Provider Identifier Standard (NPI)**

  The National Provider Identifier (NPI) is a HIPAA Administrative Simplification Standard. The NPI is a unique identification number assigned to covered health care providers. Covered health care providers and all health plans and health care clearinghouses must use the NPIs in the administrative and financial transactions adopted under HIPAA. The NPI is a 10-position, intelligence-free numeric identifier (10-digit number). This means that the numbers do not carry other information about healthcare providers, such as the state in which they live or their medical specialty.

- **Enforcement Rule**

  The HIPAA Enforcement Rule contains provisions relating to compliance and investigation, as well as the imposition of civil monetary penalties for violations of the HIPAA Administrative Simplification Rules and procedures for hearings.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

Sarbanes Oxley Act (SOX)

- Enacted in 2002, the Sarbanes-Oxley Act is designed to **protect investors and the public** by increasing the accuracy and reliability of corporate disclosures
- The key requirements and provisions of SOX are organized into **11 titles**:

Title I

Public Company Accounting Oversight Board (PCAOB) provides independent oversight of public accounting firms providing audit services ("auditors")

Title II

Auditor Independence establishes the standards for external auditor independence, intended to limit conflicts of interest and address new auditor approval requirements, audit partner rotation, and auditor reporting requirements

Title III

Corporate Responsibility mandates that senior executives take individual responsibility for the accuracy and completeness of corporate financial reports

https://www.sec.gov

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Sarbanes Oxley Act (SOX) (Cont'd)

Title IV

Enhanced Financial Disclosures describe enhanced reporting requirements for financial transactions, including off-balance-sheet transactions, pro-forma figures, and the stock transactions of corporate officers

Title V

Analyst Conflicts of Interest consist of measures designed to help restore investor confidence in the reporting of securities analysts

Title VI

Commission Resources and Authority defines practices to restore investor confidence in securities analysts

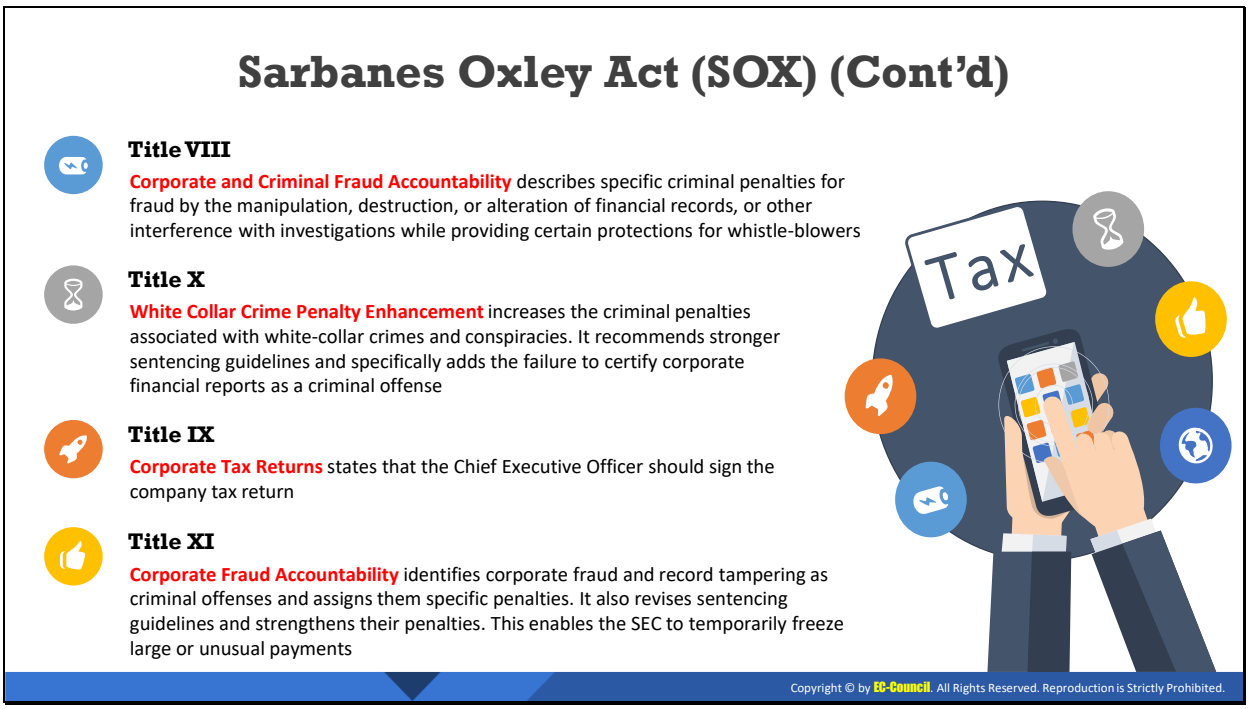
Title VII

Studies and Reports includes the effects of the consolidation of public accounting firms, the role of credit rating agencies in the operation of securities markets, securities violations and enforcement actions, and whether investment banks assisted Enron, Global Crossing, or others to manipulate earnings and obfuscate true financial conditions

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Sarbanes Oxley Act (SOX)

Source: *https://www.sec.gov*

Enacted in 2002, the Sarbanes-Oxley Act aims to protect the public and investors by increasing the accuracy and reliability of corporate disclosures. This act does not explain how an organization must store records but describes the records that organizations must store and the duration of their storage. The Act mandated several reforms to enhance corporate responsibility, enhance financial disclosures, and combat corporate and accounting fraud.

The key requirements and provisions of SOX are organized into 11 titles:

- **Title I: Public Company Accounting Oversight Board (PCAOB)**

  Title I consists of nine sections and establishes the Public Company Accounting Oversight Board to provide independent oversight of public accounting firms that provide audit services ("auditors"). It also creates a central oversight board tasked with registering audit services, defining the specific processes and procedures for compliance audits, inspecting and policing conduct and quality control, and enforcing compliance with the specific mandates of SOX.

- **Title II: Auditor Independence**

  Title II consists of nine sections and establishes standards for external auditor independence to limit conflicts of interest. It also addresses new auditor approval requirements, audit partner rotation, and auditor reporting requirements. It restricts auditing companies from providing non-audit services (such as consulting) for the same clients.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **Title III: Corporate Responsibility**

  Title III consists of eight sections and mandates that senior executives take individual responsibility for the accuracy and completeness of corporate financial reports. It defines the interaction between external auditors and corporate audit committees and specifies the corporate officers' responsibility for the accuracy and validity of corporate financial reports. It enumerates specific limits on the behaviors of corporate officers and describes specific forfeitures of benefits and civil penalties for non-compliance.

- **Title IV: Enhanced Financial Disclosures**

  Title IV consists of nine sections. It describes enhanced reporting requirements for financial transactions, including off-balance-sheet transactions, pro-forma figures, and the stock transactions of corporate officers. It requires internal controls to ensure the accuracy of financial reports and disclosures and mandates both audits and reports on those controls. It also requires timely reporting of material changes in financial conditions and specific enhanced reviews of corporate reports by the SEC or its agents.

- **Title V: Analyst Conflicts of Interest**

  Title V consists of only one section that discusses the measures designed to help restore investor confidence in the reporting of securities analysts. It defines the code of conduct for securities analysts and requires that they disclose any knowable conflicts of interest.

- **Title VI: Commission Resources and Authority**

  Title VI consists of four sections and defines practices to restore investor confidence in securities analysts. It also defines the SEC's authority to censure or bar securities professionals from practice and defines the conditions to bar a person from practicing as a broker, advisor, or dealer.

- **Title VII: Studies and Reports**

  Title VII consists of five sections and requires the Comptroller General and the Securities and Exchange Commission (SEC) to perform various studies and to report their findings. The required studies and reports include the effects of the consolidation of public accounting firms, the role of credit rating agencies in the operation of securities markets, securities violations, enforcement actions, and whether investment banks assisted Enron, Global Crossing, and others to manipulate earnings and obfuscate true financial conditions.

- **Title VIII: Corporate and Criminal Fraud Accountability**

  Title VIII, also known as the "Corporate and Criminal Fraud Accountability Act of 2002," consists of seven sections. It describes specific criminal penalties for the manipulation, destruction, or alteration of financial records or interference with investigations, while also providing certain protections for whistle-blowers.

- **Title IX: White-Collar-Crime Penalty Enhancement**

  Title IX, also known as the "White Collar Crime Penalty Enhancement Act of 2002," consists of six sections. This title increases the criminal penalties associated with white-

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

collar crimes and conspiracies. It recommends stronger sentencing guidelines and specifically adds failure to certify corporate financial reports as a criminal offense.

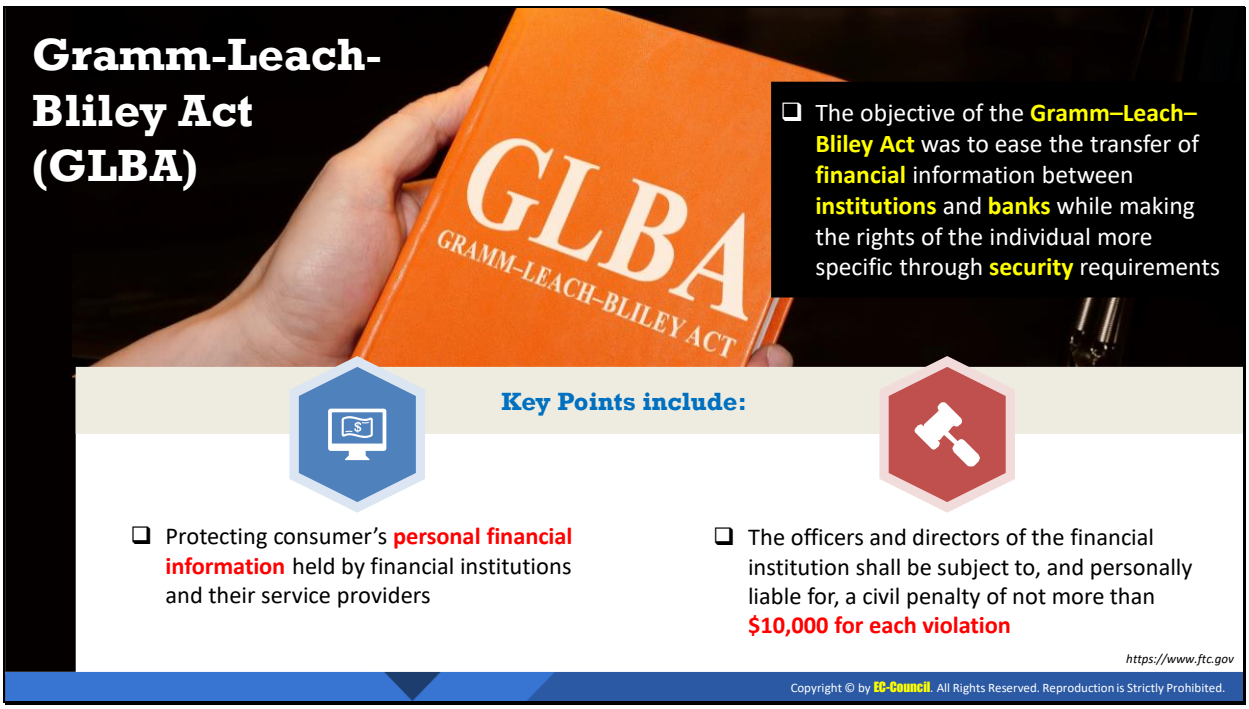
- **Title X: Corporate Tax Returns**

  Title X consists of one section that states that the Chief Executive Officer should sign the company tax return.

- **Title XI: Corporate Fraud Accountability**

  Title XI consists of seven sections. Section 1101 recommends the following name for the title: "Corporate Fraud Accountability Act of 2002." It identifies corporate fraud and records tampering as criminal offenses and joins those offenses to specific penalties. It also revises sentencing guidelines and strengthens penalties. Doing so enables the SEC to temporarily freeze "large" or "unusual" transactions or payments.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Gramm-Leach-Bliley Act (GLBA)

Source: *https://www.ftc.gov*

The Gramm-Leach-Bliley Act (GLB Act or GLBA) is a United States federal law that requires financial institutions to explain how they share and protect their customers' private information. The Act requires financial institutions—companies that offer consumers financial products or services such as loans, financial or investment advice, or insurance—to explain their information-sharing practices to their customers and to safeguard sensitive data. The objective of the GLBA is to ease the transfer of financial information between institutions and banks, while making the rights of the individual through security requirements more specific.

In this regard, the key points include:

- Protecting consumer's personal financial information held by financial institutions and their service providers are the key points of the financial privacy provisions of the GLBA. Companies should give consumers privacy notices that explain the GLBA's information-sharing practices, while customers can limit the sharing of their information.
- If an organization violates GLBA, then
  - It is subject to a civil penalty of not more than $100,000 for each violation;
  - Officers and directors of an organization shall be subject to, and personally liable for, a civil penalty of not more than $10,000 for each violation; and
  - The organization and its officers and directors shall also be subject to fines or imprisonment for not more than five years, or both.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- The top information protection requirements of GLBA include
  - Financial Privacy Rules to be provided for consumers with privacy notice after the relationship is established with the consumer; and
  - Safeguards Rules, which require organizations to develop a written information security plan describing its processes and procedures for protecting clients' NPI.
- The Security and Encryption Requirements for GLBA include
  - Organizations to establish required standards that related to the administrative, technical, and physical security of customer records and information; and
  - Organizations to implement encryption to reduce the risk of disclosure or alteration of information—for example, strong key management practices, robust reliability, and securing the encrypted communication's endpoints.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

General Data Protection Regulation (GDPR)

Source: *https://gdpr.eu*

The General Data Protection Regulation (GDPR) is the toughest privacy and security law in the world. Though it was drafted and passed by the European Union (EU), it imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU. The regulation was put into effect on May 25, 2018. The GDPR will levy harsh fines against those who violate its privacy and security standards, with penalties reaching into the tens of millions of euros.

With the GDPR, Europe is signaling its firm stance on data privacy and security at a time when more people are entrusting their personal data with cloud services and breaches are a daily occurrence. The regulation itself is large, far-reaching, and fairly light on specifics, making GDPR compliance a daunting prospect, particularly for small and medium-sized enterprises (SMEs).

GDPR Data Protection Principles

The GDPR includes seven protection and accountability principles outlined in Article 5.1-2:

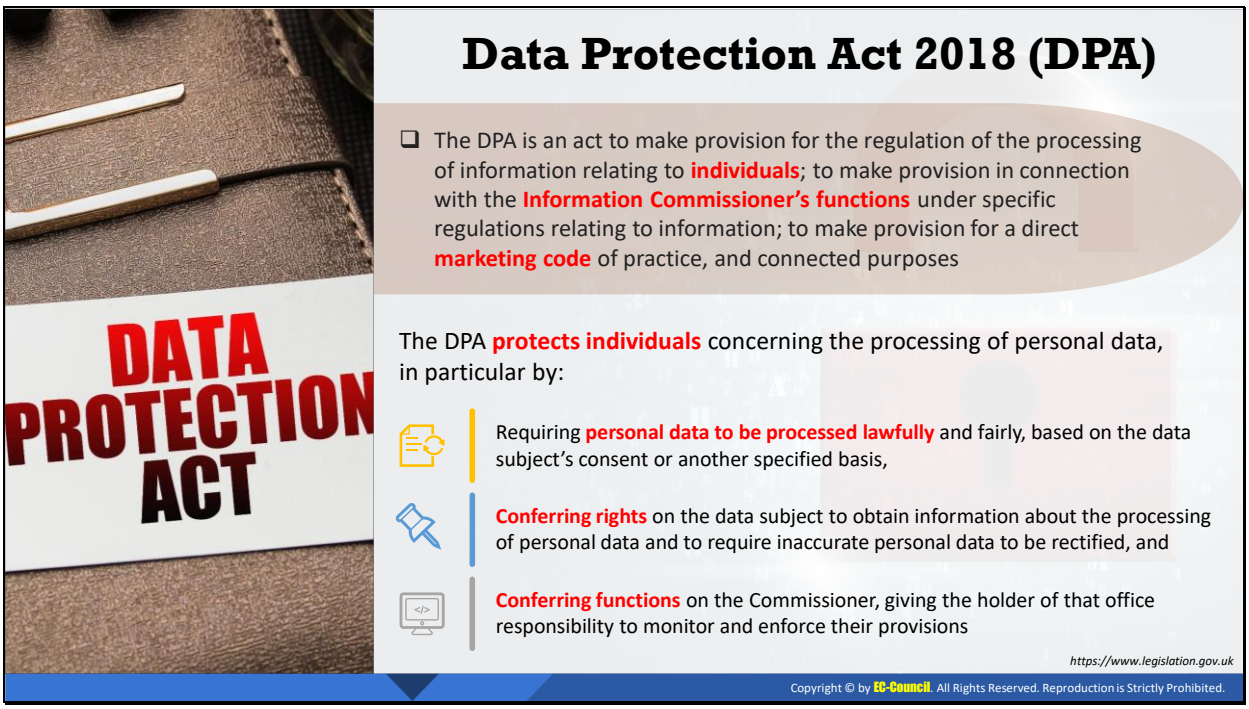
- **Lawfulness, fairness, and transparency**: Processing must be lawful, fair, and transparent to the data subject.
- **Purpose limitation:** You must process data for the legitimate purposes specified explicitly to the data subject when you collected it.
- **Data minimization:** You should collect and process only as much data as absolutely necessary for the purposes specified.
- **Accuracy:** You must keep personal data accurate and up to date.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **Storage limitation:** You may only store personally identifying data for as long as necessary for the specified purpose.
- **Integrity and confidentiality:** Processing must be done in such a way as to ensure appropriate security, integrity, and confidentiality (e.g. by using encryption).
- **Accountability:** The data controller is responsible for being able to demonstrate GDPR compliance with all of these principles.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Data Protection Act 2018 (DPA)

Source: *https://www.legislation.gov.uk*

The DPA 2018 sets out the framework for data protection law in the UK. It updates and replaces the Data Protection Act 1998 and came into effect on 25 May 2018. It was amended on 01 January 2021 by regulations under the European Union (Withdrawal) Act 2018, to reflect the UK's status outside the EU.

The DPA is an act to make provision for the regulation of the processing of information relating to individuals; to make provision in connection with the Information Commissioner's functions under certain regulations relating to information; to make provision for a direct marketing code of practice; and for connected purposes.

The DPA also sets out separate data protection rules for law enforcement authorities, extends data protection to some other areas such as national security and defense, and sets out the Information Commissioner's functions and powers.

Protection of personal data

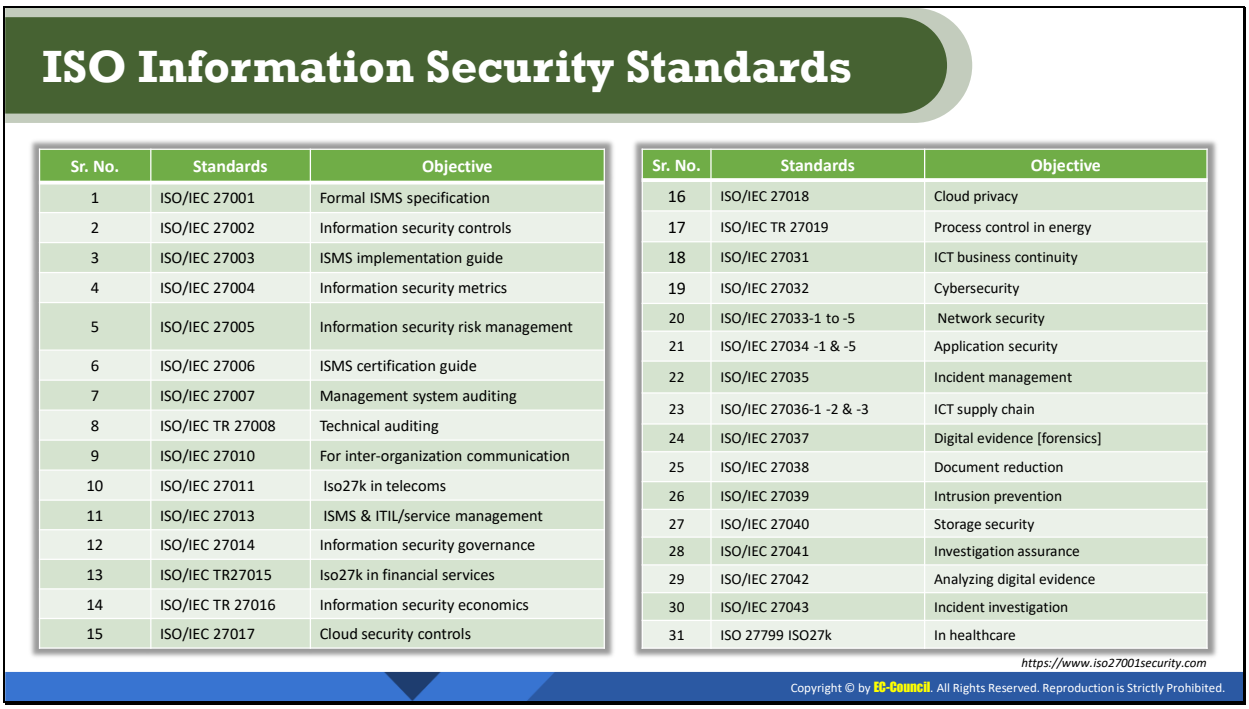
1. The DPA protects individuals with regard to the processing of personal data, in particular by:
    a. Requiring personal data to be processed lawfully and fairly, on the basis of the data subject's consent or another specified basis,
    b. Conferring rights on the data subject to obtain information about the processing of personal data and to require inaccurate personal data to be rectified, and
    c. Conferring functions on the Commissioner, giving the holder of that office responsibility for monitoring, and enforcing their provisions.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

2. When carrying out functions under the GDPR, the applied GDPR and this Act, the Commissioner must have regard to the importance of securing an appropriate level of protection for personal data, taking account of the interests of data subjects, controllers and others and matters of general public interest.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



ISO Information Security Standards

Sr. No.	Standards	Objective
1	ISO/IEC 27001	Formal ISMS specification
2	ISO/IEC 27002	Information security controls
3	ISO/IEC 27003	ISMS implementation guide
4	ISO/IEC 27004	Information security metrics
5	ISO/IEC 27005	Information security risk management
6	ISO/IEC 27006	ISMS certification guide
7	ISO/IEC 27007	Management system auditing
8	ISO/IEC TR 27008	Technical auditing
9	ISO/IEC 27010	For inter-organization communication
10	ISO/IEC 27011	Iso27k in telecoms
11	ISO/IEC 27013	ISMS & ITIL/service management
12	ISO/IEC 27014	Information security governance
13	ISO/IEC TR27015	Iso27k in financial services
14	ISO/IEC TR 27016	Information security economics
15	ISO/IEC 27017	Cloud security controls

Sr. No.	Standards	Objective
16	ISO/IEC 27018	Cloud privacy
17	ISO/IEC TR 27019	Process control in energy
18	ISO/IEC 27031	ICT business continuity
19	ISO/IEC 27032	Cybersecurity
20	ISO/IEC 27033-1 to -5	Network security
21	ISO/IEC 27034 -1 & -5	Application security
22	ISO/IEC 27035	Incident management
23	ISO/IEC 27036-1 -2 & -3	ICT supply chain
24	ISO/IEC 27037	Digital evidence [forensics]
25	ISO/IEC 27038	Document reduction
26	ISO/IEC 27039	Intrusion prevention
27	ISO/IEC 27040	Storage security
28	ISO/IEC 27041	Investigation assurance
29	ISO/IEC 27042	Analyzing digital evidence
30	ISO/IEC 27043	Incident investigation
31	ISO 27799 ISO27k	In healthcare

https://www.iso27001security.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

ISO Information Security Standards

Source: *https://www.iso27001security.com*

- **ISO/IEC 27001**

  ISO/IEC 27001 formally specifies an Information Security Management System (ISMS), a suite of activities concerning the management of information security risks. The ISMS is an overarching management framework through which an organization identifies, analyzes, and addresses its information security risks. The ISMS ensures that the security arrangements are fine-tuned to keep pace with changes to the security threats, vulnerabilities, and business impacts—an important aspect in such a dynamic field and a key advantage of ISO27k's flexible risk-driven approach compared with, for example, PCI–DSS.

- **ISO/IEC 27002**

  ISO/IEC 27002 is relevant to all types of organizations, including commercial enterprises of all sizes (from one-man-bands up to multinational giants), not-for-profits, charities, government departments, and quasi-autonomous bodies, or any organization that handles and depends on information. The specific information security risk and control requirements may differ in detail, although there is common ground—for instance, most organizations need to address the information security risks relating to their employees plus contractors, consultants, and the external suppliers of information services.

- **ISO/IEC 27003**

  ISO/IEC 27003 guides the design of an ISO/IEC 27001-compliant ISMS, leading up to the initiation of an ISMS implementation project. It describes the process of ISMS

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

specification and design from inception to the production of implementation project plans, covering the preparation and planning activities *prior* to the actual implementation.

- **ISO/IEC 27004**

  ISO/IEC 27004 concerns the measurements relating to information security management; these are commonly known as "security metrics".

- **ISO/IEC 27005**

  The standard provides guidelines for information security risk management and supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach.

- **ISO/IEC 27006**

  ISO/IEC 27006 is the **accreditation standard** that guides certification bodies on the formal processes they must follow when auditing their client's Information Security Management Systems (ISMSs) against ISO/IEC 27001 in order to certify or register them compliant. The accreditation processes laid out in the standard give assurance that ISO/IEC 27001 certificates issued by accredited organizations are valid.

- **ISO/IEC 27007**

  ISO/IEC 27007 provides guidance for accredited certification bodies, internal auditors, external/third-party auditors, and others auditing ISMSs against ISO/IEC 27001 (i.e., auditing the management system for compliance with the standard).

  ISO/IEC 27007 reflects and largely refers to ISO 19011, the ISO standard for auditing quality and environmental management systems—with "management systems" being the common factor linking it to the ISO27k standards. It provides additional ISMS-specific guidance.

- **ISO/IEC TR 27008**

  This standard provides guidance for all auditors regarding ISMS controls selected through a risk-based approach (e.g., as presented in a statement of applicability) for information security management. It supports the information security risk management process as well as internal, external, and third-party audits of ISMS by explaining the relationship between the ISMS and its supporting controls. It provides guidance on how to verify the extent to which the required ISMS controls are implemented. Further, it supports any organization using ISO/IEC 27001 and ISO/IEC 27002 to satisfy assurance requirements, and is a strategic platform for information security governance.

- **ISO/IEC 27010**

  This standard provides guidance in relation to sharing information about information security risks, controls, issues, and/or incidents that span the boundaries between industry sectors and/or nations, particularly those affecting "critical infrastructure."

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- **ISO/IEC 27011**

  This ISMS implementation guide for the telecom industry was developed jointly by ITU Telecommunication Standardization Sector (ITU-T) and ISO/IEC JTC1/SC 27, with the identical text being published as *both* ITU-T X.1051 *and* ISO/IEC 27011.

- **ISO/IEC 27013**

  This standard provides guidance on implementing an integrated information security and IT service management system based on both ISO/IEC 27001:2005 (ISMS) and ISO/IEC 20000-1:2011.

- **ISO/IEC 27014**

  ISO/IEC JTC1/SC 27, in collaboration with the ITU-T, has developed a standard specifically aimed at helping organizations govern their information security arrangements.

- **ISO/IEC TR 27015**

  This is a guideline intended to help financial services organizations (e.g., banks, insurance companies, and credit card companies) implement ISMSs using the ISO27k standards.

  Although the financial services sector already labors under a vast swathe of risk and security standards (such as ISO TR 13569 "Banking Information Security Guidelines," SOX and Basel II/III), the ISMS implementation guidance developed by SC 27 reflects ISO/IEC 27001 and 27002, along with various general-purpose security standards such as Control Objectives for Information and Related Technologies(COBIT) and the PCI–DSS requirements.

- **ISO/IEC TR 27016**

  This standard helps management appreciate and understand the financial impacts of information security in the context of an ISO27k ISMS, along with political, social, compliance, and other potential impacts on an organization that collectively influence how much it needs to invest in protecting its information assets.

- **ISO/IEC 27017**

  This standard provides guidance on the information security aspects of cloud computing, recommending and assisting with the implementation of a cloud-specific information security controls supplementing the guidance in ISO/IEC 27002 and other ISO27k standards.

- **ISO/IEC 27018**

  This standard provides guidance aimed at ensuring that cloud service providers (such as Amazon and Google) offer suitable information security controls to protect the privacy of their customer's clients by securing personally identifiable information entrusted to them. The standard will be followed by ISO/IEC 27017, covering the wider information security angles of cloud computing, other than privacy.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- **ISO/IEC TR 27019**

  This standard (a Technical Report) is intended to help organizations in the energy industry interpret and apply ISO/IEC 27002:2005 in order to secure their electronic process control systems.

- **ISO/IEC 27031**

  ISO/IEC 27031 provides guidance on the concepts and principles behind the role of information and communications technology in ensuring business continuity.

  The standard

  - Suggests a structure or framework (actually a set of methods and processes) for any organization, whether private, governmental, or non-governmental;
  - Identifies and specifies all relevant aspects including performance criteria, design, and implementation details for improving information and communications technology (ICT) readiness as part of an organization's ISMS; thus, it helps ensure business continuity; and
  - Enables an organization to measure its ICT continuity, security, and, hence, readiness to survive a disaster in a consistent and recognized manner.

- **ISO/IEC 27032**

  ISO/IEC 27032 addresses "cybersecurity" or "cyberspace security," defined as the "preservation of confidentiality, integrity and availability of information in the Cyberspace." In turn "the cyberspace" is defined as "the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form."

- **ISO/IEC 27033-1 to -5**

  ISO/IEC 27033 is a multi-part standard derived from the existing five-part network security standard ISO/IEC 18028. It is being substantially revised, and not only renamed, to fit into the ISO27k suite.

- **ISO/IEC 27034 -1 & -5**

  ISO/IEC 27034 offers guidance on information security to those specifying, designing and programming or procuring, and implementing and using application systems, that is, business and IT managers, developers and auditors, and ultimately the end-users of ICT. The aim is to ensure that computer applications deliver the desired or necessary level of security in support of an organization's ISMS, adequately addressing many ICT security risks.

- **ISO/IEC 27035**

  Information security controls are imperfect in various ways: controls can be overwhelmed or undermined (e.g., by competent hackers, fraudsters, or malware), fail in service (e.g., authentication failures), work partially or poorly (e.g., slow anomaly

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

detection), or be more or less completely missing (e.g., not [yet] fully implemented, not [yet] fully operational, or never even conceived because of failures upstream in risk identification and analysis). Consequently, information security incidents are bound to occur to some extent, even in organizations that take their information security extremely seriously.

- **ISO/IEC 27036 -1 -2 & -3**

  ISO/IEC 27036 is a multi-part standard offering guidance on the evaluation and treatment of information security risks involved in the acquisition of goods and services from suppliers. The implied context is business-to-business relationships—than retailing—and information-related products. The terms acquisition and acquirer are used rather than purchase and purchasing, since the process and the risks are much the same whether or not the transactions are commercial**.**

- **ISO/IEC 27037**

  This standard provides guidance on identifying, gathering/collecting/acquiring, handling, and protecting/preserving digital forensic evidence, that is, "digital data that may be of evidential value" for use in court. The fundamental purpose of the ISO27k digital forensics standards is to promote best practice methods and processes for forensic capture and investigation of digital evidence. While individual investigators, organizations, and jurisdictions may well retain certain methods, processes, and controls, it is hoped that standardization will (eventually) lead to the adoption of similar, if not identical approaches internationally. This makes it easier to compare, combine, and contrast the results of such investigations even when performed by different people or organizations and potentially across different jurisdictions.

- **ISO/IEC 27038**

  Digital data sometimes have to be revealed to third parties, occasionally even published to the public, for reasons such as disclosure of official documents under Freedom of Information laws or as evidence in commercial disputes or legal cases. "Redaction" is the conventional term for the process of denying file recipients' knowledge of certain sensitive data within the original files.

- **ISO/IEC 27039**

  Intrusion detection systems (IDSs) are largely automated systems for identifying attacks on and intrusions into a network or system by hackers and raising the alarm. Intrusion prevention systems (IPSs) take the automation a step further by automatically responding to certain types of identified attack—for example, by closing off specific network ports through a firewall to block identified hacker traffic. Intrusion detection and prevention systems combine features of both IDSs and IPSs.

- **ISO/IEC 27040**

  The proposers of this standard claim that the information security aspects of data storage systems and infrastructures have been neglected because of misconceptions and limited familiarity with the storage technology, or in the case of (some) storage

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

managers and administrators, a limited understanding of the inherent risks or basic security concepts.

- **ISO/IEC 27041**

  The fundamental purpose of the ISO27k digital forensics standards is to promote best practice methods and processes for forensic capture and investigation of digital evidence. While individual investigators, organizations, and jurisdictions may well retain certain methods, processes, and controls, it is hoped that standardization will (eventually) lead to the adoption of similar, if not identical, approaches internationally. This makes it easier to compare, combine, and contrast the results of such investigations even when performed by different people or organizations and potentially across different jurisdictions.

- **ISO/IEC 27042**

  The fundamental purpose of the ISO27k digital forensics standards is to promote best practice methods and processes for the forensic capture and investigation of digital evidence. While individual investigators, organizations, and jurisdictions may well retain certain methods, processes, and controls, it is hoped that standardization will (eventually) lead to the adoption of similar, if not identical, approaches internationally. This makes it easier to compare, combine, and contrast the results of such investigations even when performed by different people or organizations and potentially across different jurisdictions.

- **ISO/IEC 27043**

  The fundamental purpose of the digital forensics standards ISO/IEC 27037, 27041, 27042, 27043, and 27050 is to promote best practice methods and processes for forensic capture and investigation of digital evidence. While individual investigators, organizations, and jurisdictions may well retain certain methods, processes, and controls, it is hoped that standardization will (eventually) lead to the adoption of similar, if not identical, approaches internationally. This makes it easier to compare, combine, and contrast the results of such investigations even when performed by different people or organizations and potentially across different jurisdictions.

- **ISO/IEC 27799 ISO27k**

  This standard provides guidance to health care organizations and other custodians of personal health information on how best to protect the confidentiality, integrity, and availability of such information by implementing ISO/IEC 27002. Specifically, it addresses the special information security management needs of the health sector and its unique operating environments. While the protection and security of personal information is important to all individuals, corporations, institutions, and governments, there are special requirements in the health sector that need to be met to ensure the confidentiality, integrity, adaptability, and availability of personal health information.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

The Digital Millennium Copyright Act (DMCA)

Source: *https://www.copyright.gov*

The DMCA is an American copyright law that implements two 1996 treaties from the World Intellectual Property Organization (WIPO): the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty. In order to implement US treaty obligations, the DMCA defines legal prohibitions against circumvention of the technological protection measures employed by copyright owners to protect their works, and against the removal or alteration of copyright management information. The DMCA contains five titles:

- **Title I**: **WIPO TREATY IMPLEMENTATION**

  Title I implements the WIPO treaties. First, it makes certain technical amendments to US law in order to provide the appropriate references and links to the treaties. Second, it creates two new prohibitions in Title 17 of the U.S. Code—one on circumvention of the technological measures used by copyright owners to protect their works and one on tampering with copyright management information—and adds civil remedies and criminal penalties for violating the prohibitions.

- **Title II: ONLINE COPYRIGHT INFRINGEMENT LIABILITY LIMITATION**

  Title II of the DMCA adds a new section 512 to the Copyright Act to create four new limitations on liability for copyright infringement by online service providers. A service provider bases these limitations on the following four categories of conduct:

  - Transitory communications
  - System caching
  - The user-directed storage of information on systems or networks

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- Information location tools

New section 512 also includes special rules concerning the application of these limitations to nonprofit educational institutions.

- **Title III: COMPUTER MAINTENANCE OR REPAIR**

Title III of the DMCA allows the owner of a copy of a program to make reproductions or adaptations when necessary to use the program in conjunction with a computer. The amendment permits the owner or lessee of a computer to make or to authorize the making of a copy of a computer program in the course of maintaining or repairing that computer.

- **Title IV: MISCELLANEOUS PROVISIONS**

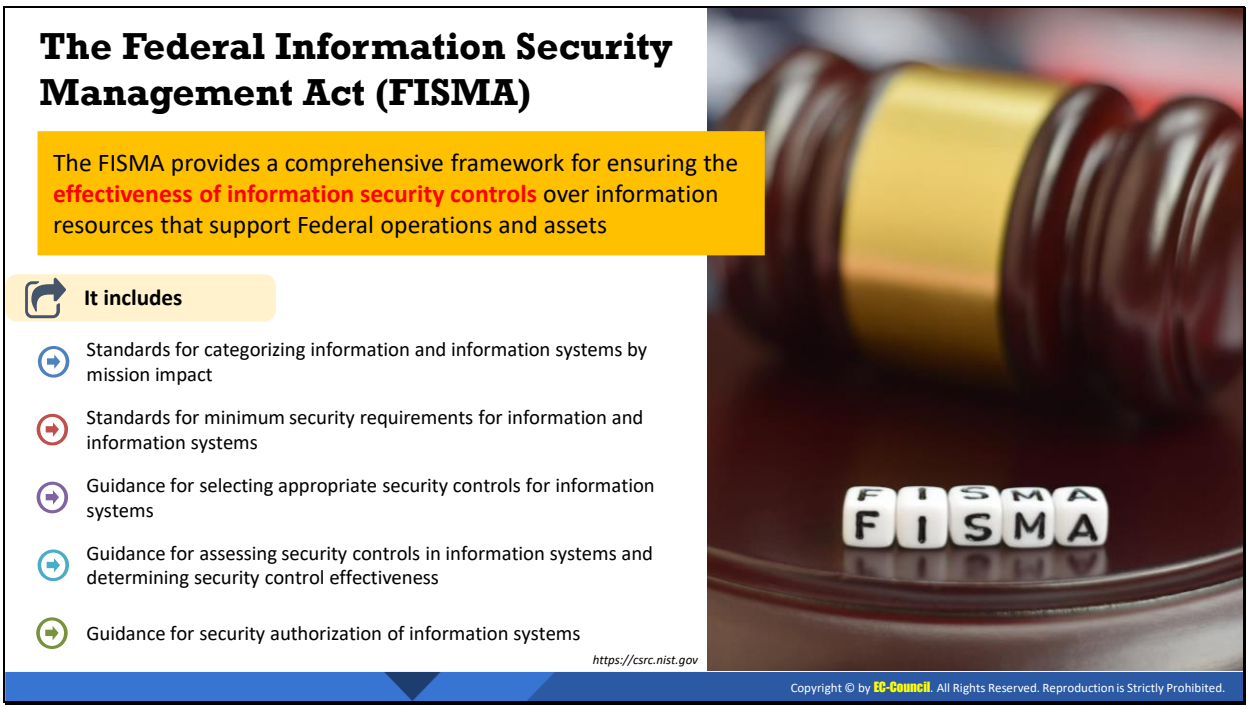
Title IV contains six miscellaneous provisions. The first provision announces the Clarification of the Authority of the Copyright Office; the second grants exemption for the making of "ephemeral recordings"; the third promotes study by distance education; the fourth provides an exemption for Nonprofit Libraries and Archives; the fifth allows Webcasting Amendments to the Digital Performance Right in Sound Recordings, and, finally, the sixth provision addresses concerns about the ability of writers, directors and screen actors to obtain residual payments for the exploitation of motion pictures in situations where the producer is no longer able to make these payments.

- **Title V: PROTECTION OF CERTAIN ORIGINAL DESIGNS**

Title V of the DMCA, entitles the Vessel Hull Design Protection Act (VHDPA). This act creates a new system for protecting the original designs of certain useful articles that make the article attractive or distinctive in appearance. For purposes of the VHDPA, "useful articles" are limited to the hulls (including the decks) of vessels no longer than 200 feet.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



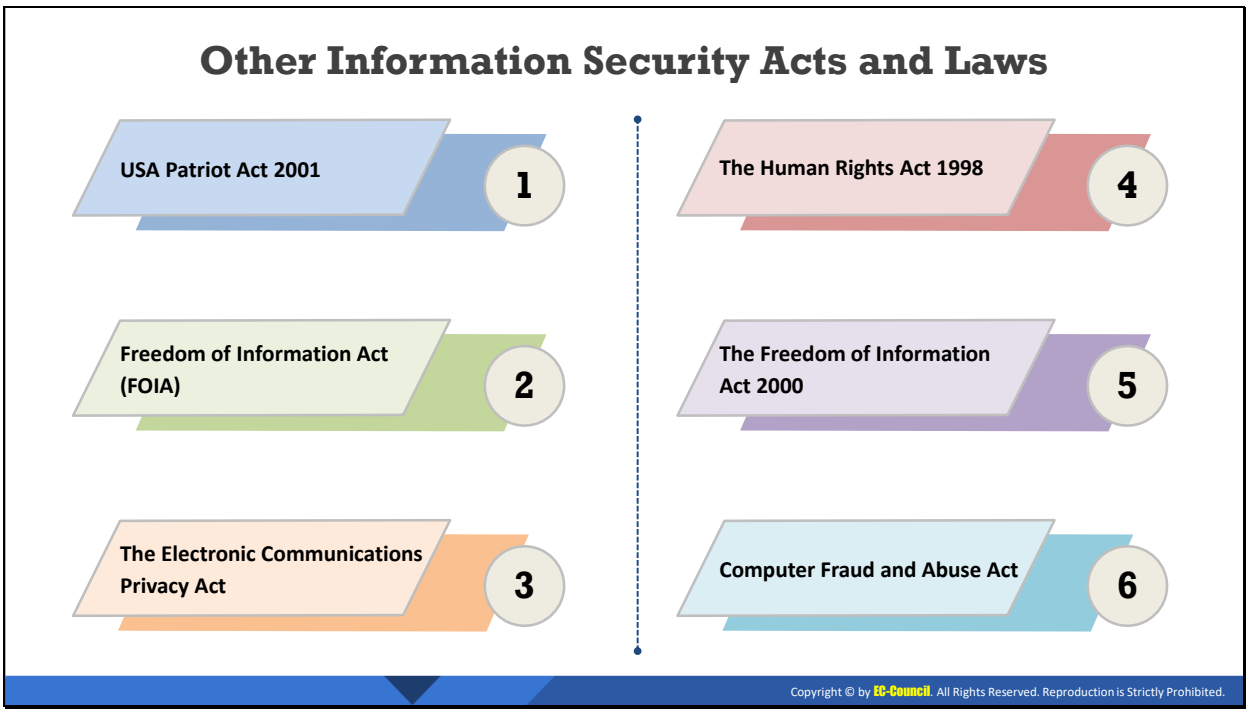
The Federal Information Security Management Act (FISMA)

Source: *https://csrc.nist.gov*

The Federal Information Security Management Act of 2002 was enacted to produce several key security standards and guidelines required by Congressional legislation. The FISMA provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets. It requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or another source. The FISMA framework includes:

- Standards for categorizing information and information systems by mission impact
- Standards for the minimum security requirements for information and information systems
- Guidance for selecting appropriate security controls for information systems
- Guidance for assessing security controls in information systems and determining their effectiveness
- Guidance for the security authorization of information systems

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Other Information Security Acts and Laws

USA Patriot Act 2001

Source**:** *https://www.fincen.gov*

The purpose of the USA PATRIOT Act is to deter and punish terrorist acts in the U.S. and around the world and enhance law enforcement investigatory tools, including

- To strengthen U.S. measures to prevent, detect, and prosecute international money laundering and financing of terrorism;
- To subject to special scrutiny foreign jurisdictions, foreign financial institutions, and classes of international transactions or types of accounts that are susceptible to criminal abuse;
- To require all appropriate elements of the financial services industry to report potential money laundering; and
- To strengthen measures to prevent use of the U.S. financial system for personal gain by corrupt foreign officials and facilitate repatriation of stolen assets to the citizens of countries to whom such assets belong.

Freedom of Information Act (FOIA)

Source*: http://www.foia.gov*

The Freedom of Information Act (FOIA) has provided the public the right to request access to records from any federal agency. It is often described as the law that keeps citizens informed about their government. Federal agencies are required to disclose any information requested

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

under the FOIA unless it falls under one of nine exemptions that protect interests such as personal privacy, national security, and law enforcement.

The Electronic Communications Privacy Act

Source**:** *https://it.ojp.gov*

The Electronic Communications Privacy Act and the Stored Wire Electronic Communications Act are commonly referred together as the Electronic Communications Privacy Act (ECPA) of 1986. The ECPA updated the Federal Wiretap Act of 1968, which addressed interception of conversations using "hard" telephone lines, but did not apply to interception of computer and other digital and electronic communications. Several subsequent pieces of legislation, including The USA PATRIOT Act, clarify and update the ECPA in order to keep pace with the evolution of new communications technologies and methods, including easing restrictions on law enforcement access to stored communications in some cases.

The Human Rights Act 1998

Source**:** *https://www.legislation.gov.uk*

This Act buttresses the rights and freedoms guaranteed under the European Convention on Human Rights; it makes provision with respect to holders of certain judicial offices who become judges of the European Court of Human Rights, and for other related purposes.

The Freedom of Information Act 2000

Source**:** *https://www.legislation.gov.uk*

This Act makes provision for the disclosure of information held by public authorities or by persons providing services for them and to amend the Data Protection Act 1998 and the Public Records Act 1958, and for related purposes.

Computer Fraud and Abuse Act

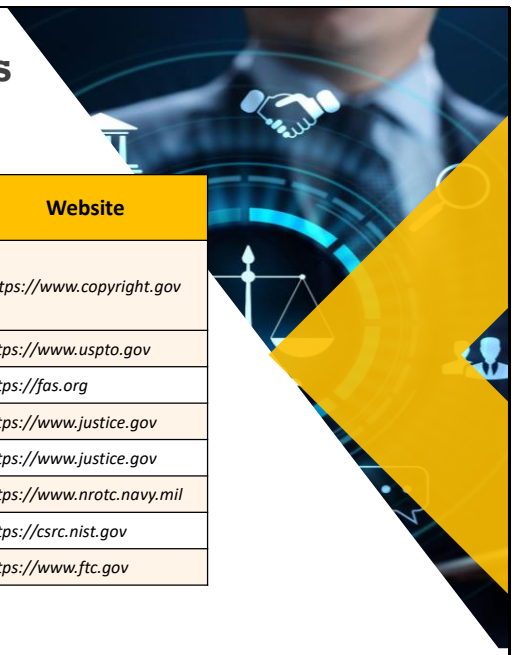
Source**:** *https://ilt.eff.org*

The Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, is an amendment made in 1986 to the Counterfeit Access Device and Abuse Act 1984, and essentially states that, whoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer, and if the conduct involves an interstate or foreign communication, shall be punished under the Act. In 1996 the CFAA was, again, broadened by an amendment that replaced the term “federal interest computer” with the term “protected computer” 18 U.S.C. § 1030. While the CFAA is primarily a criminal law intended to reduce the instances of malicious interferences with computer systems and address federal computer offenses, an amendment in 1994 allows civil actions to be brought under the statute as well.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

Cyber Law in Different Countries



Country Name	Laws/Acts	Website
United States	Section 107 of the Copyright Law mentions the doctrine of "fair use"	*https://www.copyright.gov*
	Online Copyright Infringement Liability Limitation Act	
	The Lanham (Trademark) Act (15 USC §§ 1051 - 1127)	*https://www.uspto.gov*
	Foreign Intelligence Surveillance Act	*https://fas.org*
	Protect America Act of 2007	*https://www.justice.gov*
	Privacy Act of 1974	*https://www.justice.gov*
	National Information Infrastructure Protection Act of 1996	*https://www.nrotc.navy.mil*
	Computer Security Act of 1987	*https://csrc.nist.gov*
	Federal Identity Theft and Assumption Deterrence Act	*https://www.ftc.gov*

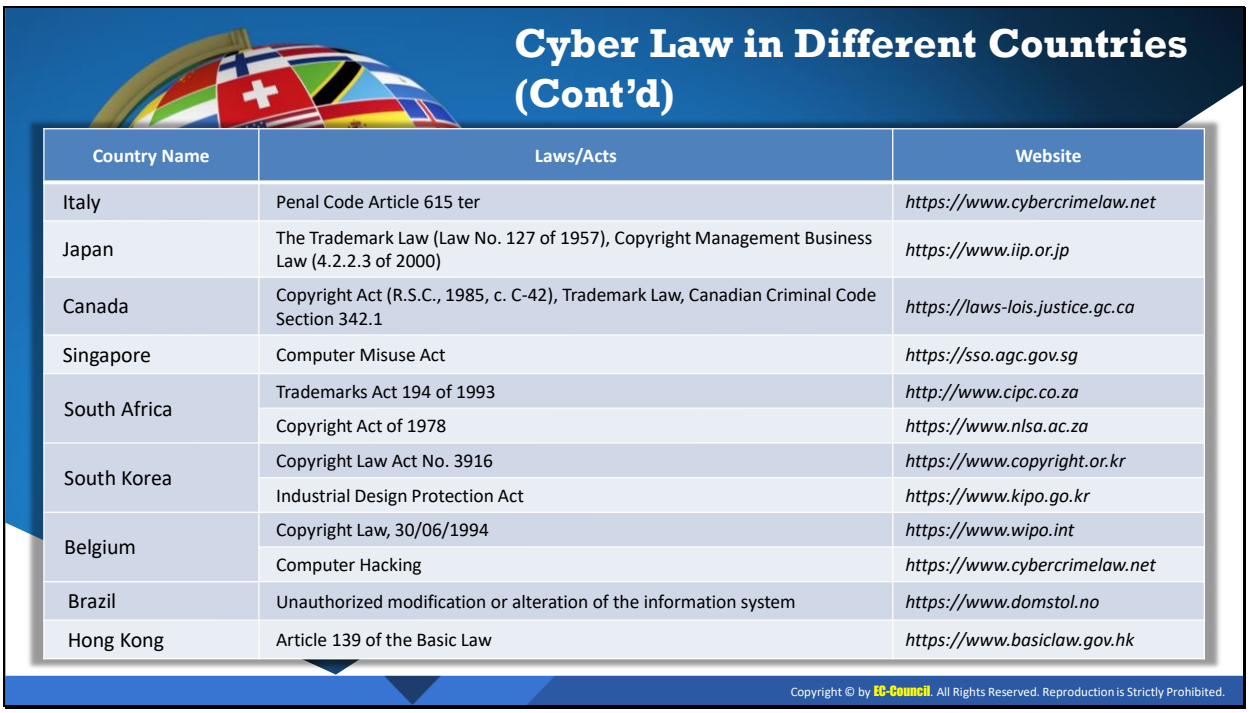
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cyber Law in Different Countries (Cont'd)

Country Name	Laws/Acts	Website
Australia	The Trade Marks Act 1995	*https://www.legislation.gov.au*
	The Patents Act 1990	
	The Copyright Act 1968	
	Cybercrime Act 2001	
United Kingdom	The Copyright, Etc. and Trademarks (Offenses And Enforcement) Act 2002	*https://www.legislation.gov.uk*
	Trademarks Act 1994 (TMA)	
	Computer Misuse Act 1990	
	The Network and Information Systems Regulations 2018	
	Communications Act 2003	
	The Privacy and Electronic Communications (EC Directive) Regulations 2003	
	Investigatory Powers Act 2016	
	Regulation of Investigatory Powers Act 2000	
China	Copyright Law of the People's Republic of China (Amendments on October 27, 2001)	*http://www.npc.gov.cn*
	Trademark Law of the People's Republic of China (Amendments on October 27, 2001)	
India	The Patents (Amendment) Act, 1999, Trade Marks Act, 1999, The Copyright Act, 1957	*http://www.ipindia.nic.in*
	Information Technology Act	*https://www.meity.gov.in*
Germany	Section 202a. Data Espionage, Section 303a. Alteration of Data, Section 303b. Computer Sabotage	*https://www.cybercrimelaw.net*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Cyber Law in Different Countries

Cyberlaw or Internet law refers to any laws that deal with protecting the Internet and other online communication technologies. Cyberlaw covers topics such as Internet access and usage, privacy, freedom of expression, and jurisdiction. Cyber laws provide an assurance of the integrity, security, privacy, and confidentiality of information in both governmental and private organizations. These laws have become prominent due to the increase in Internet usage around the world. Cyber laws vary by jurisdiction and country, so implementing them is quite challenging. Violating these laws results in punishments ranging from fines to imprisonment.

Country Name	Laws/Acts	Website
United States	Section 107 of the Copyright Law mentions the doctrine of "fair use"	https://www.copyright.gov
	Online Copyright Infringement Liability Limitation Act	
	The Lanham (Trademark) Act (15 USC §§ 1051 - 1127)	https://www.uspto.gov
	Foreign Intelligence Surveillance Act	https://fas.org
	Protect America Act of 2007	https://www.justice.gov
	Privacy Act of 1974	https://www.justice.gov
	National Information Infrastructure Protection Act of 1996	https://www.nrotc.navy.mil
	Computer Security Act of 1987	https://csrc.nist.gov
	Federal Identity Theft and Assumption Deterrence Act	https://www.ftc.gov
Australia	The Trade Marks Act 1995	https://www.legislation.gov.au

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

	The Patents Act 1990	
	The Copyright Act 1968	
	Cybercrime Act 2001	
United Kingdom	The Copyright, Etc. and Trademarks (Offenses And Enforcement) Act 2002	https://www.legislation.gov.uk
	Trademarks Act 1994 (TMA)	
	Computer Misuse Act 1990	
	The Network and Information Systems Regulations 2018	
	Communications Act 2003	
	The Privacy and Electronic Communications (EC Directive) Regulations 2003	
	Investigatory Powers Act 2016	
	Regulation of Investigatory Powers Act 2000	
China	Copyright Law of the People's Republic of China (Amendments on October 27, 2001)	http://www.npc.gov.cn
	Trademark Law of the People's Republic of China (Amendments on October 27, 2001)	
India	The Patents (Amendment) Act, 1999, Trade Marks Act, 1999, The Copyright Act, 1957	http://www.ipindia.nic.in
	Information Technology Act	https://www.meity.gov.in
Germany	Section 202a. Data Espionage, Section 303a. Alteration of Data, Section 303b. Computer Sabotage	https://www.cybercrimelaw.net
Italy	Penal Code Article 615 ter	https://www.cybercrimelaw.net
Japan	The Trademark Law (Law No. 127 of 1957), Copyright Management Business Law (4.2.2.3 of 2000)	https://www.iip.or.jp
Canada	Copyright Act (R.S.C., 1985, c. C-42), Trademark Law, Canadian Criminal Code Section 342.1	https://laws-lois.justice.gc.ca
Singapore	Computer Misuse Act	https://sso.agc.gov.sg
South Africa	Trademarks Act 194 of 1993	http://www.cipc.co.za
	Copyright Act of 1978	https://www.nlsa.ac.za
South Korea	Copyright Law Act No. 3916	https://www.copyright.or.kr
	Industrial Design Protection Act	https://www.kipo.go.kr
Belgium	Copyright Law, 30/06/1994	https://www.wipo.int
	Computer Hacking	https://www.cybercrimelaw.net
Brazil	Unauthorized modification or alteration of the information system	https://www.domstol.no
Hong Kong	Article 139 of the Basic Law	https://www.basiclaw.gov.hk

Table 3.7: Cyber Law in Different Countries

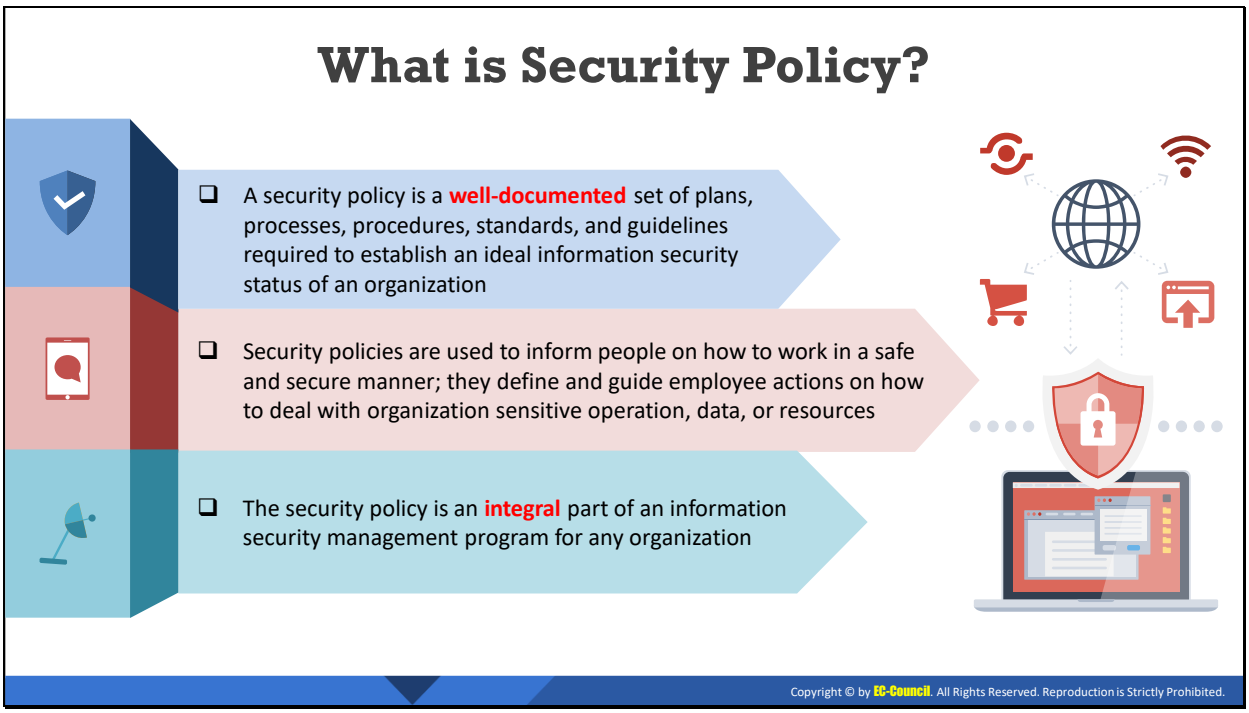
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

Learn to Design and Develop Security Policies

Organizations need to design and develop security policies and procedures to ensure availability, confidentiality, and integrity across the network. This section explains the need for a security policy, its characteristics, contents, and types of security policies.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



What is Security Policy?

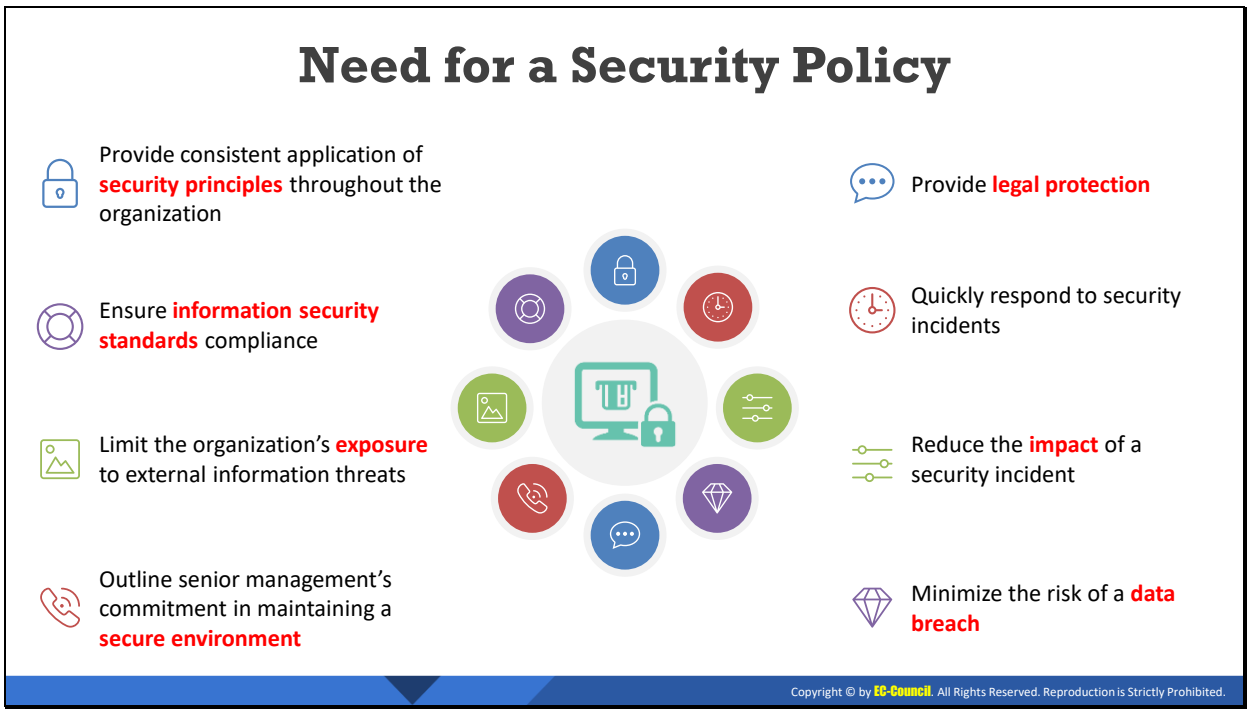
A security policy is a well-documented set of plans, processes, procedures, standards, and guidelines required to establish an ideal information security status of an organization. Security policies are used to inform people on how to work in a safe and secure manner; they define and guide employee actions on how to deal with organization sensitive operation, data, or resources. The security policy is an integral part of an information security management program for any organization

Security policy is a high-level document, or set of documents, describing the security controls to implement in order to protect a company. It maintains confidentiality, availability, integrity, and asset values. Security policies form the foundation of a security infrastructure. Without them, it is impossible to protect the company from possible lawsuits, lost revenue, and bad publicity, or even basic security attacks. Such policies accomplish three goals:

- Reduce or eliminate the legal liability to employees and third parties;
- Protect confidential and proprietary information from theft, misuse, unauthorized disclosure, or modification; and
- Prevent computing resource waste.

A security policy comprises objectives, rules for behavior, and requirements to secure an organization's network and computer systems. Security policies function as a connecting medium between the objectives and security requirements, as well as to help users, staff, and managers protect technology and information assets. The policy provides a baseline to acquire, configure, and audit computer systems and networks. A security policy defines a set of security tools for preventing attacks on the entire network in order to keep malicious users away from an organization and provide control over perilous users within an organization.

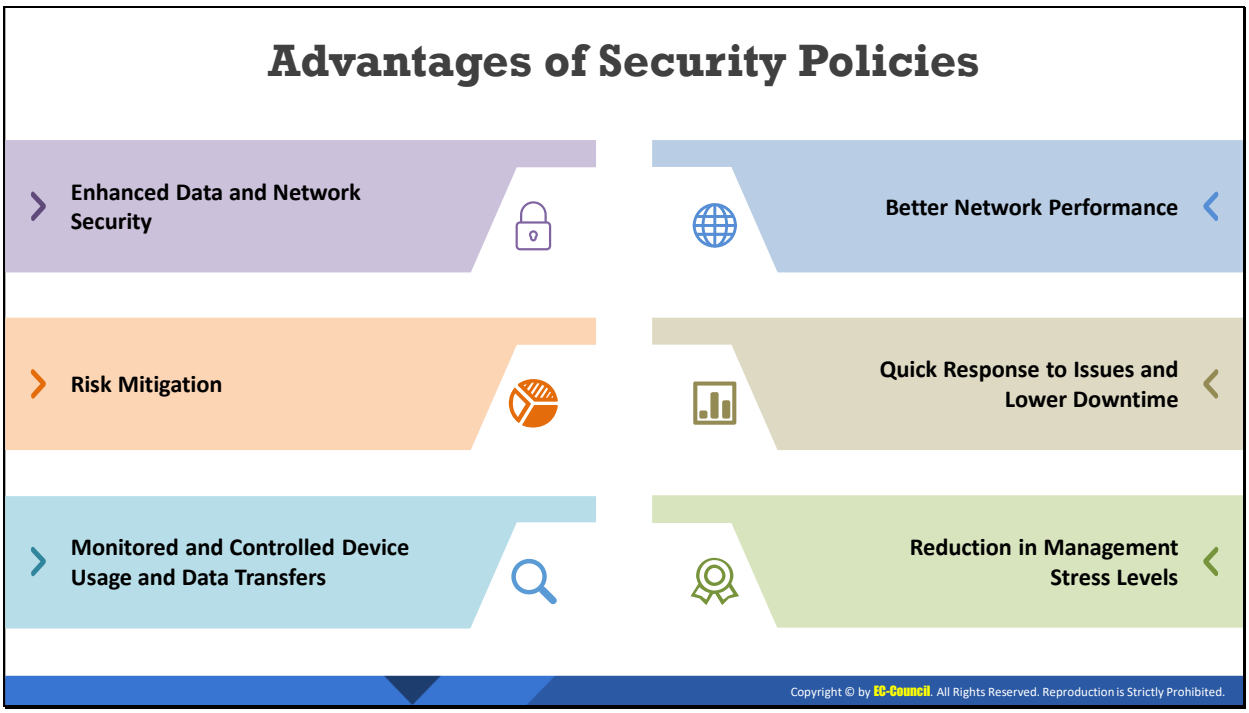
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Need for a Security Policy

- The number of devices used across an organization is increasing, which is, in turn, increasing the size and complexity of the information being transferred, networks being used, and storage space. At the same time, the likelihood of security threats originating from various vulnerabilities is increasing. A security policy enables an organization to combat such threats and protect it from losing information.
- A security policy provides consistent application of security principles throughout the company to ensure secure functioning of services. It ensures compliance to information security industry standards, building a trust-based relationship with clients. It helps limit a company's exposure to external information threats, while indicating senior management's commitment to maintaining a secure environment.
- Further, security policy provides legal protection by defining what rules to use on the network, how to handle confidential information, and the proper use of encryption, which together reduce liability and exposure of an organization's data.
- Security polices reduce the risk of damaging security incidents by identifying the vulnerabilities and predicting the threats before they occur.
- They also comprise procedures and techniques to minimize the risk of an organization's data leak or loss by adopting backup and recovery options.
- Ensure information security standards compliance.
- Enhance the overall data and network security.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Advantages of Security Policies

- **Enhanced Data and Network Security:** Organizations implement a policy based on their network, which enhances their data security. It facilitates protection when sharing information among other systems on a network.
- **Risk Mitigation:** The risks involved from external sources are reduced by implementing and deploying security policy. If an employee follows the policy exactly, it becomes nearly impossible for an organization to lose its data and resources.
- **Monitored and Controlled Device Usage and Data Transfers:** Although policies are being implemented thoroughly by employees, administrators should regularly monitor the traffic and external devices used in the system. Monitoring and auditing the incoming and outgoing traffic should always be done on regular intervals.
- **Better Network Performance:** When security policies are implemented correctly and the network is monitored regularly, no unnecessary loads exist. The data transmission speed in the system increases, providing an overall performance enhancement.
- **Quick Response to Issues and Lower Downtime:** Policy deployment and implementation enables faster response rates when resolving network issues.
- **Reduction in Management Stress Levels:** The role of management becomes less stressful when policies are implemented. Every policy must be followed by every employee in an organization. If this occurs, management will be less burdened by potential malicious attacks on the network.
- **Reduced Costs:** If employees follow the policies correctly, the cost of each intrusion is reduced as well as the impact on an organization.

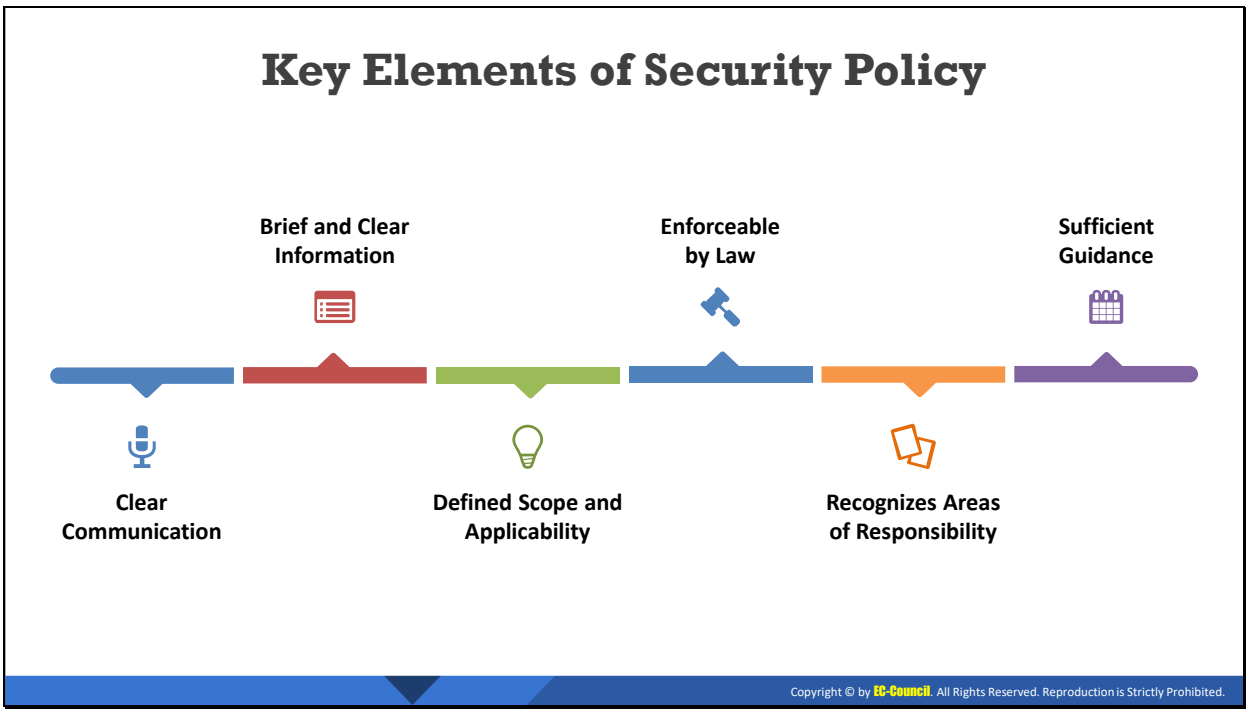
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Characteristics of a Good Security Policy

Features of a Good Security Policy:

1. **Concise and Clear:** A security policy needs to be concise and clear, which ensures easy deployment in the infrastructure. Complex policies become hard to understand and employees may not implement them as a result.
2. **Usable:** Policies must be written and designed, so they may be used easily across various sections of an organization. Well-written policies are easy to manage and implement.
3. **Economically Feasible:** Organizations must implement policies that are economical and enhance the security of an organization.
4. **Understandable:** Policies must be easy to understand and follow.
5. **Realistic:** Policies must be practical based on reality. Using fictional items in a policy will only hurt an organization.
6. **Consistent:** Organizations must have consistency when implementing their policies.
7. **Procedurally Tolerable:** Procedural policies should be employer–employee friendly.
8. **Cyber and Legal Laws, Standards, Rules and Regulations Compliance:** Any policy that is implemented must comply with all rules and regulations regarding cyber laws.

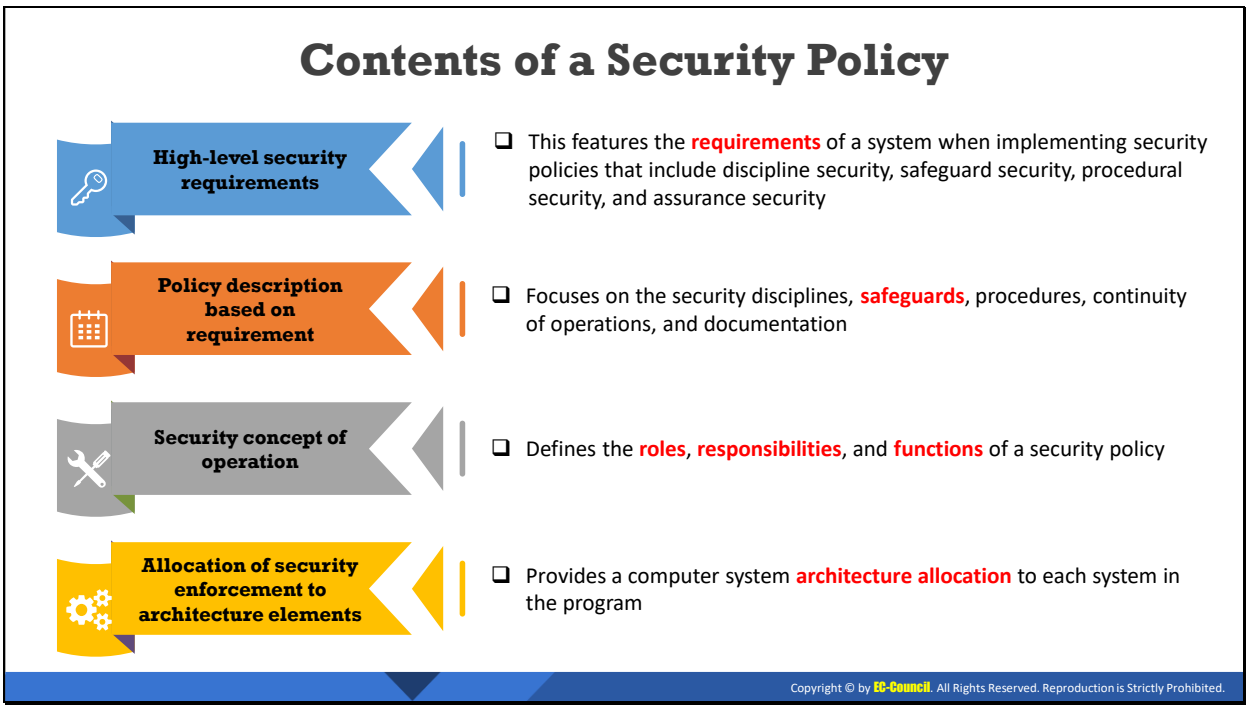
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Key Elements of Security Policy

- **Clear Communication:** Communication must be clear when designing a security policy. A communication gap leads to undesirable results. At the same time, some policies may be infeasible for users or a network. Keep communication channels clear.
- **Brief and Clear Information:** Any information provided to developers regarding the creation of the network policy must be clear and understandable. Failure to do so would hamper network security expectations.
- **Defined Scope and Applicability:** The scope identifies the items that must be covered, hidden, protected, or public, and how to secure them. The network policy addresses a wide range of issues from physical to personal security.
- **Enforceable by Law:** The security policy must be enforceable by law. Penalties should be imposed in the event of a policy breach. Penalties for a violation must be addressed when the policy is created.
- **Recognizes Areas of Responsibility:** The network policy must recognize the responsibilities of employees, the organization, and third parties.
- **Sufficient Guidance:** A good network policy must have proper references to other policies; this helps guide and redefine the scope and the objectives of the policy.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Contents of a Security Policy

Security Policy Implementation

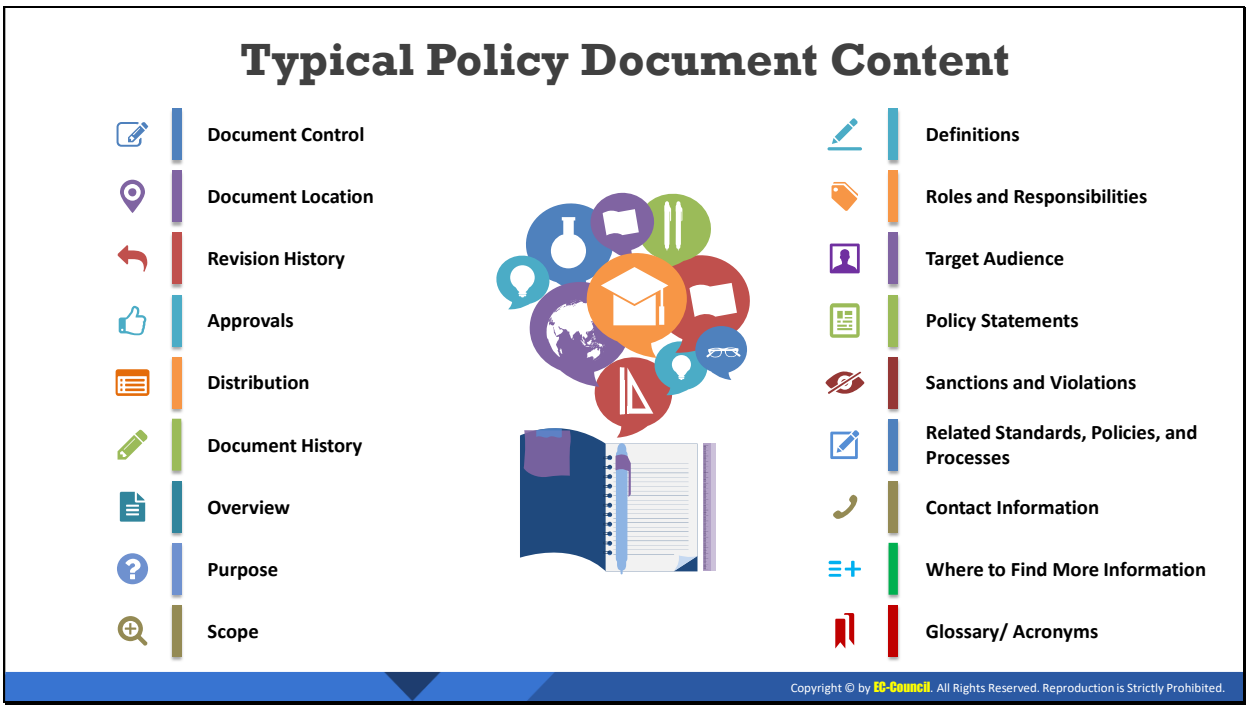
There are four aspects in security policy implementation.

- **High-level Security Requirements:** This features the requirements of a system when implementing security policies that include discipline security, safeguard security, procedural security, and assurance security. Security requirements include all requirements for a system to implement security policies. These are further divided into four types:
  - **Discipline Security Requirements:** Actions to be taken for various components that need to be secured such as computer security, operations security, network security, personnel security, and physical security
  - **Safeguard Security Requirements:** Protective measures required such as protective measures for access control, malware protection, audit, availability, confidentiality, integrity, cryptography, identification, and authentication
  - **Procedural Security Requirements:** Access policies, accountability, continuity of operations, and documentation
  - **Assurance Security Requirements:** Policies used with the compliance of various standards, certifications, and accreditations
- **Policy Description Based on Requirement**: Policy description mainly focuses on the security disciplines, safeguards, procedures, continuity of operations, and documentation. Each subset of this policy describes how the system's architecture elements will enforce security.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **Security Concept of Operation:** This concept defines the roles, responsibilities, and functions of a security policy. It focuses on the mission, communications, encryption, user and maintenance rules, idle time management, privately owned versus public domain, shareware software rules, and virus protection policy.
- **Allocation of Security Enforcement to Architecture Elements:** This policy allocates computer system architecture to each system in the program.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Typical Policy Document Content

The following are the important policy sections:

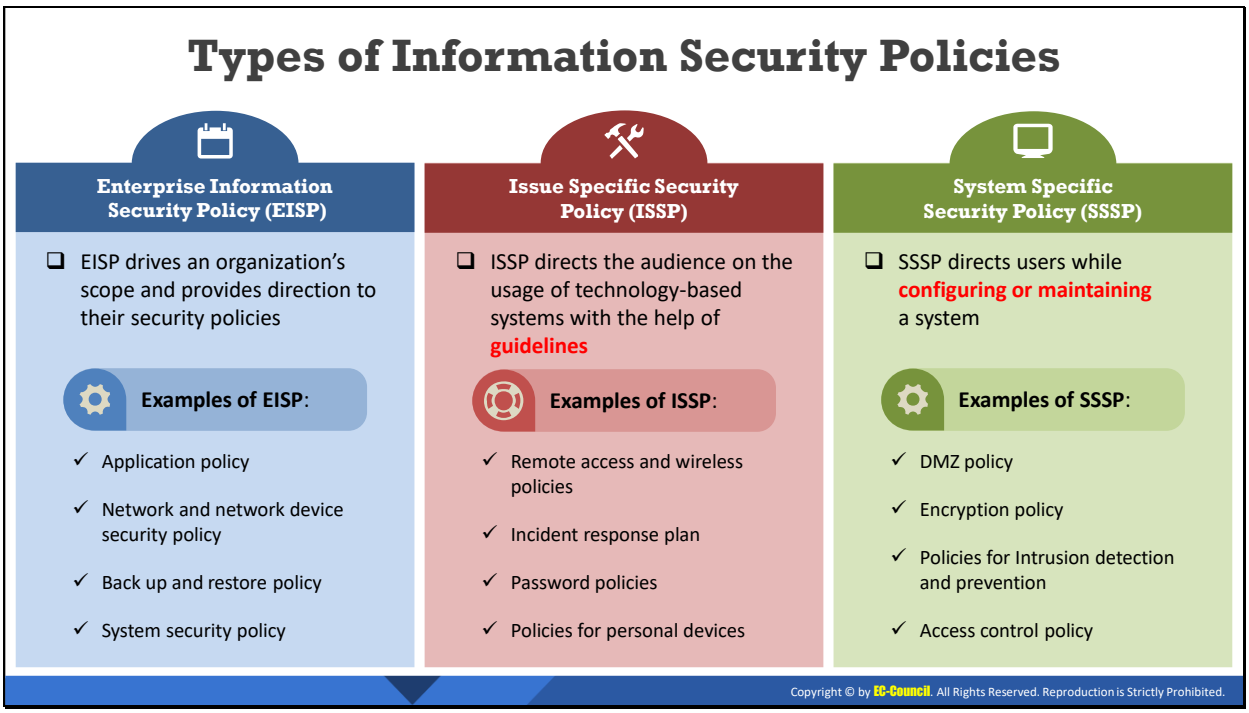
- **Document Control** is a procedure to store, modify, manage, distribute, and track policy documents.
- **Document Location** is the location where the policy document is stored.
- **Revision History** allows viewing the history of changes made to policy and by whom those changes were made; it also allows reverting to previous policies.
- **Version Number** ensures that all changes/updates to policy are tracked correctly.
- **Approvals** ensure that policies are approved in the correct manner from start to completion.
- **Distribution** ensures that policies are conveyed correctly throughout.
- **Document History** consists of documents having critical information about the policies.
- **Overview** of a security policy provides background information on the issues that the policy needs to address.
- **Purpose** is a detailed explanation of why the policy needs to be framed.
- **The scope** includes information about who and what the policy covers.
- **Definitions** define the terms used in the policy.
- **Roles and Responsibilities** are defined for the employees and management.
- **Target Audience** consists of the users and clients the policy is created for.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **Policies** are statements on each aspect of the policy.
- **Sanctions and Violations** define the allow/deny processes clients and users must follow.
- **Related Standards, Policies, and Processes** consist of a set of standards, policies, and processes that are connected or associated with the policies used.
- **Contact Information** includes information about who to contact in case of a policy sanction and/or violation.
- **Where to Find More Information** contains additional information and sources used for creating the policies.
- **Glossary/Acronyms** list the different terms and abbreviations used in the policy.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Types of Information Security Policies

In an organization, policies are crucial for information security planning, design, and deployment. These policies provide measures to handle issues and the technologies that could help users accomplish their security goals. The policy also explains how the software or equipment functions in an organization.

Information technology enterprises deploy security policies such as:

Enterprise Information Security Policy (EISP)

EISP drives an organization's scope and provides direction to their security policies. These policies support organizations by offering ideology, purpose, and methods to create a secure environment for enterprises. It establishes a method for development, implementation, and management of security programs. These policies also ensure the proposed information security framework requirements are met. Examples of EISP include application policy, network and network device security policy, security policy auditing, backup and restore policy, system security policy, and policies for servers.

Issue Specific Security Policy (ISSP)

ISSP directs the audience on the usage of technology-based systems with the help of guidelines. These policies address specific security issues in an organization. The scope and applicability of these security policies are completely dependent on the type of issue and the methods used by them. It specifies the necessary technologies along with preventive measures such as authorization of user access, privacy protection, and fair and responsible use of technologies. Examples of ISSP include remote access and wireless policies, incident response plan, password policies, policies for personal devices, user account policies, and internet and web usage policies.

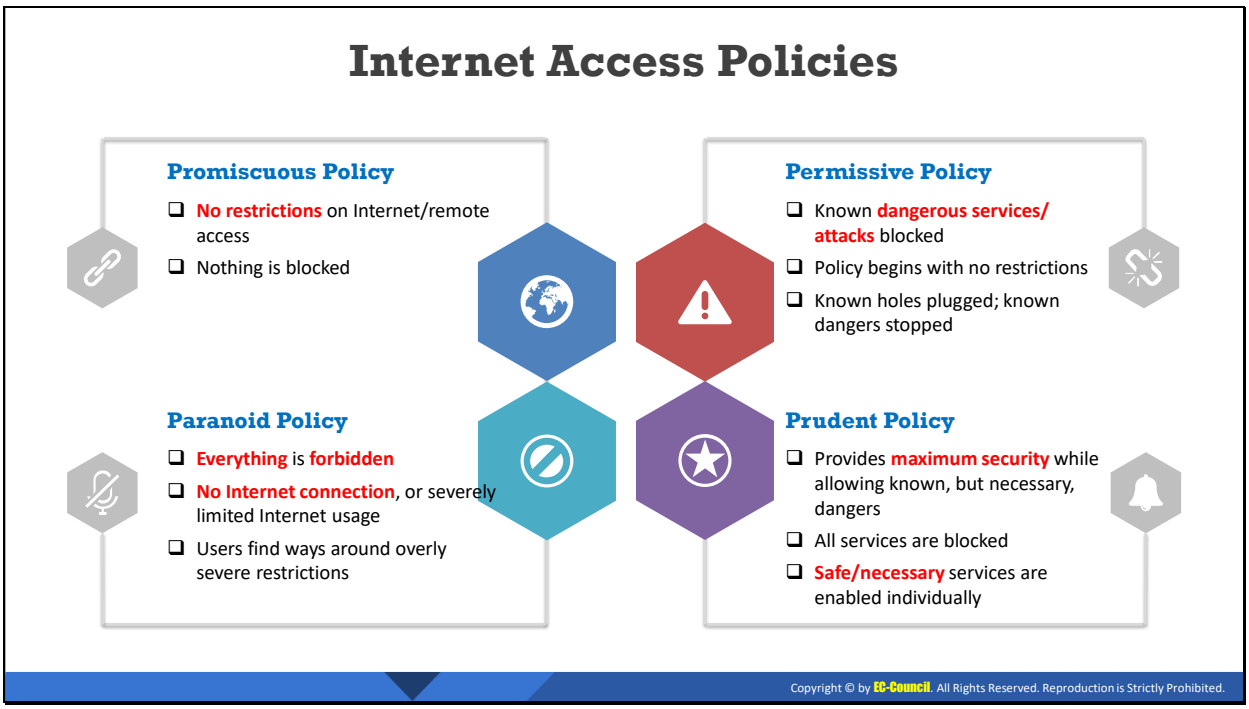
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

System Specific Security Policy (SSSP)

SSSP directs users while configuring or maintaining a system. The implementation of these policies focuses on the overall security of a particular system in an organization. An organization often develops and manages this type of policy, including the procedures and standards, for system maintenance. The technologies used by an organization should also be included in system-specific policies. It addresses the implementation and configuration of technology and user behavior. Examples of SSSP include DMZ policy, encryption policy, acceptable use policy, policies for secure cloud computing, policies for intrusion detection and prevention, and access control policy.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Internet Access Policies

Internet access policies define the restricted use of the Internet. It is important for employees to know which of their actions is restricted while accessing the Internet. The Internet access policy helps keep employees informed on acceptable browsing. An Internet policy includes guidelines for permissible use of the Internet, system security, network setup, and IT service.

Internet access policies broken down into the four categories below:

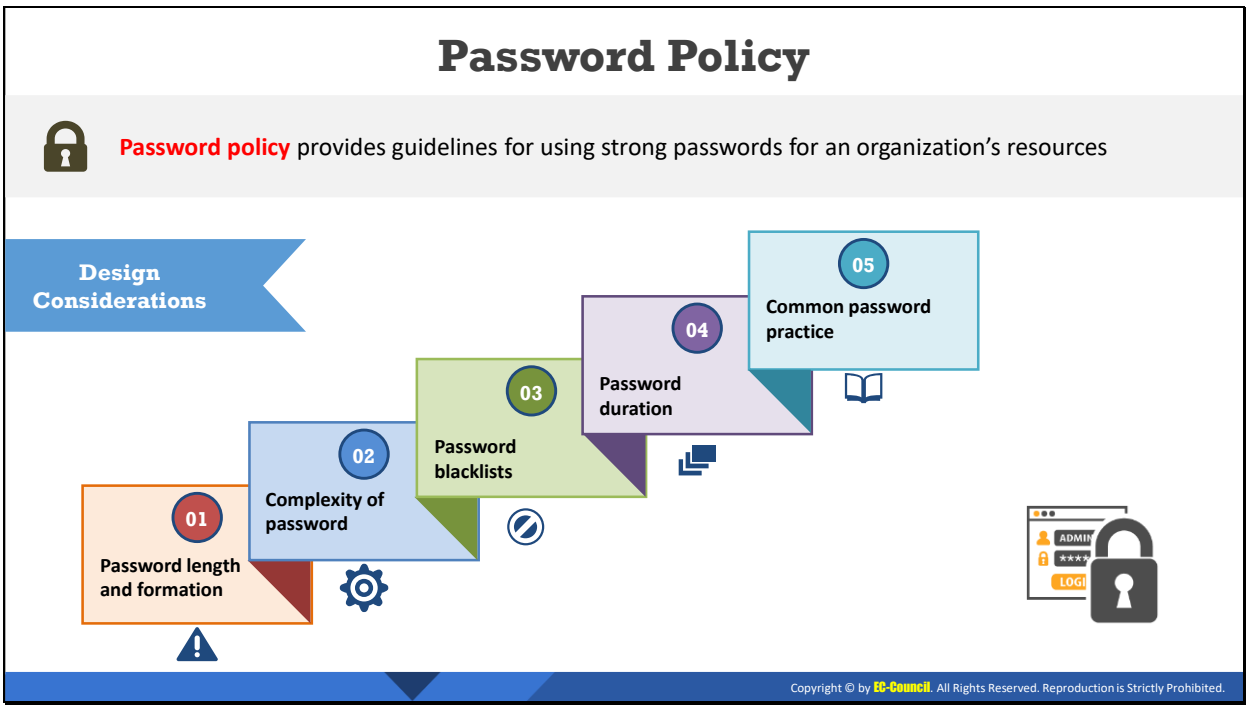
1. **Promiscuous Policy:** This policy does not impose any restrictions on the usage of system resources. For example, with a promiscuous Internet policy, there is no restriction on Internet/remote access, nothing is blocked. A user can access any site, download any application, and access a computer or a network from a remote location. While this can be useful in corporate businesses where people travel or work at branch offices and need to access an organizational network, it also opens the computer to threats such as malware, viruses, and Trojans. Because of free Internet access, this malware can come in the form of attachments without user knowledge. Network defenders must be extremely alert while choosing this type of policy.
2. **Permissive Policy:** This policy is wide open, and only known dangerous services/attacks or behaviors are blocked. For example, in a permissive Internet policy, the majority of Internet traffic is accepted, except for several well-known and dangerous services/attacks. Because only known attacks and exploits are blocked, it is impossible for network defenders to monitor current exploits. They are always playing catch-up with new attacks and exploits.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

3. **Paranoid Policy:** A paranoid policy forbids everything. There is a strict restriction on all company computers, whether it is system or network usage. There is either no Internet connection or severely limited Internet usage. Users often try to circumvent such severe restrictions.
4. **Prudent Policy:** A prudent policy starts with all services blocked. The Network defender enables safe and necessary services individually. This provides maximum security and logs all activity such as system and network activities. According to this policy, nonessential services/procedures that cannot be made safe are not allowed.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Password Policy

A password policy is a set of rules to increase system security by encouraging users to employ strong passwords to access an organization's resources and to keep them secure. The purpose of the policy is to protect an organization's resources by creating robust protected passwords. The policy statement should include a standard practice for creating a robust password. For example, the password should

- Have a length between 8 and 14 characters;
- Include both uppercase and lowercase letters, numerical digits, and special characters;
- Special characters (@, %, $, &, or ;);
- Be case sensitive, whereas username or login ID may not be; and
- Be unique when changing the old password. Thus, regarding password history, old passwords cannot be reused.
  - Maximum password age: 60 days
  - Minimum password age: No limit

Some of the components of a password policy include:

- **Password Length and Formation**

  This policy includes the length of the password. The password length varies according to an organization. The formation of a password includes:
  - One or more numerical digits;
  - Special characters such as @, #, and $;

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- Use uppercase and lowercase letters;
- Avoid using personal information; and
- Use of company name in the password is prohibited.

- **Password Blacklists**

  A password blacklist contains a list of words that are prohibited from use as passwords because of their familiarity. These blacklists help in preventing the usage of common passwords.

- **Password Duration**

  This policy suggests users change their passwords regularly—usually every 90 or 180 days. Changing a memorized password is hard for the user, but it is necessary to avoid password stealing.

- **Common Password Practices**

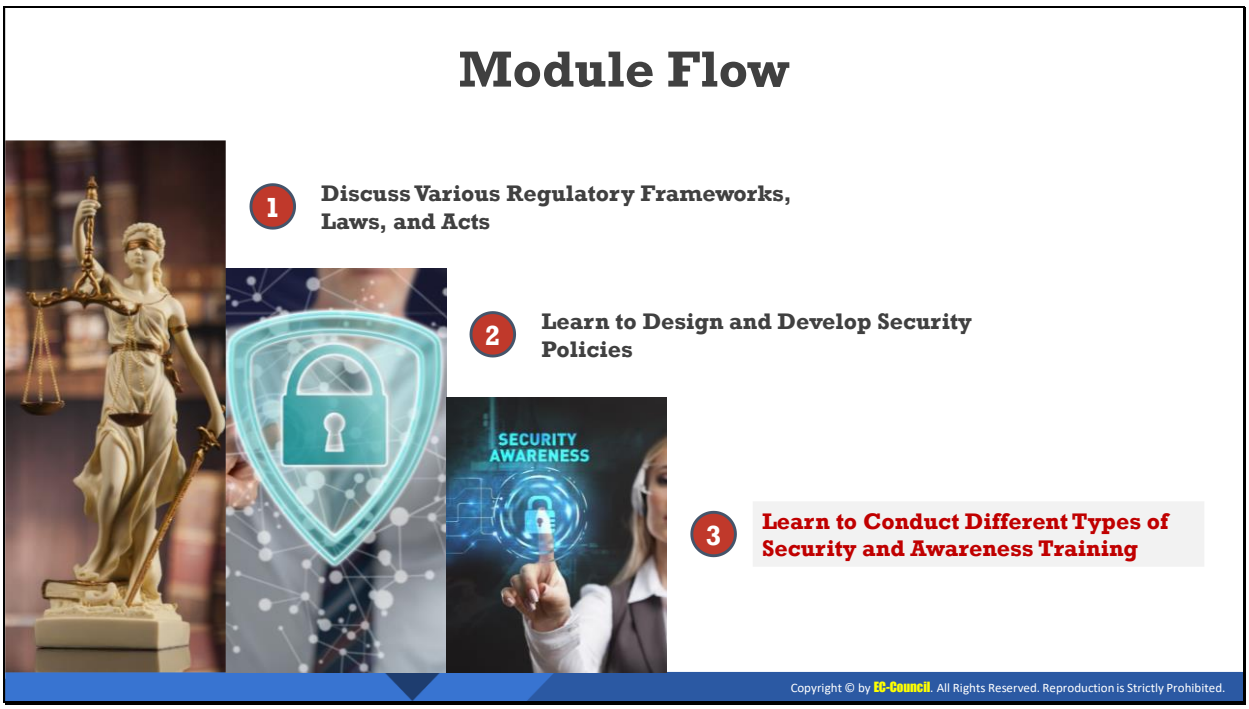
  The password policy statement should include guidance or best practices on creating, storing, and managing passwords. For example, it should include guidelines such as

  - Do not share your computer user account details.
  - Do not keep a common password for all accounts.
  - Do not share passwords.
  - Never write the password anywhere, instead remember it.
  - Employees should not communicate their password through email, phone, or instant messages even to the administrator.
  - Do not leave the machine unattended. Always log off or lock the system when leaving the desk.
  - Keep different passwords for the OS and frequently used applications.

The password policy should include a disclaimer that informs all users of the consequences of not following the guidelines stated in the password policy. The disclaimer should involve all employees, including top management. Disclaimers can include verbal or written warnings or termination.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

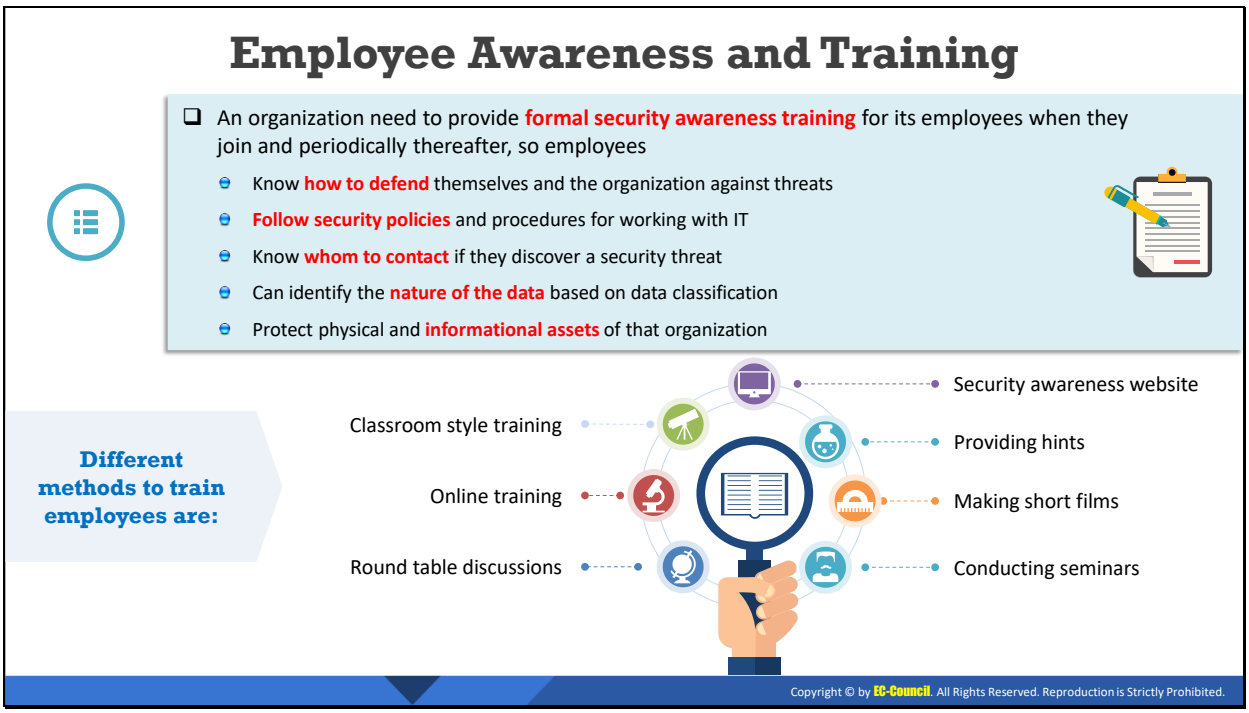
https://t.me/learningnets



Learn to Conduct Different Types of Security and Awareness Training

Employee and user training play an important part in the governance of the overall security of an organization. An untrained employee or user can pose a considerable risk to an organization. Hence, it is important to make them aware about security policies, and conduct other awareness training programs to maintain organization security. This section explains the importance of conducting security awareness trainings and keys aspects to be covered in different types of training.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Employee Awareness and Training

Employees are one of the primary assets of an organization and can be part of an organization's attack surface. The actions of an employee—such as negligence, errors, susceptibility to social engineering, or clicking spam links—can lead to an attack. An employee awareness training initiated during orientation and periodically thereafter can enhance protection. The training is typically related to the knowledge and attitudes of employees tasked with the security of physical and informational assets.

- Expertise to defend themselves and an organization against threats;
- Follow security policies and procedures for working with information technology;
- Know whom to contact if they discover a security threat;
- Should be able to identify the nature of data based on data classification;
- Protect the physical and informational assets of an organization when the employees come into contact with them—for example, contacting with secrets, privacy concerns, and classified information;
- Know how to handle critical information such as review of employee nondisclosure agreements;
- Know the proper methods for protecting critical information on systems with password policy and the use of two-factor authentication;
- Know the consequences of failing to secure information, which may result in employment loss; and

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- An organization should provide security awareness training to employees to meet regulatory requirements if they want to comply with a certain regulatory framework.

The different methods to train employees include:

- Classroom style training
- Online training
- Round table discussions
- Security awareness website
- Providing hints
- Making short films
- Conducting seminars
- Simulation employee training
- Hands-on training
- Lectures
- Coaching/mentoring
- Case studies
- Management specific activities
- Group discussions and activities

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Employee Awareness and Training: Security Policy

Security policy training teaches employees how to **perform** their duties and to comply with the security policy. Organizations should train new employees before granting them access to the network or provide limited access until the completion of their **training.**

Security policy training and procedures are required to ensure security and effective network management.

- The security policy training program helps employees appropriately recognize and respond to security threats in real time. The training teaches employees understand the importance of data on their devices or systems. Employees adapt themselves to secure computing habits.
- The security policy training makes employees aware of new updates on probable vulnerabilities that can occur if they do not follow the policies.
- Security policy training and awareness helps minimize security breaches in an organization. Early identification of a breach decreases the cost to an organization.
- Security policy awareness among users helps notify them about new security policies through published policy documentation and descriptive security documentation for users, for example.
- Employees following the security policy reduce their possibility of being subject to potential fines or legal actions.
- An effective training program will help employees monitor their computing behavior and inform their security concerns to management. The training will enhance the overall compliance with the company's security policies and procedures.

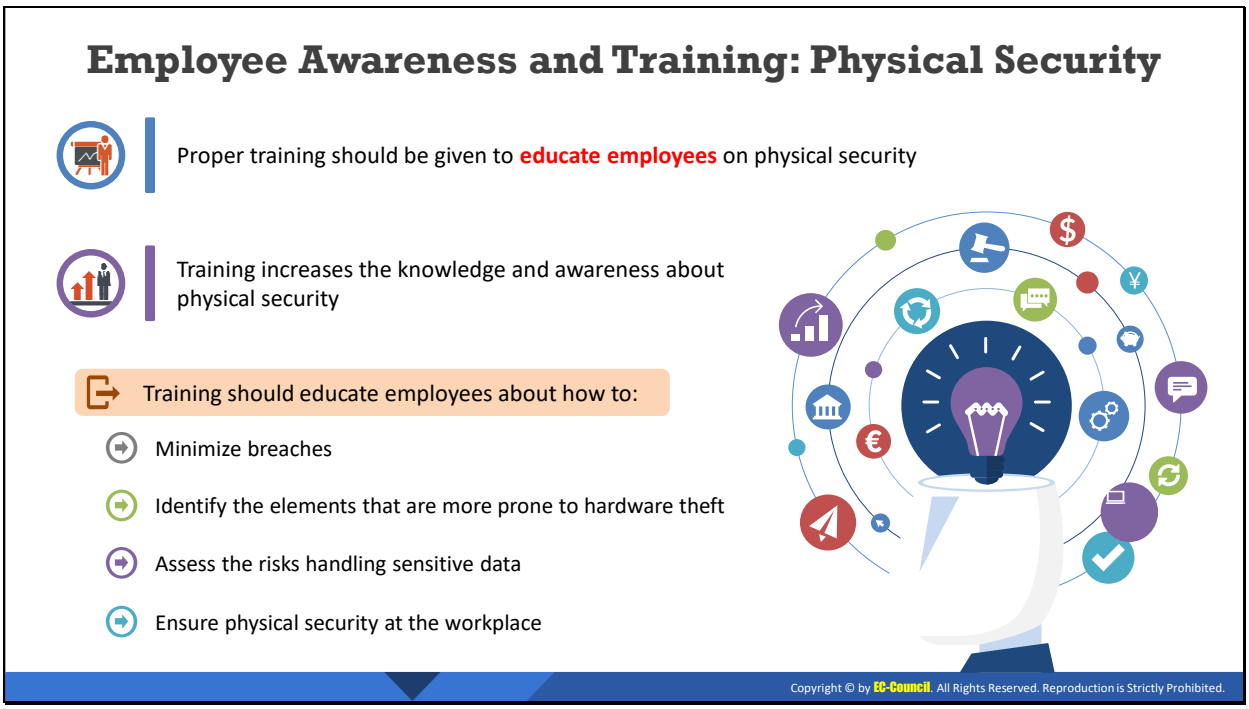
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Advantages

- Effective implementation of a security policy
- Policies are followed and not just enforced
- Creates awareness on compliance issues
- Helps an organization enhance its network security

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Employee Awareness and Training: Physical Security

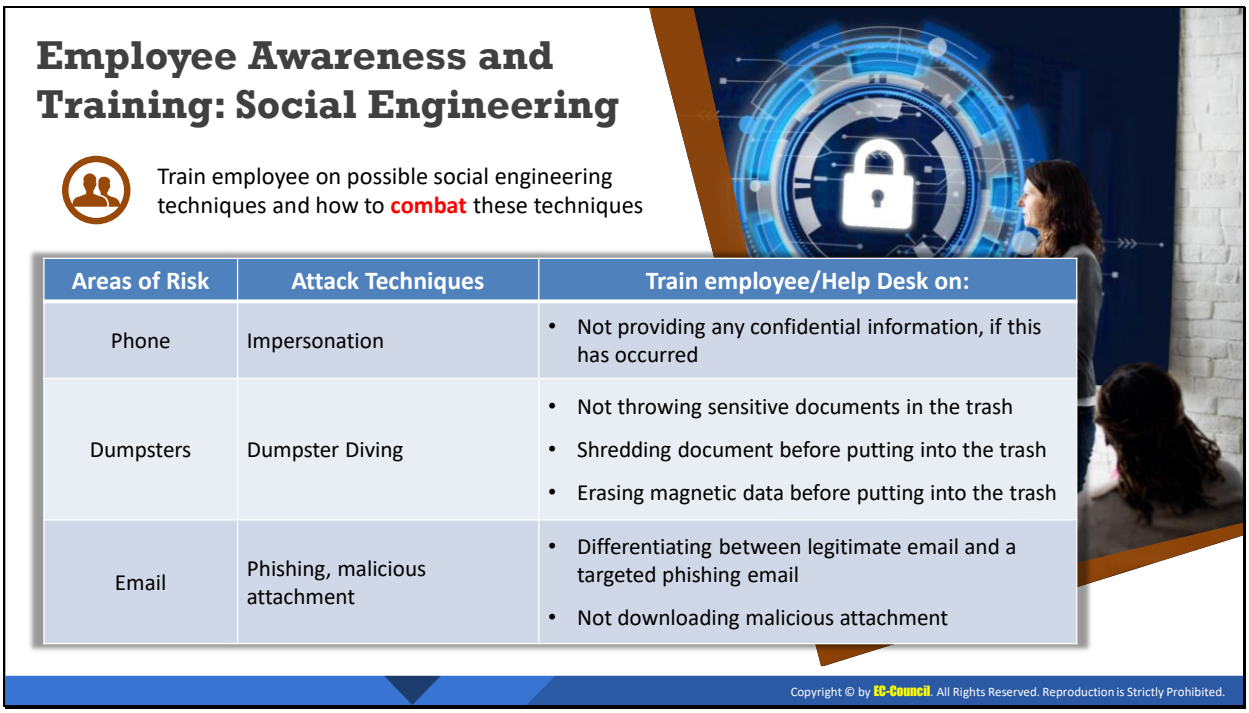
Well-trained and skilled personnel can minimize the risk of a physical security threat to a great extent. An organization should provide proper physical security awareness training to all its employees. Training increases the knowledge and awareness about physical security. Training should educate employees about how to:

- Minimize breaches
- Identify the elements that are more prone to hardware theft
- Assess the risks handling sensitive data
- Ensure physical security at the workplace

The training or awareness program should

- Provide methods to reduce attacks;
- Examine all devices and the chances of a data attack;
- Teach the risks of carrying sensitive information;
- Teach the importance of having security personnel;
- Inform employees about whom should report to about suspicious activities;
- Teach what to do when employees leave systems and workplaces unattended; and
- Teach the disposal procedures for disposing critical paper documents and storage media.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Employee Awareness and Training: Social Engineering

A simple social engineering awareness training can be cost-effective. It is useful in reminding employees about an organization's policies, which can ultimate help employees recognize and prevent social engineering attacks. Employees must be trained on possible social engineering techniques and how to combat social engineering techniques.

Areas of Risk	Attack Techniques	Train employee/Help Desk on:
Phone	Impersonation	▪ Not providing any confidential information, if this has occurred
Dumpsters	Dumpster Diving	▪ Not throwing sensitive documents in the trash ▪ Shredding document before putting into the trash ▪ Erasing magnetic data before putting into the trash
Email	Phishing, malicious attachment	▪ Differentiating between legitimate email and a targeted phishing email ▪ Not downloading malicious attachment

Table 3.8: Social Engineering Attack Awareness and Training

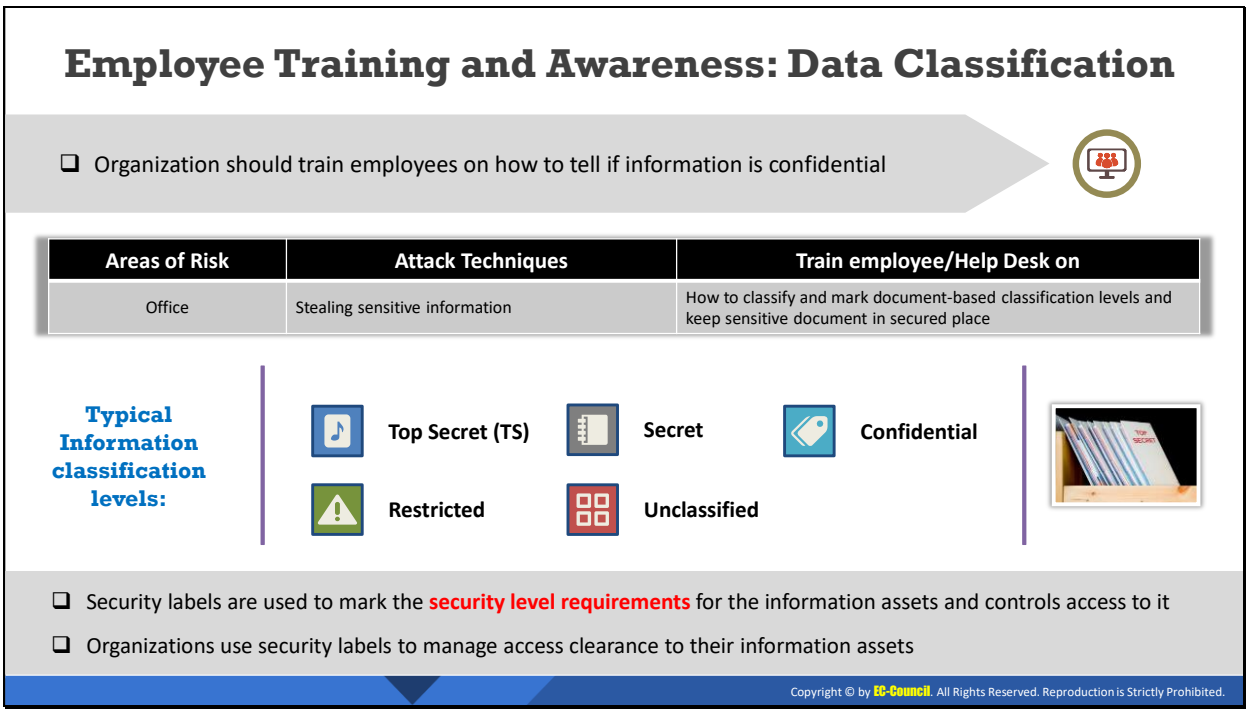
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Some of the social engineering techniques the employees should be aware of include:

- Physical social engineering (tail-gaiting, piggy-backing);
- Changing passwords (attacker poses as an authority and asks to change the username and password);
- Name-drop (using the higher authority's name to gain access to something);
- Relaxing conversation (trying to build up a rapport with the employee); and
- New hire (attacker poses as a new employee to take a tour around the office).

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Employee Training and Awareness: Data Classification

Organization should train employees on how to tell if information is confidential. Security labels are used to mark the security level requirements for the information assets and controls access to it. Organizations use security labels to manage access clearance to their information assets. Security labels are used to restrict access to information in high and low security areas as a part of mandatory access control decisions. This enables easy understanding for users with and without permission to access and easy clearance of a large group of users. It defines the sensitivity of the data or the object and authorizations required for accessing the object or data. It provides a list of users who can access the document or the device and enables the user to understand the documents that they can access.

Areas of Risk	Attack Techniques	Train employee/Help Desk on
Office	Stealing sensitive information	How to classify and mark document-based classification levels and keep sensitive document in secured place

Table 3.9: Data Classification Training and Awareness

Security labels are categorized into different types based on who can access the data or object.

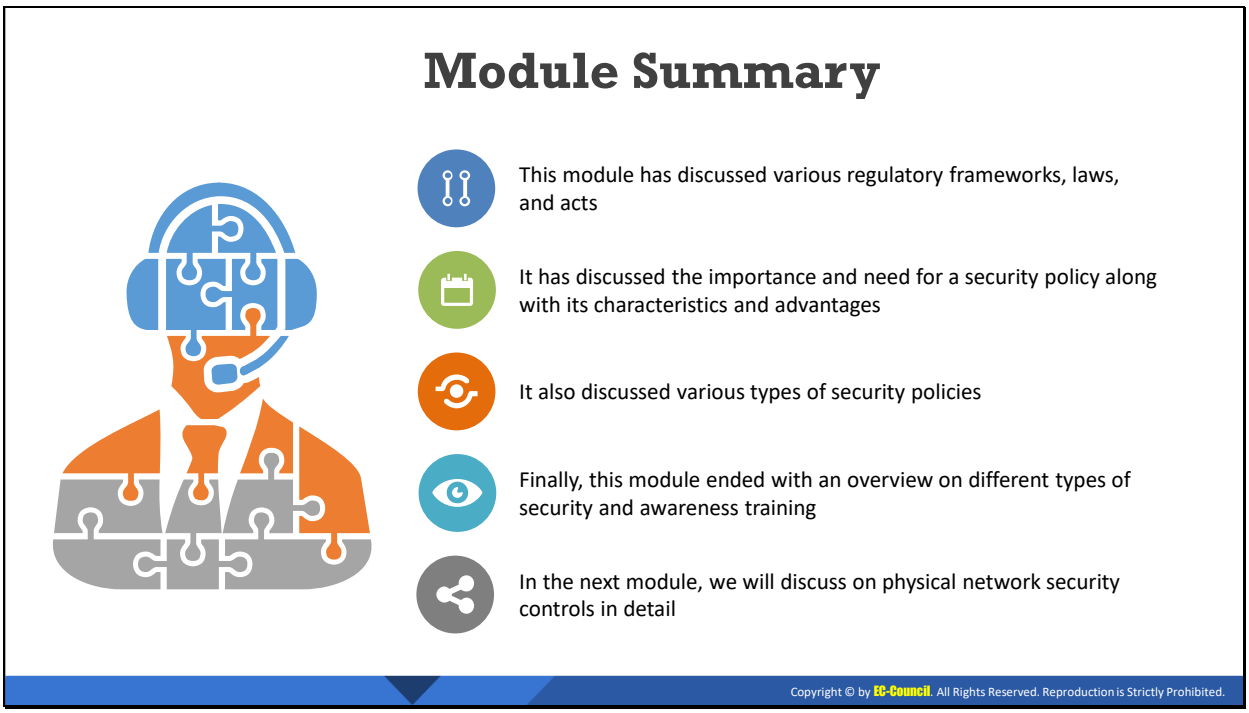
- **Unclassified**: No access permissions are required in order to access unclassified documents. Any person at any level may access these documents.
- **Restricted**: Only a few people can access the data or object. Sensitive data may be restricted for use in an organization because of its technical, business, and personal issues.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **Confidential**: Confidential data or objects exposed may lead to financial or legal issues in an organization. Documents may be highly confidential or only confidential. Revealing these data—whether confidential or highly confidential—will lead to loss of critical information.
- **Secret**: Users authorized to access secret files may access secret, confidential, restricted, and unclassified data. Users cannot access documents or objects labeled as top secret, as it requires a higher clearance level.
- **Top Secret:** Users accessing top secret documents may access top secret, secret, confidential, restricted, and unclassified data.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Module Summary

This module discussed various regulatory frameworks, laws, and acts. Further, it discussed the importance and need for a security policy, along with its characteristics and advantages. It also explained various types of security policies. Finally, this module presented an overview on different types of security and awareness training.

In the next module, we will discuss physical network security controls in detail.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

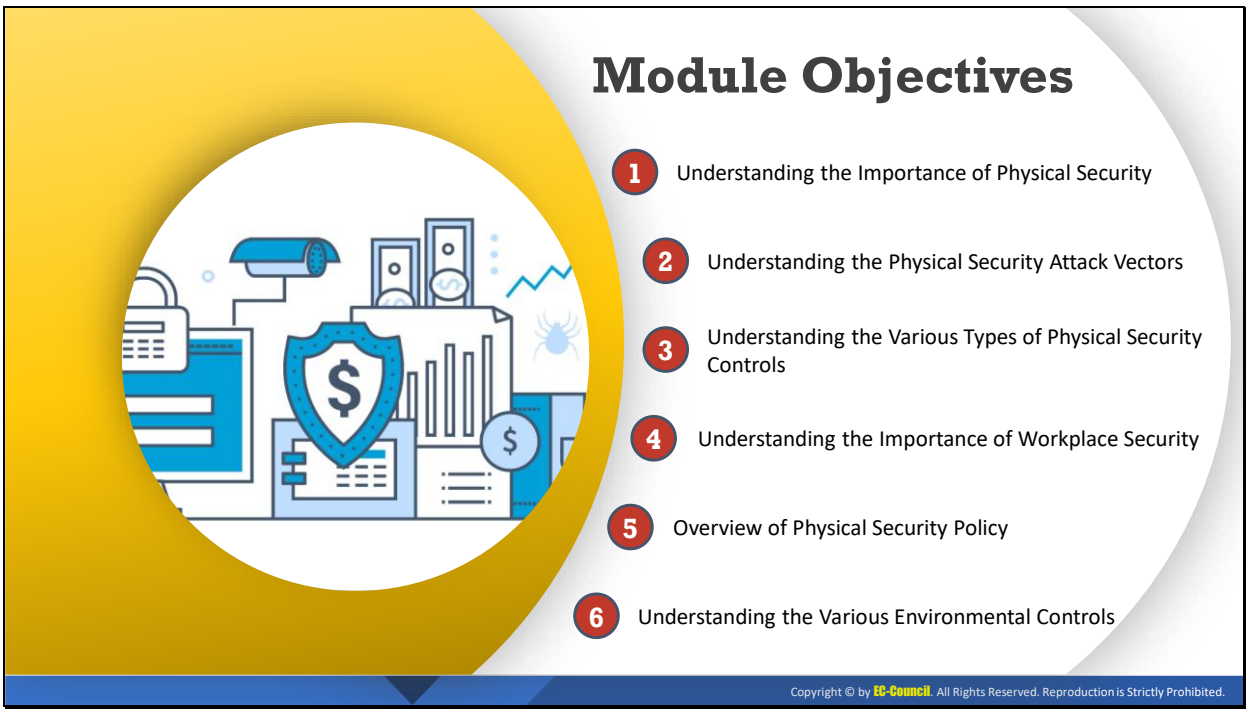
EC-Council

N|DE
Network Defense Essentials

Module 04

Network Security Controls - Physical Controls

https://t.me/learningnets



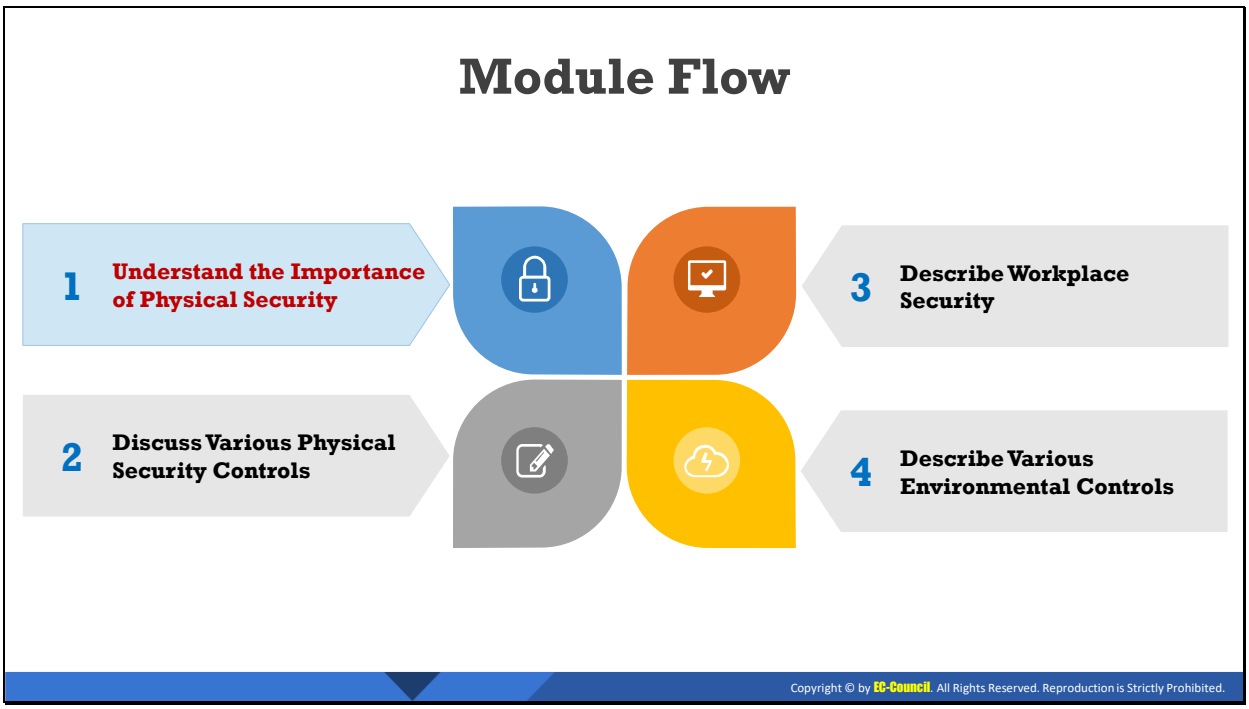
Module Objectives

Physical security plays a major role in every organization. It entails the protection of critical information, network infrastructure, physical equipment and devices, facilities, personnel, etc. from environmental disasters, terrorism, vandalism, and theft. Physical security is becoming a challenging task with the increased usage of devices such as USB drives, laptops, smartphones, and tablets because malicious actors can easily gain physical access to such devices and steal sensitive data. This module explains the importance of physical security, various physical security controls, importance of workplace security, and various environmental controls.

At the end of this module, you will be able to:

- Understand the importance of physical security
- Understand the physical security attack vectors
- Describe the various types of physical security controls
- Explain the importance of workplace security
- Understand physical security policy
- Understand the various environmental controls

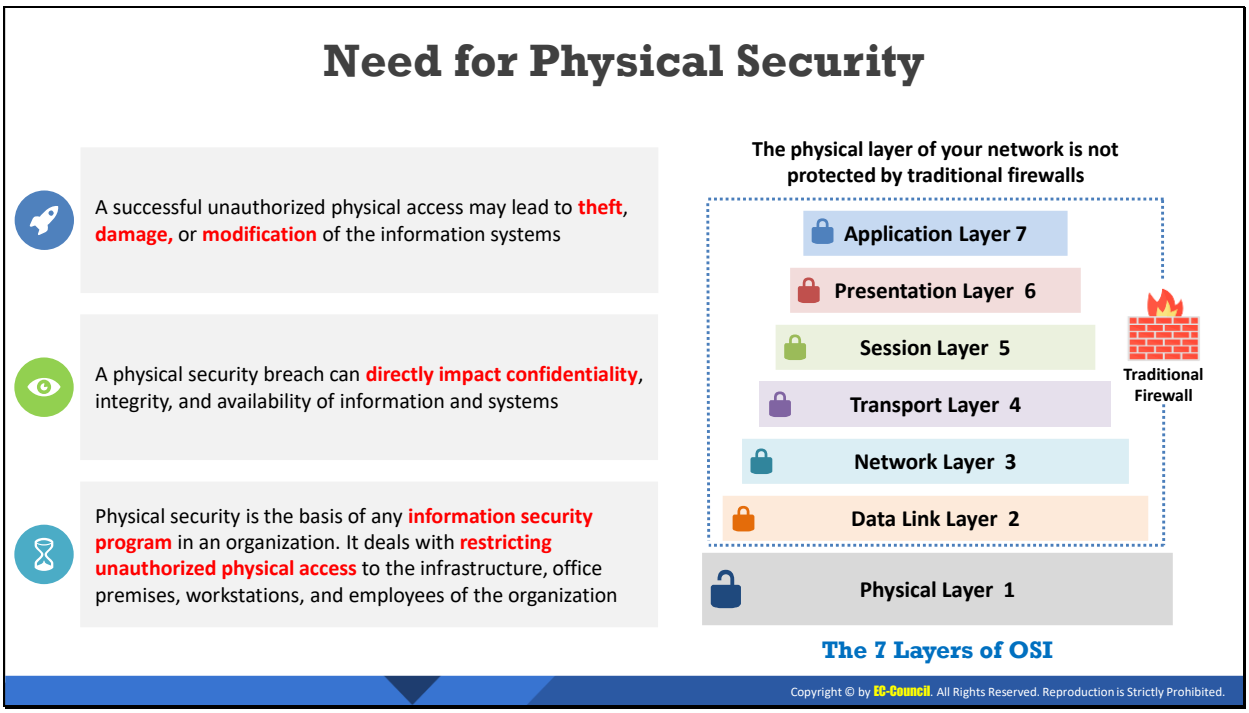
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Understand the Importance of Physical Security

Physically safeguarding systems and networks is the top priority of network security. This section explains the importance of physical security in organizations.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Need for Physical Security

Although cyber-attacks are becoming increasingly complex, attackers continue to use various techniques to compromise the physical security of an organization. However, organizations are increasingly focusing on strengthening their IT security, which overshadows physical security. Physical security is the most overlooked aspect of security, and this fact has been brought to the notice of many organizations over the last five years. Knowing this fact, attackers are taking advantage of loopholes to compromise the physical security of organizations. According to data collected by the US Department of Health and Human Services Breach Portal, physical security breaches are among the most frequently occurring security incidents in organizations.

According to the findings of the fifth annual Horizon Business Continuity Institute (BCI) Scan Report, physical security is now perceived as a growing concern for business continuity professionals. According to this report, a degree of concern has been expressed with regard to the possibility of both an act of terrorism and a security incident such as vandalism, theft, or fraud disrupting the organization at some point.

Physical security breaches are vastly different from other security breaches. They can be performed with little to no technical knowledge. Physical security concerns arise because conventional security measures such as firewalls and IDSes do not ensure physical security. Deploying a firewall at various levels ensures security from different types of attacks but does not ensure the physical security of the organization. A conventional firewall is entirely unrelated to physical security as it works above the physical layer of the OSI model. Thus, conventional firewalls do not protect the physical layer of a network.

A successful attempt at unauthorized physical access may lead to the theft, damage, or modification of information systems. A physical security breach can directly impact the confidentiality, integrity, and availability of information and systems. Therefore, physical

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

security forms the basis of any information security program in an organization. It entails restricting unauthorized physical access to the infrastructure, office premises, workstations, and employees of the organization.

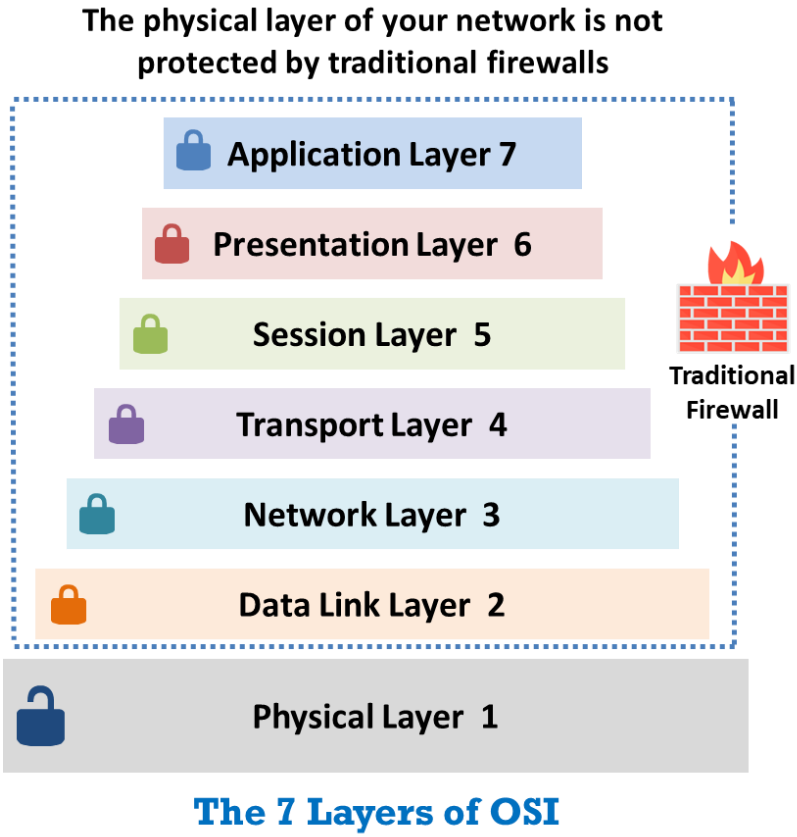


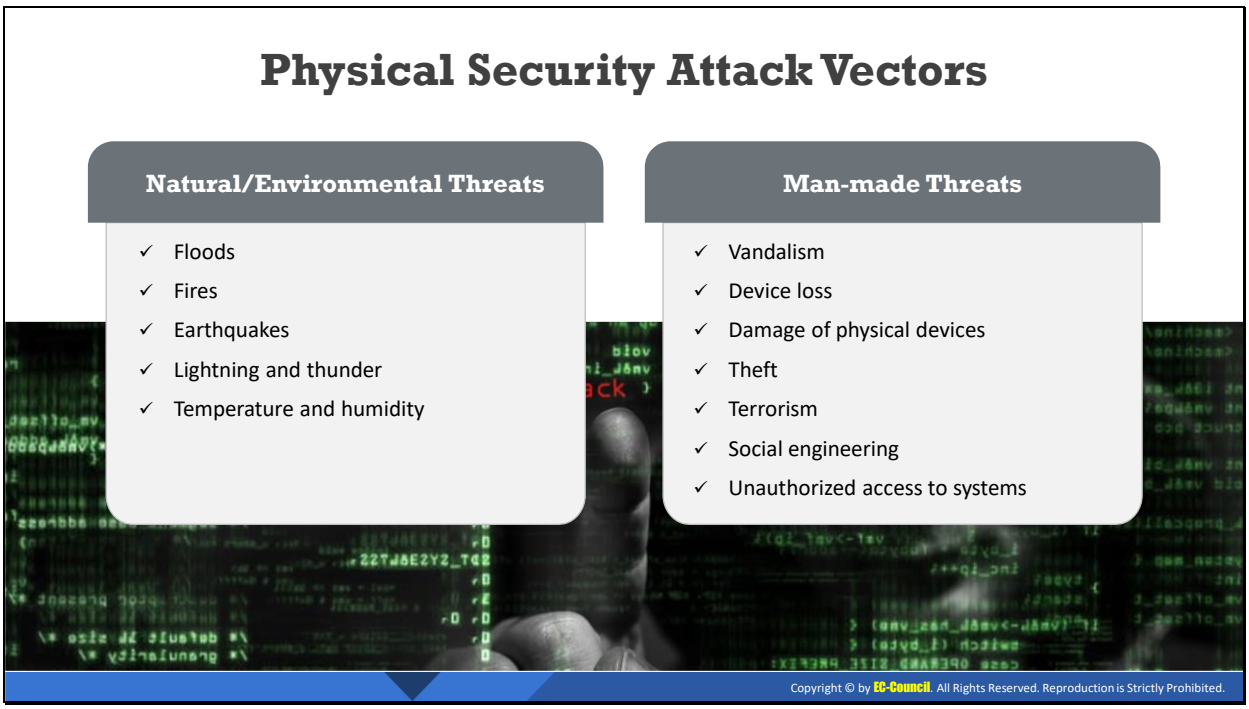
Figure 4.1: OSI layers and physical security

Physical security cannot be ensured in the same manner as network, application, or database security, and separate security measures are required for physical security. Physical security should be implemented at the physical layer of the OSI model.

A physical layer includes the following:

- All cabling and network systems
- Physical access to cables and systems
- Power support for cables and systems
- Environment supporting the systems

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Physical Security Attack Vectors

Organizations are at a risk of the following types of physical security threats.

Natural/Environmental Threats

- **Floods:** Floods commonly occur because of heavy rains or the melting of ice. Floods may affect electrical systems and server rooms in an organization. Server rooms located in the basement have a greater chance of being affected by floods.
- **Fires:** Fires mainly occur because of short circuits or poor building materials. They may affect the operational facility and computer rooms in an organization. Fires can damage the hardware, cabling system, and other important components.
- **Earthquakes:** An earthquake is the sudden release of stored energy in the Earth's crust that creates seismic waves. It disrupts the physical infrastructure in an organization. It damages computers and other hardware devices and documents in the sensitive areas inside an organization. Moreover, it can affect the safety or security of the organization. Earthquakes mainly affect the cabling, the wiring system, and the physical building itself. Any damage to the cabling system affects the working of the computer systems.
- **Lightning and thunder**: Lighting and thunder occur because of environmental changes. It necessitates the shutdown of all outdoor activities. Lightning and thunder lead to power and voltage fluctuations that, in turn, affect the working of systems. In particular, it may affect the memory chips and other hardware components of a system. It may lead to a short circuit in the cabling and other wiring systems if they are not covered properly. The information system may stop working with one lightning strike. Lightning may damage all electrical and electronic appliances and lead to the loss of all sensitive information.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **Temperature and humidity**: Computer systems operate in a certain range of temperatures; otherwise, they function in an inappropriate manner. Computer systems do not work well in hot areas and may become damaged if the temperature increases or decreases by extreme amounts. Although every computer has cooling systems, the performance of a computer still depends on the exterior temperature conditions. Furthermore, electrical and electronic appliances in an organization may be affected by a change in humidity. A high humidity leads to issues such as corrosion and short-circuits and damages magnetic tapes and optical storage media. A low humidity affects electronic devices mainly through electric discharge.

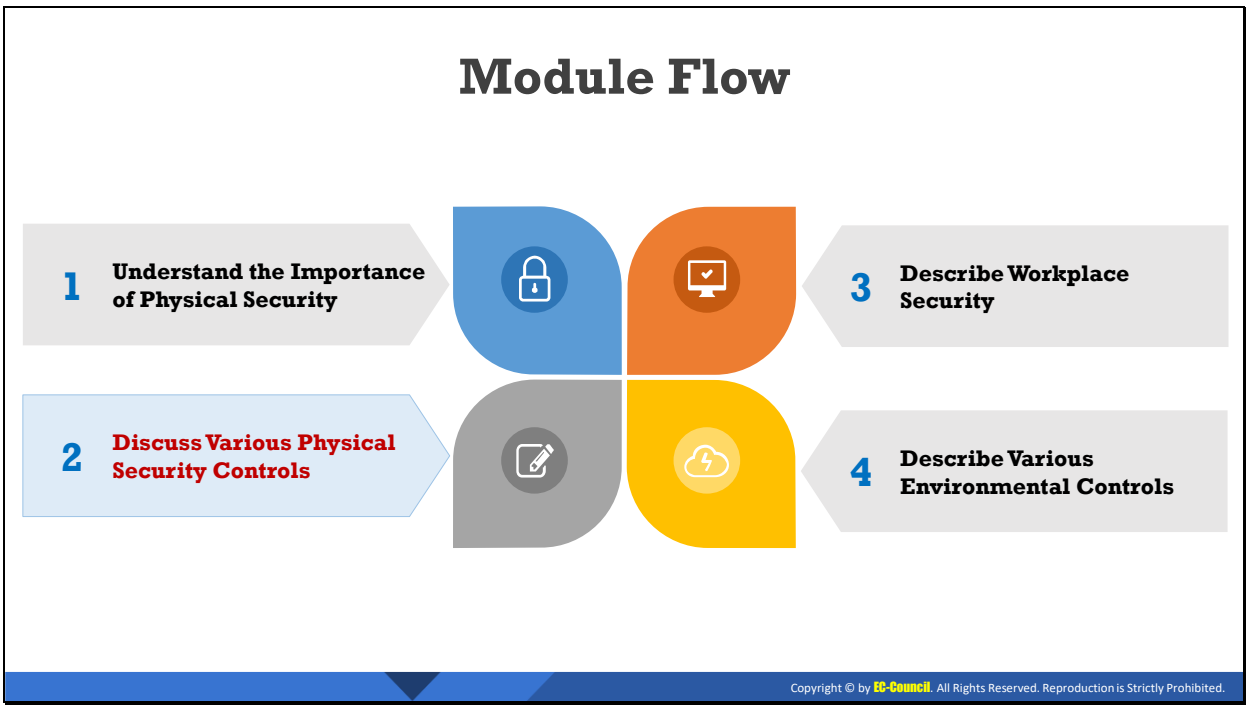
Man-made Threats

The most significant threat to physical components and the network is from man-made errors, both intentional and unintentional. There is a wide range of such possibilities, including hackers/crackers, theft, fire, and human error. Some examples of human error that may lead to man-made threats are the unintentional pressing of an incorrect button and unplugging of the wrong device. Typical man-made threats include mechanical errors, electrical disturbance, pollution, radio-frequency interference, and explosion.

- **Vandalism**: Disgruntled employees or former employees may attempt to compromise a system by willingly breaking or harming system components. During civil unrest or a disaster, there is a chance of systems being mishandled.
- **Device loss**: Unauthorized access may lead to the loss of important information and devices. Device theft is a concern if devices are not properly secured.
- **Damage to physical devices:** Improper device maintenance activities such as the improper handling of a device or information, failure to replace damaged devices, and poor cabling can damage physical devices to a great extent.
- **Theft:** Lack of proper security and locks may result in equipment theft.
- **Terrorism:** Terrorism activities such as the planting of a vehicle bomb, human bomb, or postal bomb in and around the organization's premises impact physical security in many ways.
- **Social engineering:** Social engineering is defined as an illegal act of acquiring personal information from people. An attacker can gain unauthorized physical access by performing social engineering on an organization's employees.
- **Unauthorized access to systems**: Both internal and external users can attempt to gain unauthorized access to a system or information about the organization.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

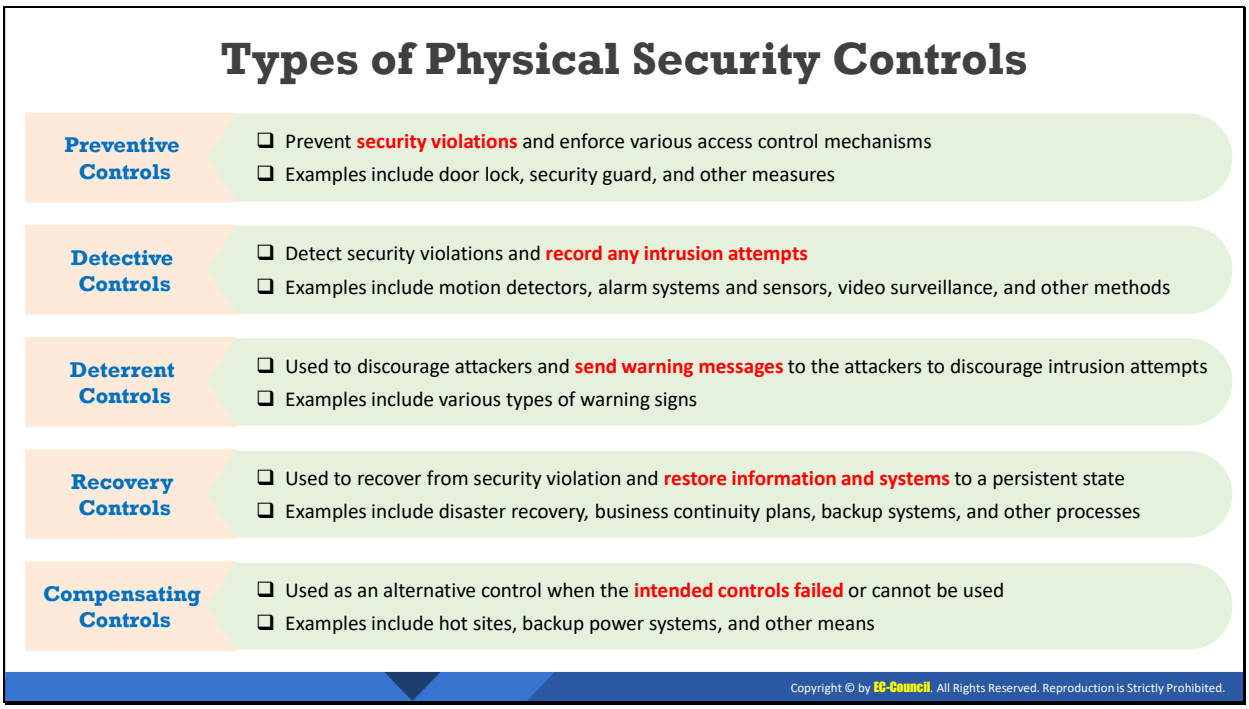
https://t.me/learningnets



Discuss Various Physical Security Controls

This section explains various physical security controls that can be used in organizations.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Types of Physical Security Controls

Physical security controls are categorized based on their functionality and the plane of application. Based on their functionality, the types of physical security control include the following.

- **Preventive Controls**

  These controls prevent security violations and enforce various access control mechanisms. Preventive controls may be physical, administrative, or technical. Examples include door locks and security guards.

- **Detective Controls**

  These controls detect security violations and record any intrusion attempts. They act when preventive controls fail. Examples include motion detectors, alarm systems and sensors, and video surveillance.

- **Deterrent Controls**

  These controls may not prevent access directly. They are used to discourage attackers and send warning messages to them to discourage an intrusion attempt. Examples include various types of warning signs.

- **Recovery Controls**

  These controls are used in serious situations to recover from security violations and restore information and systems to a persistent state. Examples include disaster recovery, business continuity plans, and backup systems.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **Compensating Controls**

  These controls are used as alternatives when the primary controls fail or cannot be used. They do not prevent any attack attempt but attempt restoration using techniques such as restoring from a backup. Examples include hot sites and backup power systems.

Based on the plane of application, the types of security controls include the following.

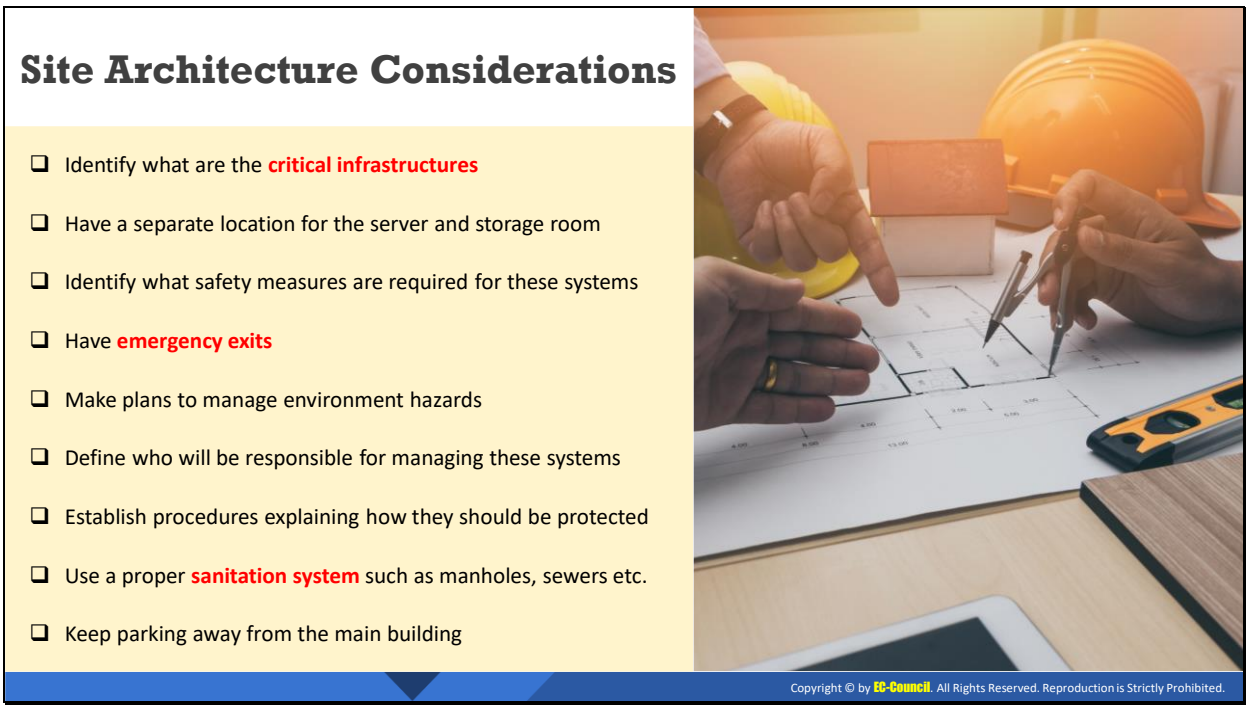
- Physical security controls such as doors, secure facilities, fire extinguishers, and flood protection
- Administrative security controls such as the organization's policies, procedures, and guidelines to provide information security
- Technical security controls such as IDSes/IPSes, firewalls, and authentication systems

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Location Considerations

Organizations should consider various factors that may affect physical security before planning to buy or lease a building. The factors to consider may include the facility location, neighboring buildings, joint tenancy risks, power and water supply, sewage systems, proximity to public and private roads, transportation, emergency support, fire stations, hospitals, airports, local crime or rate of riots, and prior security incidents in the surrounding area. The location should not be prone to natural disasters such as floods, tornadoes, earthquakes, hurricanes, excessive snow or rainfall, mudslides, and fires.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Site Architecture Considerations

After gaining adequate information about the facility location, the planning and designing of the internal infrastructure and architecture should be performed. While planning and designing the site architecture, an organization should prepare a list of all of its assets in the facility.

The organization should consider the following points while designing the infrastructure and architecture.

- Decide the number of entrances required for the building, including the main entrance, staircase, parking, lift, hallway, and reception area.
- Find the neighboring facilities around the site location and check the internal and external architecture for them. Talk to the supervisors or owners of the buildings to gain additional insights about the surroundings.
- Analyze the assets that can be impacted by catastrophic failures as well as the visibility of assets to outsiders.
- Consider the joint tenancy factor; if the facility is shared with other companies, consider their impact on the organization's sensitive information and critical assets.
- Identify the necessary critical infrastructure that is required for managing the physical security, storing sensitive data, and running business operations effectively.
- Ensure a separate location for the server and storage room.
- Identify what safety measures are required for these systems.
- Implement emergency exits.
- Make plans to manage environmental hazards.

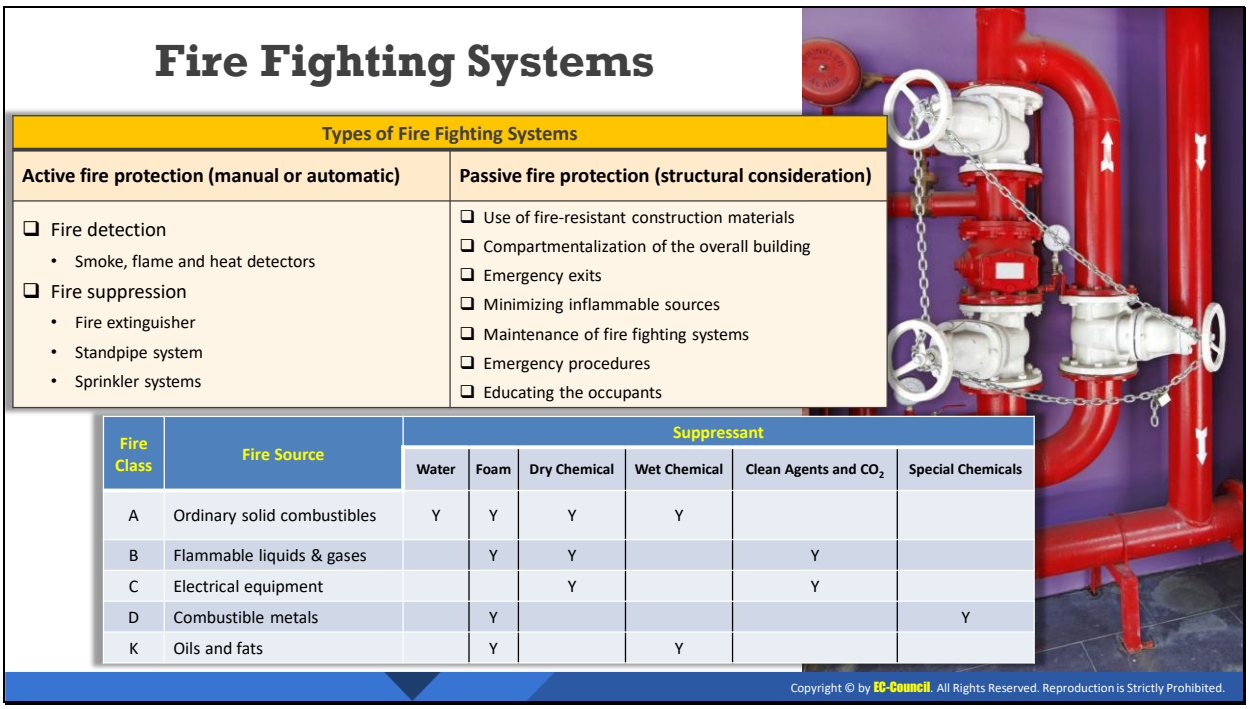
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- Define who will be responsible for managing these systems.
- Establish procedures explaining how they should be protected.
- Use a proper sanitation system including manholes and sewers.
- Keep parking away from the main building.

These critical infrastructure systems may not use standard IT for safety, performance, and reliability, but they are critical to business operations. An improper or faulty implementation of certain physical measures such as electricity, backup, storage facilities, lighting, wiring, and cooling systems can be critical to the business operations of the organization.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Fire Fighting Systems

Fire is an incident that can occur with or without warning and is usually attributed to man-made errors, short circuits, and defective or faulty equipment. Fire protection is an important aspect of physical security. Firefighting systems mainly detect fire incidents and alert the occupants to them. Fire incidents may be identified either manually or automatically.

The types of firefighting systems include the following.

Active Fire Protection

Active fire protection alerts the occupants of an organization regarding a fire incident. This type of fire protection system is generally used in commercial places, process industries, and warehouses to protect storage vessels, processing plants, etc. The main aim of implementing an active fire protection system is to control the spread of fire and extinguish it as soon as possible, thereby facilitating the clearance of occupants in an organization. The system requires a certain number of actions to handle fire incidents. These actions may be performed either manually or automatically.

Certain active fire systems include water sprinklers, fire/smoke alarm systems, spray systems, and fire extinguishers. Fire/smoke alarms indicate the presence of any fire or smoke in the building. Water sprinklers reduce the spread of fire, and fire extinguishers help put out fire. Water sprinklers fall under the category of automatic fire protection systems, whereas fire extinguishers and standpipes fall under the category of manual fire protection systems.

Active fire protection systems include the following.

- **Fire detection system:** A fire detection system helps detect a fire incident before allowing the fire to spread.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Automatic fire detection systems include the following components.

- **Smoke detectors:** Smoke detectors generally detect smoke and send alerts about the suspected fire incident in an organization. Upon detection of smoke, the detectors send an alarm to the fire alarm control panel or generate an audio/visual alarm.
- **Flame detectors:** Flame detectors mainly detect flames in a fire incident. Flame detectors normally include sensors that detect flames. The working of a flame detector is as follows:
  - An alarm is generated on fire flame detection.
  - Gas supply is cut through the fuel line.
  - The fire suppression system is activated.

  Flame detectors work more efficiently and faster than smoke detectors and heat detectors.
- **Heat detectors:** Heat detectors are used to detect and respond to the thermal energy generated by fire incidents. Heat detectors are further classified into fixed-temperature heat detectors and rate-of-rise heat detectors.

- **Fire suppression:** A fire suppression system is used to extinguish fire without much human intervention. Fire suppression systems regulate destruction and device loss. They can be classified into manual and automatic. Commonly used fire suppression systems include the following.
  - **Fire extinguisher:** Fire extinguishers aim to extinguish fires at the initial stage. They are not useful in the case of a fire covering a large area. A fire extinguisher normally consists of an agent that is discharged inside a cylindrical vessel. Fire extinguisher systems need to be checked often to ensure that they work properly in case of fire. Fire extinguishers are usually inspected yearly or bi-yearly by trained professionals. They can also be recharged.

    Dry chemicals, water, wet chemicals, water additives, clean agents, and carbon-dioxide are used as agents in fire extinguisher systems. Below table provides details for selecting the proper extinguisher based on various types of fire sources.

Fire Class	Fire Source	Suppressant					
		Water	**Foam**	**Dry Chemical**	**Wet Chemical**	**Clean Agents and CO_2**	**Special Chemicals**
A	Ordinary solid combustibles	Y	Y	Y	Y		
B	Flammable liquids and gases		Y	Y		Y	

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

C	Electrical equipment			Y		Y	
D	Combustible metals		Y				Y
K	Oils and fats		Y		Y		

Table 4.1: Classification of fire extinguishers

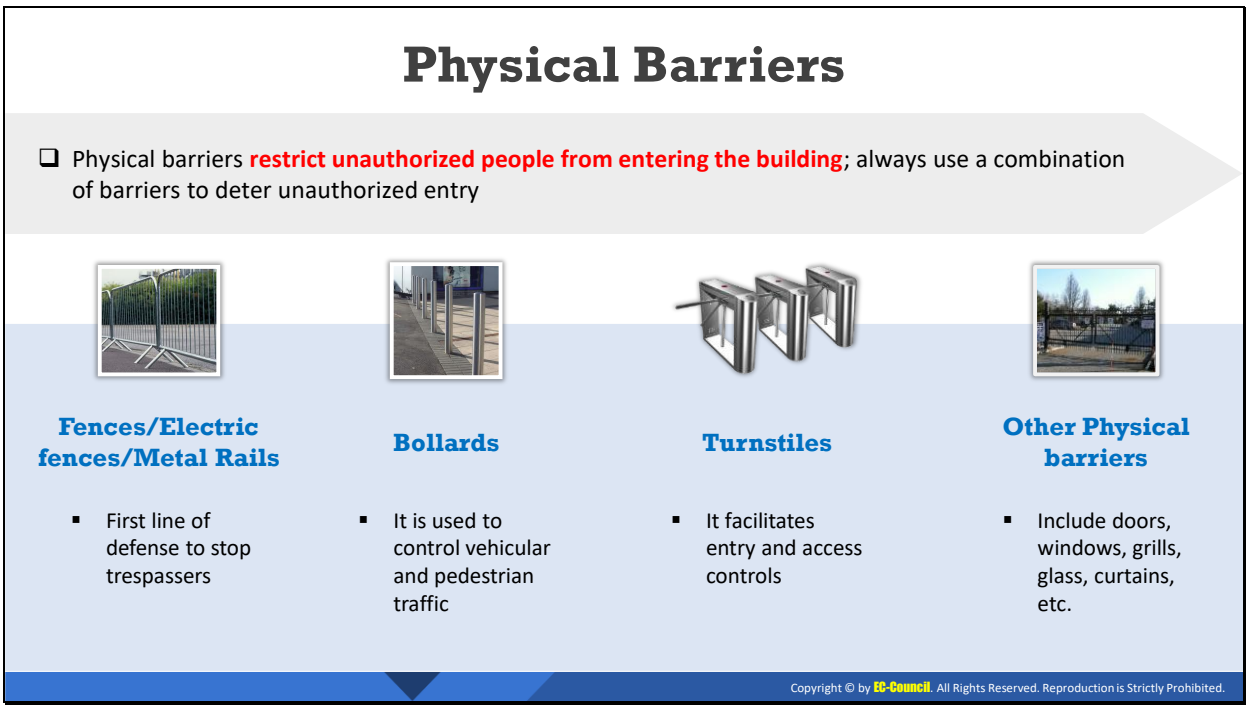
- **Standpipe system:** Standpipe systems connect hose lines to the water supply. They provide a pre-piped water system for organizations as well as water supply to hose lines in certain locations. The three types of standpipe systems are Class I – A, Class II – A, and Class III – A. These types differ in terms of the thickness of the hose lines used and the volume of water used for fire suppression.
- **Sprinkler system:** Fire sprinkler systems maintain a water supply system to supply water to a water distribution piping system that controls sprinklers. The sprinklers are used to avoid loss to human lives and assets. These are mainly used in areas that firefighters cannot reach with their hose lines.

Passive Fire Protection

Passive fire protection systems are used to prevent fire from spreading further across the organization. Fire-resistant doors, windows, and walls may be used for passive fire protection. It facilitates the protection of the building's occupants and reduces the rate of damage due to the fire. Passive fire protection systems do not need to be activated by other systems, and no operational assistance is required in implementing passive fire protection systems.

- Passive fire protection is implemented in the following ways:
  - Minimal use of flammable materials
  - Building additional floors and rooms in a building to slow down the spread of fire
  - Providing adequate training to the occupants regarding the procedures to follow in case of fire
  - Proper maintenance of fire-related systems
  - Adequate number of emergency exits
- The following are the steps to manage fire incidents:
  - Detect fire.
  - Evacuate occupants in the building to a safe location.
  - Notify the fire department and safety department regarding the fire.
  - Shut down all electrical and electronic systems to prevent the fire from spreading.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Physical Barriers

Many factors determine the physical security of an organization. These factors are essential considerations and contribute to the successful operation of physical security in an organization. The main goal of physical security is the control and prevention of unauthorized access, while physical barriers restrict unauthorized people from entering the building. Physical barriers define the physical boundary of an area and divide vehicle traffic from pedestrians. The use of a physical barrier deters and delays outsiders from entering the premises. An intruder or outsider can compromise a barrier by spending time and money as well as planning and contemplating on the site architecture. To discourage these intruders, it is a good policy to use a multilayer approach that includes external barriers, middle barriers, and internal barriers. External barriers include fences and walls; although they are built to form a structure, they inadvertently act as an obstruction. Middle barriers are equipment used to obstruct traffic and people. Internal barriers include doors, windows, grills, glass, and curtains.

The following are different types of physical barriers used in a building.

- **Fences/electric fences/metal rails:** These form the first line of defense against a trespasser and are the most commonly used type of physical barriers worldwide. Fences/metal rails/electric fences generally mark restricted and controlled areas and prevent unauthorized access.

  The aim of deploying physical barriers is as follows:

  - Block and deter attackers
  - Mark the boundary of the organization
  - Protect security guards from external attacks

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- Prevent the entry of vehicles
- Protect against explosive attacks

Figure 4.2: Metal rails

- **Bollards:** A bollard may be defined as a short vertical post that controls and restricts motor vehicles in parking areas, offices, etc. This facilitates the easy movement of people. Bollards are mainly used in building entrances, pedestrian areas, and areas that require safety and security. It is effective in controlling pedestrian and vehicle traffic in sensitive areas.

Figure 4.3: Bollards

- **Turnstiles:** This type of physical barrier allows entry to only one person at a time. Entry can be achieved only by the insertion of a coin, ticket, or pass. It allows security personnel to closely watch the people entering the organization and stop any suspicious persons at the gate. However, the use of a turnstile can hamper the fast evacuation of occupants in case of a fire emergency.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Figure 4.4: Turnstiles

- **Other Barriers:** These include doors, windows, grills, glass, and curtains installed to limit access to certain areas.
  - **Doors:** Doors can be used as a good structure to control the access of users in a restricted area. Door security may be increased with the installation of CCTV cameras, proper lighting systems, locking technology, etc.
  - **Windows**: An intruder can use windows to gain unauthorized access to restricted areas. Proper security measures should be considered while installing windows. Some of these considerations include the following:
    - Method of opening the window
    - Assembling and construction of the window
    - Technique used in locking the window
    - Hinges used for the window
  - **Grills:** Grills should be used with doors and windows to strengthen security. Grills may be used for internal as well as external security.
  - **Glass:** Sliding glass doors and sliding glass windows also strengthen physical security.

Figure 4.5: Other Barriers

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- The following are security considerations for physical barriers:
  - Use a combination of barriers to deter unauthorized entry.
  - Use bullet-resistant windows and glass.
  - Install doors both at the main entrance and inside the building.
  - Lock doors and windows.
  - Use electric security fences to detect the climbing and cutting of wires.
  - Use alarms to alert security personnel of any intrusions through fences.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Security Personnel

Security personnel/guards are hired to implement, monitor, and maintain the physical security of an organization. They are responsible for developing, evaluating, and implementing security functions such as the installation of security systems to protect sensitive information from loss, theft, sabotage, misuse, and compromise. Hiring skilled and trained security personnel can be an effective security measure for any organization. They play a crucial role in physical security. However, organizations generally do not consider this a core competency to invest in as part of their strategic plan.

Organizations should hire security personnel by themselves and provide adequate training on physical security. Alternatively, they can contact dedicated physical security service firms to handle physical security for them. There are organizations dedicated to training security officers, providing standardized procedures, and managing security on a 24 × 7 × 365 schedule by sharing guards across different organizations.

The following are the people involved in physical security.

- **Guards**: Their responsibilities include screening visitors and employees at the main gates or entrance; documenting names and other details about visitors; conducting regular patrols on the premises; inspecting packages, luggage, and vehicles; managing vehicle traffic; and guiding visitors to the reception area after noting their details. Guards should maintain visitor logs and record entry and exit information. Guards generally handle the use of CCTV cameras as a deterrent as well as a mechanism to detect and possibly prevent an intrusion.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

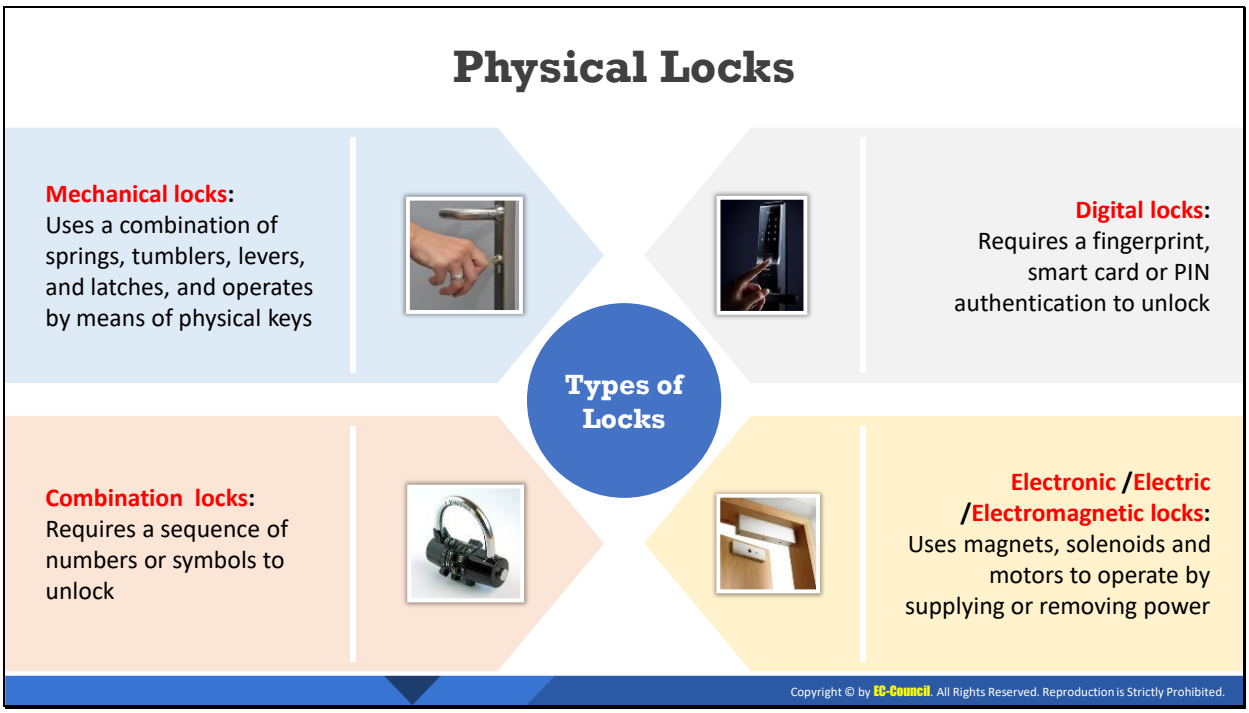
- **The plant's security officers/supervisors**: Their responsibilities include training and monitoring the activities of the guards; assisting guards during crisis situations; handling crowds; and maintaining the keys, locks, lights, greenery, etc. of the facility.
- **Safety officers**: Their responsibilities include implementing and managing safety-related equipment installed around the facility and ensuring the proper functioning of this equipment.
- **Chief information security officer (CISO)**: In the past, it was common for the CISO of an organization to be an extremely technically competent individual who has held various positions with an enterprise security function or even has a networking or systems background. Today, a CISO is required to be much more than technically competent. The modern CISO must have a diversified set of skills to successfully dispatch their duties and establish the appropriate level of security and security investment for their organization.

Continuous training for security personnel can provide great benefits and an effective team for the organization. Regardless of the position, security-related personnel should be selected based on the experience and qualification required for the job. Executives should thoroughly evaluate the personnel's past experiences and, based on this information, provide adequate training to fill the gap between the ability and skills necessary for the job.

An organization should train newly hired security personnel in the following areas:

- Organizational culture, ethics, and professionalism
- Security policies and procedures
- Policy enforcement
- Trespassers and crowd management
- Handling emergency situations
- Human and public relations
- Patrolling procedures
- Managing workplace violence
- First aid and medical assistance
- Fire prevention
- Vehicle traffic management
- Handling foreign guests, invitees, etc.
- Report writing

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Physical Locks

Various types of locking systems are available to improve the restriction of unauthorized physical access. The organization should select an appropriate locking system according to their security requirements.

The following are the different types of locks.

- **Mechanical locks**: These provide an easy method to restrict unauthorized access in an organization. Mechanical locks come with or without keys. There are two types of mechanical locks.
  - **Warded lock**: A warded lock contains a spring-loaded bolt attached to a notch. A key inserted into the notch moves the bolt backward and forward. Only the correct key can be inserted into the notch, which blocks incorrect keys.
  - **Tumbler lock**: A tumbler lock consists of metal pieces inside a slot in the bolt. This prevents the bolt from moving. A correct key contains grooves that allow the bolt to move by raising the metal pieces above the bolt. Tumbler locks are further classified into pin tumbler, disk tumbler, and lever tumbler locks.
- **Digital locks:** Digital locks require fingerprints, smart cards, or keypad PINs to unlock. It is easy to handle and does not require keys, eliminating the chance of forgetting or losing keys. It provides automatic locking for doors. The user only has to use their fingerprint impression, swipe their smart card, or enter the PIN to unlock it.
- **Electric/electromagnetic locks**: Electric locks or electronic locking systems operate on electric current. Locking and unlocking are achieved by supplying and eliminating power. The locks are activated or deactivated mainly using magnets or motors. They do not require keys to be maintained for the locking system.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

An electromagnetic lock or magnetic lock consists mainly of an electromagnet and an armature plate. The locking device can be of two types: fail safe and fail secure. Fail secure locks remain locked even during power loss, whereas fail safe locks remain inactive when de-energized. The electromagnetic part may be placed on a door frame, and the armature plate may be placed on the door. The magnetic flux created by the electromagnet creates an attractive force towards the armature plate, which initiates the door closing process.

- **Combination locks:** These require the user to provide a combination of numbers and letters to unlock. Users may enter the combination sequence either through a keypad or by using a rotating dial that intermingles with several other rotating discs. Combination locks do not use keys for functioning.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

Concealed Weapon/Contraband Detection Devices

Contraband detection devices act as an important physical security control as they restrict undesirable activities and/or a person carrying contraband from entering the premises. Contraband refers to illegal materials such as explosives, bombs, and weapons, which should be banned from the premises. An attempt to enter the premises with contraband can be considered an act of terrorism. Contraband detection devices are able to detect such substances, even when they are covered by other objects.

Different types of devices are used to detect contraband materials; examples are handheld metal detectors, walkthrough metal detectors, and X-ray inspection systems.

- Walkthrough metal detectors are mainly used in airport terminals, schools, sports stadiums, etc. They help check people who have admission to certain areas. Furthermore, walkthrough detectors should be maintained and properly monitored. They should be deployed at each entry point of the organization.

Figure 4.6: Walkthrough metal detectors

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

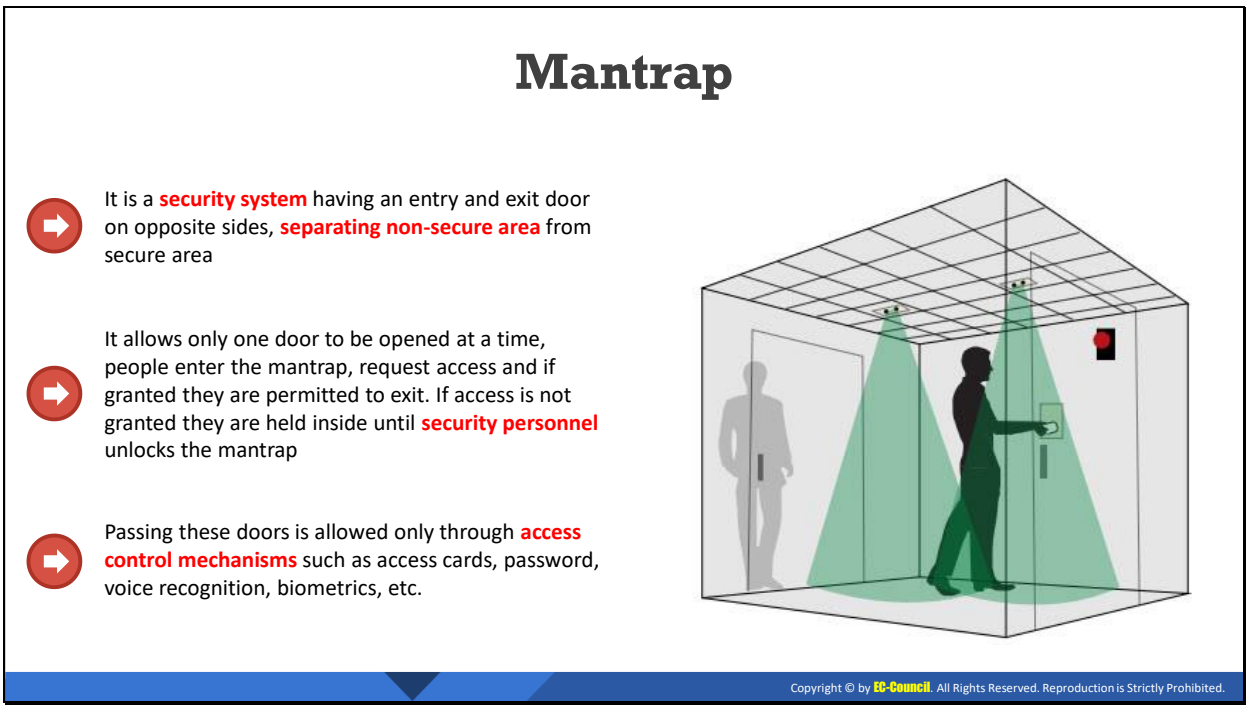
- Handheld metal detectors allow people to be screened more closely and detect suspicious objects. Handheld detectors are used in most places where walkthrough detectors are used.

Figure 4.7: Metal detectors

- X-ray inspection systems are easy to handle and use. They use X-rays instead of visible light to screen objects.

Figure 4.8: X-ray inspection system

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Mantrap

A mantrap is another type of physical access security control that is used for catching trespassers. It is most widely used to separate non-secure areas from secure areas and prevents unauthorized access. It is a mechanical locking mechanism consisting of a small space with two sets of interlocking doors. The first set of doors must close before the second set opens. User authentication at mantrap doors is performed using smart cards, keypad PINs, or biometric verification. It operates automatically, is useful in authorizing visitors, reduces the manpower required for security systems, and guarantees the safety of the organization.

Working of Mantraps

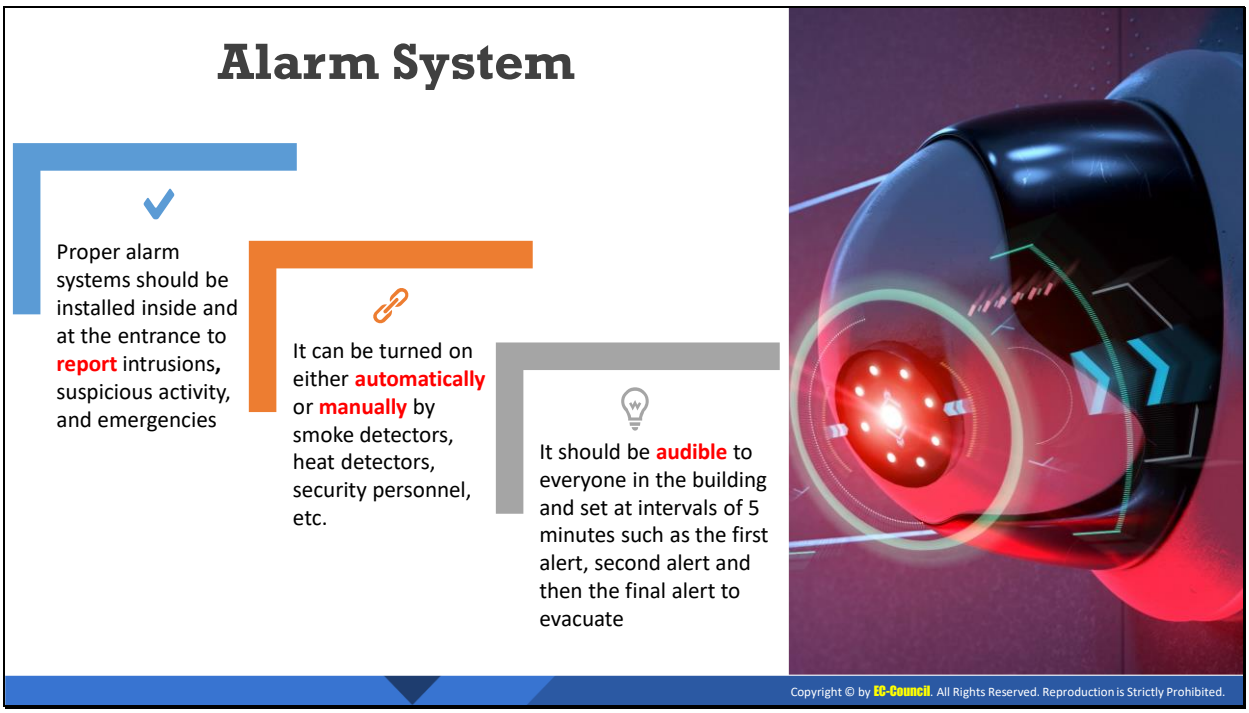
- **Step 1:** The mantrap authenticates the person attempting access.
- **Step 2:** The first door opens after authentication. The person walks in.
- **Step 3:** The first door closes soon after the person enters the room. Now, the person is locked inside the room. This signals the unlocking of the second door.
- **Step 4:** The second door opens with the person walking out of the room. The first door is automatically locked soon after the second door opens.
- **Step 5:** The second door enters the locked state soon after the person walks out.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Warning Signs

Warning signs are generally used to restrict unauthorized access in an organization. Warning signs are placed at entrance points, boundaries of the locality, and sensitive areas. They should be visible to users such that people understand prohibited areas and avoid entering them. Warning signs also help organizations prevent a large number of people from entering sensitive areas. They are generally placed in all sensitive areas that have a threat of damage to assets or life or disclosure of information. For example, warning signs are typically placed on electrical fences because unknowingly touching the electric fence may pose a threat to life. Examples of warning signs are “RESTRICTED AREA,” “WARNING,” “CAUTION,” “DANGER,” and “BEWARE.”

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Alarm System

Alarms are used to draw attention in case of a breach or an attempted breach. Alarm sounds can be of different types based on the facility; examples include sirens, flash lighting with a sound, emails, and/or voice alerts. The organization should divide large facilities such as buildings, floors, sections, and offices into small security zones; depending on their significance, the appropriate alarm system should be installed. Security zones that store high-priority data are given multilevel security systems such as access restriction with access control devices, biometrics, surveillance, locks, and alarms to draw attention in an event of intrusion. Alarms can be turned on either automatically or manually by smoke detectors, heat detectors, security personnel, etc. They should be audible to everyone in the building and set with three alerts to evacuate in intervals of 5 min. Organizations should have a proper power backup for alarm systems so that they work in emergencies and during power shutdowns. All wiring and components of an alarm should be protected from tampering, and the alarm box should be concealed with proper locks and limited access. Proper management and regular assessments of the alarm system should be performed with emergency drills.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Video Surveillance

Video surveillance refers to monitoring activities in and around the premises using closed-circuit television (CCTV) systems. Video surveillance is considered an important component of physical security. These systems protect an organization's assets and buildings from intruders, theft, etc. A CCTV system is used as part of the organization's security system. It covers a large area and is often placed near gates, the reception, hallways, and at the workplace. It captures footage of illicit activities inside the premises and helps monitor activities inside, outside, and at the entrance. CCTV systems are even programmed to capture motion and initiate an alarm whenever a motion or an object is detected. They help identify activities that need attention, collect images as evidence, and aid in an alarm system. The devices used for video surveillance should be automatic, powerful, and capable of pan/tilt/zoom to capture the action and store them for later review.

Many aspects need to be considered for the installation, management, and maintenance of a video surveillance system in an organization; these include the camera, lens, resolution, recording time, recording equipment, cabling, monitoring system, storage devices, and centralized control system/equipment. Recording activities through CCTV and storing this footage for reference can also help facilities provide evidence in a court of law. It is also important to decide the type of lens, resolution, and area the camera should cover, and the time and date of the footage should be recorded. Another important aspect is the storage of video recordings and the storage duration. The organization must decide what will happen to old video recordings and how they will be disposed of.

The following are a few considerations for video surveillance systems:

- Install surveillance systems at the parking lot, reception, lobby, and workstation.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- Place output devices such as printers, scanners, and fax machine in public view and under surveillance.
- Integrate surveillance with an alarm system.
- Establish a policy for the duration for which recorded videos should be kept and later disposed.
- Store all devices in secure locations with limited access.
- Use proper disposal procedures such as content deletion, overwriting, and physical destruction.

The following are the different types of CCTV cameras available commercially.

- **Dome CCTV:** Mainly used for indoor security and surveillance purposes, dome CCTV cameras are built as dome-shaped devices to prevent any damage to the camera or destruction. It is impossible to locate the direction to which such cameras are moving; thus, they allow for observing areas at a wide angle and cover larger areas. Speed dome CCTV camera units provide a facility with pan/tilt/zoom and spin features, allowing the operator to move the camera according to their need.

Figure 4.9: Dome CCTV camera

- **Bullet CCTV:** Bullet CCTV cameras are used for indoor and outdoor surveillance. They are generally placed in protective covers that keep away dust, rain, or any other disturbance. A bullet CCTV camera usually has a long, cylindrical, and tapered shape that facilitates long-distance surveillance.

Figure 4.10: Bullet CCTV camera

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **C-mount CCTV:** A C-mount CCTV camera consists of detachable lenses, which provide surveillance with a coverage distance of more than 40 ft. Other CCTV camera lenses provide a coverage distance of only 35–40 ft. The C-mount allows different lenses to be used according to the distance to be covered.

Figure 4.11: C-Mount CCTV camera

- **Day/night CCTV:** Day/night CCTV cameras are commonly used for outdoor surveillance. They can capture images even in low light and darkness. These types of cameras do not require infrared illuminators to capture images. They can capture clear images under glare, direct sunlight, reflections, etc.

Figure 4.12: Day/night CCTV camera

- **Infrared night-vision CCTV:** Infrared night-vision CCTV cameras are commonly used for outdoor surveillance and can capture images in complete darkness. Infrared LEDs are used for areas having poor lighting.

Figure 4.13: Infrared night-vision CCTV camera

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- **Network/IP CCTV:** Network/IP CCTV cameras are available as both wired and wireless models. They allow sending images over the Internet. A wireless IP camera is easier to install than a wired camera because the former does not require any cabling.

Figure 4.14: Network/IP CCTV camera

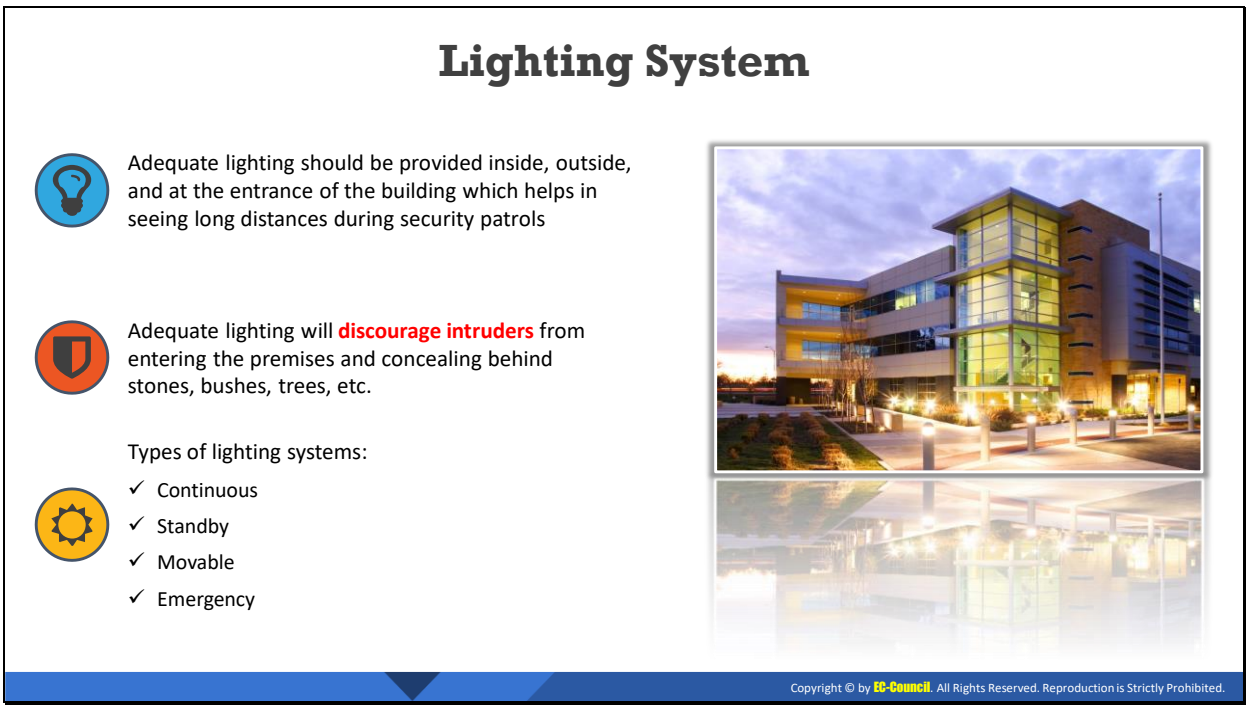
- **Wireless CCTV:** Wireless CCTV cameras are easier to install than wired cameras and use different modes for wireless transmission.

Figure 4.15: Wireless CCTV camera

- **High-definition CCTV**: High-definition CCTV cameras are mainly used in sensitive locations that require greater attention. They allow operators to zoom into a particular area.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

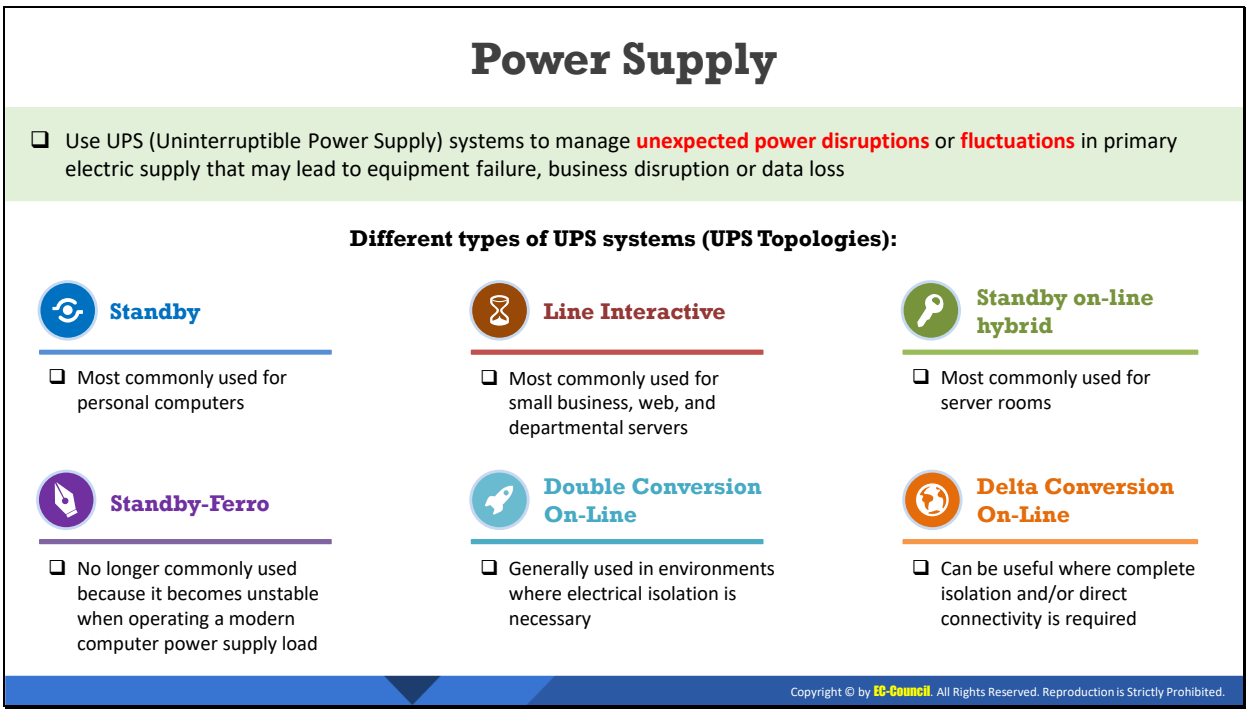


Lighting System

Security lighting is an important aspect of the physical security of a facility. If an organization has not implemented an adequate lighting system in and around its premises, the function or performance of all other security measures can be drastically degraded. For example, if the organization does not have lighting at rear corners, near bushes, plants, parking, and near surveillance cameras, then it is difficult to find people or objects hidden in these locations. With poor lighting, it is difficult to identify people entering the premises, and an intruder may act as an employee or use tricks to circumvent the security systems. The lighting systems to install in an area depend on the layout and sensitivity of the area. Alternate power systems such as generators should be installed to handle power failures and emergencies.

- **Continuous lighting**: Continuous lighting refers to fixed sets of lights arranged such that they provide continuous lighting to a large area throughout the night.
- **Standby lighting**: Standby lighting is used whenever any suspicious activity is detected by security personnel or by an alarm system. These systems operate either manually or automatically.
- **Movable lighting**: Movable lighting is a manually controlled lighting system that provides lighting at night or only when needed. These systems are normally used as an extension of a continuous or standby lighting system.
- **Emergency lighting**: Emergency lighting is used mainly during power failures or when other regular lighting systems fail to operate properly.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Power Supply

Facilities may suffer blackouts or power outages that could make systems inoperable unless appropriate alternative power management capabilities are implemented. Power outages could impact the ability to provide IT services as expected as well as the ability to provide physical security. Power spikes, surges, or blackouts could result in excessive or insufficient power and could damage equipment.

Consider the following security measures to handle blackouts or power outages.

- Be prepared for power fluctuations.
- Use an uninterruptible power supply (UPS) to manage power outages.
- Safeguard systems from environmental threats.
- Protect systems from the adverse effects of static electricity at a workplace.
- Use plugging equipment properly.

A UPS allows computers to function properly during a power failure. It protects computers during fluctuations in the power supply as well. A UPS contains a battery that senses power fluctuations in the primary device. Users need to save all their data when the UPS senses a power fluctuation. The operator must provide procedures to follow at the time of power loss. A UPS is commonly used to protect computers, data centers, telecommunication equipment, etc.

The following are the different types of UPS include.

- **Standby:** Standby UPSes are the most commonly used type of UPS for personal computers. A standby UPS is an offline battery backup facilitating the maintenance of

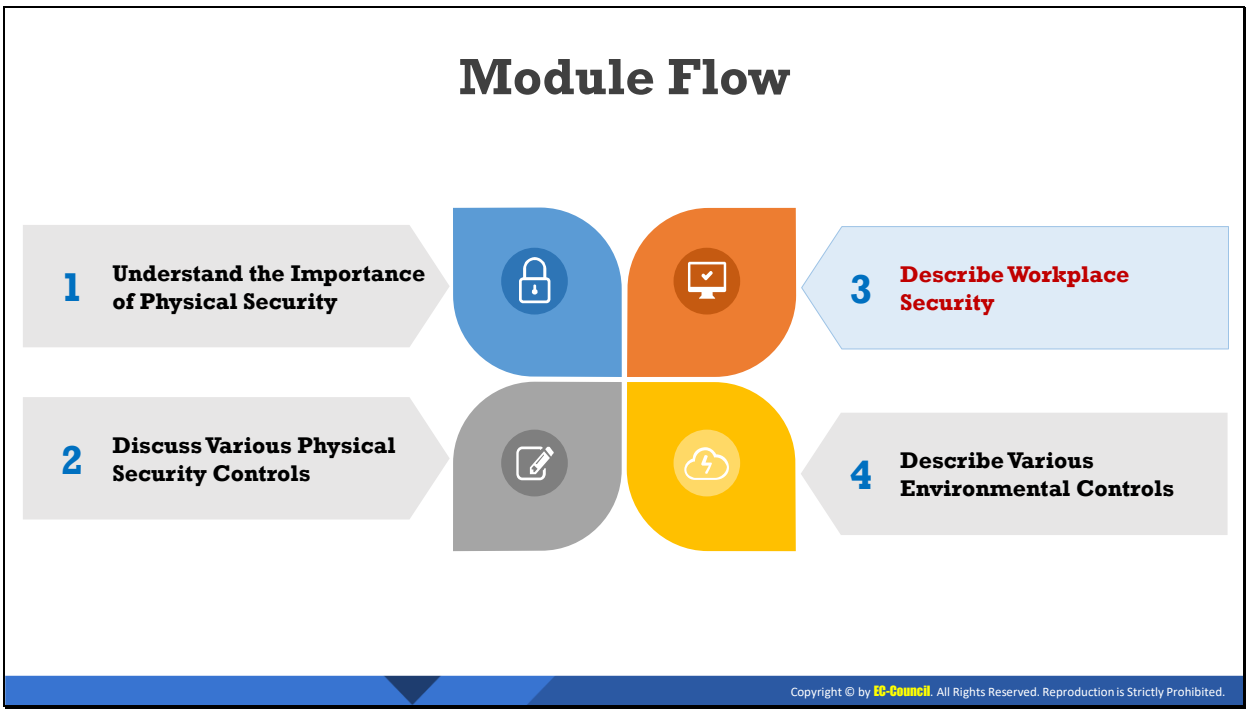
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

the primary device during a power fluctuation. A standby power supply contains AC-DC circuitry that connects to the UPS during a power fluctuation.

- **Line interactive:** Most commonly used for small business, web, and departmental servers, line interactive mainly handles continuous power fluctuations. This method of power supply needs very little battery usage.
- **Standby online hybrid:** Most commonly used for server rooms, standby online hybrid UPSes are mainly used to supply power below 10 kVA. They are connected to the battery during a power failure.
- **Stand by Ferro:** In this type of UPS, a Ferro resonant transformer is used for filtering the output. A standby Ferro UPS provides ample time for switching from the main power supply to battery power. This type of UPS is no longer commonly used because it becomes unstable when handling a modern computer's power load.
- **Double conversion online:** Generally used in environments where electrical isolation is necessary, a double conversion online UPS is used to supply power above 10 kVA. It provides an ideal electric output presentation, but its power components are subject to continuous wear, reducing its dependability. It exhibits a transfer time only during a large current load.
- **Delta conversion online:** A delta conversion online UPS can be useful when complete isolation and/or direct connectivity is required. It contains an inverter that supplies the load voltage. It can be used to supply power in the range between 5 kVA and 1 MW. It controls the power input performance and charging of the UPS battery.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

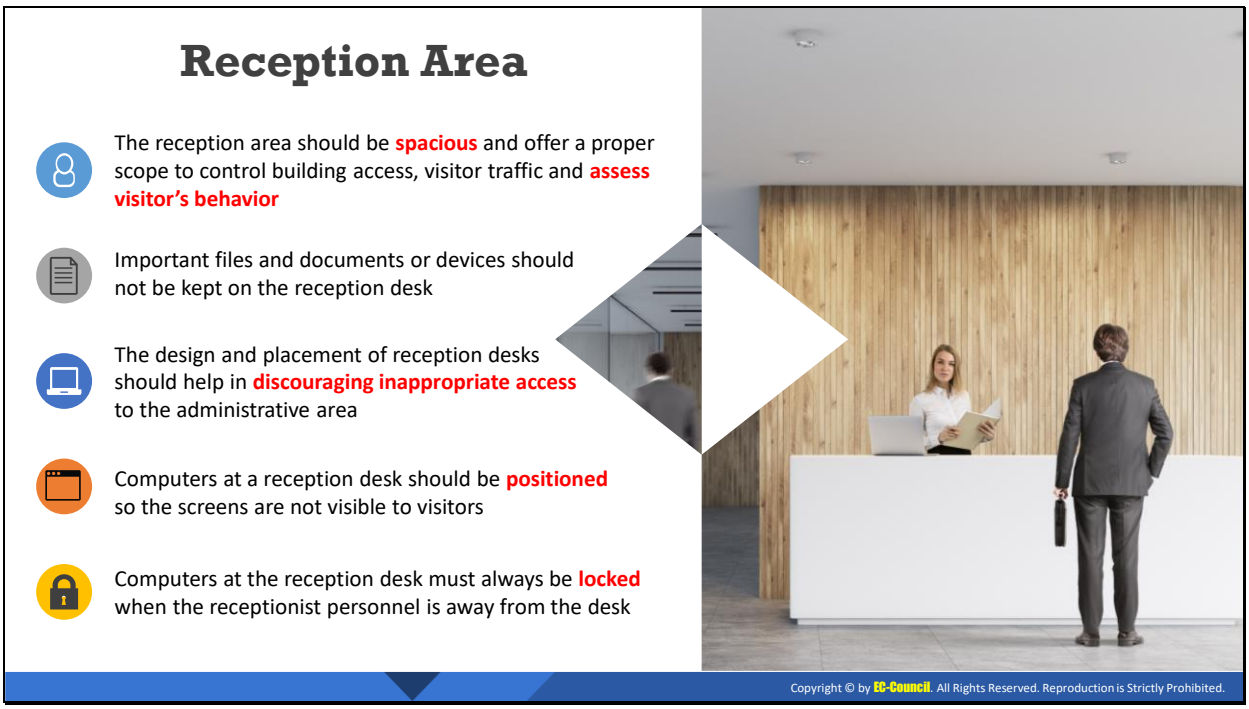
https://t.me/learningnets



Describe Workplace Security

This section explains workplace security in an office environment.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

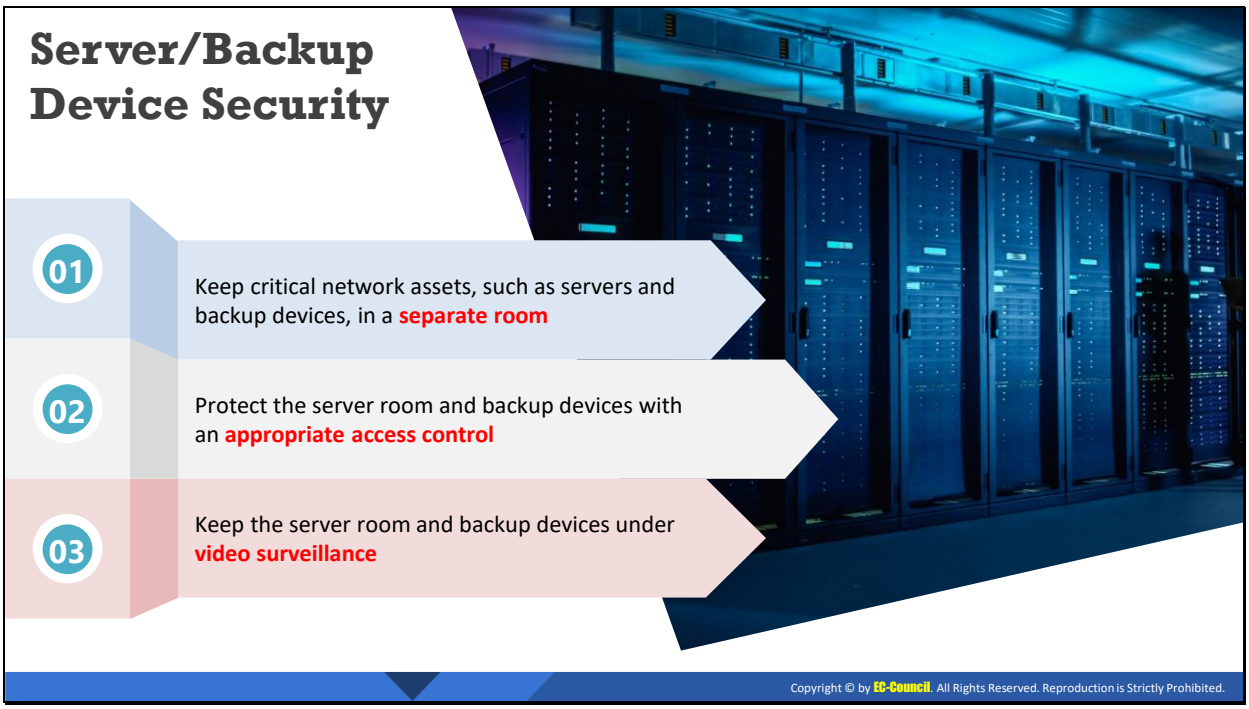


Reception Area

The reception area is the initial point of contact for an individual approaching the organization. The reception area can be vulnerable to physical security breaches as it provides easy access to strangers. Organizations often have regular visits from clients, the general public, invitees, etc. and require staff to greet, assist, and direct them. Receptionists should be able to recognize or identify any unusual behavior from people such as solicitors and peddlers, charity organizations, and ex-employees. The reception personnel should maintain eye contact and non-confrontational facial expressions or posture while meeting people. They should be proficient enough to handle emergency situations and follow procedures to call immediate attention, issue alarms, call for radio, administer first aid, etc.

The reception area should be spacious and should offer the scope to control building access and visitor traffic as well as assess visitor behaviors. Reception personnel should observe people entering the building. They should notice and record odd behavior from strangers. Benchmarks should be implemented to judge people arriving at the organization. Their intentions must be noted, and the personnel should identify whether a person is searching for someone or something. Important files and documents or devices should not be kept on the reception desk. The design and placement of reception desks should help in discouraging inappropriate access to the administrative area. Computers at a reception desk should be positioned so that the screens are not visible to visitors and must always be locked when the reception personnel is away from the desk.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



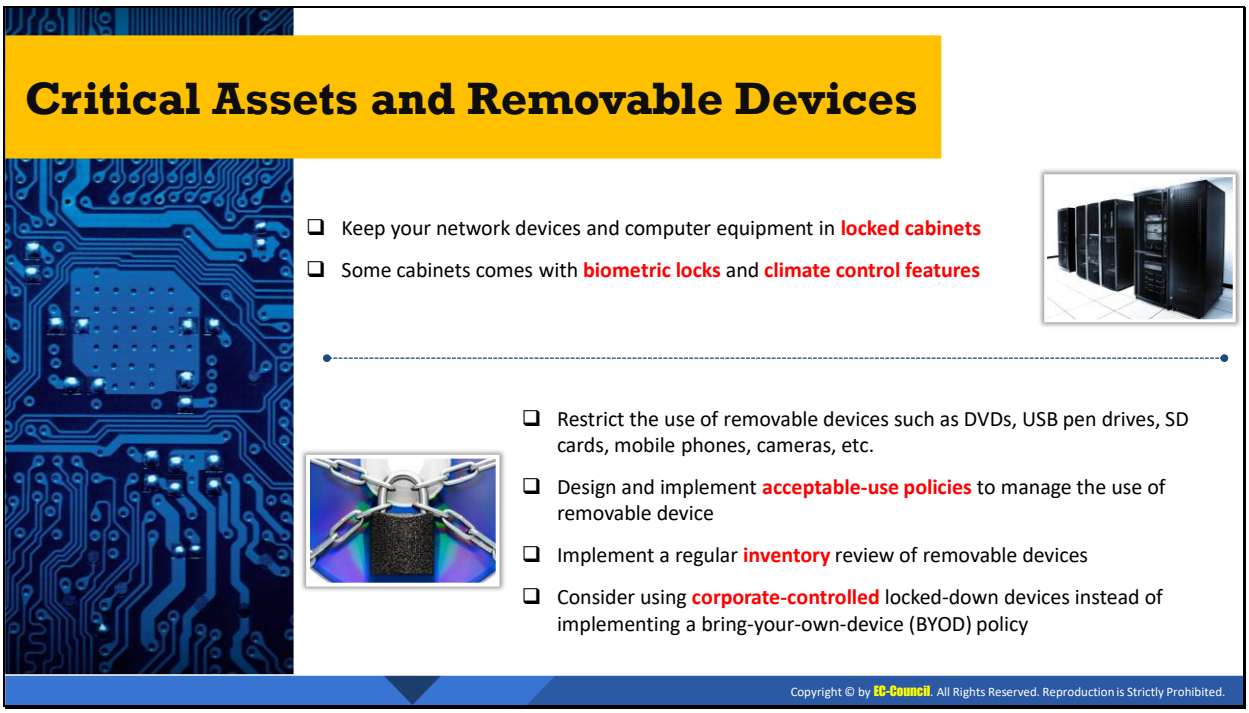
Server/Backup Device Security

An organization should consider the physical security of their critical servers and backup devices. Physical access to these devices should be restricted to only approved personnel.

The following are the typical physical security measures for server and backup devices:

- Keep the server and backup devices in a separate room. This reduces the accessibility of these devices for the public and unknown people.
- Mount CCTV, smart card, and biometric authentication to track and monitor unauthorized physical access to the server and backup devices.
- Use rack mount servers. This prevents attackers from stealing or damaging the servers.
- The server should be attached to a UPS that protects it from file damage or corruption due to temporary power loss.
- Keep the devices in locked drawers, cabinets, or rooms.
- Backup devices should be stored at off-site locations and secured.
- Discourage employees from taking backups on DVDs, USB drives, or external hard disks. Ensure that the backups are locked at all times in a drawer, safe, or separate room.
- Do not allow employees to leave an area while carrying a backup device. Use motion sensing alarms to detect the movement of any backup device.
- Implement full disk encryption on backup devices.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

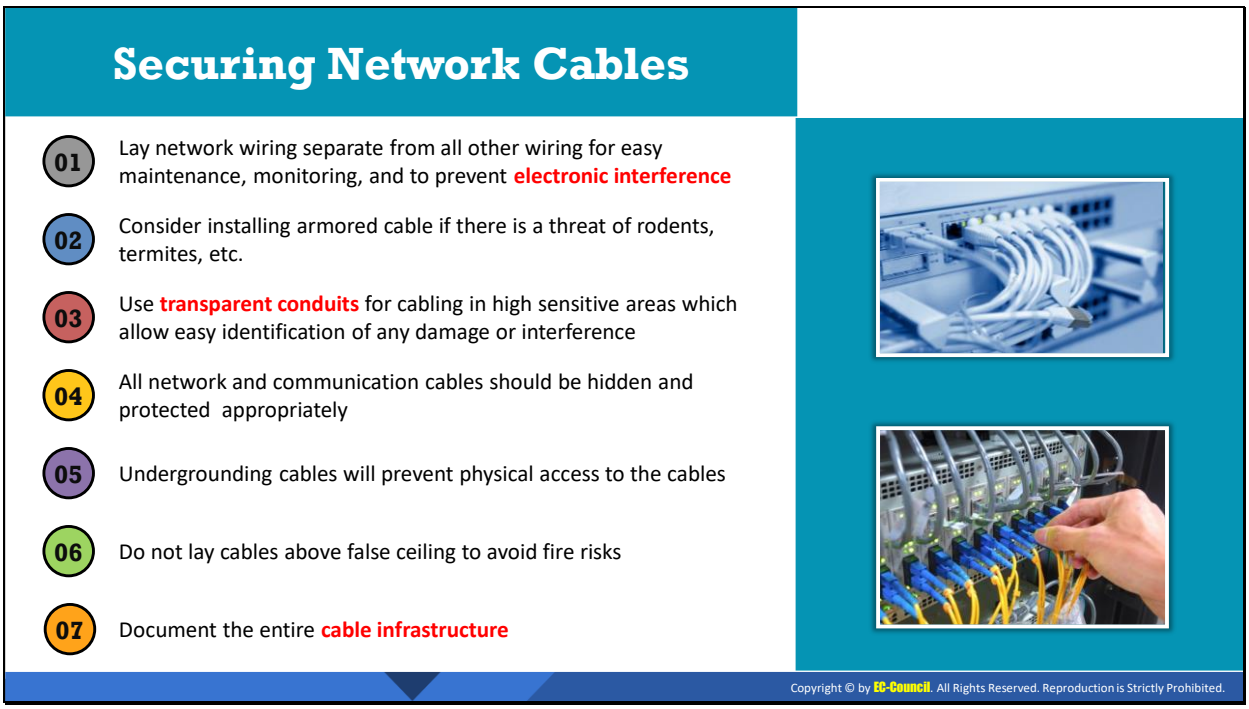


Critical Assets and Removable Devices

An organization should always pay attention to the security of its server and backup storage devices. At the same time, the organization should not ignore the security of other critical assets such as workstations, routers and switches, printers, other network equipment, and removable devices. The organization should employ all the physical security measures of server/backup devices for critical assets and removable devices. Furthermore, organizations must keep their network devices and computer equipment in locked cabinets. Some cabinets come with biometric locks and climate control features. Restrict the use of removable devices such as DVDs, USB pen drives, SD cards, mobile phones, and cameras. Design and implement acceptable-use policies to manage the use of removable devices. Implement a regular inventory review of removable devices. Consider using corporate-controlled locked-down devices instead of implementing a bring-your-own-device (BYOD) policy.

- **Workstations**: Workstations at unoccupied desks, empty offices, reception desk, etc. are relatively more vulnerable to physical security breaches. Disconnect or remove such unoccupied workstations or otherwise lock the doors to the room where the workstation is located.
- **Routers and switches**: Keep these critical network devices in locked rooms.
- **Printers**: Like servers and workstations, printers can store important information, should be bolted down, and installed at separate locations.
- **Removable devices**: Portable removable devices such as laptops, handheld computers, mobile devices, SD cards, USB, and Bluetooth devices can pose physical security risks. Keep these devices in a drawer or safe, or permanently attach a cable lock.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Securing Network Cables

Network cable security is often overlooked as an aspect of physical security. The organization should consider the importance of cable security before planning and installing any cabling. Network cabling should be neat; else, an organization can suffer from unplanned downtime. With flawed or insecure network cabling, an attacker can easily access sensitive information by bypassing other security controls. The risks associated with network cabling are wiretapping, physical damage, and theft.

The following are the considerations for securing network cabling:

- Lay network wiring separately from all other wiring for easy maintenance, monitoring, and preventing electronic interference.
- Consider installing armored cable if there is a threat of rodents, termites, etc.
- Use transparent conduits for cabling in highly sensitive areas to allow the easy identification of any damage or interference.
- All network and communication cables should be hidden and protected appropriately.
- Undergrounding cables prevent physical access to the cables.
- Do not lay cables above a false ceiling to avoid fire risks.
- Access to cabling pathways and spaces should be restricted to authorized personnel only.
- Create redundancy to avoid a single point of failure in case of a disaster.
- Document the entire cable infrastructure.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Types of Cable Used in Network Cabling

- **Unshielded Twisted Pair (UTP) Cable**

  A UTP cable reduces crosstalk and interference between pairs of wires but is prone to wiretapping. An attacker can easily tap the information transmitted through network cables.

  - **Advantages**
    - Easy to install
    - Suitable for domestic and office Ethernet connections
  - **Disadvantages**
    - Highly susceptible to electromagnetic and radio-frequency interference
    - Less commonly used for long-distance networking

- **Shielded Twisted Pair (STP) Cable**

  In an STP cable, each pair of wires is individually shielded with foil. It is less susceptible to external interference as the shielding absorbs all the EMI and RFI signals.

  - **Advantages**
    - Immune to crosstalk and interference
    - Ensures secure data transmission
  - **Disadvantages**
    - More expensive than UTP cables
    - More difficult to install than UTP cables

- **Fiber-optic Cable**

  A fiber-optic cable is made of glass or plastic. Fiber-optic cabling is the least susceptible to wiretapping threats.

  - **Advantages**
    - Can carry information over relatively great distances
    - Immunity to electromagnetic interference
    - No crosstalk
  - **Disadvantages**
    - Limited physical arc of the cable
    - Highly expensive
    - Need for optical transmitters and receivers

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- **Coaxial Cable**

  A coaxial cable is made of a single copper conductor at its center. A plastic layer insulates the center conductor and a braided metal shield, which prevents interference from fluorescent lights, motors, etc.

  - **Advantages**
    - Can carry information over relatively great distances
    - Moisture resistant
  - **Disadvantages**
    - Does not bend easily and difficult to install

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Securing Portable Mobile Devices

The use of portable mobile devices in an organization has increased over the past few years. The risk of physical security threats to these devices has also increased. These devices are often vulnerable to physical threats such as theft, loss, damage, and resale. The organization should take proper care to handle any security incidents related to these devices.

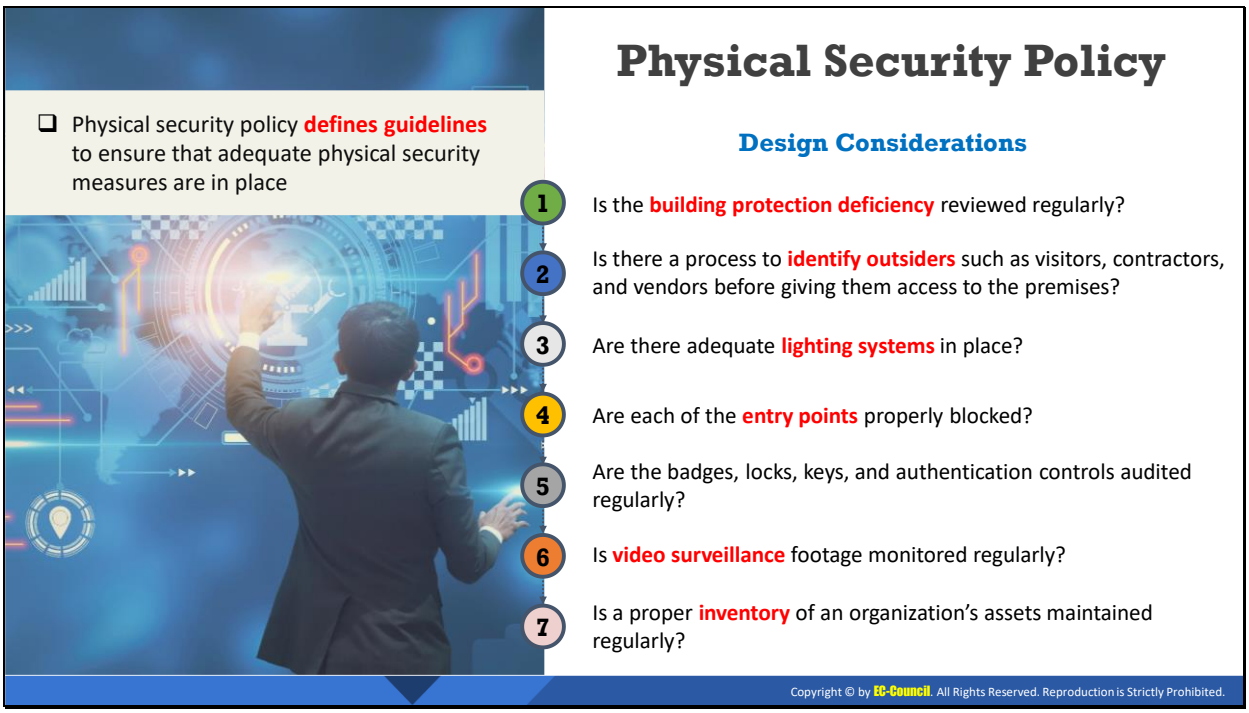
- Apply all security measures common to network devices such as servers, backup devices, and portable devices.
- Physically secure the mobile device location.
- Apply proper access control procedures for these devices.
- Use cables and locks to safeguard laptops.
- Encrypt hard drives to make it impossible to access files when a drive is lost or stolen.
- Install anti-theft software that can remotely lock and track devices using a data connection.
- Install device tracking software that can assist in recovering stolen/lost devices.
- Enable or install a remote wipe feature to erase data stored in devices.
- Do not lend a device to third parties.
- Do not leave a device unattended in public places.
- Label the device or attach a sticker with the name and contact details of the user so that the device can be returned if lost.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- Enable the lockout option so that the device is locked when consecutive unsuccessful attempts to login are made.
- Use a docking station that permanently affixes the laptop to the desktop and also locks the laptop securely in one place.
- Use security gadgets such as motion detectors and alarms to issue alerts when the laptop is moved without authorization.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



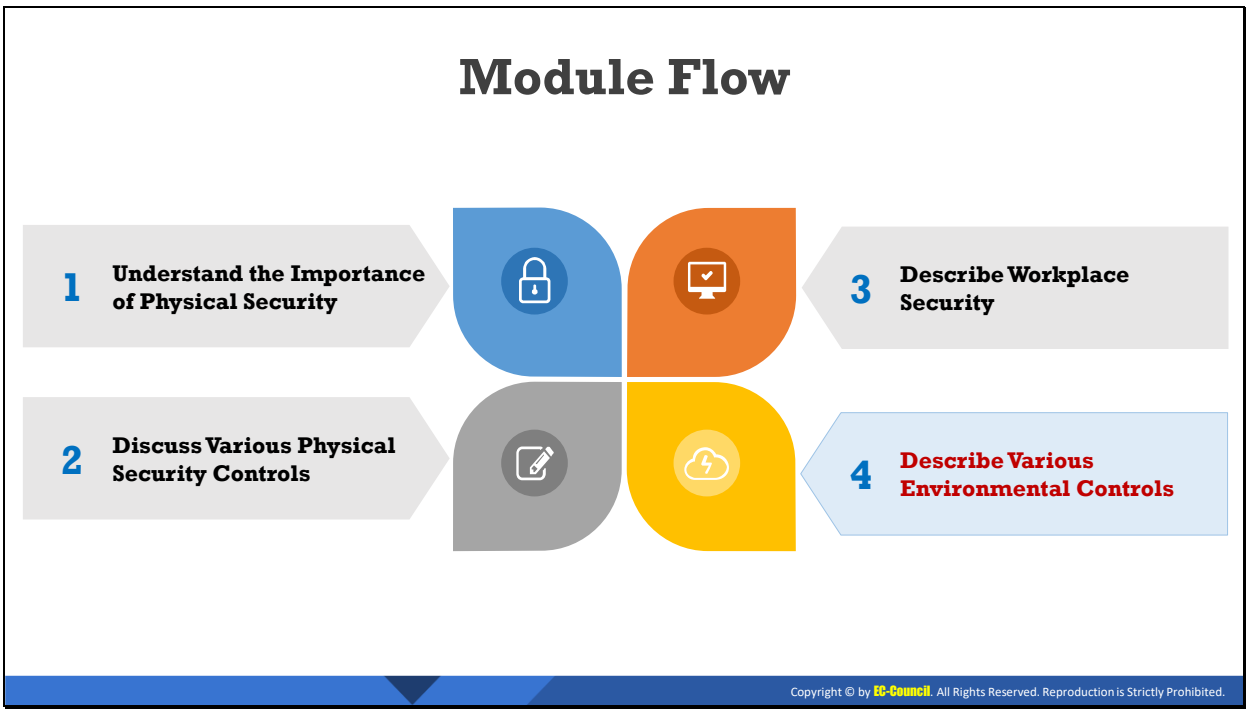
Physical Security Policy

The physical security policy defines guidelines to ensure that adequate physical security measures are implemented. It is the security provided in terms of physical assets, which can be damaged physically. In IT organizations, where large amounts of physical assets are handled, the assets are prone to damage during installations or transfer from offshore to local locations. Care must be taken in terms of the frequency of monitoring and analyzing risks, and the training provided to the people handling or working with the physical assets must be monitored. Designing a physical security policy helps an organization maintain certain norms to be followed by employees to reduce the probability of loss.

Design Considerations

- Is the building protection deficiency reviewed regularly?
- Is there a process to identify outsiders such as visitors, contractors, and vendors before granting them access to the premises?
- Are adequate lighting systems installed?
- Are each of the entry points properly blocked?
- Are badges, locks, keys, and authentication controls audited regularly?
- Is video surveillance footage monitored regularly?
- Is the inventory of the organization's assets maintained regularly?

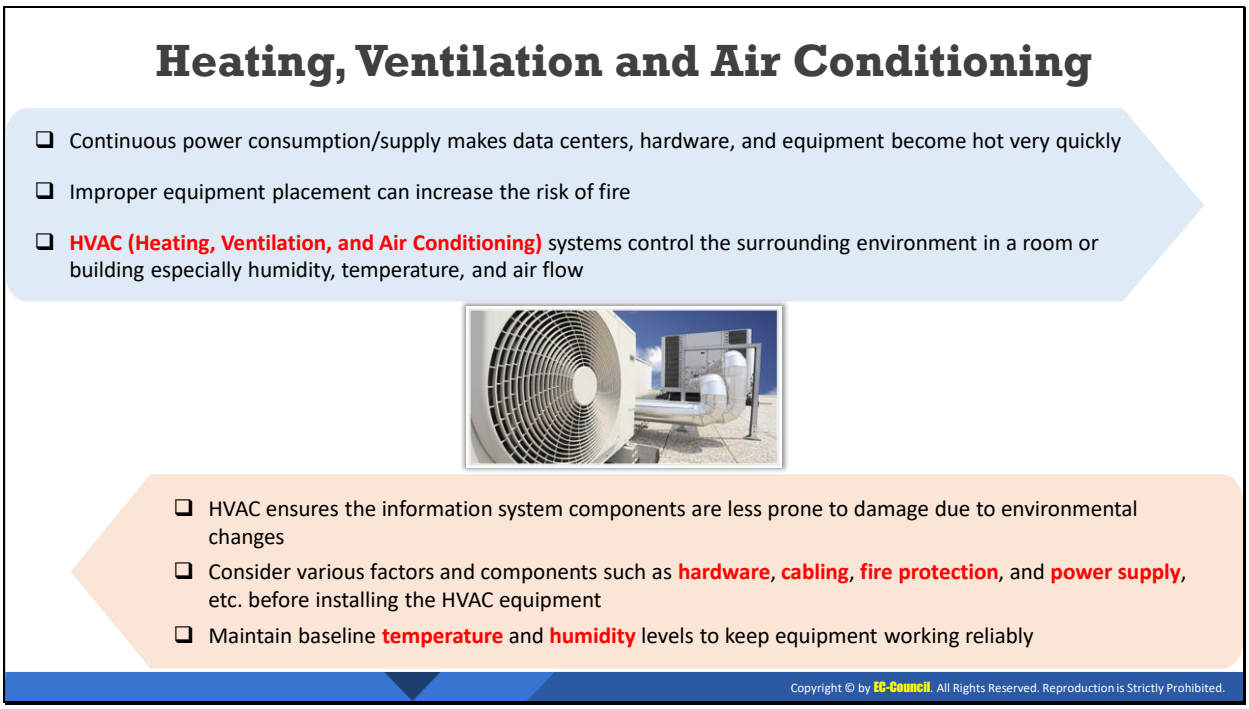
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Describe Various Environmental Controls

This section explains various environmental controls.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Heating, Ventilation, and Air Conditioning (HVAC)

Continuous power consumption/supply can cause data centers, hardware, and equipment to become hot very quickly. Furthermore, improper equipment placement can increase the risk of fire. The HVAC is a special system that controls the environment in a room or building, especially the humidity conditions of the air and ventilation. It is deployed to maintain comfortable temperatures in a room so that the hardware is not affected by moisture and changes in the air. In these controlled conditions, the hardware and components are also safer and less prone to damage due to environmental factors. The HVAC also purifies the air in rooms and removes smoke, odor, heat, and dust particles. An environment where the air is odor-free and clean and the humidity is controlled provides a good atmosphere for the people working with that organization. These ventilation systems are desired mostly in medium- to large-scale organizations that use heavy equipment and employ a large number of people. A pre-programmed sensing device is used to check for changes in the temperature, and the HVAC acts accordingly. The HVAC can also be manually controlled. Before installing the HVAC equipment, the organization must consider various factors and components such as hardware, cabling, fire protection, and power supply. Baseline temperature and humidity levels must be maintained to keep equipment working reliably. Equipment that emits hot or cold air should be continuously monitored.

When a refrigeration component is added to an HVAC system, it is known as an HVAC&R or HVACR (heating, ventilating, and air conditioning & refrigeration) system.

Types of HVAC Systems

- **Heating and air-conditioning split system:** The traditional and most commonly used HVAC system is the heating and air-conditioning split system. The components of this

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

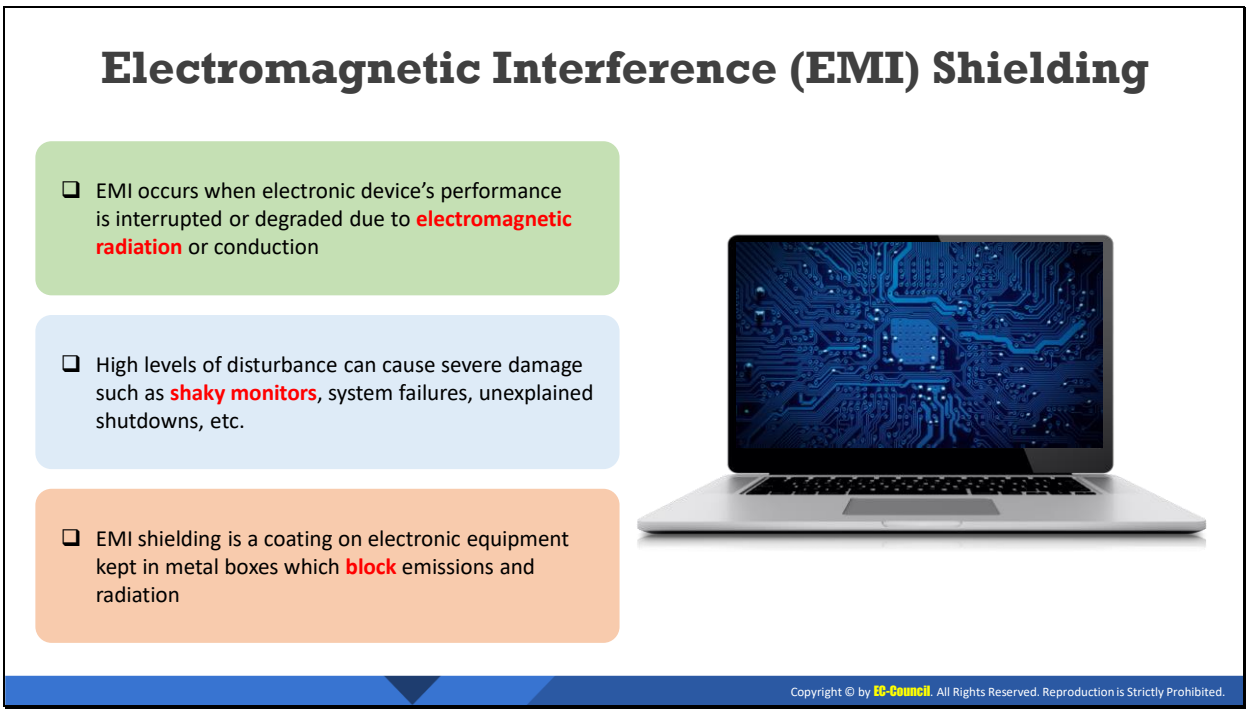
system may be found both inside and outside the building. HVAC split systems have the following components:

- An air conditioner to cool the refrigerant
- Furnaces, a fan, or an evaporator coil for converting the refrigerant and circulating the air
- A duct to allow air flow throughout the building
- Air-quality fittings such as air cleaners and air purifiers

- **Hybrid heat split system:** This is an advanced version of a split system having better energy efficiency. In this system, the heat pump realizes an electrically fueled HVAC instead of gas furnace heat. A typical hybrid heat split system includes the following components:
  - A heat pump to cool/heat the refrigerant
  - Furnaces or an evaporator coil to convert the refrigerant and circulate the air
  - A duct to allow air flow throughout the building
  - Controls or a thermostat as an interface to control the system
  - Air-quality fittings such as air cleaners and air purifiers
- **Duct-free split heating and air-conditioning system:** Most commonly used in locations where traditional split systems cannot be used, a typical duct-free split system includes the following components:
  - An air conditioner to cool the refrigerant
  - A fan coil to convert the refrigerant and circulate the air
  - Refrigerant tubing and wires to connect the outdoor unit to the fan coil
  - Controls or a thermostat as an interface to control the system
  - Air-quality fittings such as air cleaners and air purifiers
- **Packaged heating and air-conditioning system:** This is the most effect air-conditioning system and is used mainly in locations with adequate space for fixing all the components of a split system. Packaged units can be used in spaces that range from an entire building to one-room units. A packaged heating and air-conditioning system includes the following components:
  - Packaged products such as a heat pump or an air conditioner combined with a fan coil or an evaporator coil in a single unit
  - Controls or a thermostat as an interface to control the system
  - Air-quality fittings such as air cleaners and air purifiers.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



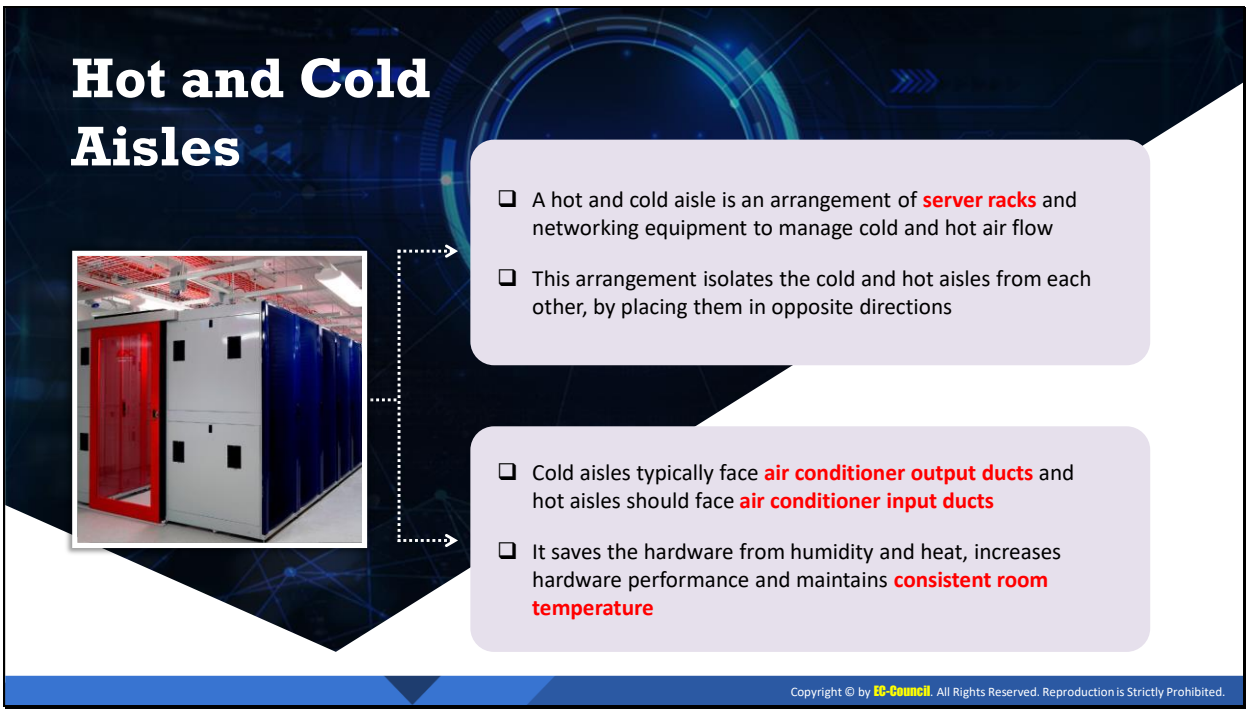
Electromagnetic Interference (EMI) Shielding

Electromagnetic radiation emitted from different electronic devices interferes with surrounding devices and causes problems with their functioning. High levels of disturbance can cause severe damage such as shaky monitors, system failures, and unexplained shutdowns. EMI shielding is the practice of coating electronic equipment with metals so that electromagnetic waves do not interfere with other devices or the field is blocked with certain materials. EMI shields separate one part of the equipment from another.

Shielding uses materials such as metals or metal foams. An electric field produces a charge on the conducting material, applying an electromagnetic field on a conductor. The conductor produces another charge, which cancels the effect of the electric charge externally applied on it. This causes no change in the conducting material. When the electric field is applied to the material, it produces eddy currents (currents that flow within a material in closed loops). These currents cancel the effect of the magnetic field. In this manner, the shielded material is protected from outside effects or disturbances.

For organizations that use heavy equipment, electronic hardware interference is a problem, and EMI shielding is needed for all devices in these types of environments. Many industries such as the telecommunication and healthcare industries prefer to use EMI shielding.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Hot and Cold Aisles

Hot and cold aisles form a systematic arrangement of equipment to maintain air flow and to save energy. Many organizations follow the hot and cold aisle alignment, which is mostly used in server rooms, data centers, etc. where heavy electronic equipment is used.

Racks of heavy equipment or servers are arranged so that the fronts of the equipment face the cold air from air conditioners. The backs of the equipment face the back of the next rack of equipment. This arrangement is followed for all the equipment in the room, pushing the hot air from the back of the equipment to one end of the room. The cooling conditions are kept so that the hot air exiting the equipment is sucked out and does not mix with the cool air inside the room. Depending on convenience, the cooling system is placed below or above the room. Cold aisles typically face air-conditioner output ducts, and hot aisles face air-conditioner input ducts. This protects the hardware from humidity and heat, increases hardware performance, and maintains a consistent room temperature.

Cold Aisle: Advantages and Disadvantages

- **Advantages:**
  - Easy to implement as it does not require any supplementary architecture to expel air
  - Requires doors only at the end
  - Relatively less expensive
  - Can easily fit into an existing data center in terms of aspects such as power and network distribution
  - Can be used with a raised floor supply space

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

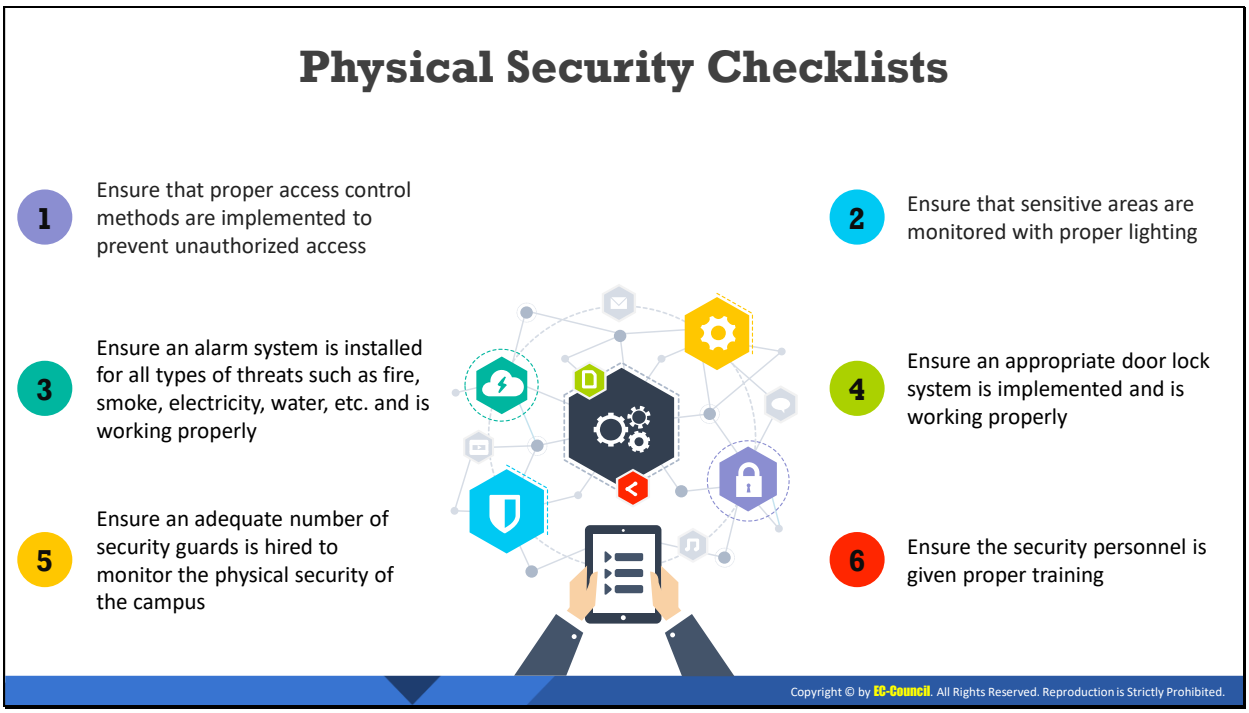
- Controls the air supply to match severe airflow

- **Disadvantages:**
  - Creates operational issues if low-density storage or communication racks are installed in the data-center space
  - Most cold aisles have ceilings immediately above the aisle, affecting fire and lighting design.
  - Air leaked from raised floors and openings under the equipment enters the air paths to the cooling units, affecting the efficiency of the system.

Hot Aisle: Advantages and Disadvantages

- **Advantages:**
  - Leakage from raised floor openings is passed over to the cold space
  - Relatively more effective
  - Works well in a slab environment by supplying an adequate volume of air and covering the exhaust air
  - Provides cooling to general data-center space
  - Perfect distribution of air throughout the space
- **Disadvantages:**
  - Always requires additional space for the flow of air from the hot aisle to the cooling unit
  - Very expensive
  - Uncomfortable for technicians during maintenance work

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Physical Security Checklists

Physical security for an organization can be built in layers or implemented by following a defense-in-depth strategy. The organization should consider implementing all the physical security controls and measures to ensure defense-in-depth physical security.

The following checklist can help an organization ensure that they are implementing the proper security controls and measures.

- **Follow copyright rules and licensing restrictions:** The organization should enforce copyright rules and licensing restrictions to prevent outsiders or insiders from creating illegal copies of copyrighted software.
- **Store all removable and important items in a locker when not in use:** Employees should lock all sensitive information and important devices in a locker. They should not leave any important information unattended, as it may catch the eye of an attacker.
- **Keep sensitive areas under surveillance:** The organization should ensure security for sensitive areas such as server rooms. CCTV surveillance and guards may be employed to maintain security in sensitive areas. The organization should enforce 24 × 7 surveillance for these areas.
- **Always advise employees to swipe their card at the entrance:** Swiping ID cards at the entrance helps an organization audit the login details of employees in case of an incident.
- **Avoid keeping any combustible material in the workplace:** Always keep combustible materials away from the workplace. This ensures the safety of the employees, the information stored, and the devices stored inside the workplace.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **Always ensure company satisfaction:** Employ security measures that guarantee the satisfaction of the employees. The policies and procedures imposed by the organization should ensure compatibility with the company infrastructure. Physical security measures imposed should detect, report, correct, and prevent attacks.
- **Evaluate the physical security of the location:** Proper security ensures the security of the employees and the information in the organization. The security of the location can be enhanced by preventing attackers from entering the workstations and server rooms as well as authenticating each person using ID cards or biometrics. Other security measures include locking cabinets, doors and windows, proper surveillance using CCTV, and proper lighting.
- **Avoid disconnecting consoles from ports:** Disconnecting cables or consoles from ports will lead to a disconnection for the user. Cables should all be connected to the ports and working properly.
- **Use of alarms and sensors during fire, smoke, etc.:** The organization should ensure the proper use of sensors and alarms to detect fire or smoke on the premises. The organization may include sensors for devices to detect any attempt to take those devices out of the organization's premises.
- **Prevent damage to hardware and software:** Any damage to the hardware or software results in damage to the information systems in the organization. Damage to the hardware leads to damage to the electronic and mechanical systems used in data processing. Damage to the software leads to damage to the programs and instructions used for data development.
- **Avoid leaving any devices or important data in parking areas or cars:** Any unattended devices or data may attract attackers and lead to the loss of these valuable items or information. The organization should employ an adequate number of security guards to monitor all parked cars. Proper lighting must be installed to watch these areas clearly. Security cameras should be employed in sensitive areas, and the personnel accessing those areas should be logged.
- **Avoid storing confidential information on mobile devices:** Storing sensitive information in a mobile device is not recommended, as it is easy to manipulate the data stored in a mobile device. Attackers may gain access to mobile devices and then acquire all of its sensitive information.
- Ensure that proper access control methods are implemented to prevent unauthorized access.
- Ensure that sensitive areas are monitored with proper lighting.
- Ensure that an alarm system is installed for all types of threats such as fire, smoke, power loss, and flood and is working properly.
- Ensure that an appropriate door lock system is implemented and is working properly.

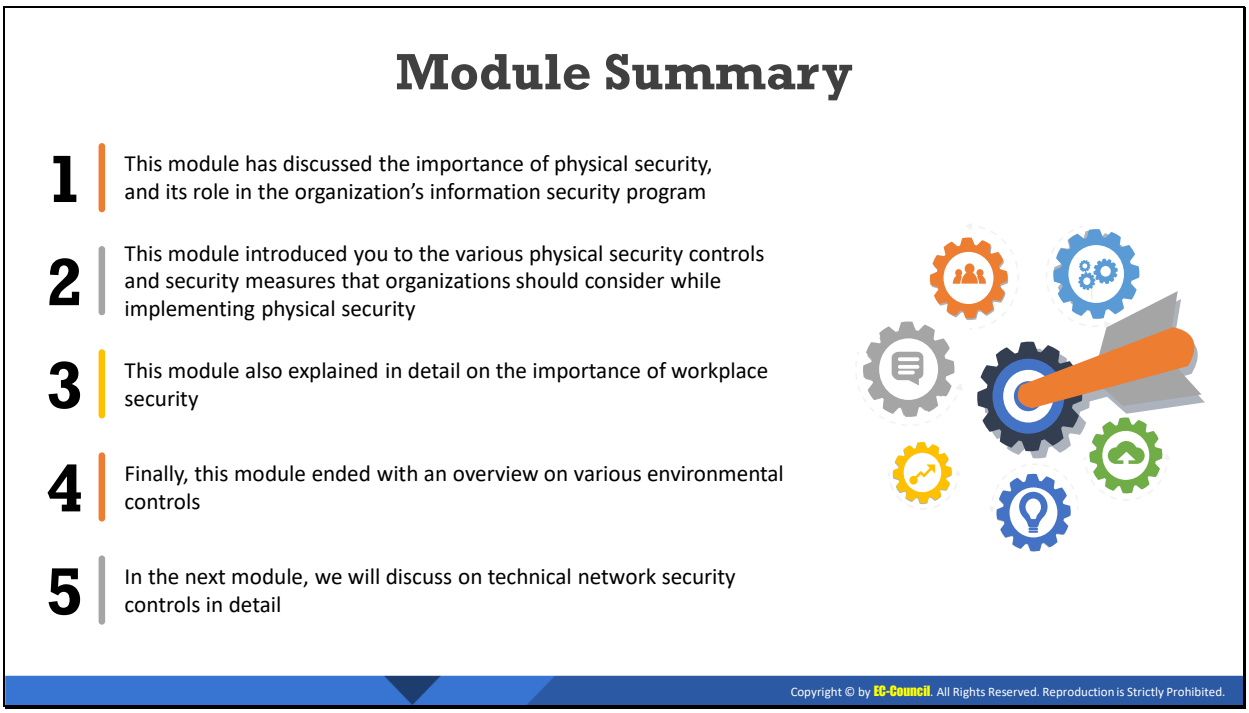
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- Ensure that an adequate number of security guards are hired to monitor the physical security of the campus.
- Ensure that the security personnel is properly trained.
- Ensure that the security personnel is hired from a trusted agency.
- Ensure that surveillance cameras are working properly and monitored regularly.
- Ensure that proper procedures are implemented for detecting and reporting physical security incidents.
- Ensure that employee contact information is maintained for use during emergencies.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Module Summary

This module discussed the importance of physical security and its role in an organization's information security program. Furthermore, this module introduced the various physical security controls and security measures that organizations should consider while implementing physical security. The module also explained in detail the importance of workplace security. Finally, this module presented an overview of various environmental controls.

In the next module, we will discuss technical network security controls in detail.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

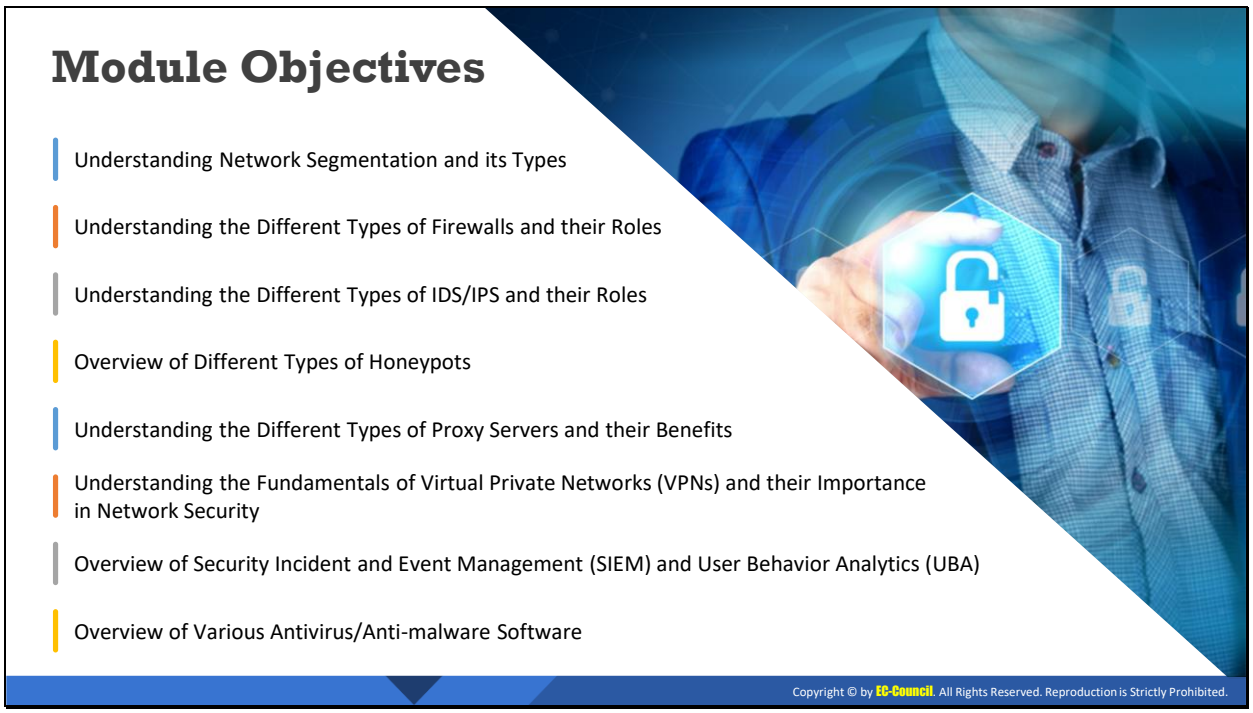
EC-Council

N|DE
Network Defense Essentials

Module 05

Network Security Controls - Technical Controls

https://t.me/learningnets



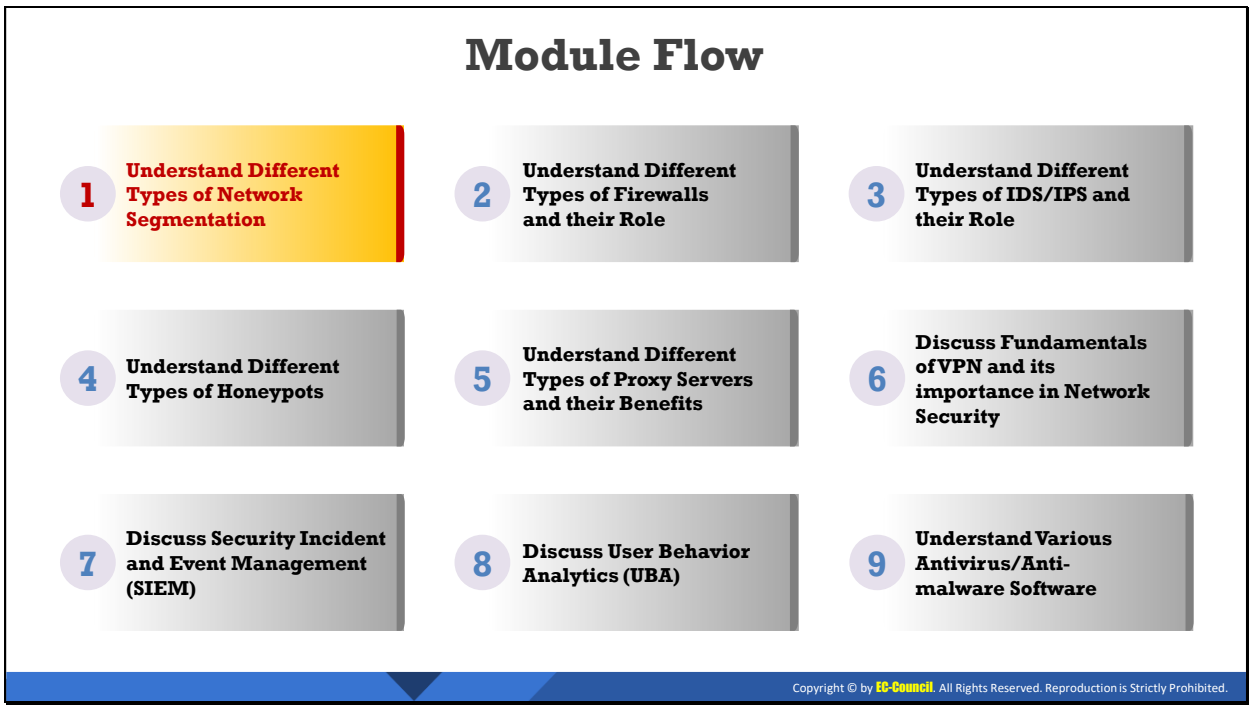
Module Objectives

The most important aspect of security controls is the protection of organizational assets such as people, property, and data. By establishing security controls, an organization can either reduce or completely mitigate risks to their assets. This module provides an overview of various technical controls that help organizations in protecting their private networks and IT assets.

At the end of this module, you will be able to do the following:

- Understand network segmentation and its types
- Describe the different types of firewalls and their roles
- Describe the different types of IDS/IPS and their roles
- Explain the different types of honeypots
- Understand the different types of proxy servers and their benefits
- Understand the fundamentals of virtual private networks (VPNs) and their importance in network security
- Explain security incident and event management (SIEM)
- Understand user behavior analytics (UBA)
- Apply various antivirus/anti-malware software

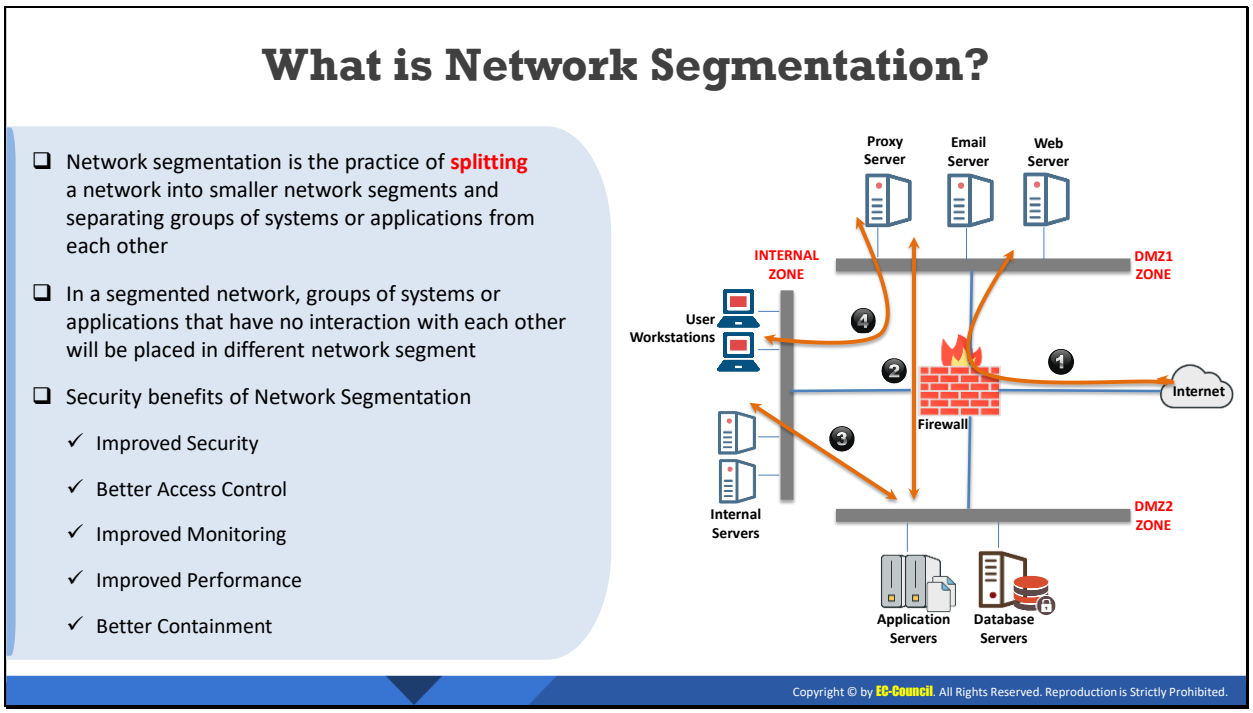
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Understand Different Types of Network Segmentation

Network segmentation enhances the network security by creating layers of the network and separating the servers containing sensitive information from the rest of the servers. The objective of this section is to explain the role of network segmentation in network security.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



What is Network Segmentation?

Network segmentation is the practice of splitting a network into smaller network segments, separating groups of systems or applications from each other. Whether it is a physical or virtual network segmentation, both can restrict communication throughout a network and also restrict network attacks. In a segmented network, groups of systems or applications that have no interaction with each other are placed on different network segments. Even if an attacker/an insider manages to penetrate the perimeter security, they cannot access the network resources from one segment to another.

Network segmentation overcomes the drawback of a traditional flat network where all the network resources (servers, workstations, etc.) are placed on the same network. If an attacker manages to penetrate through the perimeter defense, they can see and have an easy access to a flat network, since most detective tools focus on what is going outside a network. Though it is easy to manage a flat network infrastructure, it is always open to various attacks.

Security benefits of network segmentation:

- **Improved security:** It isolates network traffic to prevent access between network segments.
- **Better access control:** It allows accessing specific network resources.
- **Improved monitoring:** It provides event logging, monitoring, and denying internal connections, and detecting malicious actions.
- **Improved performance:** It reduces local traffic, with fewer hosts per subnet, and isolates broadcast traffic to the local subnet.
- **Better containment:** It limits any network issues that might occur to the local subnet.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Working Principle of Network Segmentation

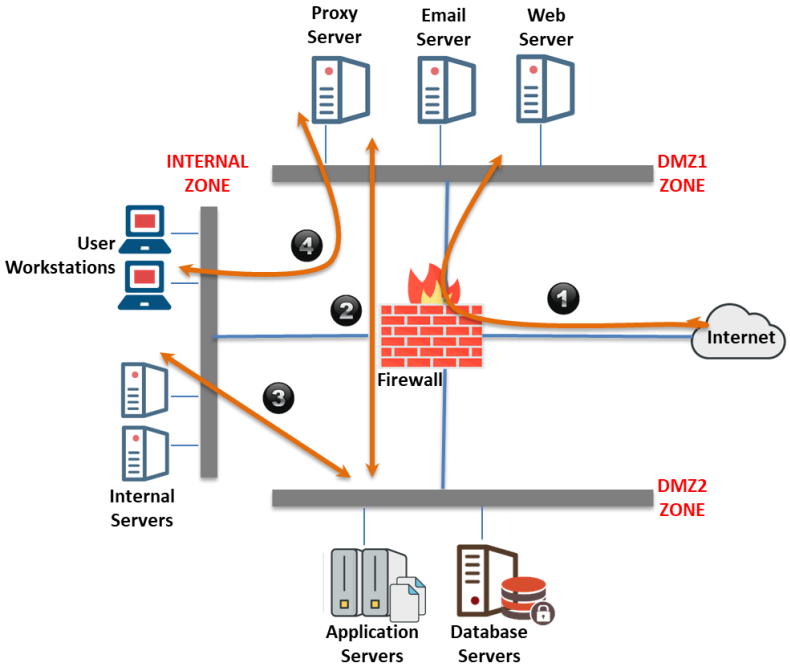


Figure 5.1: Working Principle of Network Segmentation

In the above diagram, network segmentation is used for separating servers in which one firewall, two DMZ zones (demilitarized zones and an isolated layer3 subnet), and an internal zone are used.

Web servers and email servers are separated from the servers that do not require direct internet access, since both servers need to be internet-facing and they are vulnerable to attacks. Even if one of the internet-facing servers is compromised, the separation of both servers can reduce the damage.

Bidirectional traffic is allowed from the internal zone and DMZ2 for backups/authentication via the active directory, whereas one-way traffic is only allowed from the internal zone to DMZ1. The proxy, email, and web servers of the DMZ1 are separated from the application and database servers of DMZ2 for enhanced security.

The firewall allows internet traffic to DMZ1 via certain ports (80, 25, 443, etc.) and closes all the other ports (transmission control protocol (TCP)/user datagram protocol (UDP)), whereas it does not permit internet traffic to DMZ2.

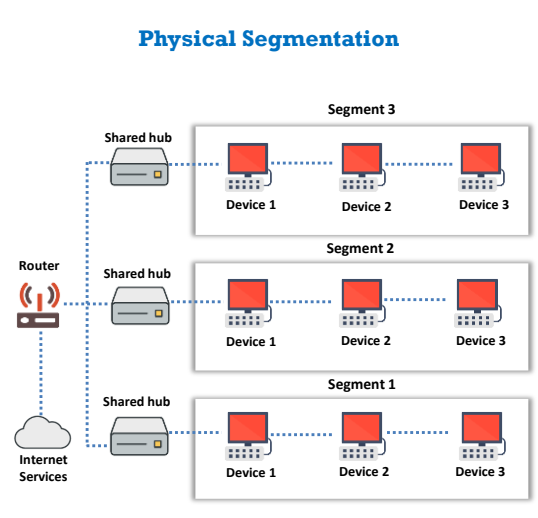
If user workstations on the internal zone require internet access, the access gets directed through an HTTP proxy server in DMZ1 since the internal zone is isolated from the internet traffic. Even if a server in DMZ1 is compromised, the internal zone will remain secured since the traffic from the internal zone to DMZ1 is permitted only in one way.

The segmentation in the above diagram represents a firewall security zone segmentation that can optimize the network security. For added security, a cloud-based web filtering solution (e.g., WebTitan, TitanHQ, SolarWinds MSP, etc.) can be used which can allow filtering of the website requests and prevent end-users from accessing malicious websites.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Types of Network Segmentation

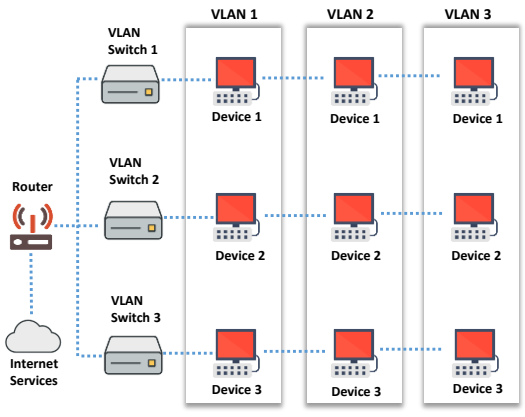
- Physical segmentation is a process of splitting a larger network into **smaller physical components**
- These segments can communicate via **intermediary devices** such as switches, hubs, or routers
- Physical network segmentation can be an easy approach to divide a network, but it is **expensive** as it occupies more space



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Network Segmentation (Cont'd)

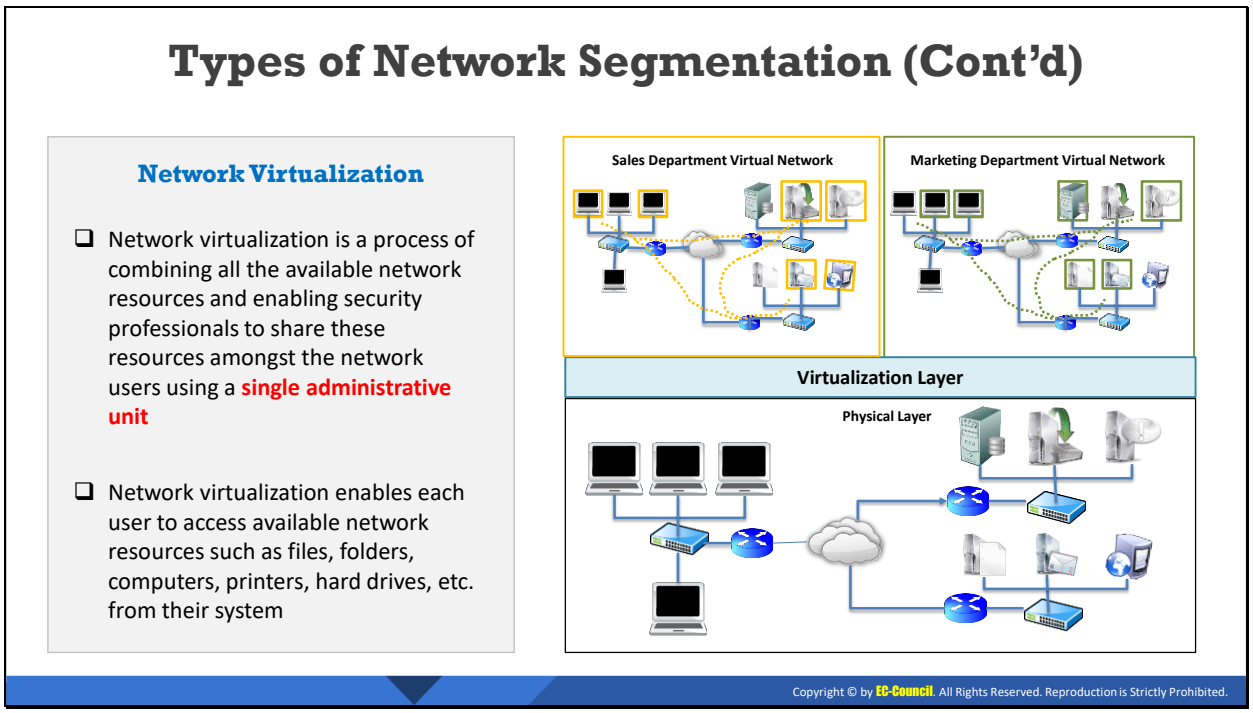
- Logical segmentation utilizes **VLANs**, which are **isolated logically** without considering the physical locations of devices
- Each VLAN is considered an **independent logical unit**, and the devices within a VLAN communicate as though they are in their own isolated network
- In this approach, **firewalls** are shared, and **switches** handle the VLAN infrastructure
- It is easier to implement and flexible to operate



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Types of Network Segmentation

Network segmentation can be implemented in three ways, namely, physical segmentation, logical segmentation, and virtualization, wherein the network is isolated physically, isolated logically (through virtual local area networks or VLANs), and entirely virtualized, respectively.

- **Physical Segmentation**: Physical segmentation is a process of splitting a larger network into smaller physical components. These segments can communicate via intermediary devices such as switches, hubs, or routers. Physical segmentation is generally used for isolating two or more devices from each other. For instance, all web servers are separated and placed in one segment, with database servers and File Transfer Protocol (FTP) servers in two other segments; these segments communicate only through their individual switches. Physical network segmentation can be an easy approach to divide a network, but it is expensive as it occupies more space and creates unwanted issues such as traffic conflicts. It is also known to be a secure mechanism but is difficult to implement as each segment in the network should have individual network connections, physical cabling, and firewall implementations.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

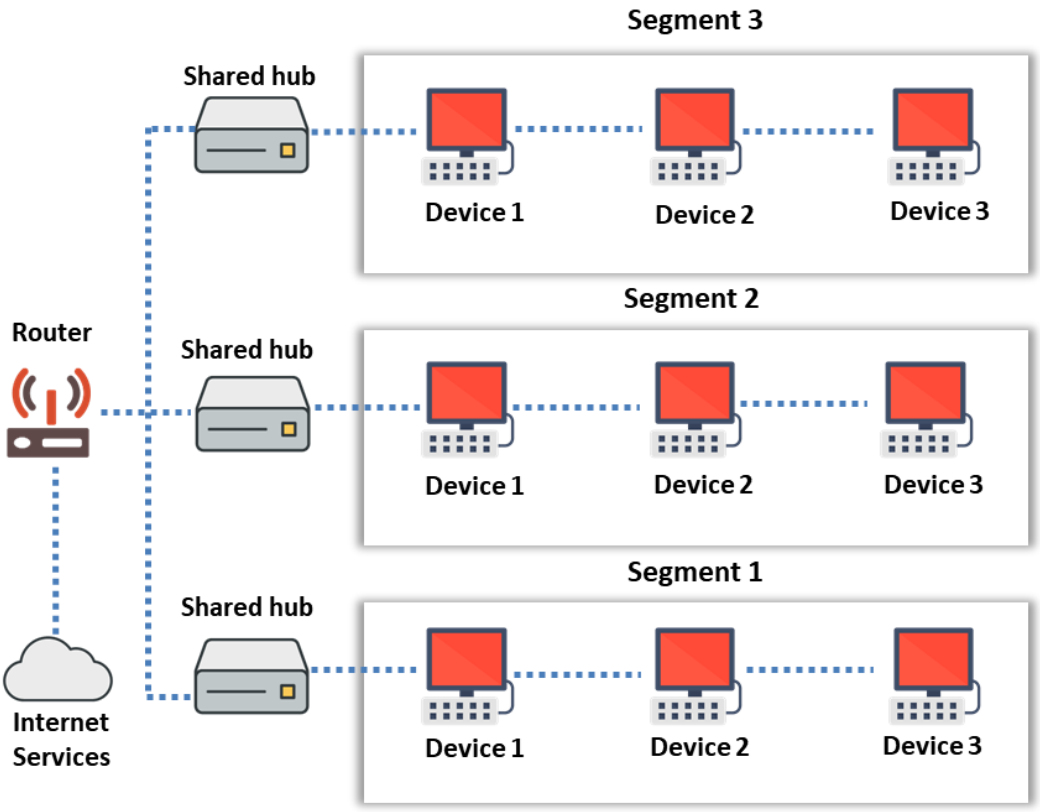


Figure 5.2: Physical segmentation of network

- **Logical Segmentation**: To overcome the problems associated with physical segmentation, organizations choose the logical segmentation of their network. Logical segmentation utilizes VLANs, which are isolated logically without considering the physical locations of devices. Each VLAN is considered an independent logical unit, and the devices within a VLAN communicate as though they are in their own isolated network. This type of segmentation is easier to implement and flexible to operate. In this approach, firewalls are shared, and switches handle the VLAN infrastructure. Logical segmentation does not need new hardware, and the provided environment is managed with the existing hardware resources. This type of segmentation employs the built-in concepts incorporated within the network infrastructure such as the creation of independent VLANs that share a physical routing device (switch), segregation of various asset types into different layer-3 subnets, and use of a router to allow data exchange between subnets.

  The following are the key advantages of logical segmentation:

  - It enables the creation of virtual workgroups irrespective of users' locations.
  - It effectively controls the network broadcast.
  - It improves security by defining which network nodes can interact with each other.
  - It eliminates the physical boundaries between users.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

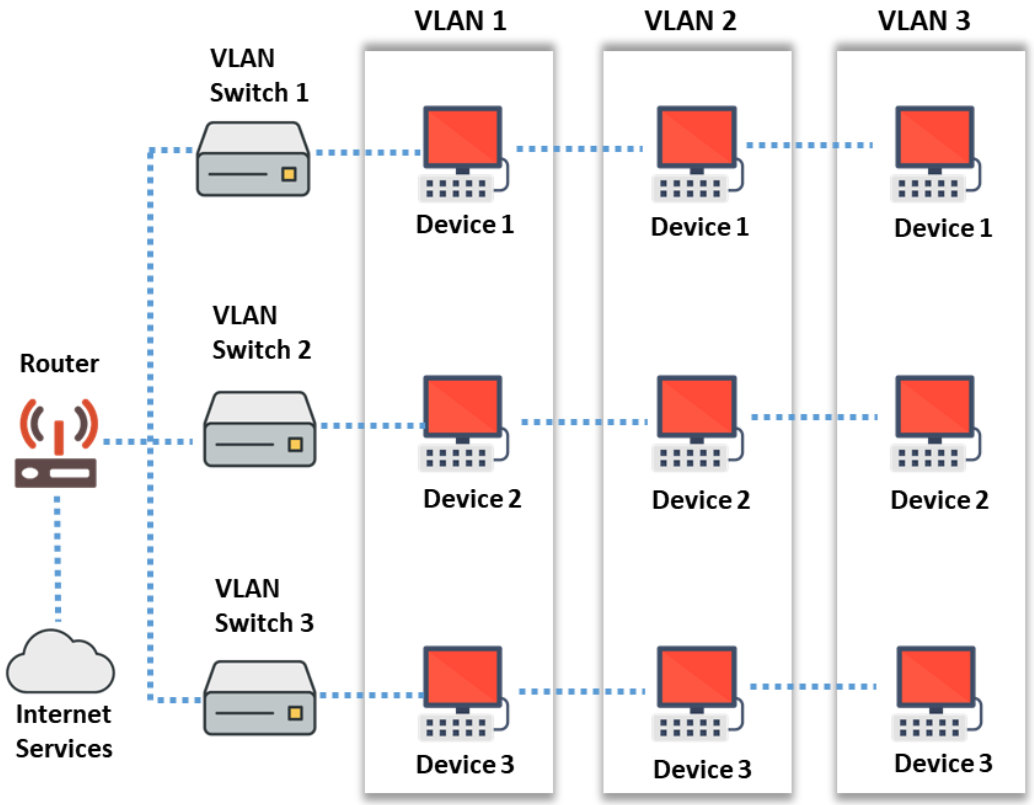


Figure 5.3: Logical segmentation of network

- **Network Virtualization**: Network Virtualization (NV) is a process of combining all available network resources and enabling security professionals to share these resources amongst the network users using a single administrative unit. It abstracts network resources traditionally allocated as actual hardware to software. NV can combine multiple physical networks into one virtual, software-based network, or divide one physical network into separate, independent virtual networks. NV provides systems and users with efficient, controlled, and secured sharing of network resources (files, folders, computers, printers, hard drives, etc.). NV splits the available bandwidth into independent channels, which can be assigned or reassigned to a particular server or device in real-time. For example, a virtual LAN (VLAN) can unite network devices into one unit irrespective of their physical location, thereby enabling the creation of a subsection of the local area network (LAN).

  The following are the key advantages of network virtualization:

  - It enables efficient, flexible, and scalable usage of the network.
  - It logically segregates the underlay administrative domain with the overlay domain.
  - It accommodates the dynamic nature of server virtualization.
  - It provides security and isolation of traffic and network details from one user to another.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

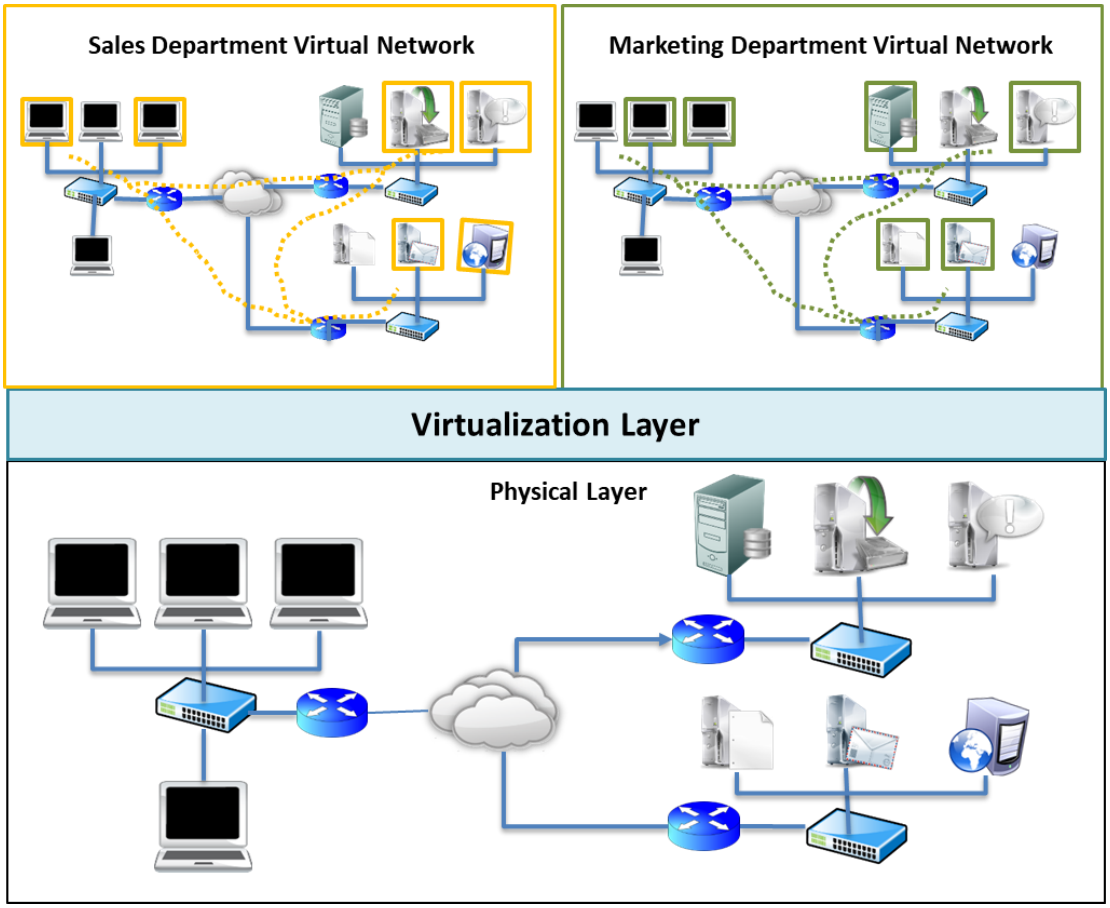
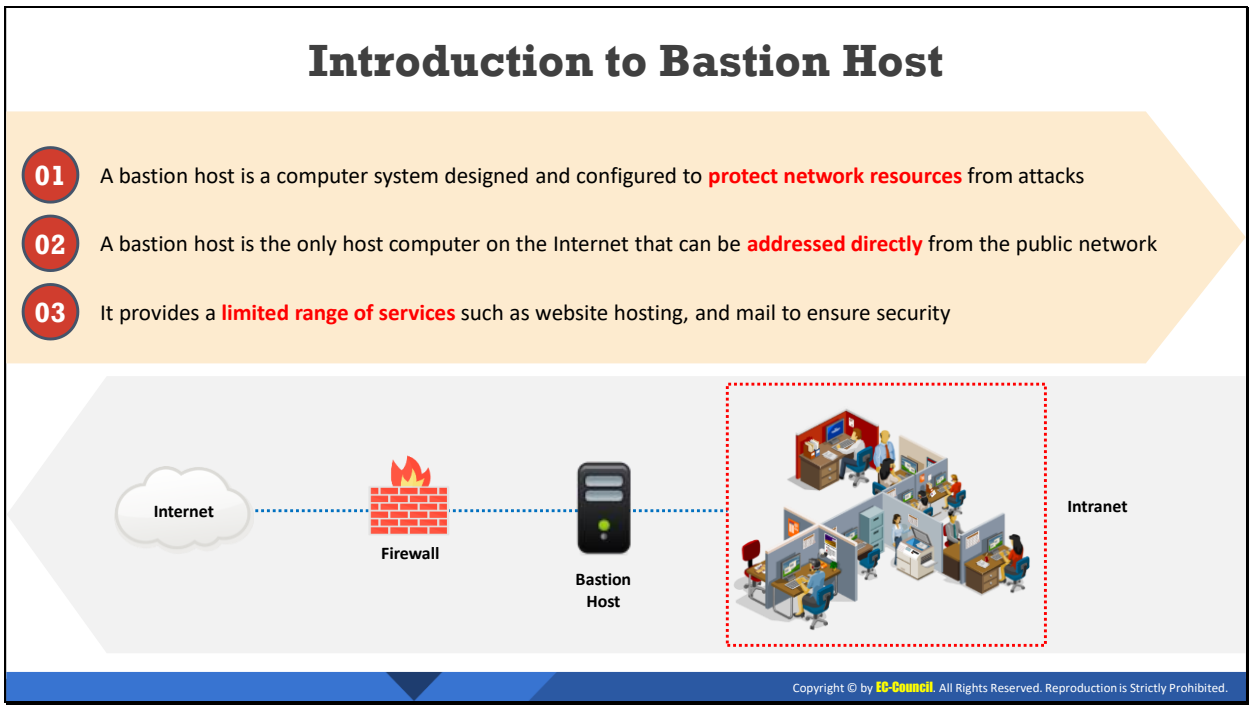


Figure 5.4: Illustration of network virtualization

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Introduction to Bastion Host

A bastion host is designed for defending a network against attacks. It acts as a mediator between inside and outside networks. A bastion host is a computer system designed and configured to protect network resources from attacks. It provides a limited range of services such as website hosting, and mail to ensure security. Traffic entering or leaving the network passes through a firewall. A bastion host has two interfaces:

- A public interface directly connected to the Internet
- A private interface connected to the intranet

A bastion host is the only host computer on the Internet that can be addressed directly from the public network. As these components are exposed to substantial risk, enormous effort is required in designing and configuring bastion hosts to minimize the probability of attacks. Various other types of bastion hosts are web, mail, Domain Name System (DNS), and FTP servers. Bastion hosts also provide packet filtering and proxy services.

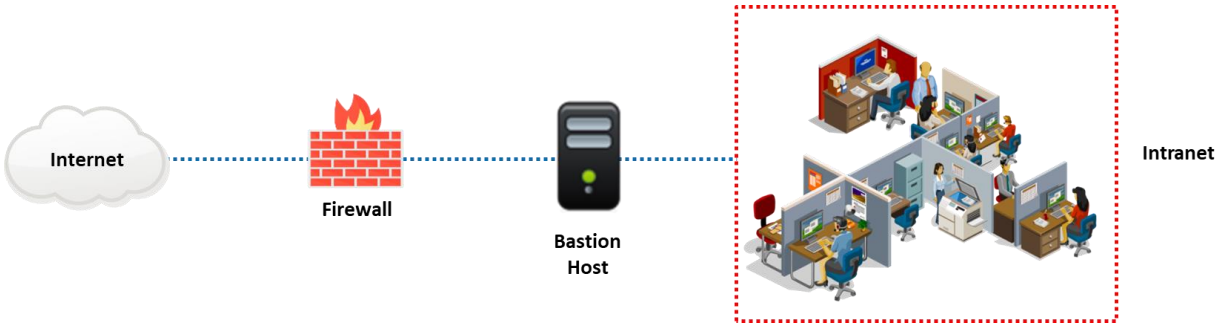


Figure 5.5: Illustration of Bastion Host

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Need for Bastion Host

A bastion host is a system that has multiple network interfaces exposed to the Internet. The operating system on such a device is made tough to create more security than on any other computer in the network. After the configuration of the computer and installation of the software, the rule sets for internal and external traffic may be installed and configured on top of the hardened operating system.

All the network services are disabled on the bastion hosts. They allow only specified Internet access. For example, there must not be any user accounts on the bastion server, which creates the possibility of a user logging on to the system and taking control of it and also accessing the Internet. Even the network file system, which offers access to files across the network, must also be disabled so that it does not create an opportunity to access the bastion server and files that can be accessed on the Internet. The safest place to place the host is in the subnet as a component of the firewall. The main advantage of placing them in their own network is that it makes it difficult to compromise them with no other resource on the network.

Bastion servers create all the logs, which can be used by the intranet administrator, to tell if there has been an attack or attempts to attack. Two copies of system logs are maintained as the backup for various security reasons. One of the possible methods to back up the security logs is by connecting the bastion host to a dedicated computer, which functions only to keep track of the secure backup logs.

Automated monitors are more complex programs than auditing software. Automated monitors frequently check the bastion server's system logs, and it raises alarms if any suspicious activities are found in the system's logs. For example, an alarm is raised if it finds any unsuccessful attempts by a user with three different logins.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

The number of bastion hosts in a firewall is not restricted to a certain number. Every bastion host can manage multiple Internet services on the same intranet. In some instances, the bastion host can be used as a victim machine. The victim machine can then be used to handle the Internet service that cannot be managed by the proxying or by those Internet services where security issues are not known. The services are substituted in the victim's machine instead of the bastion host with other services. It acts as a backup to the bastion servers even if the server is down.

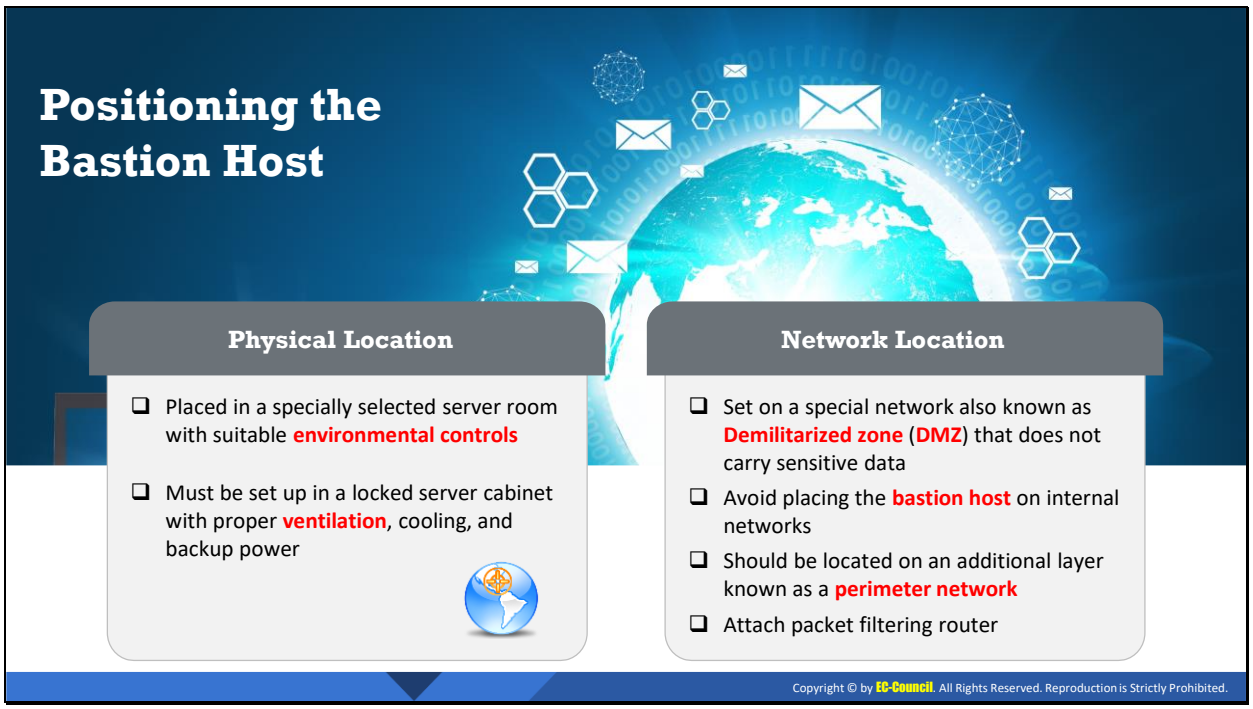
If the filtering router is placed between the bastion host and the intranet, it can be an added security. The filtering router drops all the unauthorized packets after checking all the packets between the Internet and intranet.

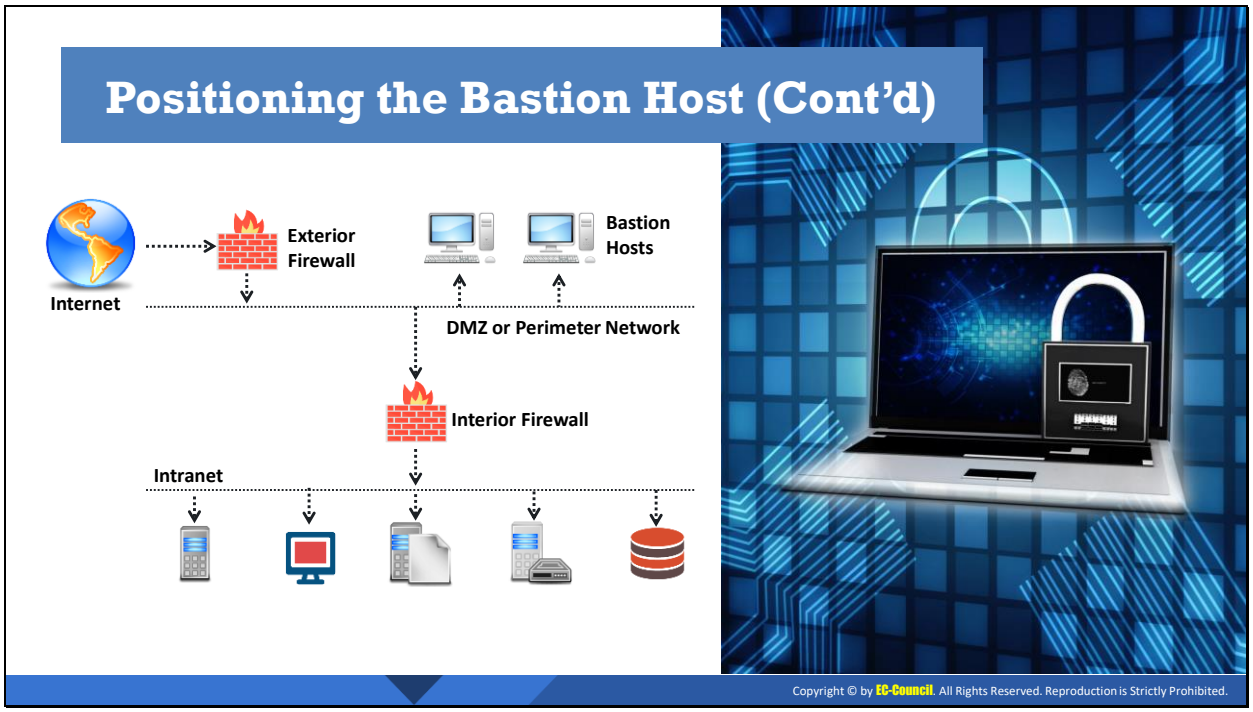
The bastion server cannot manage the requests such as sending a web page or delivering email when it receives a request for service. The request is sent across to the suitable intranet server. The intranet server processes the request, and the reply is sent back to the bastion server. The bastion server dispatches the requested service to the requester.

A few bastion servers incorporate auditing programs, which check if an attack has been launched against them. There are several ways of auditing. One can use the checksum program to audit, which is used to check if any unauthorized person has modified any software on the bastion server. The checksum is calculated based on the size of an executable program installed on the server. This program calculates the checksum to see if there are any modifications. If there are any changes in the checksum, these changes are the indications of an attack.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets





Positioning the Bastion Host

There are several options for positioning a bastion host within the network configuration, namely:

- **Physical Location:** The bastion host is placed in a specially selected server room with suitable environmental controls (against extreme weather) and the required physical

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

security devices. It must be set up in a locked server cabinet with proper ventilation, cooling, and backup power.

- **Network Location:** The host is placed on its own network, also known as the demilitarized zone, where no secret network traffic exists. It is recommended to avoid placing the bastion host on internal networks. The bastion host should be located on an additional layer known as a perimeter network, and a packet-filtering router should be attached to it.

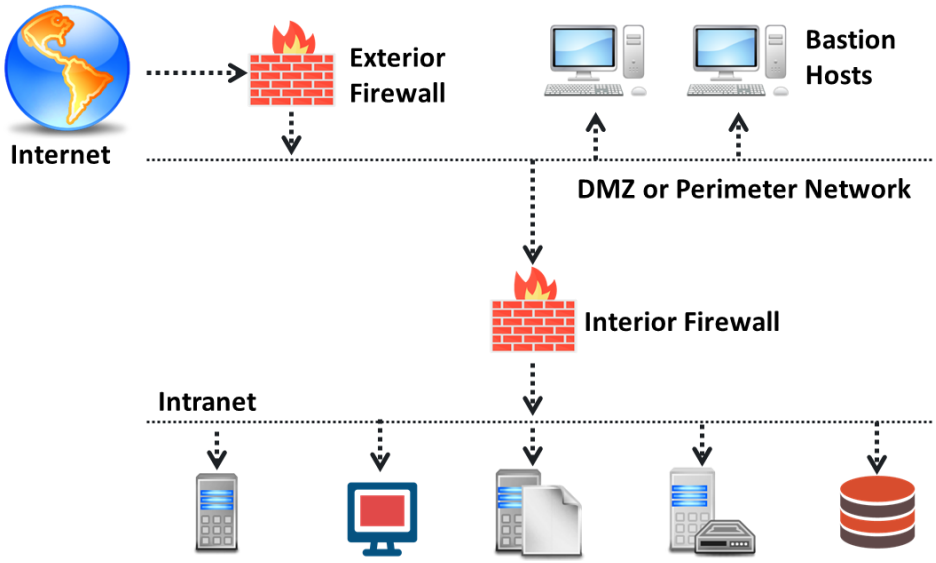
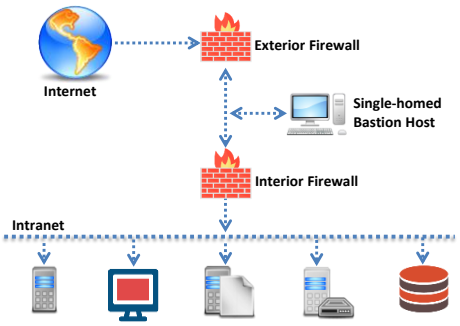


Figure 5.6: Positioning the bastion host

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Types of Bastion Hosts: Single-homed

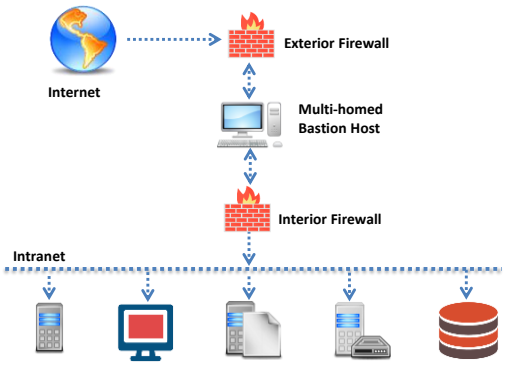
- A firewall device with only **one network interface**
- All the traffic, both incoming and outgoing, is **routed through** the bastion host
- It tests data against security guidelines and acts accordingly

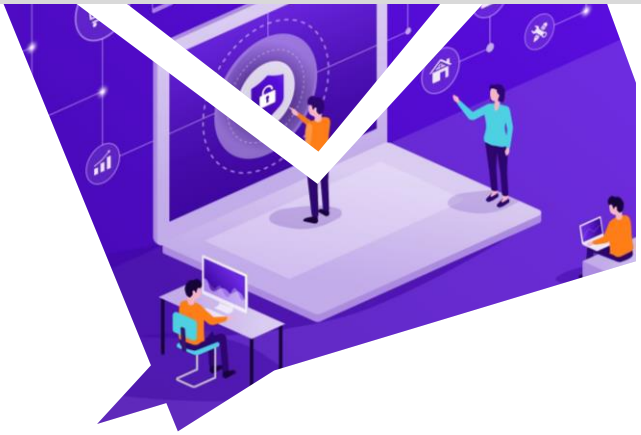


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Bastion Hosts: Multi-homed

- A firewall device with at least **two network interfaces**
- This type of bastion host is capable of separating internal and external networks, thereby **improving security**

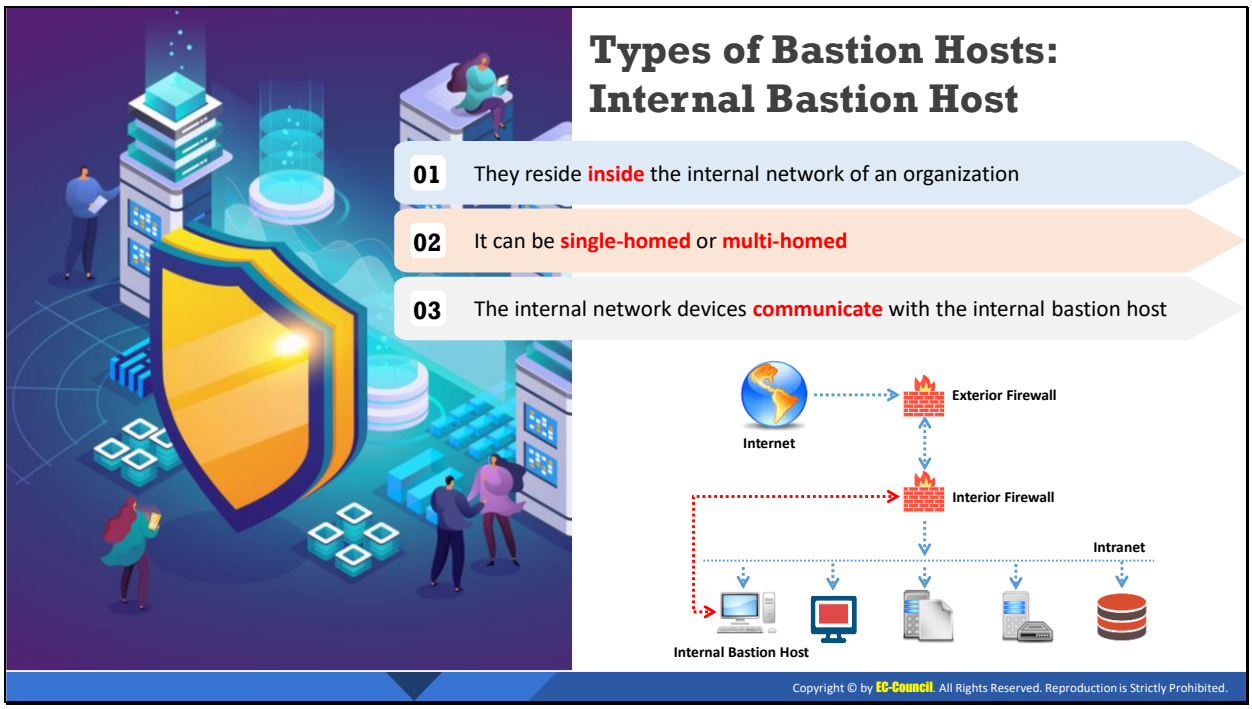


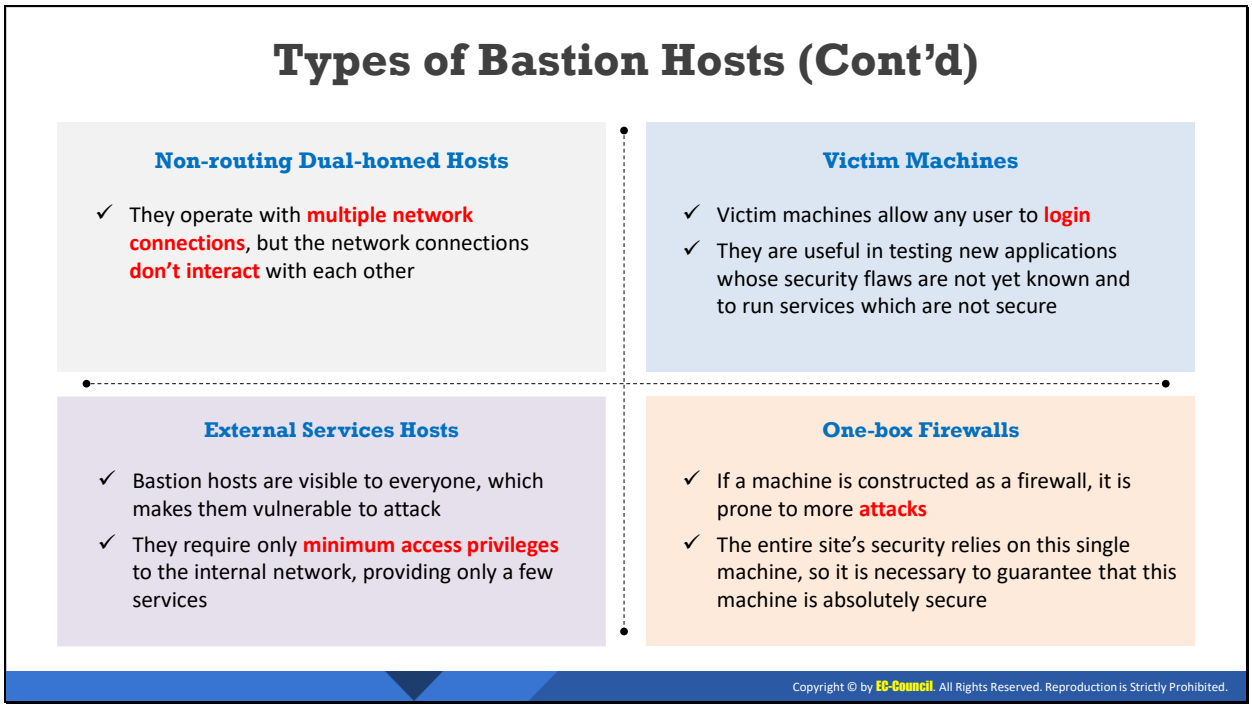


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets





Types of Bastion Hosts

In most of the configurations, the central bastion host is connected to certain internal hosts. For example, the bastion host may pass the email to an internal mail server, harmonizing with an internal name server. These internal servers are secondary bastion hosts, and they must be more organized and monitored like the bastion hosts than like internal hosts. A few services may be left enabled on these systems, but they must be configured in the same way as the bastion hosts are configured.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **Single-homed Bastion Host**

  A single-homed bastion host is a firewall device with only one network interface. All the traffic, both incoming and outgoing, is routed through the bastion host. It tests data against security guidelines and acts accordingly.

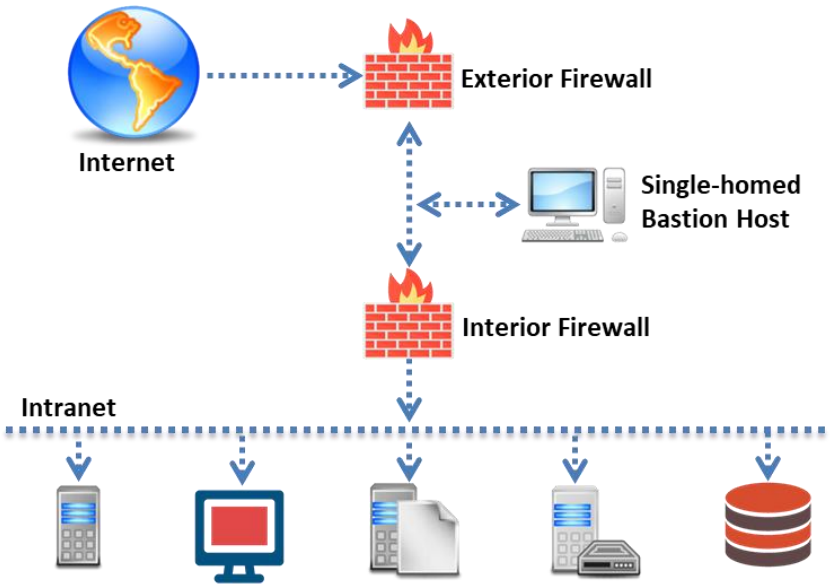


Figure 5.7: Single-homed bastion host

- **Multi-homed Bastion Host**

  A multi-homed bastion host is a firewall device with at least two network interfaces. This type of bastion host is capable of separating internal and external networks, thereby improving security.

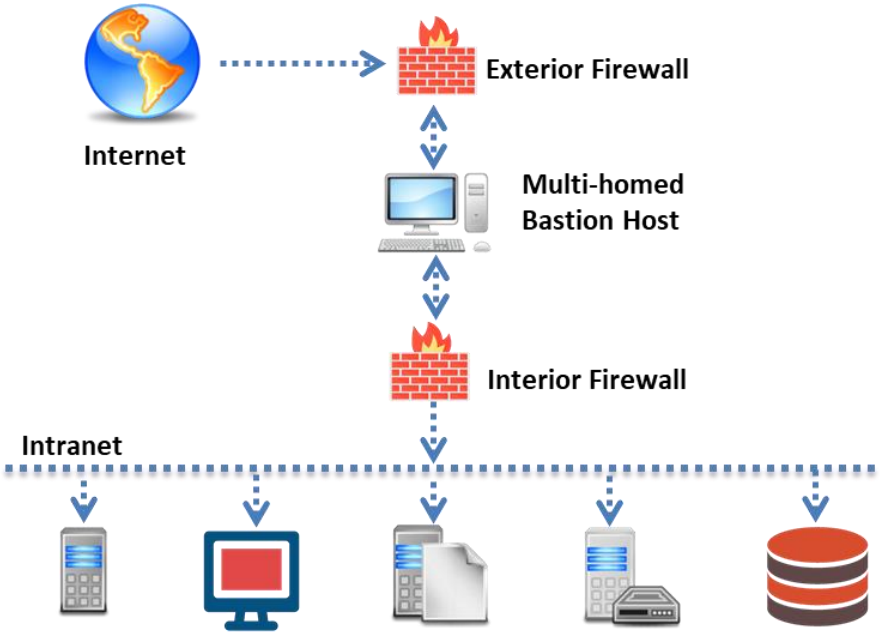


Figure 5.8: Multi-homed bastion host

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **Internal Bastion Host**

  Internal bastion hosts reside inside the internal network of an organization. They can be single-homed or multi-homed bastion hosts. The internal network devices communicate with the internal bastion host.

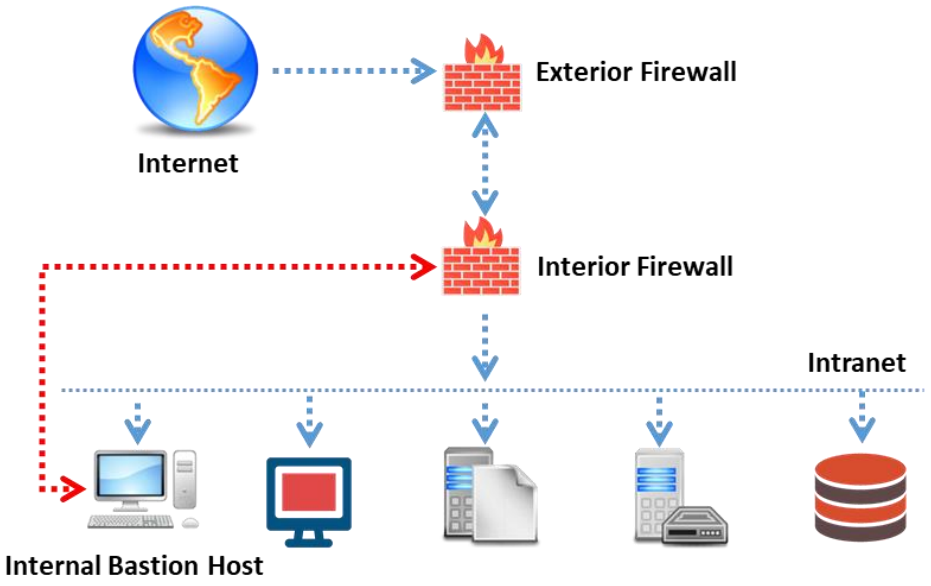


Figure 5.9: Internal bastion host

- **Non-routing Dual-homed Hosts**

  A non-routing bastion host has a dual-homed host with multiple network connections that do not interact with each other. This type of the host is completely a firewall, or it might be a component of a multi-faceted firewall. If the host is a firewall, one must be careful that the configuration and the bastion host's instructions must be followed with concern.

- **Victim Machines**

  In cases where there is a necessity to run services that are not secure and certain new applications whose security flaws are not yet known; you can use a machine (a victim machine) to install them. Such machines allow any user to log in. There is no issue, even if such machines are compromised. A victim machine is disposable in the sense that it is only used for the applications with security implications and for no other purpose.

  Victim machines are configured in the procedure similar to a typical bastion host expecting that they will always have users to log in. It will be wise if pressures are resisted, such as the user's desire for more services and programs than the ones that are provided on the usual bastion system. It must also be made sure that the user must not be comfortable with the victim machines, because the intended design may no longer work. The important factor that must be considered is that it is not reusable.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **External Services Hosts**

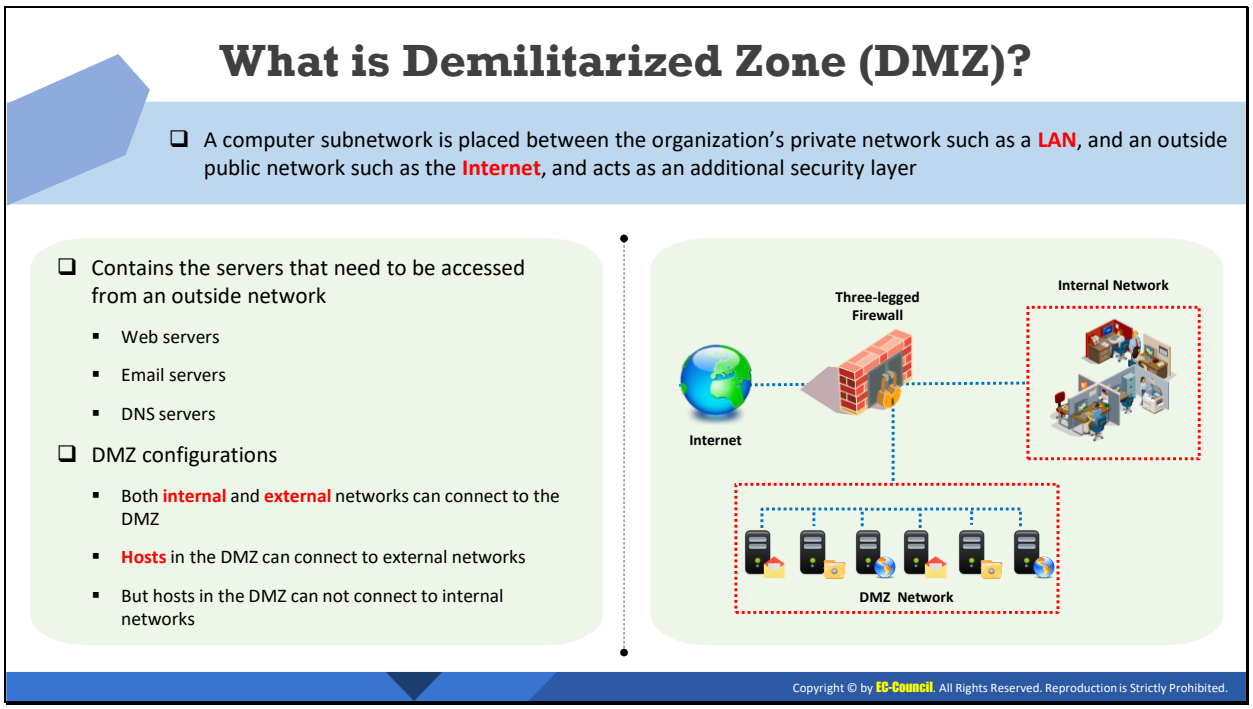
  Bastion hosts, which provide exclusive services for the Internet, have a unique concern; they are visible to everybody. This makes it vulnerable to attacks and the increased vulnerability will be prone to more successful attacks. If one of the internal services provided to the internal users is compromised, it is not obvious that the outsiders can assess the services. If one of the pages of the website is replaced, then everyone will become aware of the change and take note of it. These machines should have more security features, and they do not have minimum features to make it easier to secure. They require only minimum access privileges to the internal network.

- **One-box Firewalls**

  If the machine is constructed as a firewall, rather than as part of a wall, then it is more prone to attacks. The entire site's security relies on this one machine. It is always necessary to guarantee that this machine is absolutely secure. A replica of the original system can be used to test the new configuration without risking the Internet connection.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



What is Demilitarized Zone (DMZ)?

A Demilitarized Zone (DMZ) is a small network which is placed in between the organization's private network and an outside public network. It prevents an outsider from gaining direct access to the organization's server. For example, if an attacker uses a public network to access a DMZ host and penetrates it, then only the information on that host will be compromised. In this way, a DMZ acts as an additional security layer for networks and lowers the threat of intrusion in the internal network. A DMZ consists of the following types of servers, which need to be accessible from outside the network:

- Web servers
- Email servers
- Domain name system (DNS) servers

DMZ configurations:

- Both internal and external networks can connect to a DMZ
- Hosts in the DMZ can connect to external networks
- Hosts in the DMZ cannot connect to internal networks

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

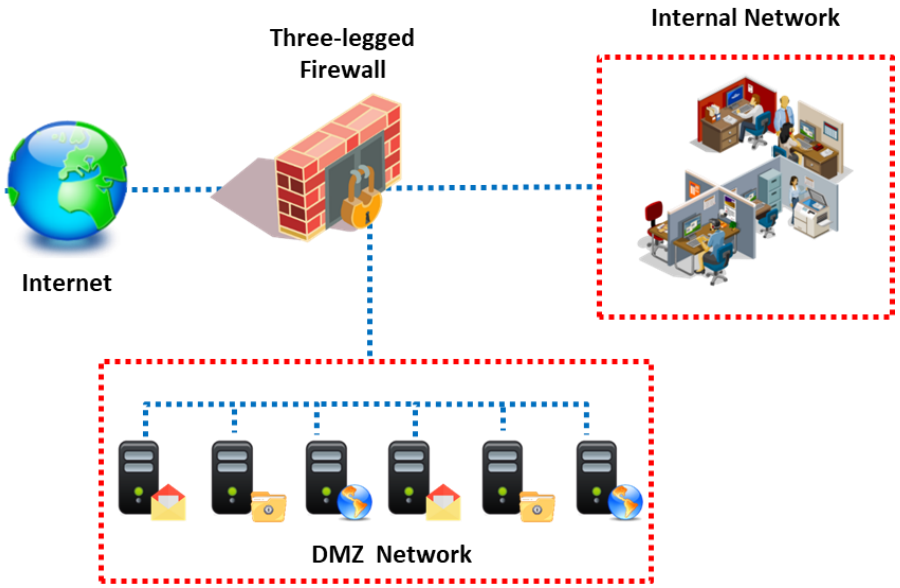
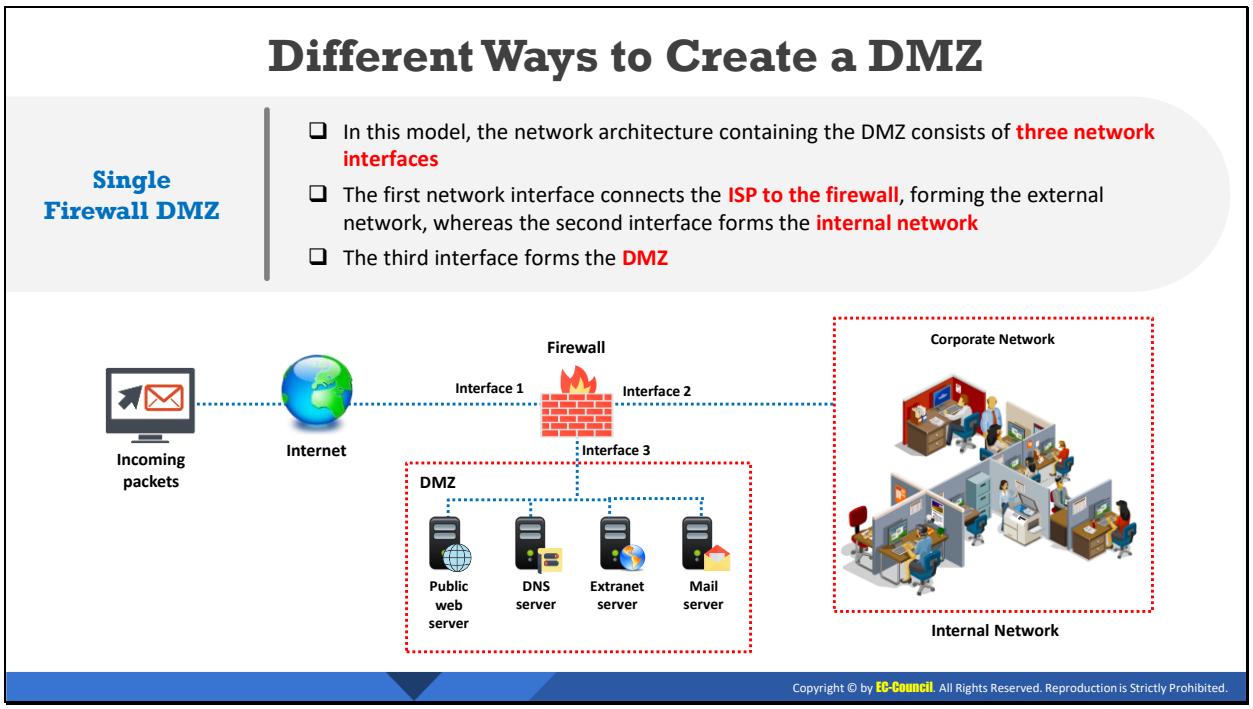


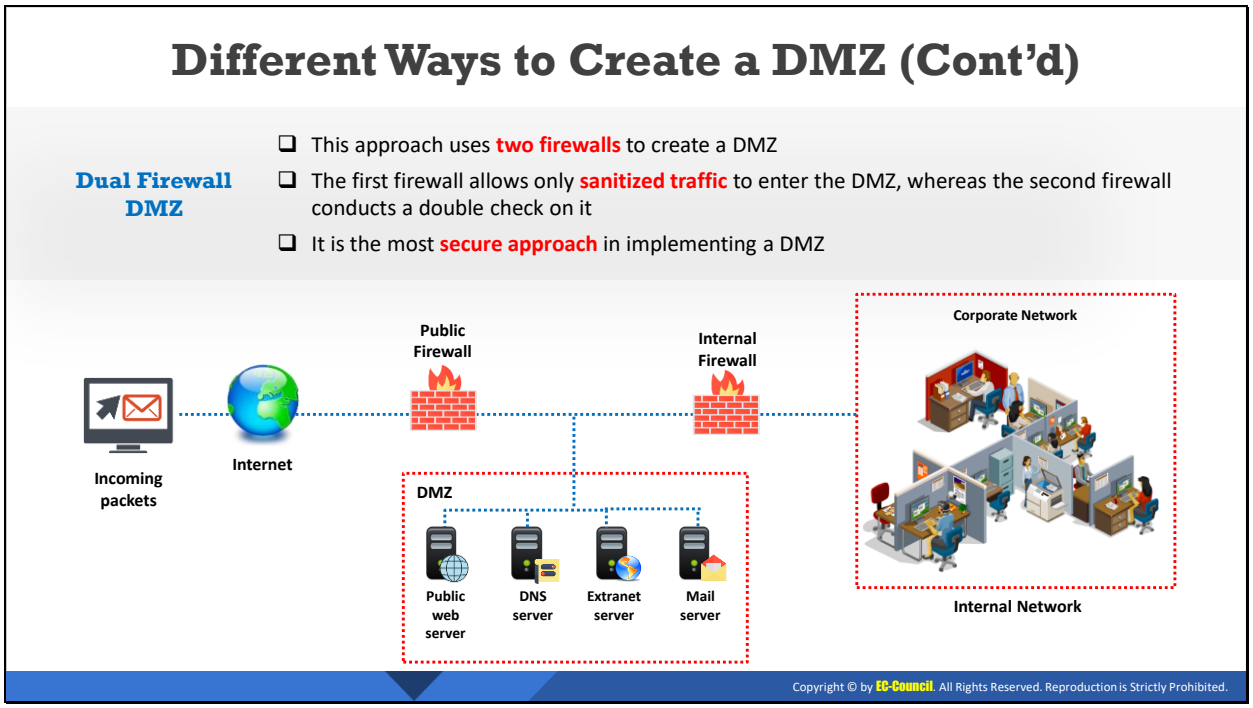
Figure 5.10: Depiction of a DMZ

Advantages of DMZ:

- Separation of DMZ from LAN enables high-level protection of LAN.
- It provides an increased control of resources.
- It uses multiple software- and hardware-based products of different platforms in order to provide an additional layer of protection.
- It provides a high level of flexibility for internet-based applications such as email, web services, etc.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets





Different Ways to Create a DMZ

Two basic methods for designing a network with a DMZ are using a single firewall (three-legged model) and using dual firewalls. It is also possible to extend these configurations according to the network requirements.

- **Single firewall DMZ**: In this model, the network architecture containing the DMZ consists of three network interfaces. The first network interface connects the internet

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

service provider (ISP) to the firewall, forming the external network, whereas the second interface forms the internal network. The third interface forms the DMZ. The firewall acts as a single point of failure and should be able to manage all the traffic to the DMZ.

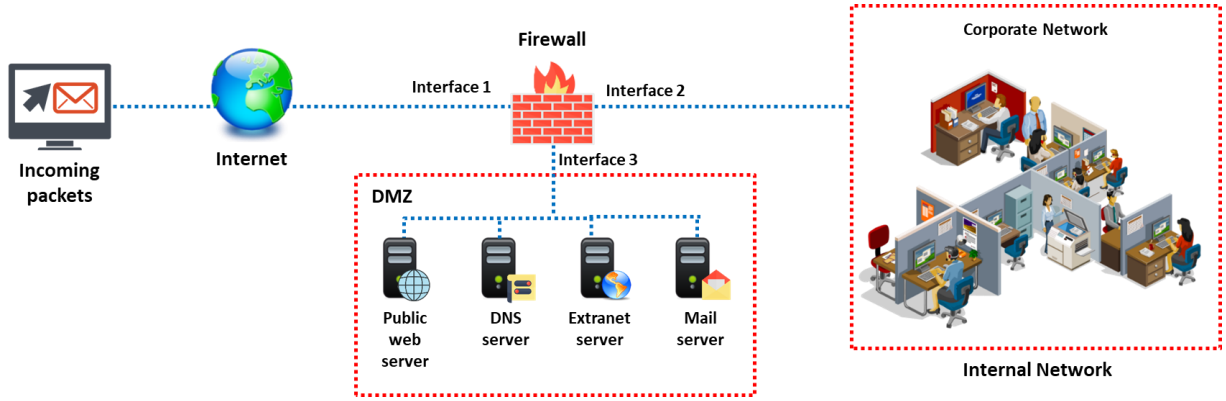


Figure 5.11: Single firewall DMZ

- **Dual firewall DMZ**: The dual firewall approach uses two firewalls to create a DMZ. The first firewall allows only sanitized traffic to enter the DMZ, whereas the second firewall conducts a double check on it. The dual firewall approach is the most secure approach in implementing a DMZ and it also adds the most complexity.

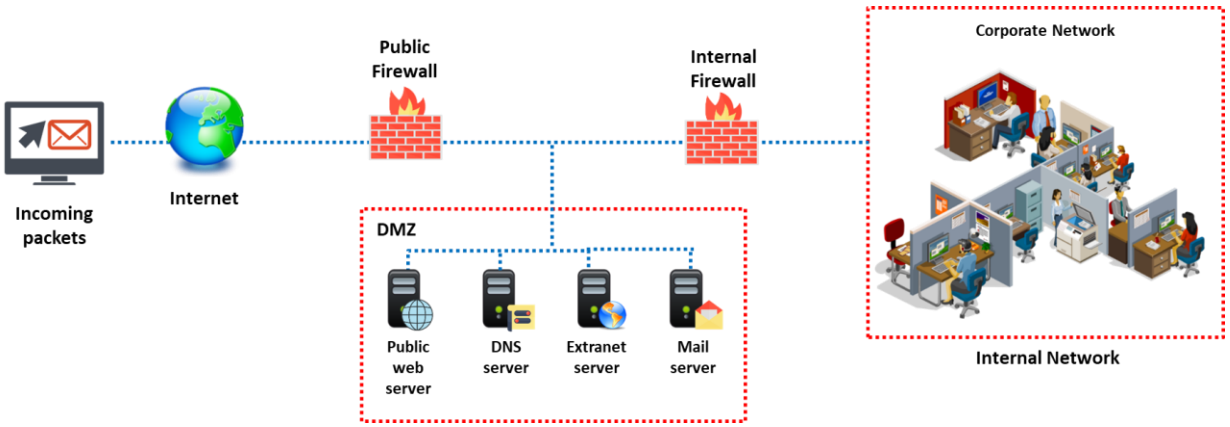
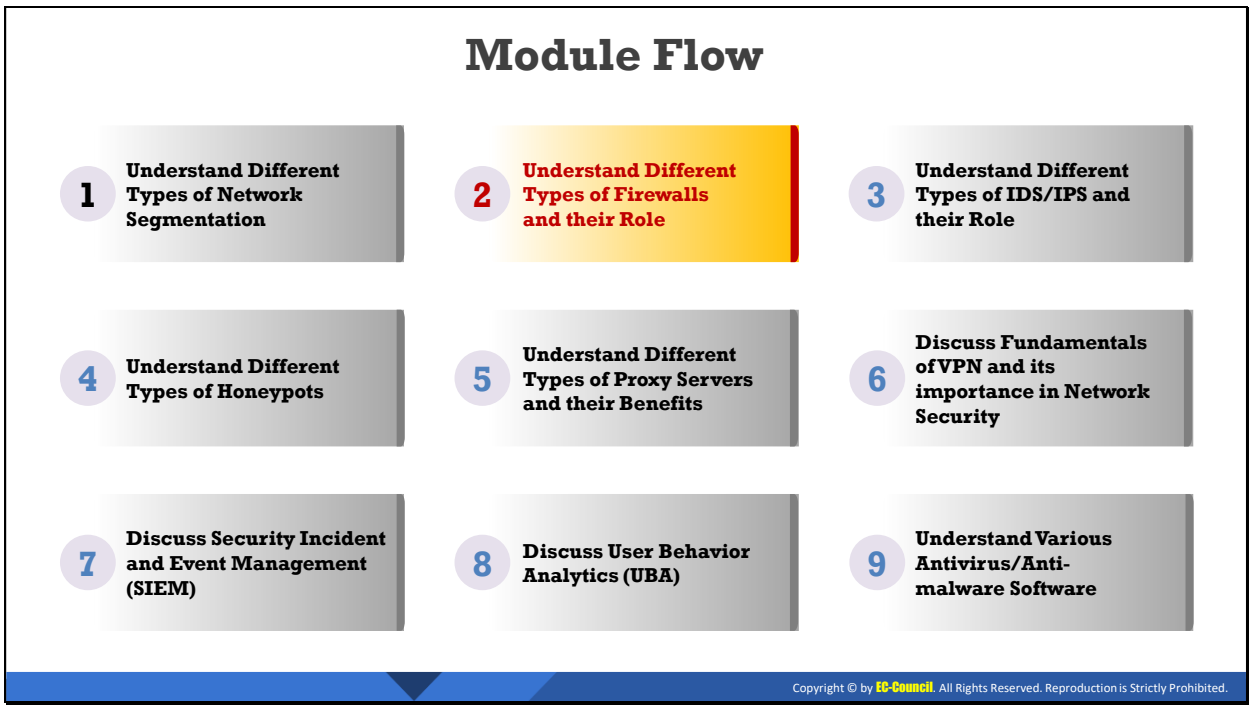


Figure 5.12: Dual firewall DMZ

Any server that requires exposure to a public network can be placed in the DMZ. It is possible for security professionals to place servers such as web servers, DNS servers, e-mail servers, and file transfer protocol (FTP) servers in the DMZ and enable access for internal and external clients.

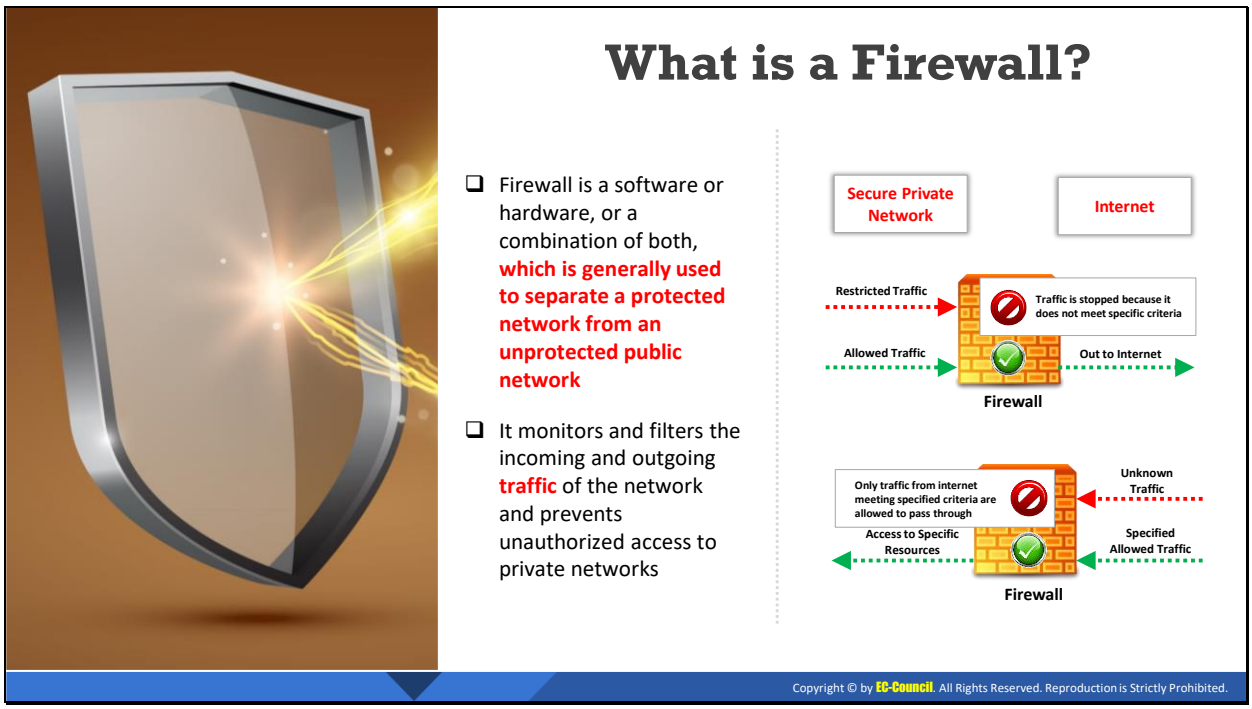
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Understand Different Types of Firewalls and their Role

This section describes firewall and different types of firewall technologies available. This includes packet filtering, stateful multilayer inspection, circuit-level gateway, application-level gateway, application proxy, network address translation (NAT), virtual private network (VPN), and next generation firewall (NGFW).

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



What is a Firewall?

A firewall is a software or hardware, or a combination of both, which is generally used to separate a protected network from an unprotected public network. A firewall is a secure, reliable, and trusted device placed in between private and public networks. It helps in protecting a private network from the users of a different network. It monitors and filters the incoming and outgoing traffic of the network and prevents unauthorized access to private networks. It has a set of rules for tracing the incoming and outgoing network traffic and is also responsible for allowing or denying traffic to pass through. These criteria are the rules and restrictions configured on the firewall and they may vary from one type of firewall to another. Generally, a firewall filters traffic based on the type of traffic, source or destination addresses, protocols, and ports.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

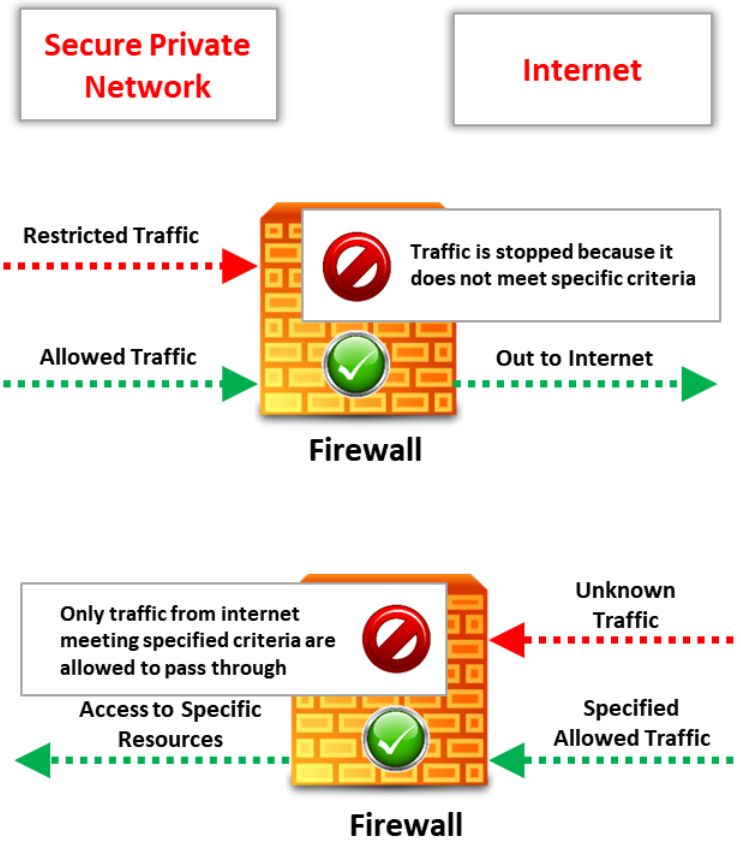


Figure 5.13: Working of a firewall

Typical use of firewalls:

- To protect the private network applications and services on the internal network from the unauthorized traffic and the public network.
- To restrict the access of the hosts on the private network and the services of the public network.
- To support a network address translation, which helps in using private IP addresses and to share a single internet connection.

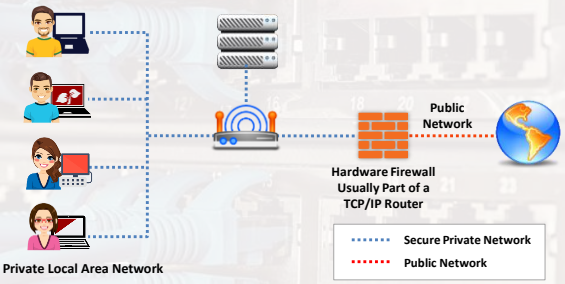
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Types of Firewalls: Hardware Firewalls

01 A hardware firewall is either a dedicated **stand-alone hardware device** or it comes as part of a router

02 The network traffic is filtered using the **packet filtering** technique

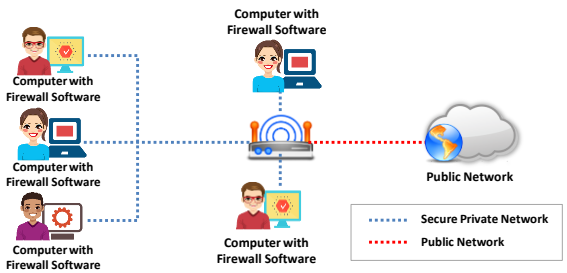
03 It is used to **filter out** the network traffic for large business networks



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Firewalls: Software Firewalls

- A software firewall is a **software program** installed on a computer, just like normal software
- It is generally used to **filter traffic** for individual home users
- It only filters traffic for the computer on which it is **installed**, not for the entire network

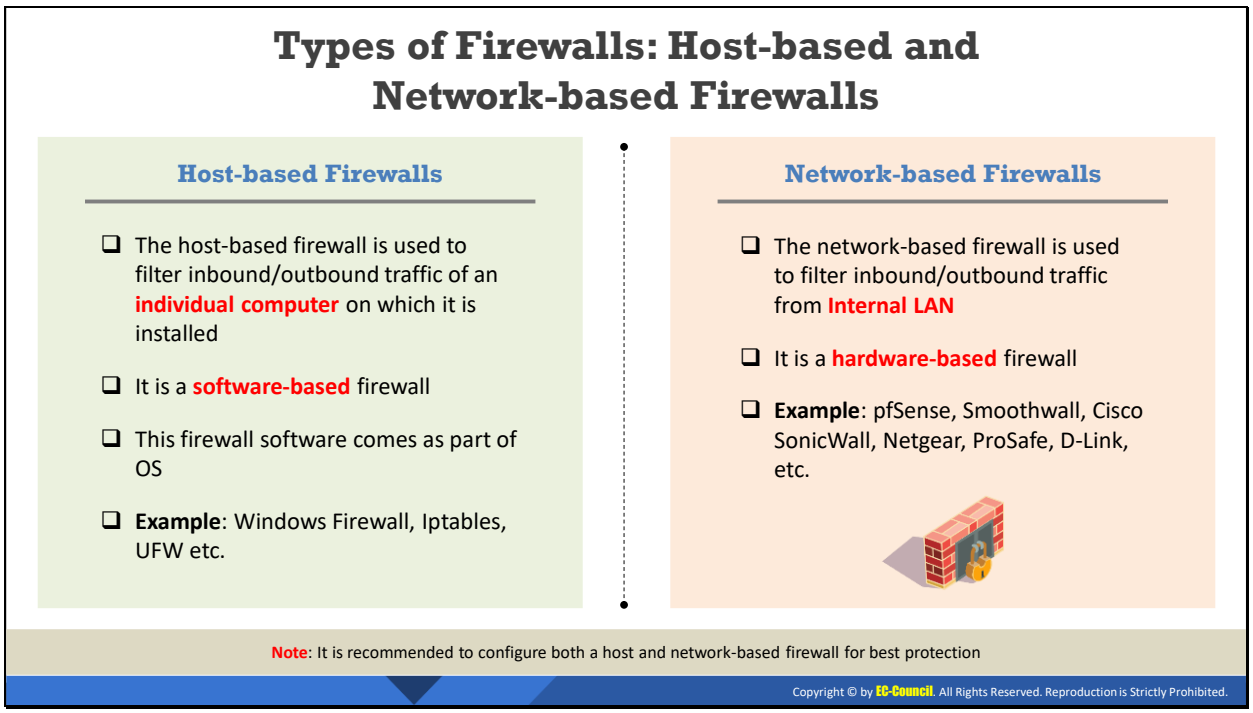


Note: It is recommended that you configure both a software and a hardware firewall for best protection

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Types of Firewalls

There are two types of firewalls.

- **Hardware Firewalls**

  A hardware firewall is a dedicated firewall device placed on the perimeter of the network. It is an integral part of the network setup and is also built into broadband routers or used as a standalone product. A hardware firewall helps to protect systems on the local network and performs effectively with little or no configuration. It employs the technique of packet filtering. It reads the header of a packet to find out the source and destination addresses and compares them with a set of predefined and/or user-created rules that determine whether it should forward or drop the packet. A hardware firewall functions on an individual system or a particular network connected using a single interface. Examples of hardware firewalls include Cisco ASA and FortiGate. Hardware firewalls protect the private local area network.

  However, hardware firewalls are expensive as well as difficult to implement and upgrade.

  Advantages:

  - Security: A hardware firewall with its operating system (OS) is considered to reduce security risks and increase the level of security controls.
  - Speed: Hardware firewalls initiate faster responses and enable more traffic.
  - Minimal Interference: Since a hardware firewall is a separate network component, it enables better management and allows the firewall to shut down, move, or be reconfigured without much interference in the network.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Disadvantages:

- More expensive than a software firewall.
- Difficult to implement and configure.
- Consumes more space and involves cabling.

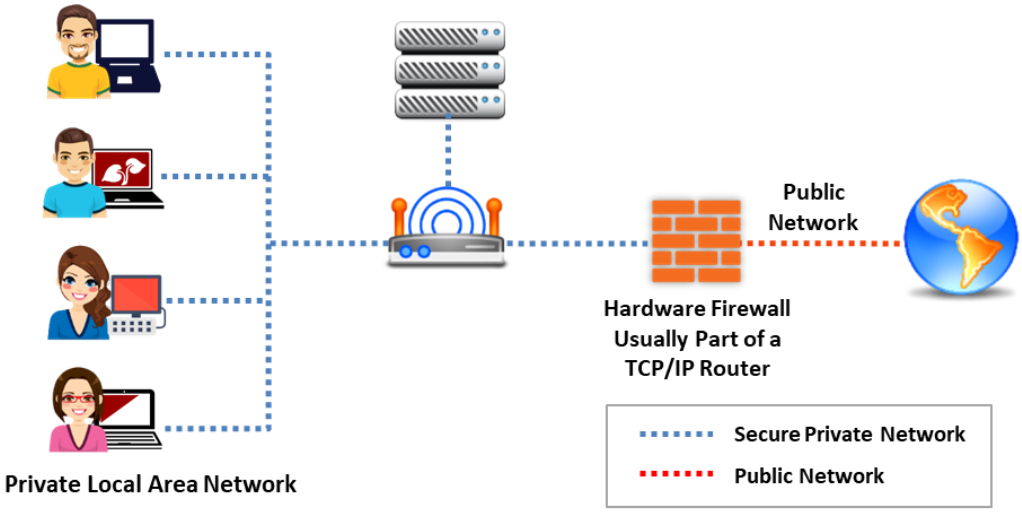


Figure 5.14: Hardware Firewall

- **Software Firewalls**

A software firewall is similar to a filter. It sits between a regular application and the networking components of the OS. It is more useful for individual home users and it is suitable for mobile users who need digital security when working outside the corporate network. Further, it is easy to install on an individual's PC, notebook, or workgroup server. It helps protect your system from outside attempts at unauthorized access and provides protection against everyday Trojans and email worms. It includes privacy controls, web filtering, and more. A software firewall implants itself in the critical area of the application/network path. It analyzes the data flow against the rule set.

The configuration of a software firewall is simple compared to that of a hardware firewall. A software firewall intercepts all requests from a network to the computer to determine if they are valid and protects the computer from attacks and unauthorized access. It incorporates user-defined controls, privacy controls, web filtering, content filtering, etc., to restrict unsafe applications from running on an individual system. Software firewalls use more resources than hardware firewalls, which reduces the speed of the system. Examples of software firewalls include those produced by Norton, McAfee, and Kaspersky.

Advantages:

- Less expensive than hardware firewalls.
- Ideal for personal or home use.
- Easier to configure and reconfigure.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Disadvantages:

- Consumes system resources.
- Difficult to uninstall.
- Not appropriate for environments requiring faster response times.

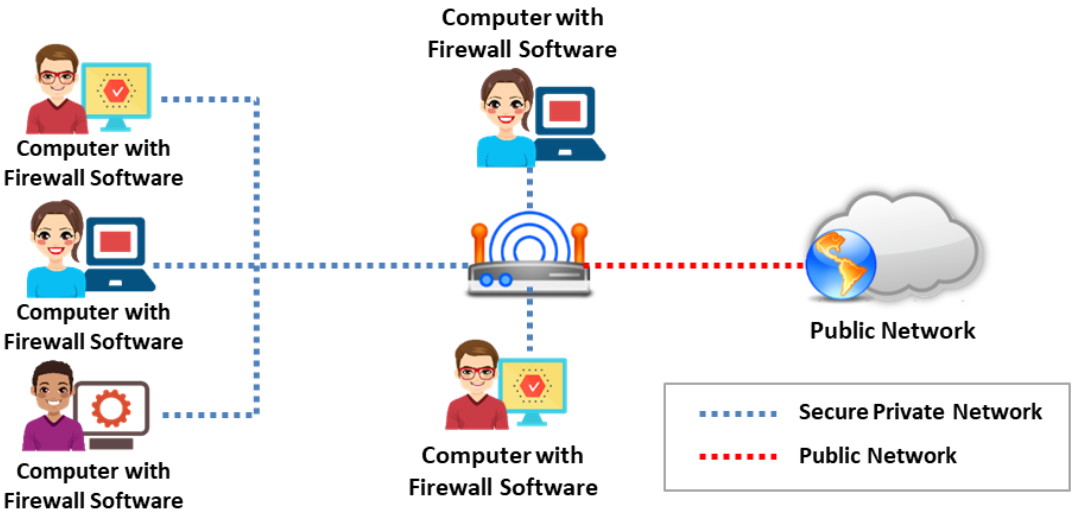


Figure 5.15: Software Firewall

Note: It is recommended that you configure both a software and a hardware firewall for best protection.

- **Host-based Firewalls**

A host-based firewall is a software-based firewall that can filter inbound/outbound traffic of an individual computer on which it is installed and checks for any malicious activity throughout the network. It comes as part of the system's OS. For example, Microsoft Firewall that is part of Windows system, Iptables, Uncomplicated Firewall (UFW), etc. The different levels of traffic analysis of these firewalls include packet analysis at the network and transport layers of the OSI model. These firewalls check the MAC address, IP address, packet source, and destination port before allowing a packet to pass. Then, a stateful filter validates the packets. In the end, the packet is validated at the application layer.

Advantages

- Provides security for devices irrespective of change in location
- Provides internal security and avoids internal attacks by allowing only authorized users
- Setup requires basic hardware/software installation
- Useful for individuals and small businesses with fewer devices as they provide customized protection

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- Provide flexibility by allowing applications and virtual machines (VMs) to take their host-based firewalls along with them when they are moved between cloud environments
- Allows configuring a single device for an individual's requirements using custom firewall rules

Disadvantages

- Not suitable for larger networks
- Provide less security because if an attacker can access a host, they can turn off the firewall or install malicious code undetected by the organization
- Must be replaced if bandwidth exceeds firewall throughput or, otherwise, more effort are needed to scale up every device if the number of hosts increase
- Costly, as they require individual installation and maintenance on every server for big organizations
- Dedicated IT staff is needed for maintaining each device

- **Network-based Firewalls**

A network-based firewall is a hardware-based firewall that can be used to filter inbound/outbound traffic on internal LAN. For example, pfSense, Smoothwall, CISCO SonicWall, Netgear, ProSafe, D-Link, etc. Such a firewall functions on the network level and filters data that traverses through the network, forming a network perimeter as the first line of defense. It functions by routing traffic to proxy servers, which manage data transmission in the network.

Advantages

- Network-based firewalls do not require individual installation and maintenance on every server.
- As any malicious traffic would exist at the network barrier, they can provide greater security than what host-based firewalls can provide a host.
- They allow scalability when a client's bandwidth demands increase.
- They offer high availability (uptime) and their security can be extended beyond a single service provider network.
- They require a limited workforce that may be needed to manage one or two sets of network firewalls.
- They are appropriate for SMEs or organizations with large networks.

Disadvantages

- They do not consider applications and vulnerabilities on a system/VM.
- They do not provide protection for host-to-host communication in the same VLAN.
- Their setup requires highly skilled resources.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

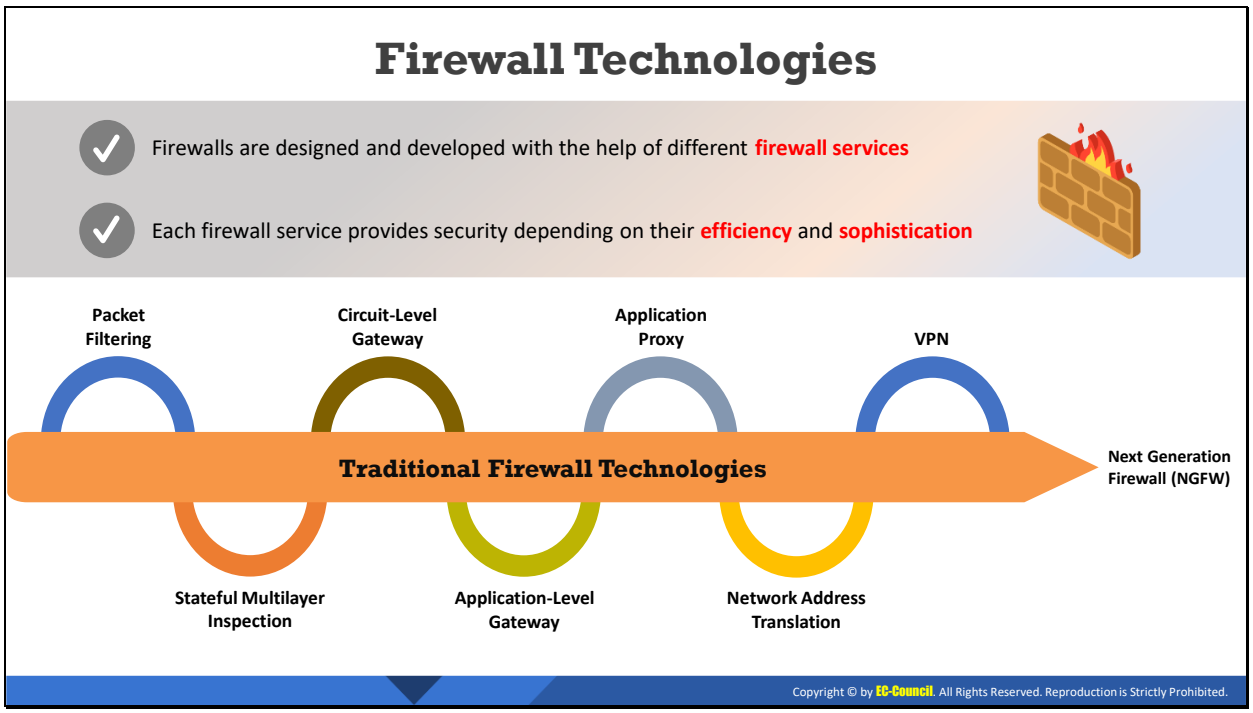
- Their cost is lower in the case of big organizations.
- Incorrect maintenance of network firewalls that function as proxy servers may decrease network performance.

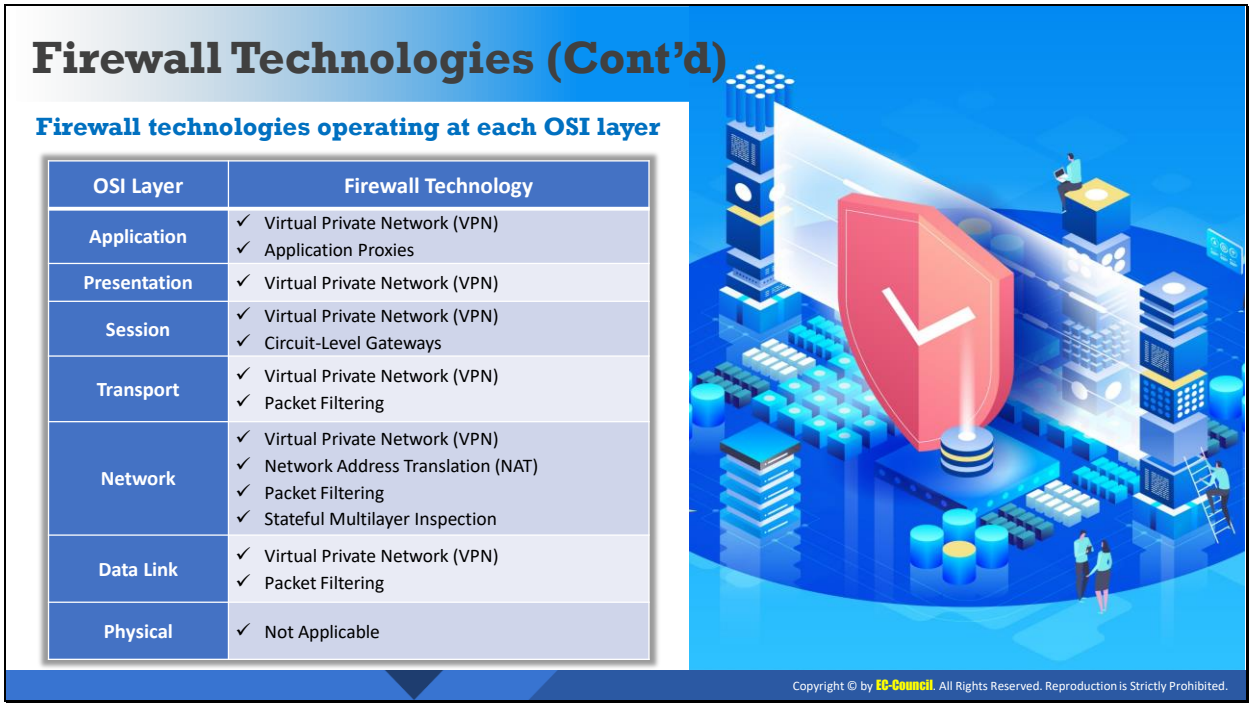
Note: It is recommended to configure both a host and network-based firewall for best protection

In the real environment, a combination of host-based and network-based firewalls provides greater security. For example, if an attacker were able to breach the network-level security, it would still be difficult to breach each host-based firewall. This combination is suitable for big organizations with complex networks, which have higher threat levels to their sensitive data and need to meet the strong compliance standards.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets





Firewall Technologies

Firewalls are designed and developed with the help of different firewall services. Each firewall service provides security depending on its efficiency and sophistication. There are different types of firewall technologies depending on where the communication is taking place, where the traffic is intercepted in the network, the state that is traced, and so on. Considering the capabilities of different firewalls, it is easy to choose and place an appropriate firewall to meet the security requirements in the best possible way. Each type of firewall has its advantages.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Several firewall technologies are available for organizations to implement their security measures. Sometimes, firewall technologies are combined with other technologies to build another firewall technology. For example, NAT is a routing technology; however, when it is combined with a firewall, it is considered a firewall technology.

The various firewall technologies are listed below:

- Packet Filtering
- Circuit-Level Gateways
- Application-Level Gateways
- Stateful Multilayer Inspection Firewall
- Application Proxy
- Network Address Translation (NAT)
- Virtual Private Network (VPN)
- Next Generation Firewall (NGFW)

The table below summarizes technologies operating at each OSI layer:

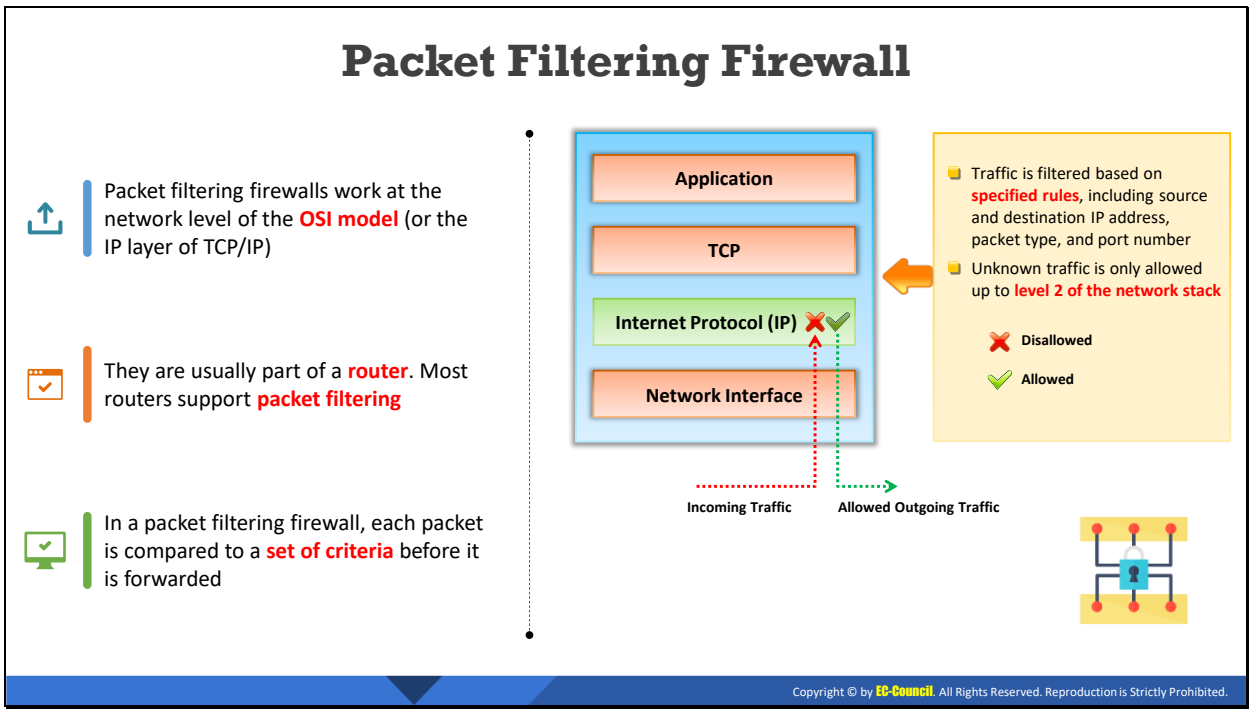
OSI Layer	Firewall Technology
Application	▪ Virtual Private Network (VPN) ▪ Application Proxies
Presentation	▪ Virtual Private Network (VPN)
Session	▪ Virtual Private Network (VPN) ▪ Circuit-Level Gateways
Transport	▪ Virtual Private Network (VPN) ▪ Packet Filtering
Network	▪ Virtual Private Network (VPN) ▪ Network Address Translation (NAT) ▪ Packet Filtering ▪ Stateful Multilayer Inspection
Data Link	▪ Virtual Private Network (VPN) ▪ Packet Filtering
Physical	▪ Not Applicable

Table 5.1: Firewall Technologies

The security levels of these technologies vary according to their efficiency levels. A comparison of these technologies can be made by allowing them to pass through the OSI layer between the hosts. The data passes through the intermediate layers from a higher layer to a lower layer. Each layer adds additional information to the data packets. The lower layer now sends the obtained information through the physical network to the upper layers and then to its destination.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Packet Filtering Firewall

Packet filtering is the most basic feature of all modern firewalls. Packet filtering firewalls work at the network level of the OSI model (or the IP layer of TCP/IP). They are usually part of a router. Most routers support packet filtering. In a packet filtering firewall, each packet is compared to a set of criteria before it is forwarded. Depending on the packet and the criteria, the firewall can:

- Drop the packet
- Forward it or send a message to the originator

They evaluate each packet based on the packet header information, including source IP address, destination IP address, source port, destination port, protocol, etc. If the packet header information does not match the ruleset, the firewall drops the packet; or else, it is forwarded. Rules can include source and destination IP address, source and destination port number, or the protocol used. When a data packet passes through the network, a packet filter checks the packet header and compares it with the connection bypass table that keeps a log of the connections passing through the network. The advantage of packet filtering firewalls is their low cost and low impact on network performance.

Traffic is filtered based on specified rules including source and destination IP address, packet type, and port number. Unknown traffic is only allowed up to level 2 of the network stack.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

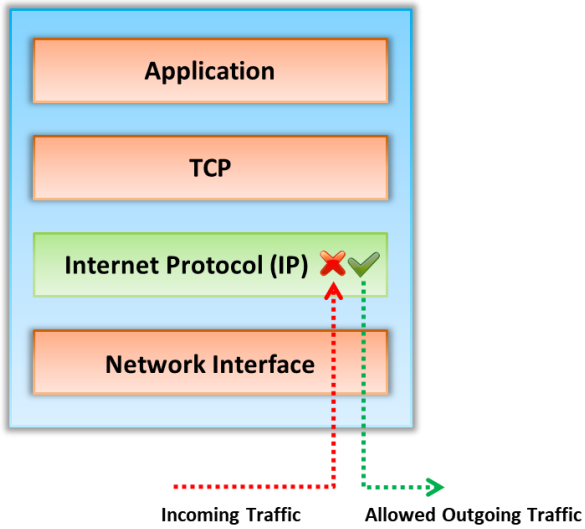


Figure 5.16: Packet Filtering Firewall

There are three methods available for configuring packet filters after determining the set of filtering rules:

- **Rule 1:** This rule states that it accepts only those packets that are safe, thereby dropping the rest.
- **Rule 2:** This rule states that the filter drops only those packets that are confirmed unsafe.
- **Rule 3:** This rule states that, if there are no specific instructions provided for any particular packet, then the user is given the chance to decide on what to do with the packet.

A network packet can pass through the network by entering the previously established connection. If a new packet enters the network, the firewall verifies the packets and checks if the new packet follows/meets the rules. It then forwards the packet to the network and enters the new data packet entry of the connection in the bypass table. A packet filtering firewall is not expensive and neither does it affect network performance. Most routers support packet filtering. Packet filtering is a relatively low-level security measure that can be bypassed by techniques such as packet spoofing, where the attacker crafts or replaces packet headers that are then unfiltered by the firewall.

As can be judged from the name, packet filter-based firewalls concentrate on individual packets and analyze their header information as well as the directed path. Traditional packet filtering firewalls make their decisions based on the following information:

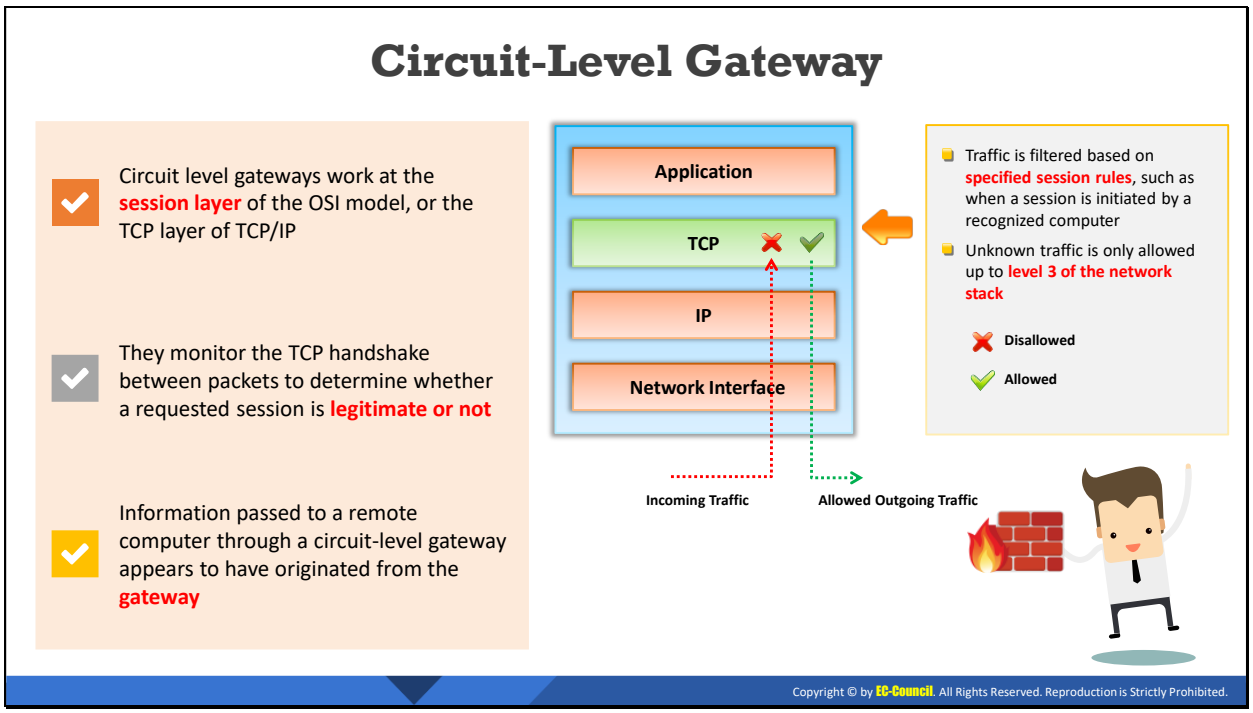
- **Source IP address:** This allows the firewall to check if the packet is coming from a valid source or not. IP header stores the information about the source of the packet and the address refers to the source system IP address.
- **Destination IP address:** This allows the firewall to check if the packet is heading toward the correct destination; the IP header of the packet stores the destination address of the packet.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **Source TCP/UDP port:** This allows the firewall to check the source port of the packet.
- **Destination TCP/UDP port:** This allows the firewall to verify the destination port of a packet to allow or deny the services.
- **TCP code bits:** This allows the firewall to check whether the packet has a SYN, ACK, or other bits set for connecting.
- **Protocol in use:** Packets carry protocols, and this field checks the protocol used and decides to allow or deny associated packets.
- **Direction:** This allows the firewall to check whether the packet is coming from a packet filter firewall or leaving it.
- **Interface:** This allows the firewall to check whether the packet is coming from an unreliable site.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Circuit-Level Gateway

Circuit level gateways work at the session layer of the OSI model, or the TCP layer of TCP/IP. They monitor the TCP handshake between packets to determine whether a requested session is legitimate or not. Information passed to a remote computer through a circuit-level gateway appears to have originated from the gateway.

The circuit-level gateway firewall uses the data present in the headers of data packets to perform its action. It is not a stand-alone firewall, but it works in coordination with other firewalls such as packet filter and application proxy to perform its functions. Information passed to a remote computer through a circuit-level gateway appears to have originated from the gateway. Thus, circuit-level gateway firewalls have the ability to hide the information of network they protect. These firewalls are relatively inexpensive.

Traffic is filtered based on specified session rules, such as when a session is initiated by a recognized computer. Unknown traffic is only allowed up to level 3 of the network stack.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

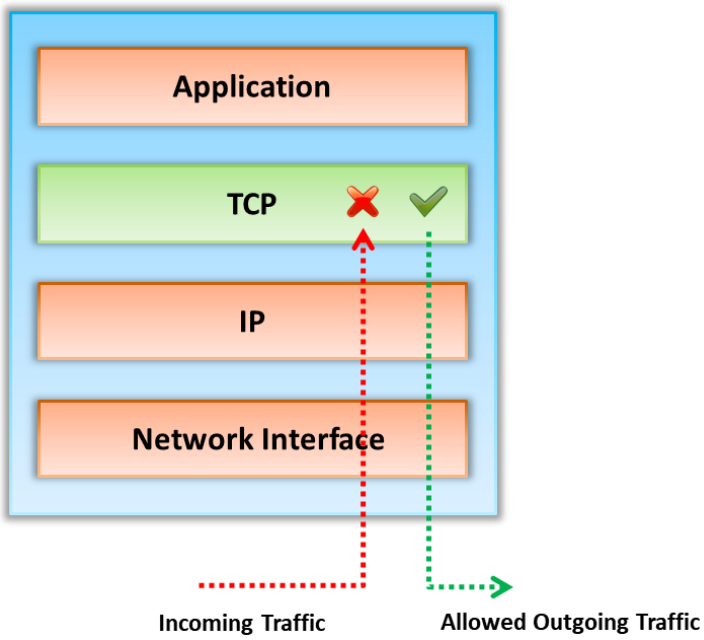


Figure 5.17: Circuit-Level Gateway

If one system wants to view information on the other system, then it sends a request to the second system and the circuit-level gateway firewall intercepts this request. The firewall forwards the packet to the recipient system with a different address. After the first system receives the reply, the firewall checks if the reply matches with the IP address of the initial system. If the reply matches, the firewall forwards the packet, otherwise it drops it.

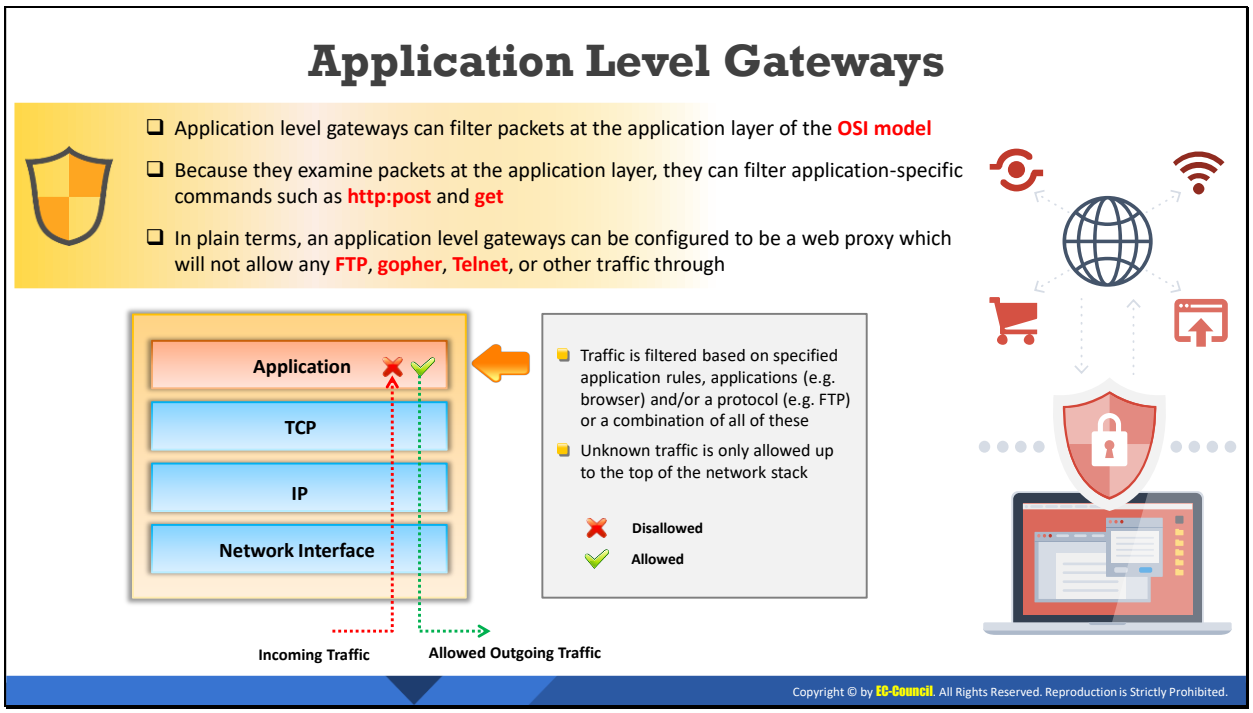
Advantages

- Hides data of the private network
- Does not filter individual packets
- Does not require a separate proxy server for each application
- Easy to implement

Disadvantages

- Cannot scan active contents
- Can only handle TCP connections

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Application Level Gateways

Application level gateways can filter packets at the application layer of the OSI model. As they examine packets at the application layer, they can filter application-specific commands such as **http:post** and **get.** In plain terms, an application level gateways can be configured to be a web proxy which will not allow any **FTP**, **gopher**, **Telnet**, or other traffic through.

An application-level gateway firewall controls input, output, and/or access across an application or service. It monitors and possibly blocks the input, output, or system service calls that do not meet the set firewall policy. Before allowing the connection, it evaluates the network packets for valid data at the application layer of the firewall.

Traffic is filtered based on specified application rules, applications (e.g. browser) and/or a protocol (e.g. FTP) or a combination of all of these. Unknown traffic is only allowed up to the top of the network stack.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

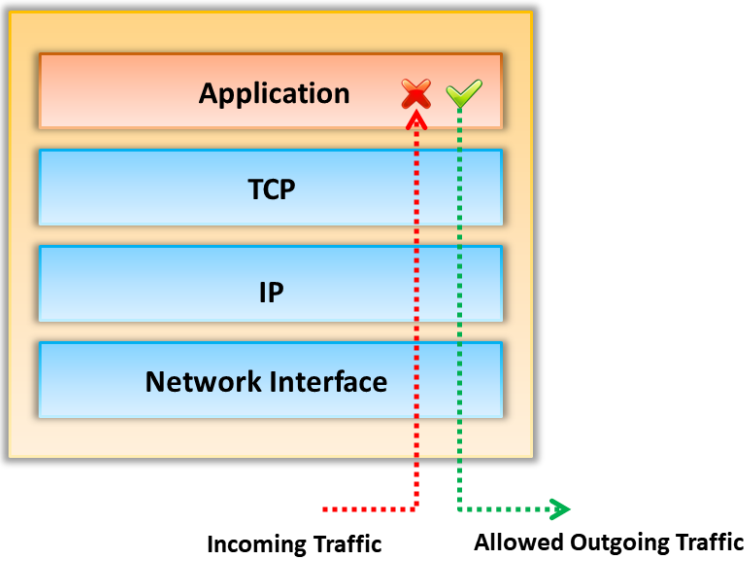


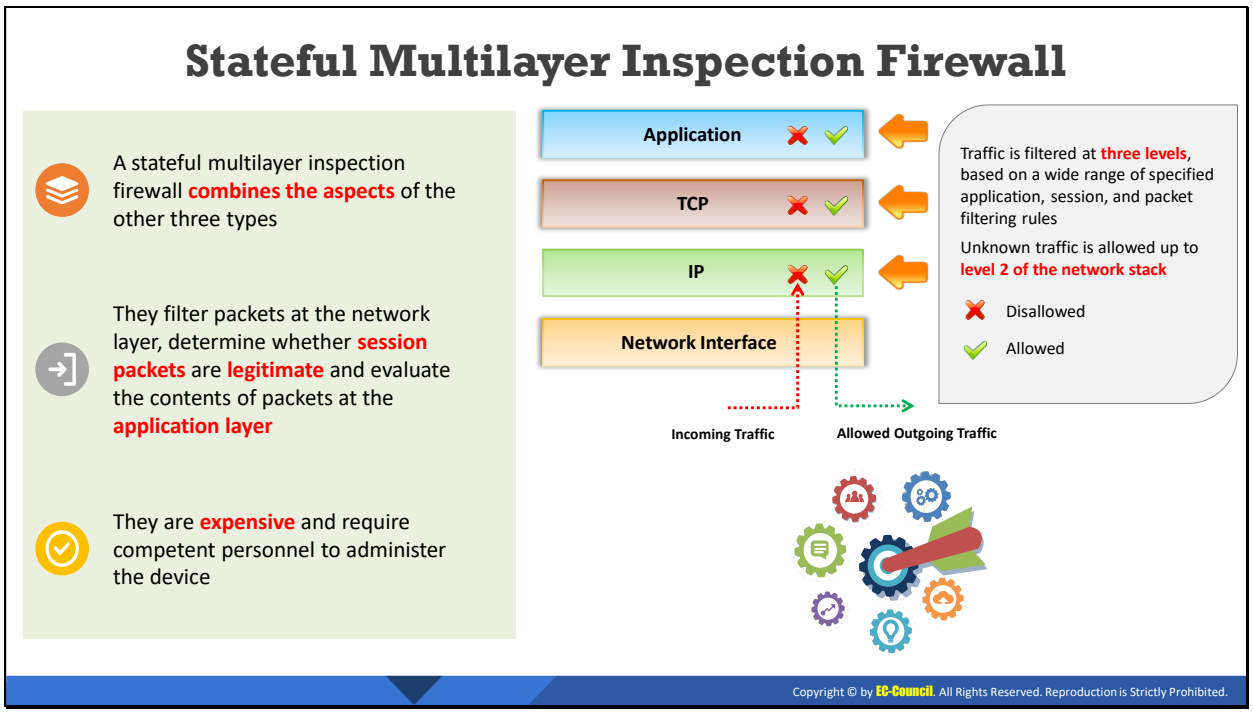
Figure 5.18: Application Level Gateway

The client and server communication does not happen directly; it happens only through a proxy server. This server acts as a gateway for two-sided communications and drops data packets acting against the firewall's policy rules.

- Application-level gateways, also called proxies, concentrate on the application layer rather than just the packets.
- They perform packet filtering at the application layer and make decisions about whether or not to transmit the packets.
- A proxy-based firewall asks for authentication to pass the packets as it works at the application layer.
- Incoming or outgoing packets cannot access services for which there is no proxy. In plain terms, design of an application-level gateway helps it to act as a web proxy and drop packets such as FTP, gopher, Telnet, or any other traffic that should not be allowed to pass through.
- As packet filtering is performed at the application level, it is possible to filter application-specific commands such as GET or POST requests.
- A content caching proxy optimizes performance by caching frequently accessed information instead of sending new requests for repetitive data transfers to the servers.

An application-level firewall checks for those packets that do not comply with the filtration rules. The unauthorized packets are dropped, and authorized packets are forwarded to the application layer of the destination.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Stateful Multilayer Inspection Firewall

Stateful multilayer inspection firewalls combine all the aspects of the previous three types of firewalls that have been discussed. They filter packets at the network layer, determine whether session packets are legitimate, and evaluate contents of packets at the application layer. They are expensive and require competent personnel to administer them. The packet filter firewall overcomes its inability to check the packet headers using stateful packet filtering.

Traffic is filtered at three levels, based on a wide range of specified application, session, and packet filtering rules. Unknown traffic is allowed up to level 2 of the network stack.

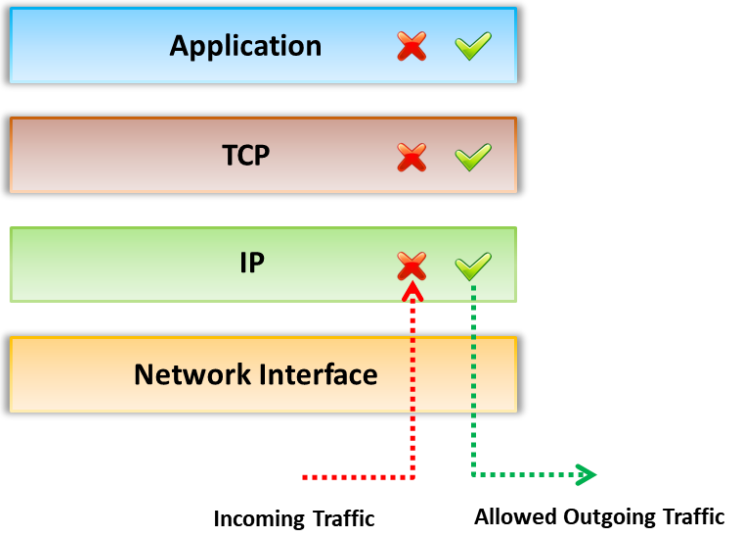


Figure 5.19: Stateful Multilayer Inspection Firewall

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

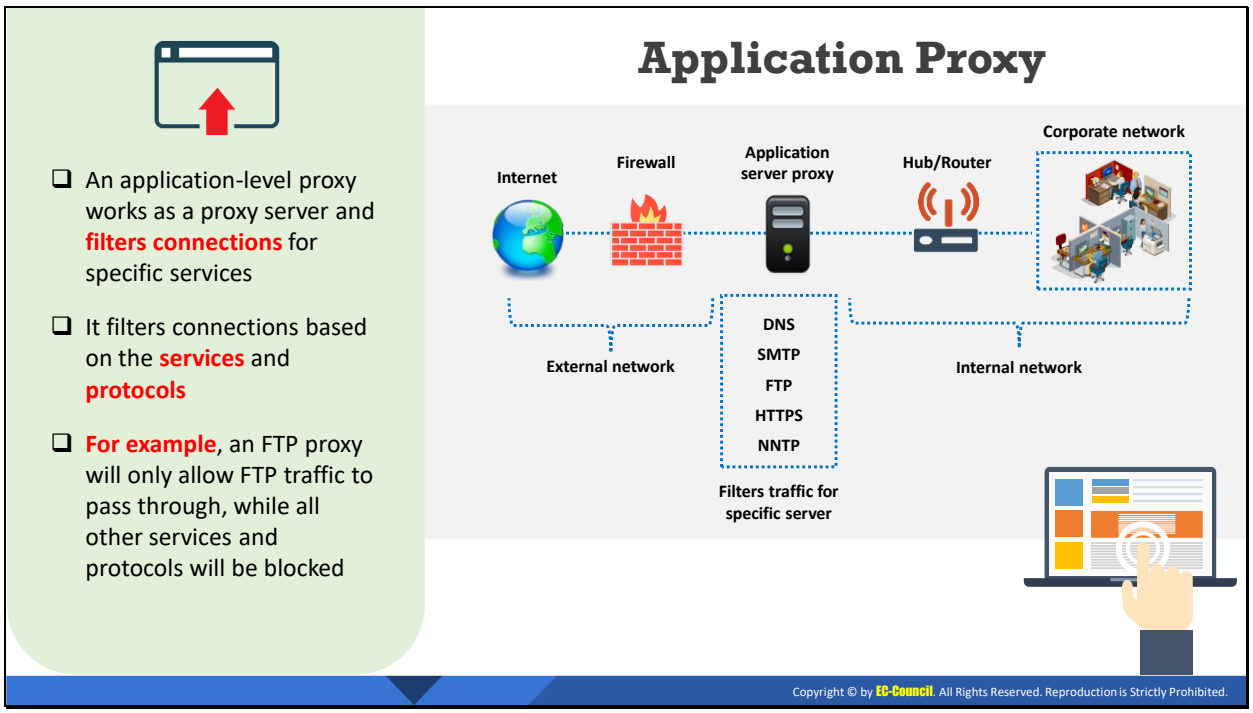
These firewalls eliminate the lack of transparency in application-level gateways as they allow a direct connection between the client and the host. These firewalls use algorithms to examine, filter, and process the application-layer data instead of using proxies. Stateful multilayer inspection firewalls have many advantages such as high level of security, better performance, and transparency to end users. They are quite expensive because of their complexity.

- Stateful multilayer firewalls can remember the packets that passed through them earlier and make decisions about future packets based on this information.
- These firewalls provide the best of both packet filtering and application-based filtering.
- Cisco Adaptive Security Appliances contain stateful firewalls.
- These firewalls track and log slots or translations.

They check for those packets that do not comply with the filtration rules and drop them at the network layer of the protocol stack. The other packets forwarded to the next layer undergo another layer of filtration to confirm whether the packets are in the proper session. Packets that are currently not a part of the session are dropped at the TCP layer. Next, packets are filtered at the application layer, enabling the user to allow only authorized actions at the firewall.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Application Proxy

An application-level proxy works as a proxy server and filters connections for specific services. It filters connections based on the services and protocols. For example, an FTP proxy will only allow FTP traffic to pass through, while all other services and protocols will be blocked.

It is a type of server that acts as an interface between the user workstation and the Internet. It correlates with the gateway server and separates the enterprise network from the Internet. It receives requests from users for services and responds to the original requests only. A proxy service is an application or program that helps forward user requests (for example, FTP or Telnet) to the actual services. Proxies are also called application-level gateways as they renew the connections and act as a gateway to the services. Proxies run on a firewall host that is either a dual-homed host or some other bastion host for security purposes. Some proxies, named caching proxies, run for the purpose of network efficiency. They keep copies of the requested data of the hosts they proxy. Such proxies can provide the data directly when multiple hosts request the same data. Caching proxies help in reducing load on network connections whereas proxy servers provide both security and caching.

A proxy service is available between a user on an internal network and a service on an outside network (Internet) and is transparent. Instead of direct communication between each, they talk with the proxy and it handles all the communication between user and the Internet service. Transparency is the key advantage when using proxy services. To the user, a proxy server presents the illusion that they are dealing directly with the real server whereas the real server thinks that it is dealing directly with the user.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

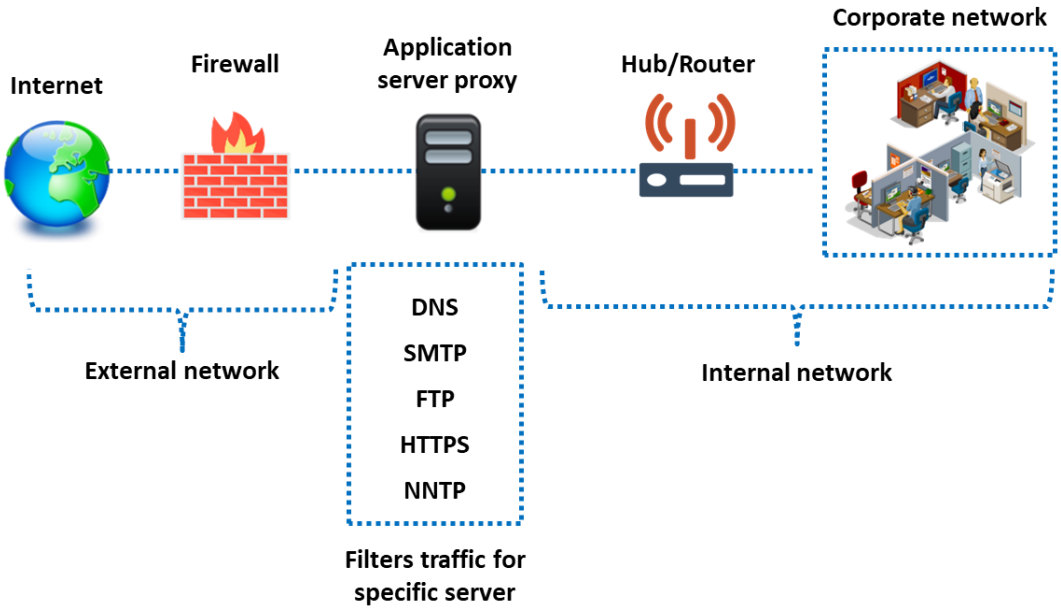


Figure 5.20: Application proxy

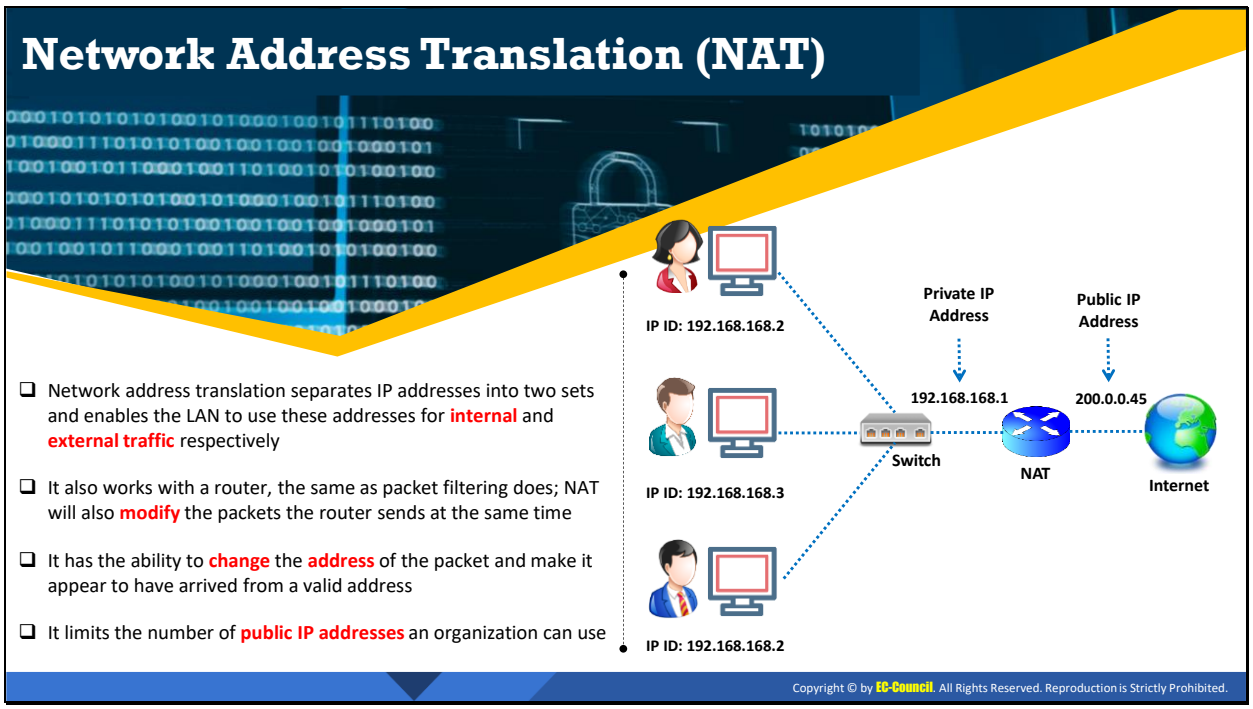
Advantages

- Proxy services can be good at logging because they can understand application protocols and allow logging in an effective way.
- Proxy services reduce the load on network links as they are capable of caching copies of frequently requested data and allow it to be directly loaded from the system instead of the network.
- Proxy systems perform user-level authentication, as they are involved in the connection.
- Proxy systems automatically provide protection for weak or faulty IP implementations as they sit between the client and the Internet and generate new IP packets for the client.

Disadvantages

- Proxy services lag behind non-proxy services until a suitable proxy software is made available.
- Each service in a proxy may use different servers.
- Proxy services may require changes in the client, applications, and procedures.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Network Address Translation (NAT)

Network address translation separates IP addresses into two sets and enables the LAN to use these addresses for internal and external traffic, respectively. A NAT helps hide an internal network layout and forces connections to go through a choke point. It works with the help of a router, helping to send packets and modifying them. When the internal machine sends the packet to the outside machine, NAT modifies the source address of the particular packet to make it appear as if it is coming from a valid address. Similarly, when the outside machine sends the packet to the internal machine NAT modifies the destination address to turn the visible address into the correct internal address. It limits the number of public IP addresses an organization can use. It can act as a firewall filtering technique where it allows only those connections which originate on the inside network and will block the connections which originate on the outside network. NATs can also modify the source and destination port numbers. NAT systems use different schemes for translating between internal and external addresses:

- Assigning one external host address for each internal address and always applying the same translation. This slows down connections and does not provide any savings in address space.
- Dynamically allocating an external host address without modifying the port numbers at the time when the internal host initiates a connection. This restricts the number of internal hosts that can simultaneously access the Internet to the number of available external addresses.
- Creating a fixed mapping from internal addresses to externally visible addresses and using port mapping so that multiple internal machines use the same external addresses.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- Dynamically allocating a pair of external host address and port each time an internal host initiates a connection. This makes the most efficient possible use of the external host addresses.

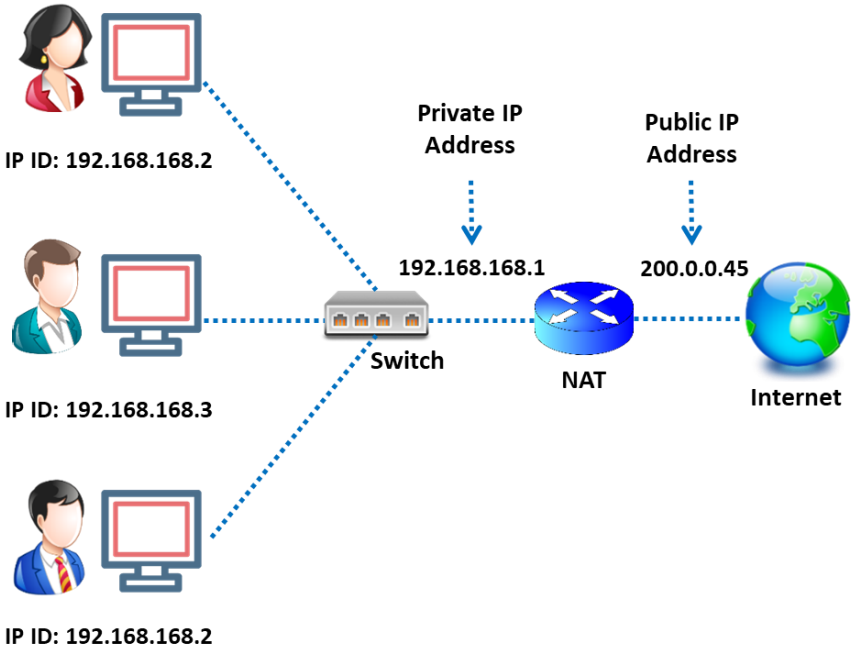


Figure 5.21: Illustration of network address translation

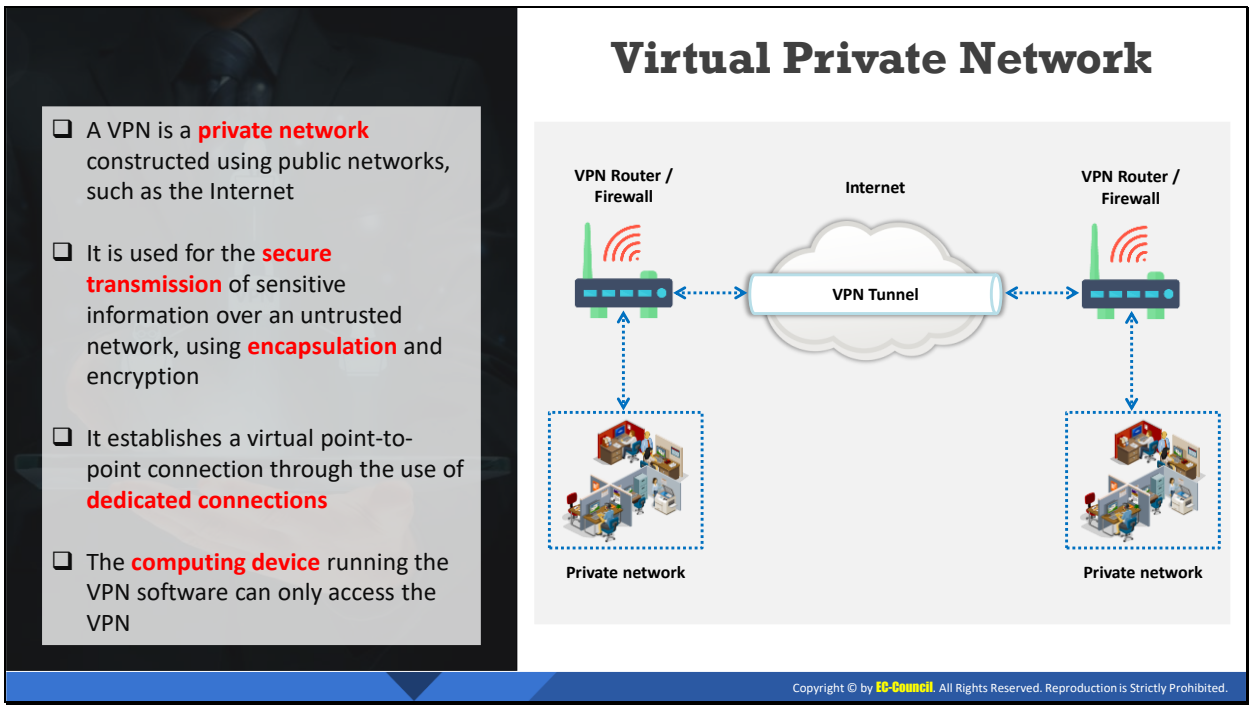
Advantages

- NAT help enforce the firewall's control over outbound connections.
- It restricts incoming traffic and allows only packets that are part of a current interaction initiated from the inside.
- It helps hide the internal network's configuration and thereby reduces vulnerability of the network or system from outside attacks.

Disadvantages

- The NAT system has to guess how long it should keep a particular translation, which is impossible to correctly guess every time.
- NAT interferes with encryption and authentication systems that ensure security of the data.
- Dynamic allocation of ports may interfere with packet filtering.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Virtual Private Network

A VPN is a private network constructed using public networks, such as the Internet. It is used for the secure transmission of sensitive information over an untrusted network, using encapsulation and encryption. It establishes a virtual point-to-point connection through the use of dedicated connections. The computing device running the VPN software can only access the VPN.

It is used for connecting Wide Area Networks (WAN). VPN allows computers of one network to connect to computers on another network. It employs encryption and integrity protection to enable utilization of a public network as a private network. A VPN performs encryption and decryption outside the packet-filtering perimeter to allow the inspection of packets coming from other sites; it encapsulates packets sent over the Internet. A VPN combines the advantages of both public and private networks. They have no relation to firewall technology, but firewalls are convenient tools for adding VPN features as they help in providing secure remote services. Any VPN that runs over the Internet employs the following principles:

- Encrypts all traffic
- Checks for integrity protection
- Encapsulates new packets, which are sent across the Internet to something that reverses the encapsulation
- Checks for integrity
- Finally, decrypts the traffic

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

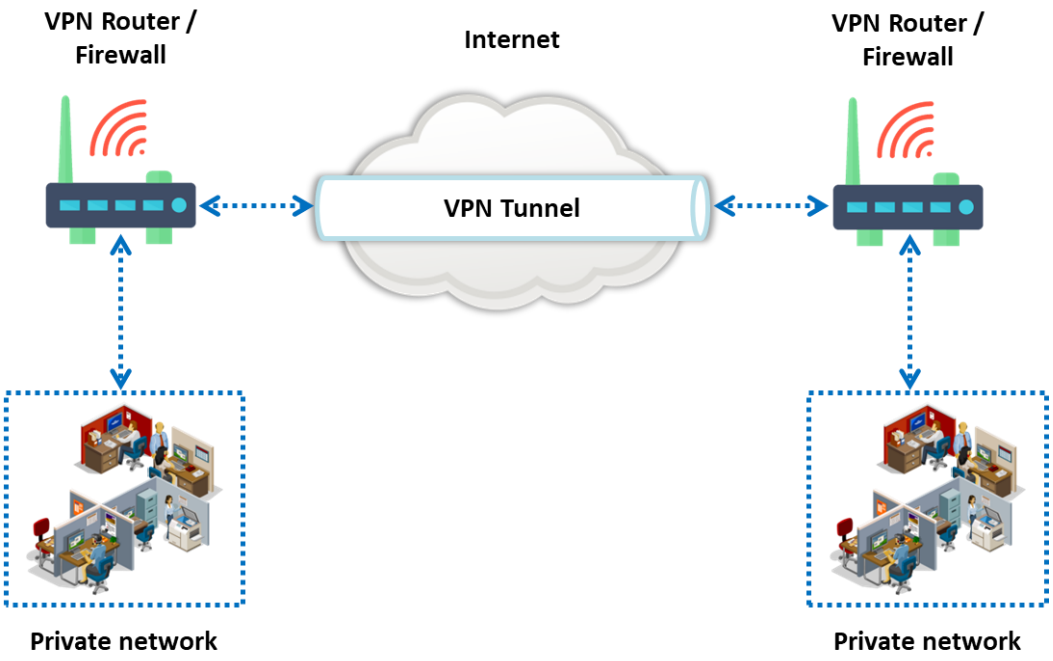


Figure 5.22: Virtual private network

Advantages

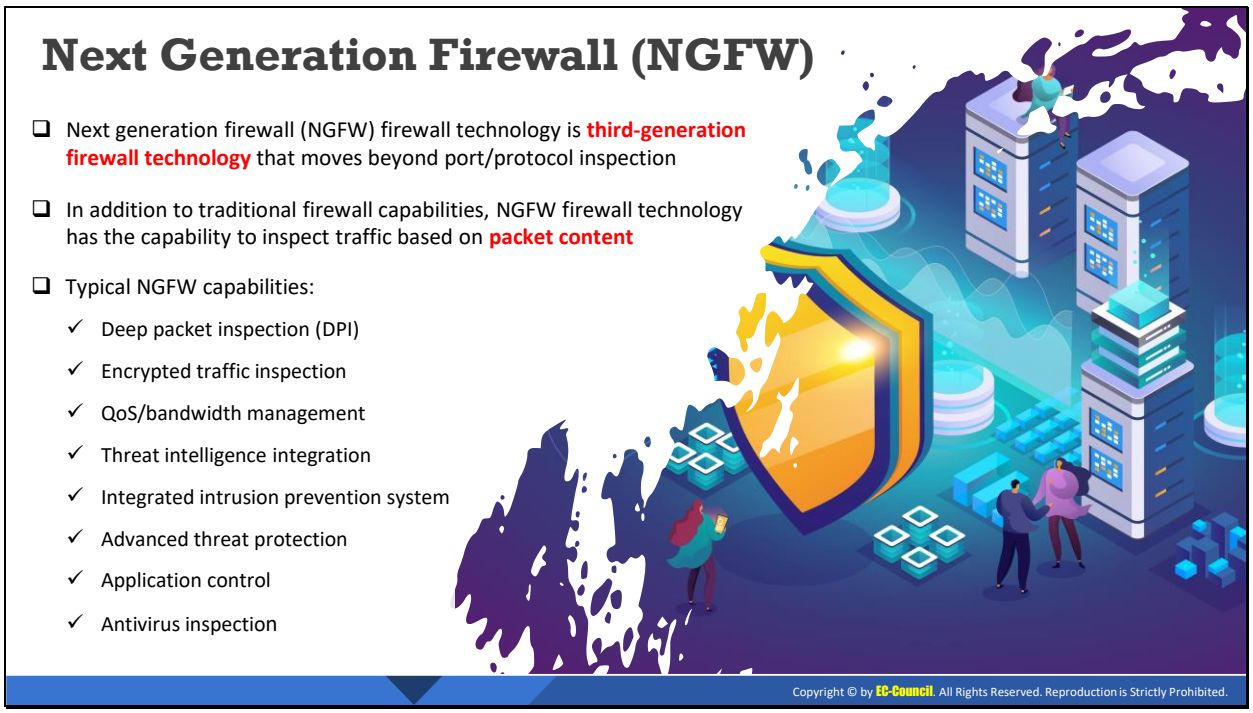
VPNs provide several security advantages, and they are listed below:

- A VPN hides all the traffic that flows through it, ensures encryption, and protects the data from snooping.
- It provides remote access for protocols while also defending against outside attacks.

Disadvantages

- As a VPN runs on a public network, the user remains vulnerable to an attack on the destination network.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Next Generation Firewall (NGFW)

An NGFW is a third-generation network security device that provides firewalling, intrusion prevention, and application control. In addition to traditional firewall capabilities, NGFW firewall technology has the capability to inspect traffic based on packet content**.** It offers packet filtering and proxy-based decision making within layers 3 and 4. It also expands its protection at the application layer (layer 7).

Features of NGFW

- Application awareness and control
- User-based authentication
- Malware protection
- Stateful inspection
- Integrated IPS
- Identity awareness (user and group control)
- Bridged and routed modes
- Ability to utilize external intelligence sources

Typical NGFW capabilities

- Deep packet inspection (DPI)
- Encrypted traffic inspection
- QoS/bandwidth management

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

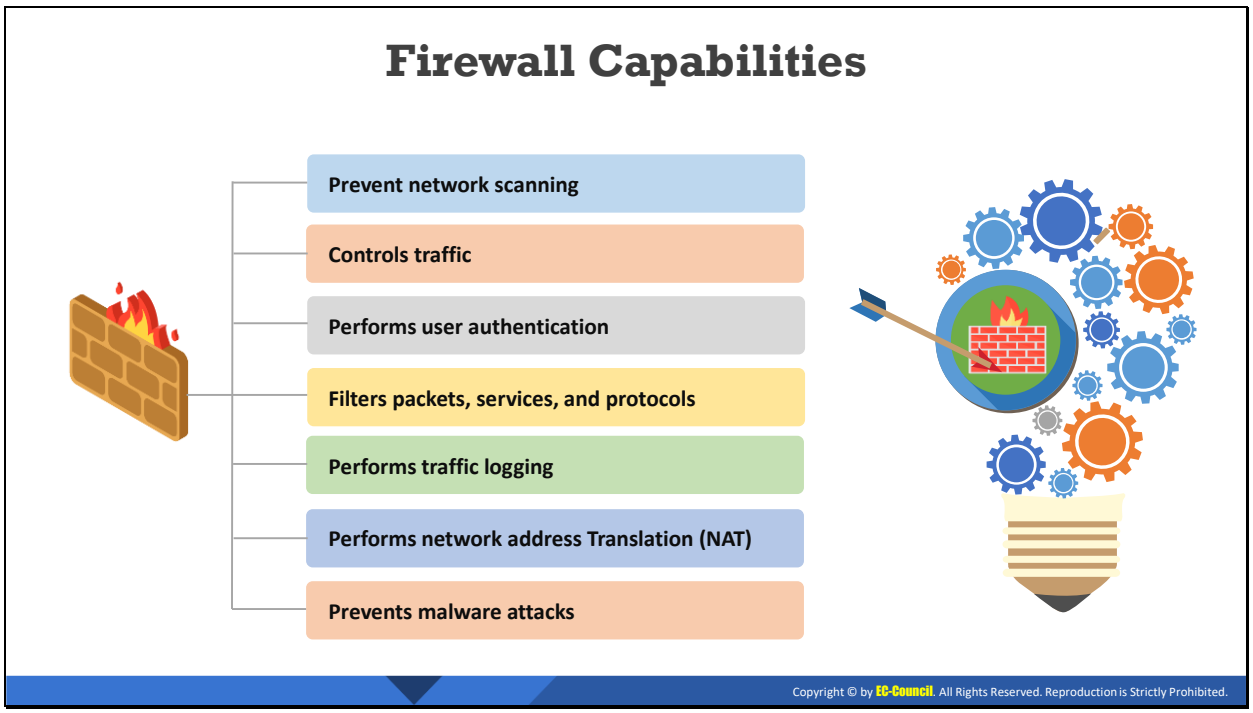
- Threat intelligence integration
- Integrated intrusion prevention system
- Advanced threat protection
- Application control
- Antivirus inspection

Advantages

- **Application-level security:** It provides application security functions such as IDS and IPS for improved packet-content filtering.
- **Single console access:** It can be accessed from a single console whereas traditional firewalls require manual setup and configuration.
- **Multilayered protection:** It provides multilayered protection by inspecting traffic from layers 2–7.
- **Simplified infrastructure:** It acts as the single authorized device for managing and updating security protocol.
- **Optimal use of network speed:** In traditional firewalls, the network speed decreases with increase in security protocol and devices, whereas with NGFW the potential throughput is consistently achieved irrespective of increase in the number of security protocols and devices.
- **Antivirus, ransomware and spam protection, and endpoint security:** NGFWs come as complete packages with antivirus, ransomware and spam protection, and endpoint security. Hence, there is no need for separate tools to monitor and control cyber threats.
- **Capability to implement role-based access:** NGFW detects user identity, which helps the organization set role-based access to their data and content. It can also work with different user roles and limit the scope of access for a user/group.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Firewall Capabilities

Be aware of a firewall's capabilities before planning for implementation. By knowing the capabilities of different types of firewalls, you will be able to decide what type to implement or whether a different security control or solution better suits your needs.

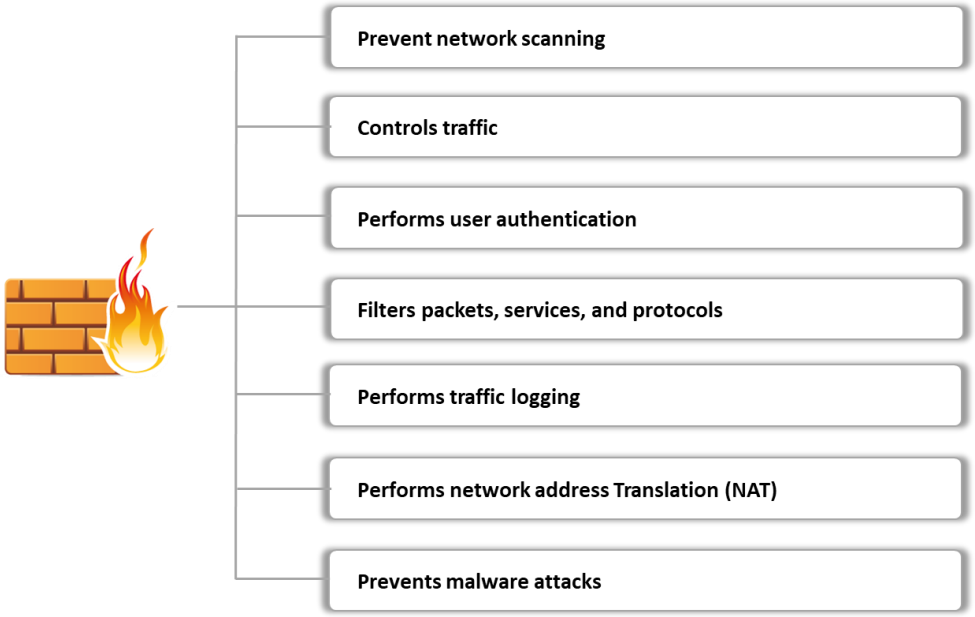


Figure 5.23: Firewall Capabilities

Listed below are the typical capabilities of a firewall:

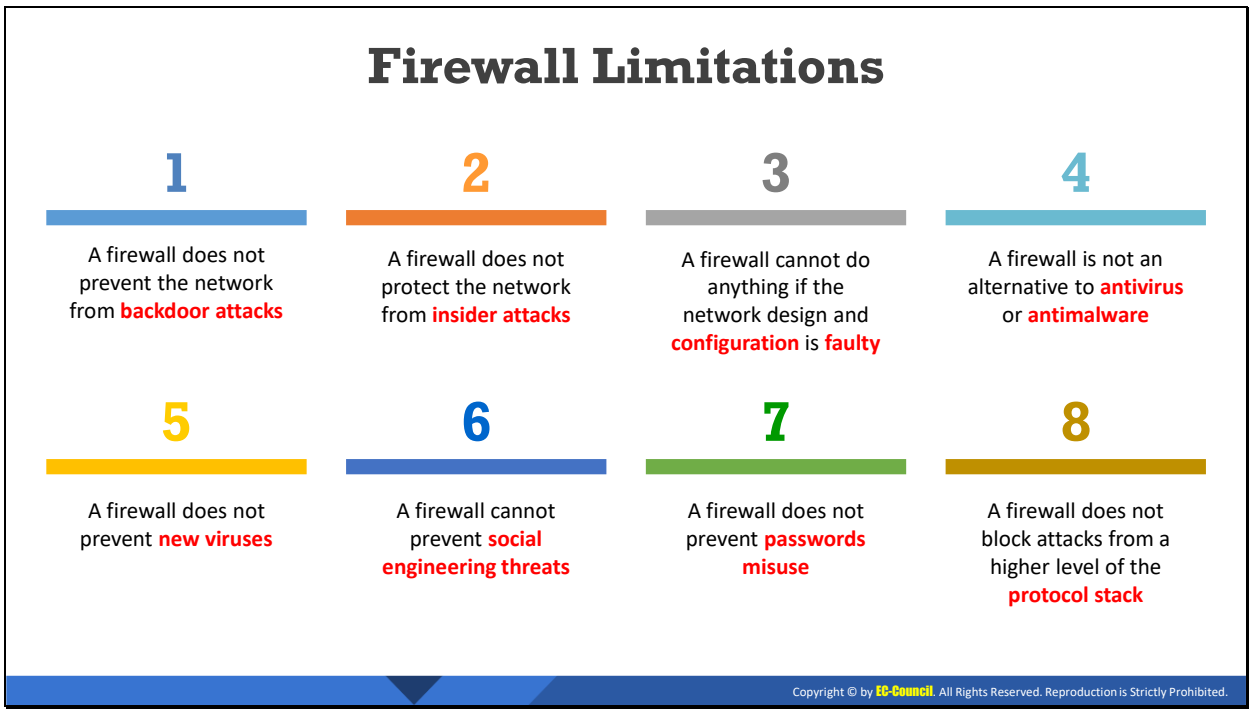
- A firewall examines all the traffic flowing through it to see if it meets the firewall ruleset criteria.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- It only permits traffic that is explicitly allowed by rules; all other traffic is normally denied by default.
- It filters both inbound and outbound traffic.
- It examines each packet passing through the network and decides whether to send the packet to the destination or not.
- It manages public access to private networked resources such as host applications.
- It logs all attempts to enter the private network and triggers an alarm when hostile or unauthorized entry is attempted.
- Firewalls work as filters and help in preventing unsafe packet flow into the private network.
- The functions of the firewall include gateway defense, carrying out defined security policies, hiding and protecting internal network addresses, reporting threats and activity, and segregating activity between trusted networks.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Firewall Limitations

Never ignore a firewall's limitations. Implementing a firewall without understanding its limitations may give one a false sense of security. Deploying a firewall solution that is not designed for a given task may fail to address the security risks the organization faces. Understanding the different types of firewalls and analyzing the limitations of each type will help in effectively balancing security with usability, performance, and cost.

Listed below are the typical limitations of firewalls:

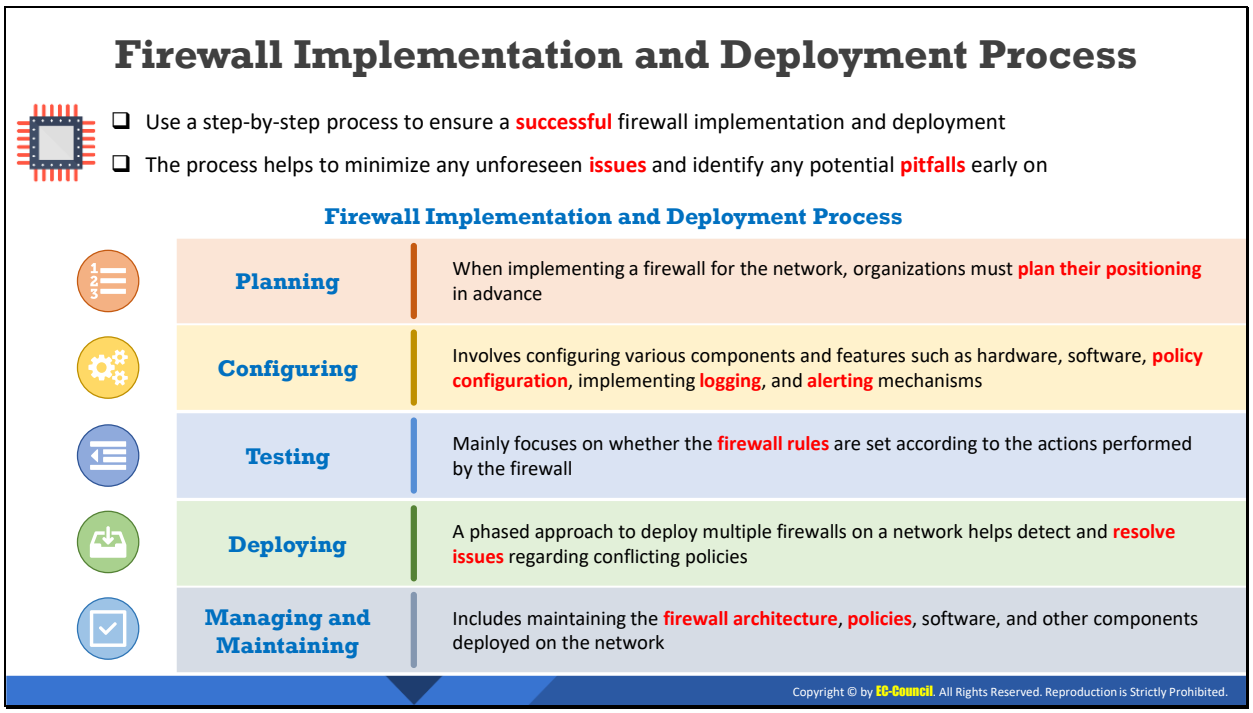
- A firewall does not protect the network from backdoor attacks. For example, a disgruntled employee who cooperates with an external attacker.
- A firewall does not protect the network from insider attacks
- A firewall cannot do anything if the network design and configuration is faulty
- A firewall is not an alternative to antivirus or antimalware. If external devices such as a laptop, mobile phone, portable hard drive, etc. are already infected and connected to the network, then firewalls cannot protect the network in such instances.
- A firewall does not prevent new viruses. Firewalls are unable to fully protect the network from all types of zero-day viruses that may try to bypass them.
- A firewall cannot prevent social engineering threats. They cannot protect the network from social engineering, insiders, and data-driven attacks where the attacker sends malicious links and emails to employees inside the network.
- A firewall does not prevent passwords misuse
- A firewall does not block attacks from a higher level of the protocol stack

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- A firewall does not protect against attacks originating from common ports and applications
- A firewall does not protect against attacks from dial-in connections
- A firewall is unable to understand tunneled traffic
- Firewalls can restrict users from accessing valuable services such as FTP, Telnet, NIS, etc. and sometimes restrict Internet access as well.
- Firewalls concentrate security at one single point, which makes other systems within the network prone to security attacks.
- They can cause a bottleneck if all the connections pass through a firewall.
- Sometimes, firewalls have less computing speed than their network interface. This can create a problem when a host with a network interface is faster than the firewall's internal processor.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Firewall Implementation and Deployment Process

A phased-based approach should be used to implement and deploy a firewall. Use a step-by-step process to ensure a successful firewall implementation and deployment. The use of a five-phased approach for implementation and deployment minimizes unforeseen issues and identifies potential pitfalls. The phases involved in implementing and deploying a firewall include planning, configuring, testing, deploying, and managing and maintaining.

- While planning a firewall implementation, consider all the requirements to determine which firewall to implement while enforcing network security policies.
- After planning, focus on configuring the firewall hardware and software components and setting up rules for the system to work effectively.
- Next, test the firewall prototype and its environment after successfully configuring the firewall. Assess its functionality, performance, scalability, and security for possible vulnerabilities and issues in the components.
- After resolving all issues encountered during the testing phase, deploy the firewall into the network.
- After successfully deploying the firewall, monitor it for component maintenance and resolving operational issues throughout its lifecycle, and consider incorporating enhancements or significant changes when needed.

Steps Involved in Firewall Implementation and Deployment

- **Planning:** When implementing a firewall for the network, organizations must plan their positioning in advance. It is critical to conduct a security risk assessment to know where a threat to the network would most likely originate and the reasons behind it.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Depending on the potential origin of threats, a layout for firewall implementation should then be built. Organizations must determine if they need to implement a firewall to enforce the new security policies.

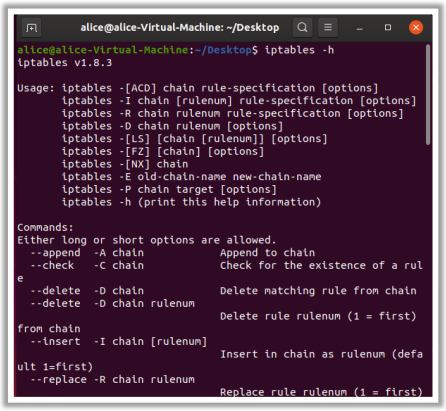
If an organization is considering implementing a firewall, remember to outline a consistent security policy in advance based on the risk assessment. The security policy must determine how basic communication will take place at the firewall, where the firewall must sit, and how to configure it.

- **Configuring:** Configuring a firewall involves configuring various components and features such as hardware, software, policy configuration, implementing logging, and alerting mechanisms.
- **Testing:** Testing a firewall involves examining it for any bugs. The firewall implementation test mainly focuses on whether the firewall rules are set according to the actions performed by the firewall. Firewall testing increases the reliability of the products using the firewall.
- **Deploying:** It is necessary to ensure the firewall is deployed according to the security policies of the organization. It is also necessary to alert the users of the deployment of the firewall. Similarly, the security policy of the firewall should be added to the network's overall policy and any configuration changes during implementation should be included. Employing a phased approach to deploy multiple firewalls on a network helps detect and resolve issues regarding conflicting policies.
- **Managing and Maintaining:** Managing a firewall includes maintaining the firewall architecture, policies, software, and other components deployed on the network. Update the policy rules when they identify new threats and if requirements change. The security of the firewall can be ensured by constantly monitoring and addressing the issues in the network. Additionally, monitor the firewall logs continuously in order to detect new threats and attacks in the network. Perform a firewall log analysis to detect security incidents.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Host-based Firewall Protection with Iptables

- Iptables is a **built-in firewall utility** for Linux OSes
- Iptables comes pre-installed on any Linux distribution. However, you can update/install it with `sudo apt-get install iptables` command

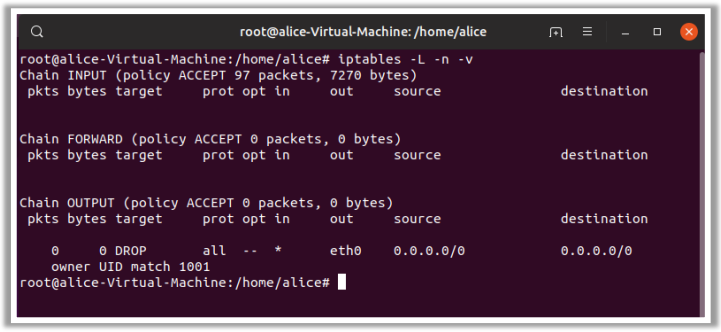


Task	Iptable Commands
Filtering non TCP packets	iptables -A INPUT -p tcp ! --syn -m state --state NEW -j DROP
Blocking XMAS scan Attack	iptables -A INPUT -p tcp --tcp-flags ALL -j DROP
Drop any NULL packets	iptables -A INPUT -f -j DROP
Drop any fragmented packets	iptables -A INPUT -f -j DROP

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

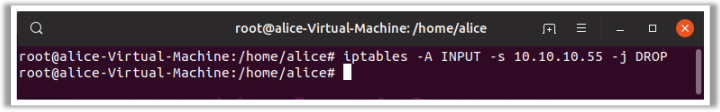
Host-based Firewall Protection with Iptables (Cont'd)

Existing rules can be checked using `sudo iptables -L -n -v` command



Specific IP address can be block using `Iptables Firewall`

`iptables -A INUPT -s 10.10.10.55 -j DROP`



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Host-based Firewall Protection with Iptables

Host-based firewalls provide enhanced security against threats. Linux systems support a kernel-based packet filter that is suitable for using host-based firewalls.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Iptables

Iptables is a command-line firewall utility that can allow or deny traffic. Iptables is preinstalled in a Linux system. In order to update or install iptables, the user needs to regain the iptables package using the command:

```
sudo apt-get install iptables
```

Every packet traversing through the filter system is assigned to an appropriate table depending on the tasks performed by the packet. The table contains chains that display the details of the destination of the packet. The tables can be used to create rules and the user has the facility to create their own chains and link them from the built-in chains. This facilitates the ability to create complex rules. However, the user needs to be extra alert while using the `iptables` command as any small error in the command can lock the system and may require the user to fix the error manually.

There are three different types of chains:

- Input: The input chain verifies the incoming connections and its behavior. Iptables compares the IP address and port of the incoming connection to a rule in the chain.
- Forward: The forward chain mainly forwards the incoming connections to its destination. The command **`iptables -L -v`** verifies whether an incoming connection needs a forward chain.
- Output: The output chain is used for output connections, wherein the chain checks for the output chain and decides whether to allow or deny the output request.

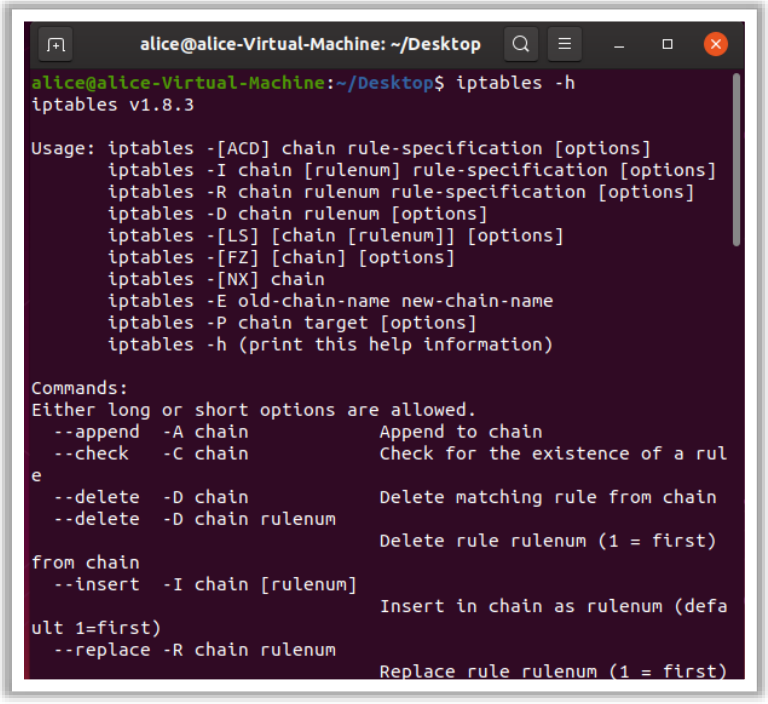


Figure 5.24 iptables chain

Example iptables firewall rules:

- Check the existing rules using the **`sudo iptables -L -n -v`** command.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

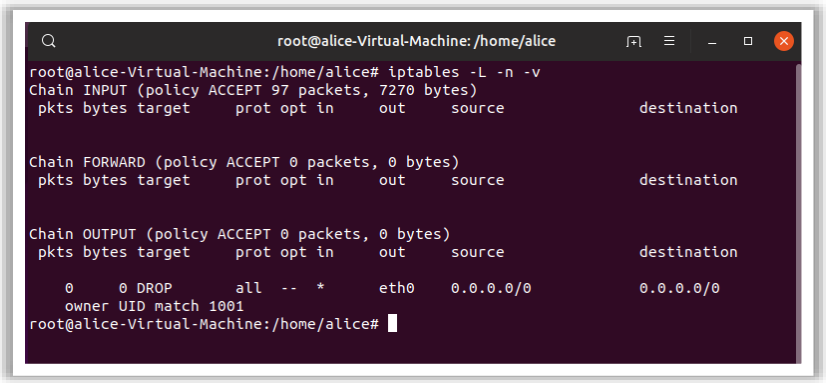


Figure 5.25: iptables firewall rules

- Check the rules for a specific table using the command **# iptables -t nat -L -v -n.**
- Block the specified IP address using iptables firewall.

  Iptables –A INUPT –s 10.10.10.55 –j DROP

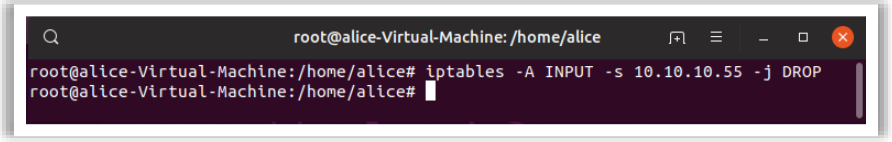


Figure 5.26: Blocking specific IP address

- Block specific port on iptables firewall using the command **# iptables -A OUTPUT -p tcp --dport xxx -j DROP.**
- Block Facebook on Iptables firewall using the command **# iptables -A OUTPUT -p tcp -d 66.220.144.0/20 -j DROP.**

Task	Iptables Commands
Filtering non-TCP packets	**iptables -A INPUT -p tcp ! --syn -m state --state NEW -j DROP**
Blocking XMAS scan attack	**iptables -A INPUT -p tcp --tcp-flags ALL -j DROP**
Drop any NULL packets	**iptables -A INPUT -f -j DROP**
Drop any fragmented packets	**iptables -A INPUT -f -j DROP**
Block network flood on Apache port	**iptables -A INPUT -p tcp --dport 80 -m limit --limit 100/minute --limit-burst 200 -j ACCEPT**
Block incoming ping requests	**# iptables -A INPUT -p icmp -i eth0 -j DROP**
Block access to a specific MAC address	**iptables -A INPUT -m mac --mac-source 00:00:00:00:00:00 -j DROP**
Block connection on network interface	**iptables -A INPUT -i eth0 -s xxx.xxx.xxx.xxx -j DROP**
Disable outgoing mails	**iptables -A OUTPUT -p tcp --dports 25,465,587 -j REJECT**

Table 5.2: Other iptables commands for various tasks

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

UFW

UFW (uncomplicated firewall) is an interface to iptables. For beginners, it is difficult to use iptables for configuring a firewall. UFW can help them by simplifying the process of configuring a firewall to make the system secure in the network. Enable UFW to protect unusual traffic

Steps to Set Up a Firewall with UFW

- Install UFW using the **`sudo apt-get install ufw`** command.

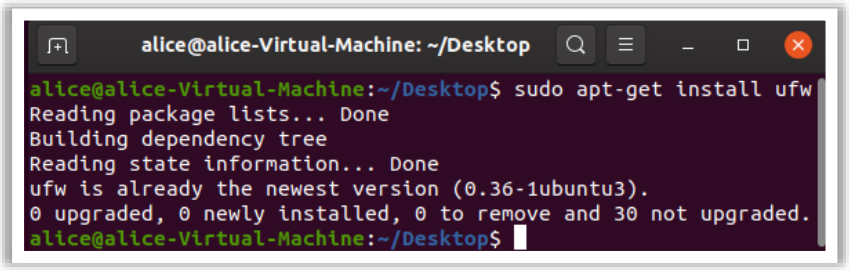


Figure 5.27: Installing UFW

- Check the status of UFW using the **`sudo ufw status verbose`** command. The output will be active or inactive. The default status of UFW is disabled.

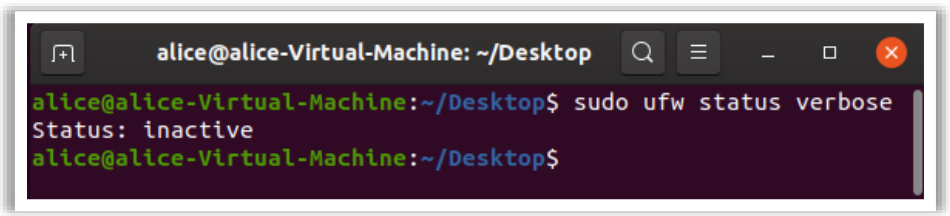


Figure 5.28: Checking status of UFW

- Enable UFW using the **`sudo ufw enable`** command.

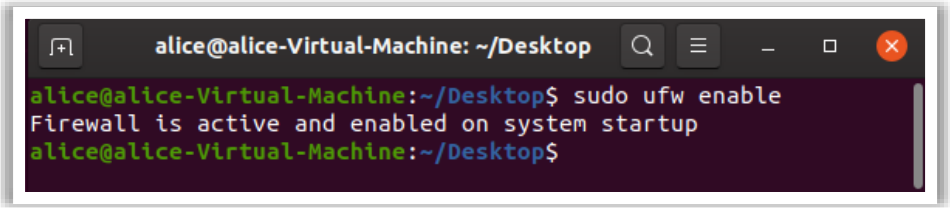


Figure 5.29: Enabling UFW

- Set default policies using the following commands.

  `sudo ufw default deny incoming`

  `sudo ufw default allow outgoing`

Add UFW Rules

There are two ways to add rules: denoting the port number and using the service name.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

A few examples and corresponding commands are discussed below.

- Allow both incoming and outcoming connections on port 22 for SSH.

  sudo ufw allow ssh

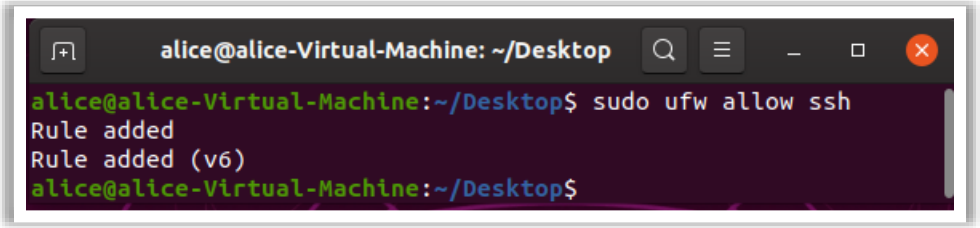


Figure 5.30: Adding UFW rules

(or)

sudo ufw allow 2000

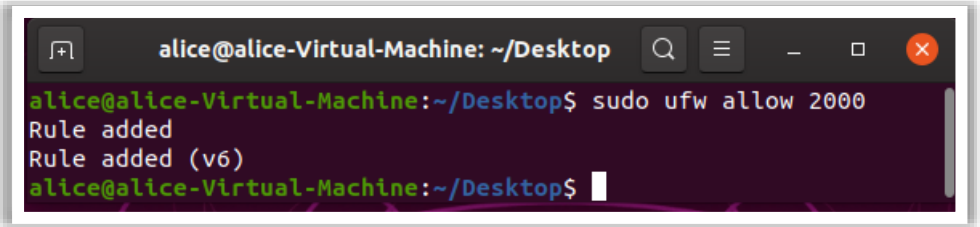


Figure 5.31: Adding UFW rules

- Deny traffic on a specific port.

  sudo ufw deny 22.

- Allow packets based on TCP or UDP.

  sudo ufw allow 80/tcp

  sudo ufw allow http/tcp

  sudo ufw allow 1725/udp

- Allow connections from an IP address.

  sudo ufw allow from 10.10.10.25

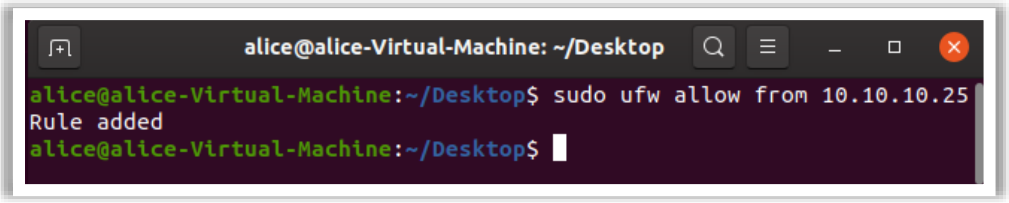


Figure 5.32: Allowing connections

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- Deny connections from an IP address

  Sudo ufw deny from 10.10.10.24.

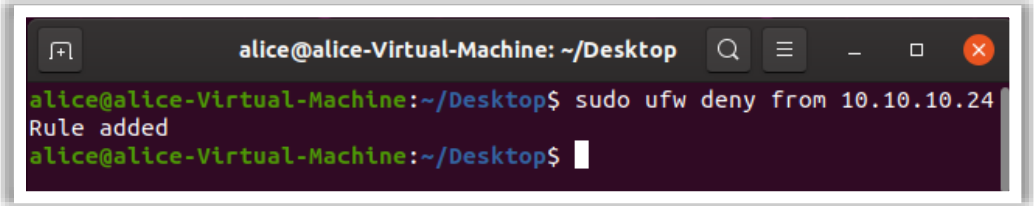


Figure 5.33: Denying connections

- Allow connections from a specific subnet.

  sudo ufw allow from 198.51.100.0/24

- Allow a specific IP address/port combination.

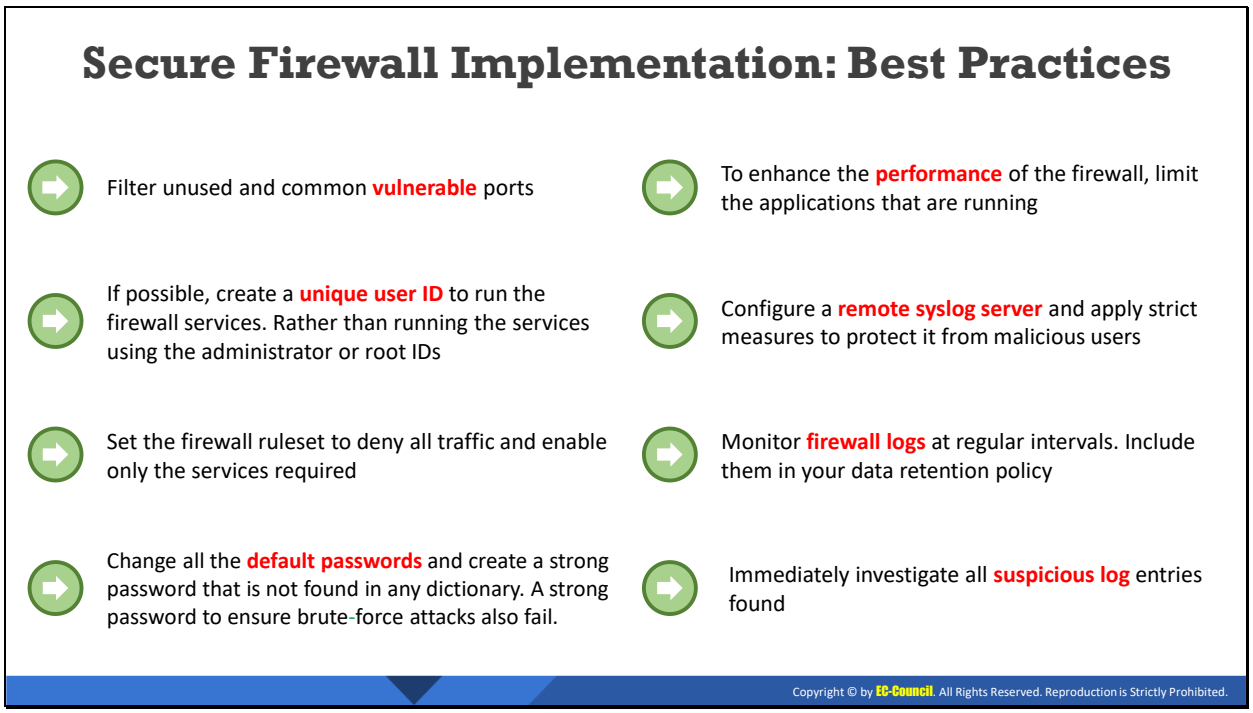
  sudo ufw allow from 198.51.100.0 to any port 22 proto tcp

- When more advanced or specific rules need to be added/removed:
  - Add the rules to the **/etc/ufw/before.rules** (**before6.rules** for IPv6) file to execute the rules.
  - There exists **after.rule** and an **after6.rule** files to add any rules that would need to be added after UFW runs the command-line-added rules.
  - An additional configuration file that is located at **/etc/default/ufw** allows the user to disable or enable IPv6, to set default rules, and set UFW to manage built-in firewall chains.

Remove UFW Rules

Delete rules using port number or service name. Use **delete** in the command while removing a rule. For example, the command to delete allowing HTTP traffic from port number 80 is **sudo ufw delete allow 80.**

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Secure Firewall Implementation: Best Practices

The following best practices will help harden firewall security:

- Filtering unused and vulnerable ports on a firewall is an effective and efficient method of blocking malicious packets and payloads. There are different types of filters in firewalls ranging from simple packet filters to complex application filters. The defense-in-depth approach using layered filters is a very effective way to block attacks.
- Configuring administrator accounts to run a firewall depends on the security requirements of the organization and different administrative roles the organization requires. A role defines the type of access the associated administrator has been granted to the firewall system. If possible, create a unique ID to run the firewall services rather than running it as administrator or root.
- While creating a firewall ruleset, organizations should first determine what type of traffic is needed to run the approved applications. Then set the firewall rules to deny all the traffic and allow only those services the organization needs.
- Change all the default passwords and create a strong password that is not found in any dictionary. A strong password to ensure brute-force attacks also fail.
- Firewalls use a complex rule base to analyze applications and determine if the traffic should be allowed through or not. Setting up firewall rules to grant access to important applications and blocking the rest will improve the performance of the firewall.
- Ensure that the date, time, and time zone on the remote syslog server matches the network configuration in order for the server to send syslog messages. Syslog data is not useful for troubleshooting if it shows the wrong date and time. In addition, configuring

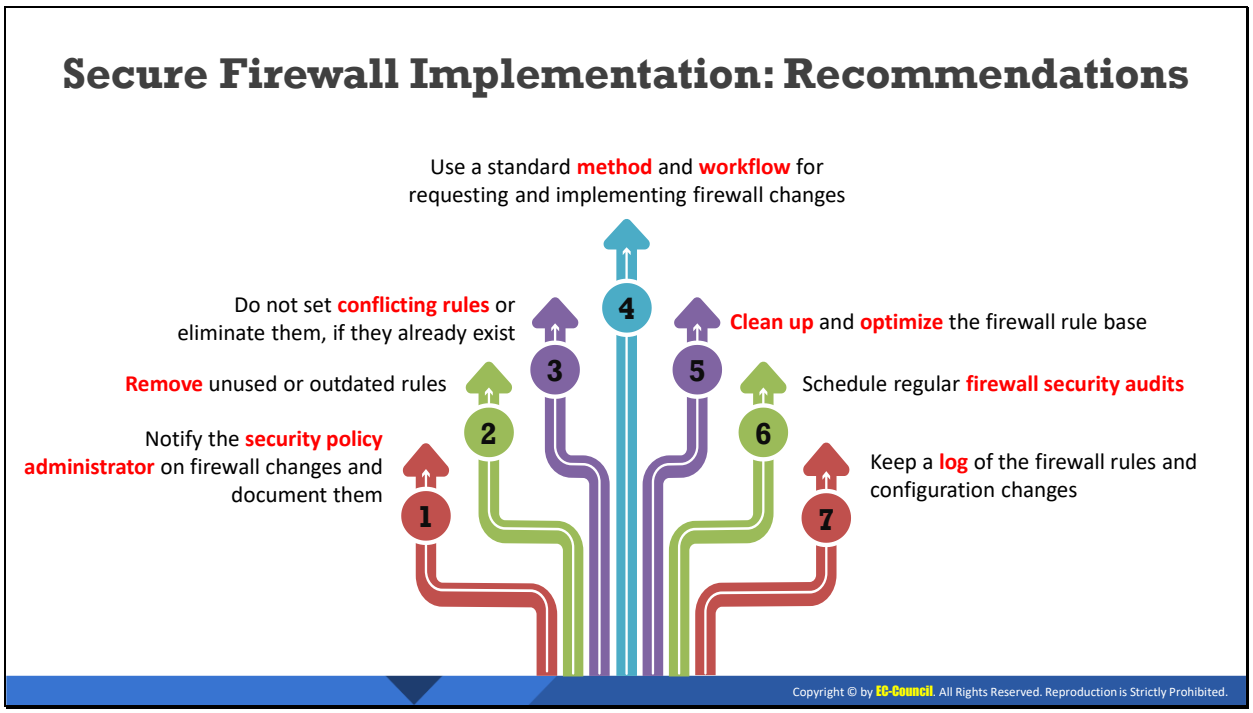
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

all network devices to use network time protocol (NTP) ensures correct and synchronized system clocks on all network devices.

- Monitor the firewall logs at regular intervals even if the company's management policy allows for some private use of its equipment. Monitoring what websites employees are visiting, what files they are sending and receiving, and even the content in their emails will assist in maintaining the network securely.
- Logging firewalls 'allow' actions offer greater insight into malicious traffic and tracking firewall 'deny' actions help identify threats.
- Take regular backups of the firewall logs—at least on a monthly basis—and store these backups on secondary storage devices for future reference or for legal issues in case there is an incident. The best way to achieve this is to use a scheduling function in the firewall. Backup the firewall before and after making a change in its rules and ensure that the backup configuration file is usable.
- Perform audits at least once every year on firewalls to evaluate the standards implemented to secure the organization's IT resources. This will offer a record of all the files employees access, including failed attempts. Ensuring every change is accounted for will greatly simplify audits and help the daily troubleshooting.
- Firewalls cannot secure the network from internal attacks. Organizations are required to implement different strategies such as policies that restrict employee usage of external devices in the internal network. For preventing any internal network attacks, install monitoring software that will help detect any suspicious internal activity.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

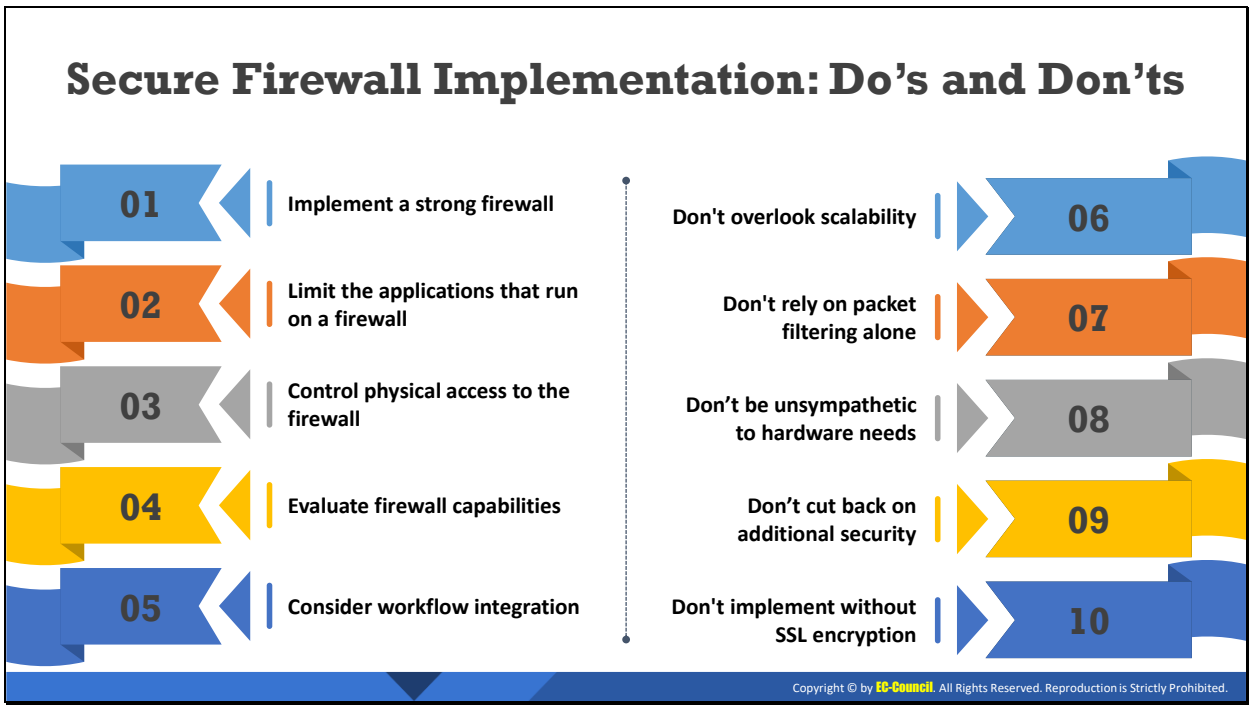
https://t.me/learningnets



Secure Firewall Implementation: Recommendations

- Notify the security policy administrator on firewall changes and document them. Document any changes made to the firewall. With firewalls, it is especially critical to document the rules that have been added or changed so that other administrators know the purpose of each rule and who to contact about them. Good documentation can make troubleshooting easier and it reduces the risk of service disruptions that are caused when a deletion or change in rule the security professional is unable to understand.
- Remove unused or outdated rules. Organizations can generate analysis reports to evaluate firewall access rules. This assists in identifying rules that overlap or are conflict with other rules in the access rule policy. Delete, move, or edit conflicting rules using the data from the report. Organizations can develop an easier to use and more efficient access rules policy if they eliminate unnecessary rules.
- Implement a consistent workflow solution to manage and streamline the firewall change process. Identify potential risks and fix configuration errors before making changes to the firewall. Reduce the time required to evaluate and implement the changes to support the network.
- Clean up and optimize the firewall rule base.
- Schedule regular firewall security audits.
- Keep a log of the firewall rules and configuration changes.

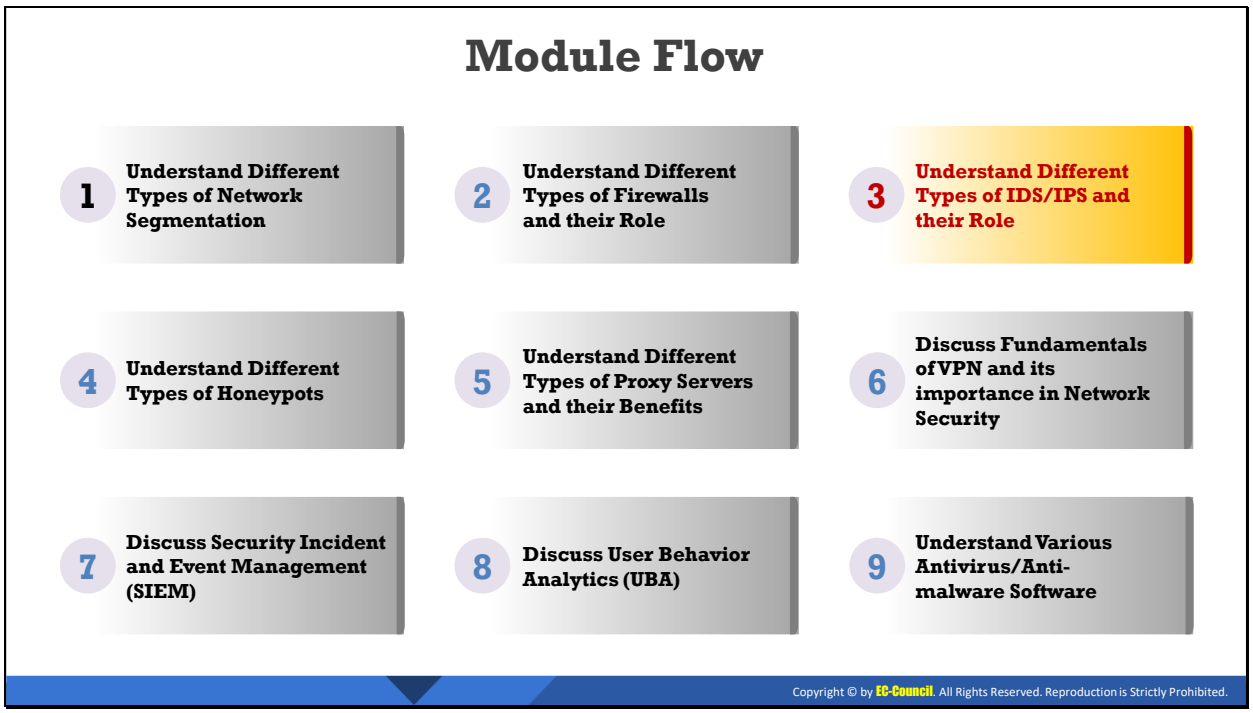
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Secure Firewall Implementation: Do's and Don'ts

- Implement a strong firewall.
- Limit the applications that run on a firewall.
- Control physical access to the firewall.
- Evaluate firewall capabilities.
- Consider workflow integration.
- Review and refine your policies and procedures.
- Incorporate trust marks.
- Take regular backups of the firewall ruleset and configuration files.
- Do not overlook scalability.
- Do not rely on packet filtering alone.
- Do not be unsympathetic to hardware needs.
- Do not cut back on additional security.
- Do not implement without SSL encryption.
- Do not allow telnet access through the firewall.
- Do not allow direct connections between the internal client and any outside services.

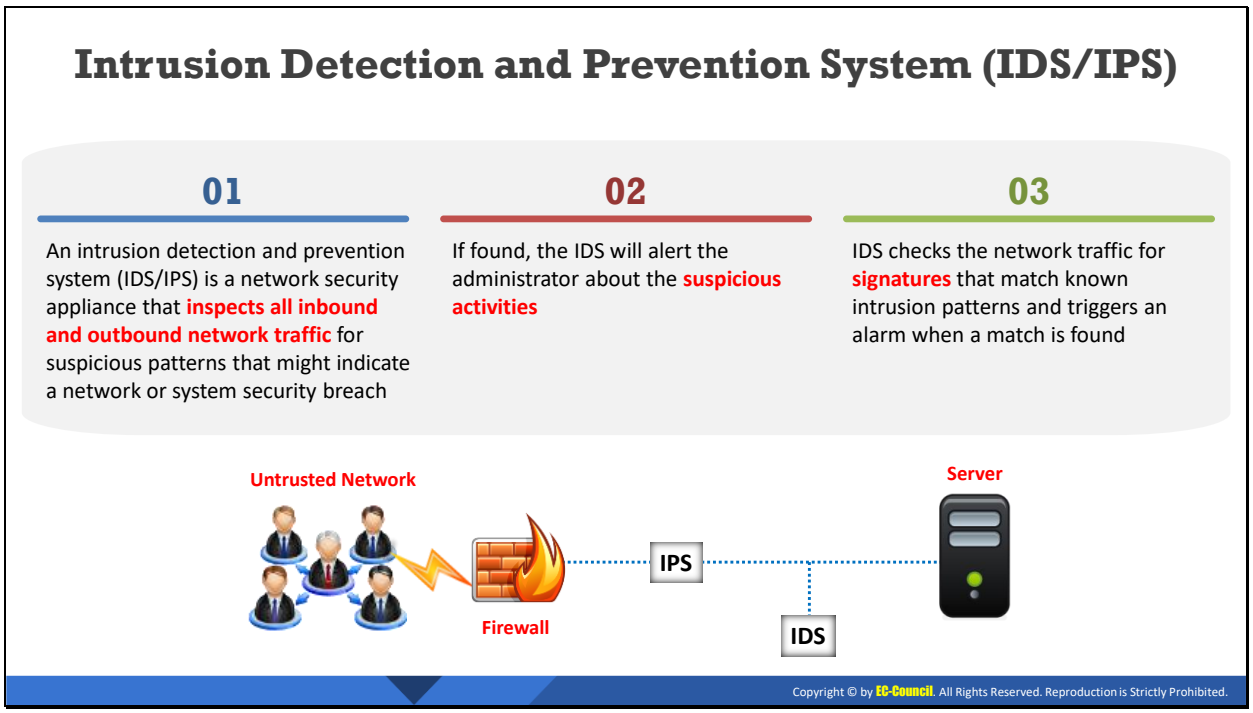
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Understand Different Types of IDS/IPS and their Role

The objective of this section is to explain different types of IDS/IPS, their role, capabilities, limitations, and concerns in implementing IDS security. This section also discusses IDS components, collaboration of IDS components in intrusion detection, deployment of network and host based IDS, types of IDS alerts, and intrusion detection tools.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Intrusion Detection and Prevention System (IDS/IPS)

An Intrusion Detection and Prevention System (IPS/IDPS) is a network security appliance which inspects all inbound and outbound network traffic for suspicious patterns that could indicate a network or system security breach, identifies suspicious activity if any, logs information of the suspicious activity, reports it and attempts to block it. An intrusion prevention system (IPS) is an extension of the intrusion detection system (IDS). An IPS can

- Send alarms
- Defragment packet streams
- Drop identified malicious packets
- Reduce TCP sequencing issues
- Reset a connection
- Block traffic from a malicious IP address
- Correct cyclic redundancy check (CRC) errors
- Clean unneeded transport and network layer options

The Intrusion Detection System (IDS) monitors all inbound and outbound network activity and identifies malicious patterns by looking for known attack signatures and warns the security professionals of suspicious activity but does not prevent them. An IDS displays an alert, logs the event, or pages an administrator, reconfigures the network to mitigate the consequences of intrusions.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

IDS vs. IPS

The key difference between an IPS and an IDS is that the IPS is implemented in-line, however the IDS sits off to the side. The traffic that is directed through an IPS either blocks or allows the packets depending on the policy and performs correction if needed. In the case of IDS, it is connected via a network tap and it monitors traffic, but cannot act directly.

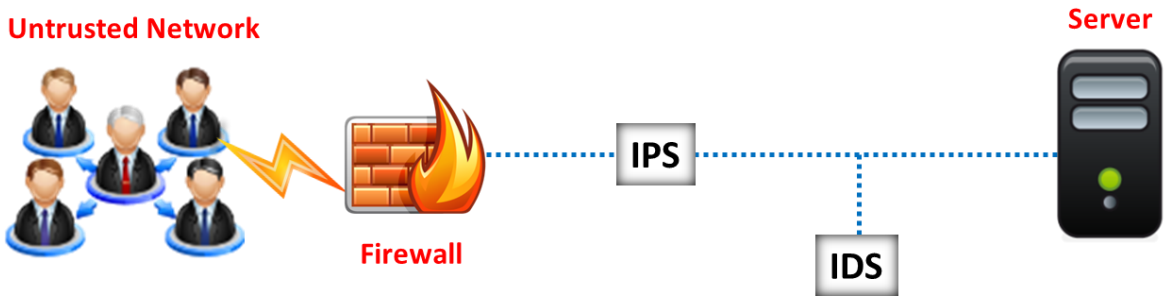
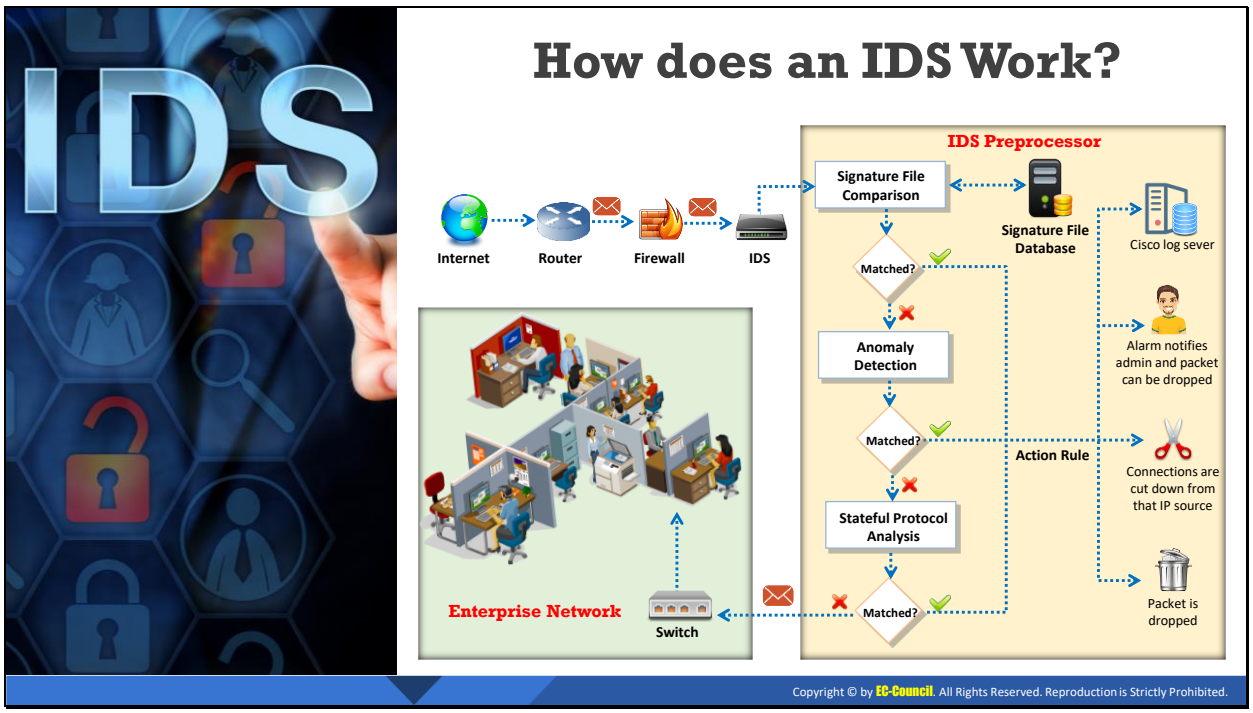


Figure 5.34: IDS vs. IPS

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



How does an IDS Work?

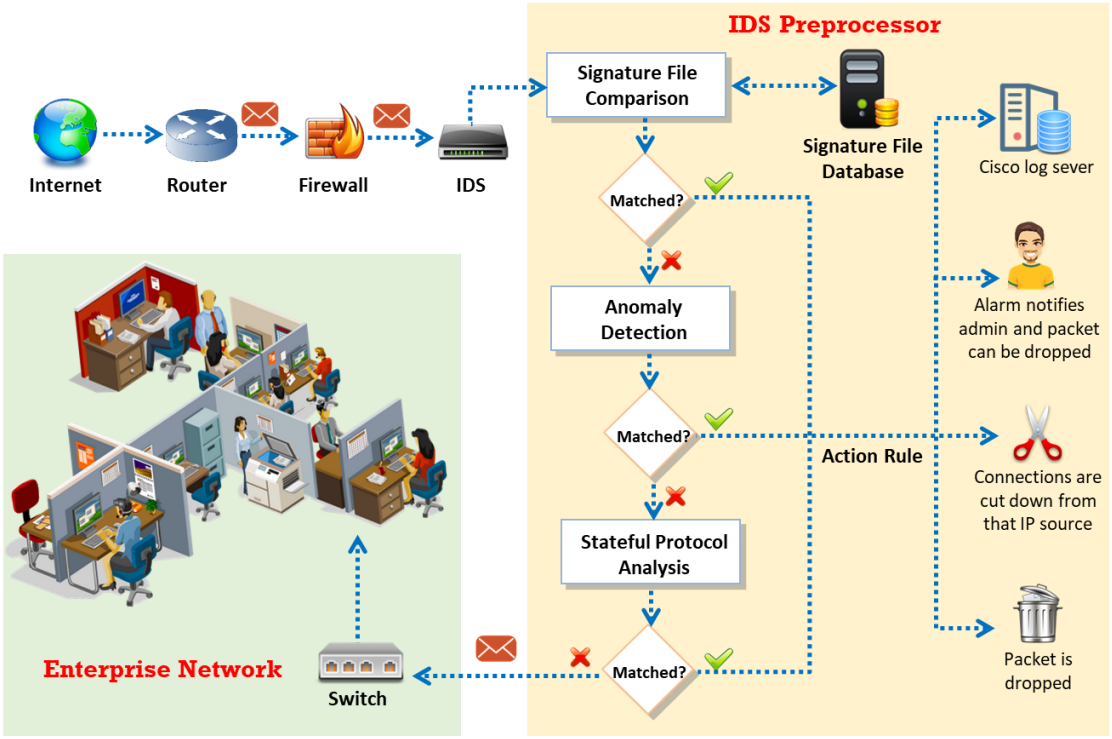


Figure 5.35: Working of an IDS

Signature-based IDS: In a signature-based IDS, the network traffic is checked with the databases that comprises of intrusions. As shown in the above figure, if an attack signature matches with any of the signatures in the signature file database, the connection will be disconnected down from the source IP, the packet will be dropped, the activity will be logged,

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

and an alarm will be initiated. Alternatively, the packet will be moved to the next step called the anomaly detection step.

Anomaly-based IDS: An anomaly-based IDS uses statistical techniques to compare the monitored traffic with the normal traffic. This method can identify new forms of attacks that are not in the IDS signature database and issue a warning. The disadvantage of this method is issuing false positive messages, which will complicate the functioning of an administrator. In the anomaly detection step, if the attack signature matches, the connections will be disconnected from the source IP, the packet will be dropped, the activity will be logged, and an alarm will be initiated. Alternatively, the packet will be sent to stateful protocol analysis.

A stateful protocol analysis is used for detecting the deviations of the protocol state, which uses predetermined profiles based on the vendor-developed definitions of malicious activity. In the stateful protocol analysis, if the packet is matched, the connections will be disconnected from the source IP, the packets will be dropped, the activity will be logged, and an alarm will be initiated. Alternatively, the packet will be passed to the network through a switch.

An IDS performs an evaluation of a network traffic for illegal activities and policy violations. It performs a vulnerability assessment for ensuring the security of the network. The following are the features of IDS:

- Evaluating system and network activities
- Analyzing vulnerabilities in a network
- Measuring the system and file reliability
- Skill to identify the possibilities of attacks
- Monitoring irregular activities in a network and system
- Evaluating the policy violations

Organizations can identify the presence of attacks or intrusions from outside a network as well as the intrusions or misuse within that network. An IDS generally performs a vulnerability assessment or scanning in order to identify the vulnerabilities in a network and to monitor the security of the network.

Firewalls prevent intrusions within a network, but do not actually issue an alert regarding an intrusion or an attack. On the other hand, IDS systems can monitor and identify the intrusions within a network as well as signal an alarm to the administrator.

Advantages of IDS:

- An IDS allows continuous monitoring and tracking of all intrusions and attacks in a network.
- An IDS provides an extra layer of security to a network.
- An IDS can also provide a log or data regarding the attack or intrusion that can be later used for investigating the incident.
- IDS requires more maintenance as compared to firewalls.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

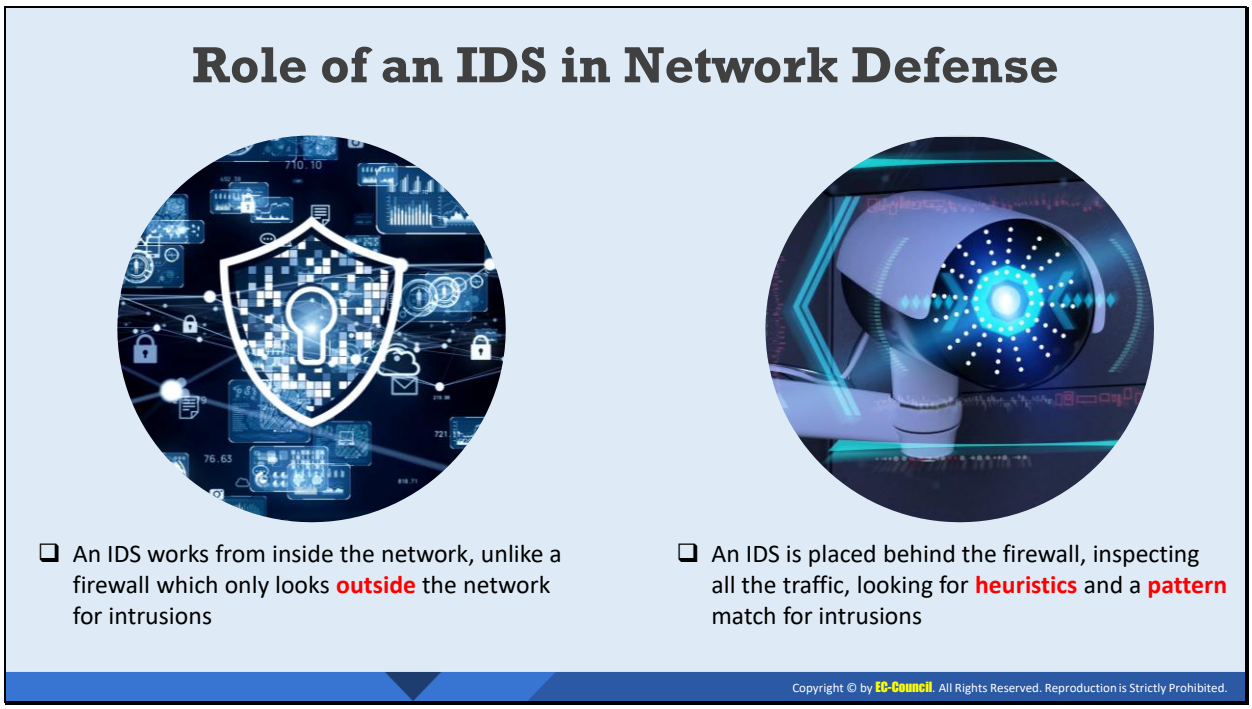
https://t.me/learningnets

Disadvantages of IDS:

- It is not always possible for an IDS to detect intrusions.
- IDS requires properly trained and experienced users to maintain it.
- IDS can raise false alarms to the network administrator.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Role of an IDS in Network Defense

Why Do We Need IDS?

Relying solely on a firewall for network security can provide a false sense of security. The firewall is simply implemented in the IT security policy to allow or deny traffic based on the policy rules. It allows certain packets to pass through or denies access if it does not meet certain criteria specified in a rule. It does not check the contents of legitimate traffic that are allowed based on the ruleset. Even legitimate traffic may contain malicious content, which is not evaluated during inspection by a firewall.

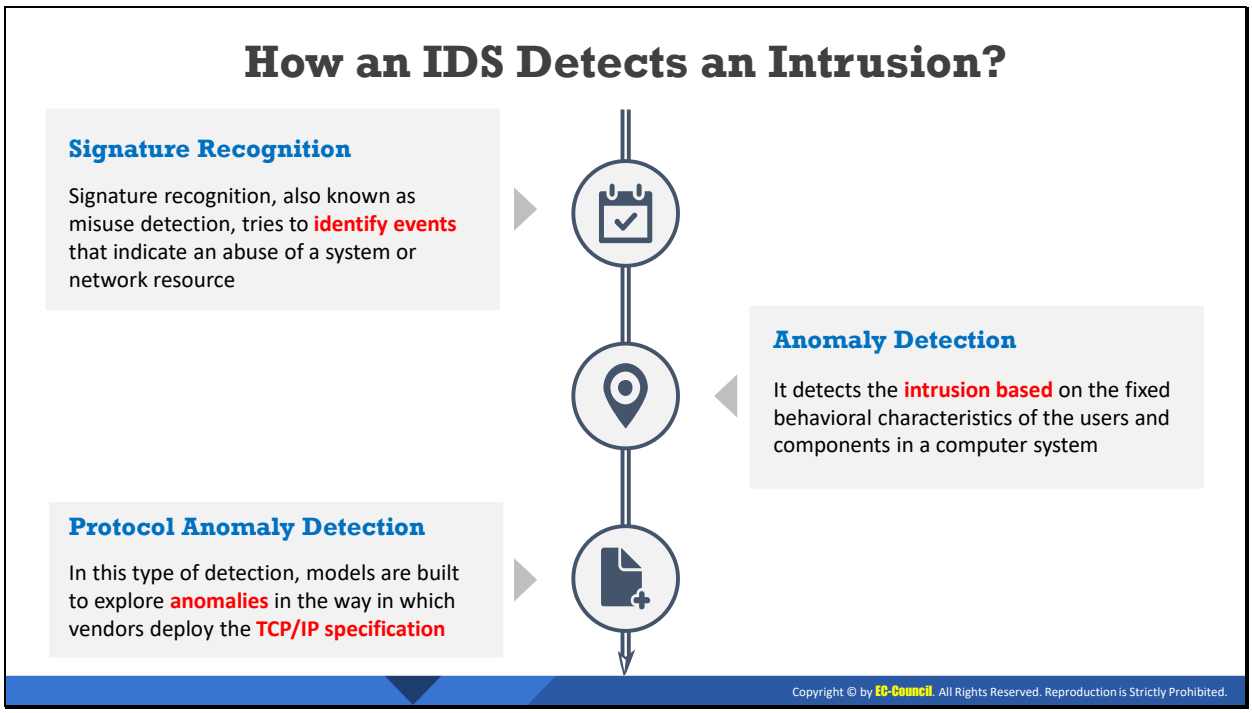
As an example, a firewall can be configured to pass traffic solely to port 80 of the Web server and to port 25 of the email server but it will not inspect the nature of the traffic flowing through either of these ports.

This is the reason why an IDS is implemented. An IDS will inspect the legitimate traffic coming from firewall and conduct signature-based analysis to identify malicious activity and raise an alarm to notify security professionals.

Role of an IDS in Network Defense

- An IDS works from inside the network, unlike a firewall which only looks outside the network for intrusions
- An IDS is placed behind the firewall, inspecting all the traffic, looking for heuristics and a pattern match for intrusions

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



How an IDS Detects an Intrusion?

An IDS uses three methods to detect intrusions in the network.

- **Signature Recognition**

  Signature recognition, also known as misuse detection, tries to identify events that indicate an abuse of a system or network. This technique involves first creating models of possible intrusions and then comparing these models with incoming events to make a detection decision. The signatures for IDS were created under the assumption that the model must detect an attack without disturbing normal system traffic. Only attacks should match the model; otherwise, false alarms could occur.

  - Signature-based intrusion detection compares incoming or outgoing network packets with the binary signatures of known attacks using simple pattern-matching techniques to detect intrusions. Attackers can define a binary signature for a specific portion of the packet, such as TCP flags.
  - Signature recognition can detect known attacks. However, there is a possibility that other innocuous packets contain the same signature, which will trigger a false positive alert.
  - Improper signatures may trigger false alerts. To detect misuse, a massive number of signatures are required. The more the signatures, the greater are the chances are of the IDS detecting attacks; however, the traffic may incorrectly match with the signatures, thus impeding system performance.
  - A large amount of signature data requires more network bandwidth. IDS compare signatures of data packets against those in the signature database. An increase in

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

the number of signatures in the database could result in the dropping of certain packets.

- **Anomaly Detection**

  Anomaly detection, or "**not-use detection**," differs from signature recognition. Anomaly detection involves a database of anomalies. An anomaly is detected when an event occurs outside the tolerance threshold of normal traffic. Therefore, any deviation from regular use is an attack. Anomaly detection detects intrusions based on the fixed behavioral characteristics of the users and components in a computer system. Establishing a model of normal use is the most challenging step in creating an anomaly detector.

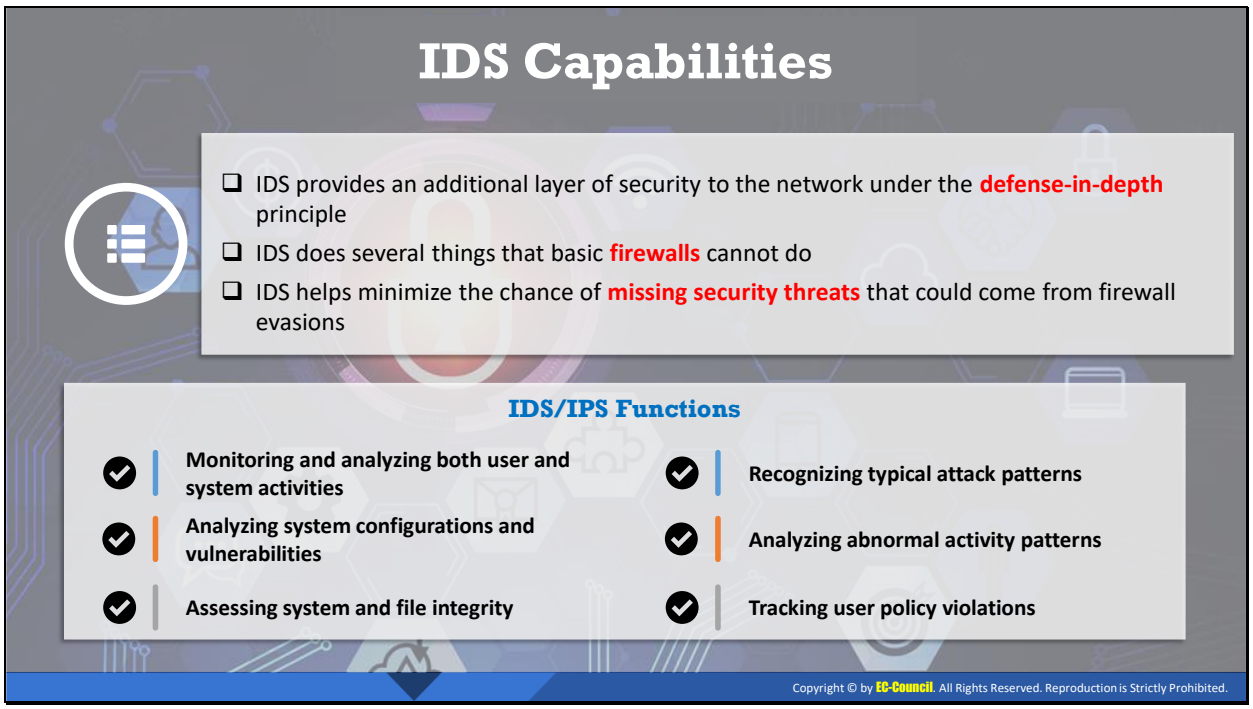
  - In the traditional method of anomaly detection, essential data are kept for checking variations in network traffic. However, in reality, there is some unpredictability in network traffic, and there are too many statistical variations, thus making these models imprecise. Some events labeled as anomalies might only be irregularities in network usage.
  - In this type of approach, the inability to construct a model thoroughly on a regular network is a concern. These models should be used to check specific networks.

- **Protocol Anomaly Detection**

  Protocol anomaly detection depends on the anomalies specific to a protocol. It identifies particular flaws in vendors' deployment of the TCP/IP protocol. Protocols are designed according to RFC specifications, which dictate standard handshakes to permit universal communication. The protocol anomaly detector can identify new attacks.

  - There are new attack methods and exploits that violate protocol standards.
  - Malicious anomaly signatures are becoming increasingly common. By contrast, the network protocol is well defined and is changing slowly. Therefore, the signature database should frequently be updated to detect attacks.
  - Protocol anomaly detectors are different from traditional IDS in terms of how they present alarms.
  - The best way to present alarms is to explain which part of the state system is compromised. For this purpose, IDS operators must have thorough knowledge of protocol design.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



IDS Capabilities

IDS provides an additional layer of security to the network under the defense-in-depth principle. IDS does several things that basic firewalls cannot do. IDS helps minimize the chance of missing security threats that could come from firewall evasions.

The main task of an IDS is detecting an intrusion attempt on a network and issuing a notification about what occurred. Detecting hostile attacks depends on several types of actions including prevention, intrusion monitoring, intrusion detection, and response. Intrusion prevention requires a well-selected combination of luring and tricking aimed at investigating threats. Diverting the intruder's attention from protected resources is another task. An IDS constantly monitors both the real system and a possible trap system and carefully examines data generated for detection of possible attacks.

Once an IDS detects an intrusion it issues alerts notifying administrators. Once the intrusion is detected and notified, the security professionals can execute certain countermeasures, which may include blocking functions, terminating sessions, backing up the systems, routing connections to a system trap, legal infrastructure, etc. An IDS is an important element of the security policy.

IDS alerts and logs are useful in forensic research of any incidents and installing appropriate patches to enable the detection of future attack attempts targeting specific people or resources.

An IDS observes computer network activity and keeps track of user policies and activity patterns to ensure they do not violate policies. It also observes network traffic and components for detecting virus and malware hidden in the form of spyware, key loggers, etc.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

An IDS works by gathering information about illicit attempts made to compromise security and then verifying them. It also records the event data and the security professional can use this data to take future preventive measures and make improvements to network security.

IDS/IPS Functions

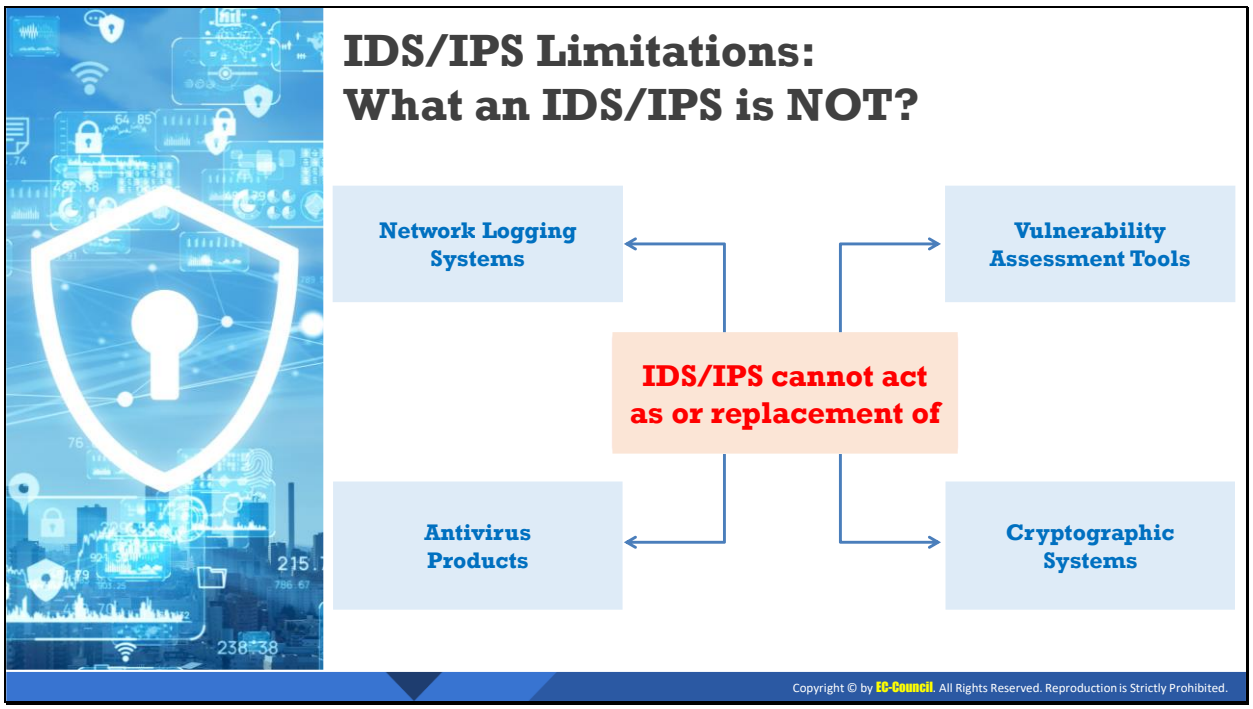
- Monitoring and analyzing both user and system activities
- Analyzing system configurations and vulnerabilities
- Assessing system and file integrity
- Recognizing typical attack patterns
- Analyzing abnormal activity patterns
- Tracking user policy violations

In addition to its core functionality of identifying and analyzing intrusions, an IDS can perform the following types of activities related to intrusion detection:

- **Records information about events:** An IDS notes down every detail regarding the monitored events and forwards the recorded information to various other systems such as centralized logging servers, security information and event management (SIEM), and enterprise management systems.
- **Sending an alert:** The IDS sends an intrusion alert to the security professional through emails, pop-up messages on the IDS user interface, etc.
- **Generating reports:** The IDS generates reports providing insight into observed events or any suspicious event that may have occurred.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

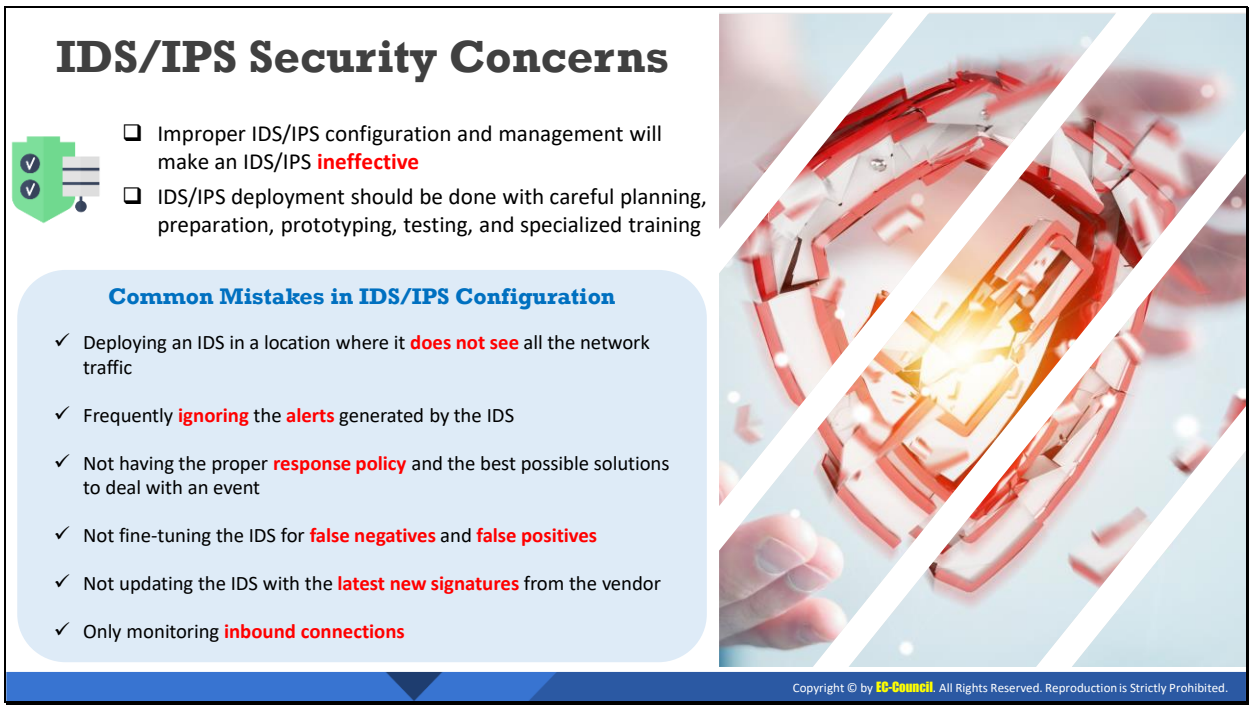


IDS/IPS Limitations: What an IDS/IPS is NOT?

Contrary to popular belief and terminology employed in the literature on IDSs, not every security device falls into this category. In particular, the following security devices should not be categorized as IDSs:

- **Network logging systems**: These devices are network traffic monitoring systems. They detect DoS vulnerabilities across a congested network.
- **Vulnerability assessment tools**: These devices check for bugs and flaws in operating systems and network services (security scanners).
- **Antivirus products**: These devices detect malicious software such as viruses, Trojan horses, worms, bacteria, logic bombs, etc. When compared feature by feature, these devices are very similar to IDSs and often provide effective security breach detection.
- **Security/cryptographic systems**: These devices protect sensitive data from theft or alteration by mandating user authentication. Examples include VPN, SSL, S/MIME, Kerberos, and RADIUS.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



IDS/IPS Security Concerns

Improper IDS/IPS configuration and management will make an IDS/IPS ineffective. IDS/IPS deployment should be done with careful planning, preparation, prototyping, testing, and specialized training.

Common Mistakes in IDS/IPS Configuration

- Deploying an IDS in a location where it does not see all the network traffic
- Frequently ignoring the alerts generated by the IDS
- Not having the proper response policy and the best possible solutions to deal with an event
- Not fine-tuning the IDS for false negatives and false positives
- Not updating the IDS with the latest new signatures from the vendor
- Only monitoring inbound connections

Included below are some mistakes and workarounds to avoid them for effective deployment of an IDS in the network:

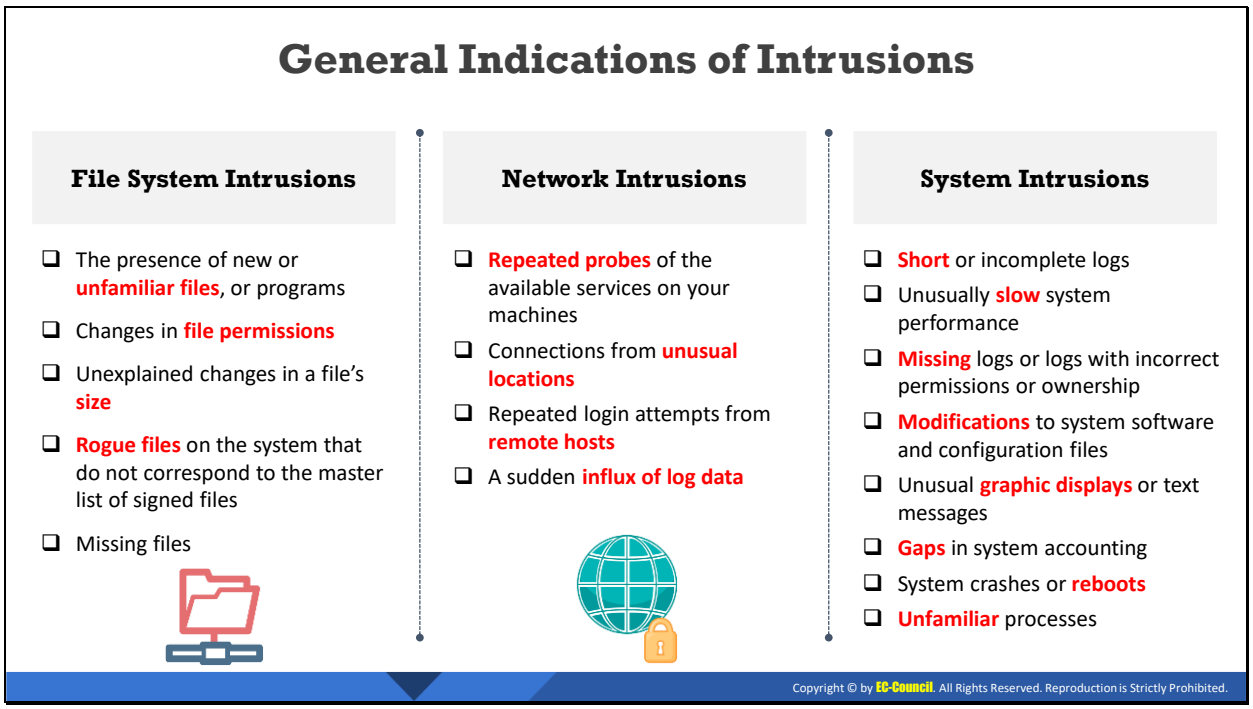
- **Deploying an IDS if the infrastructure planning is not efficient:** An improper or incomplete network infrastructure will not help the functioning of an IDS. If the tuning of the IDS does not follow the network infrastructure, it has the potential to disable the network by flooding it with alerts.
- **Incorrect sensitivity:** After the deployment of an IDS, organizations usually set its level to the highest sensitivity enabling the IDS to detect a large number of attacks. However, this also leads to a rise in the number of false positives. If an IDS generates a large

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

number of false positive alerts per day, it could cause the administrator to miss an actual alert. In the long run, ignoring these alerts can be harmful for network security.

- **Detecting an intrusion is not enough:** Organizations should also design a response policy that administrators implement in response to an incident that has occurred. This response policy should answer the following questions: What is a normal event and what is a malicious event? What is the response for every event generating an alert? The person reviewing the alerts should be aware of this action plan.
- **NIDS without IPsec:** An infrastructure that has established a NIDS without IPsec network protocols makes the network more vulnerable to intrusions. A NIDS listens to all the traffic that it senses and then compares the legitimacy of the traffic. If it encounters encrypted traffic, it can only perform packet-level analysis as the application layer contents are inaccessible. This increases the vulnerability of the network.
- **Ignoring outbound traffic:** Many organizations prefer securing and monitoring only the inbound traffic and ignore the outbound traffic. It is important to place IDS sensors throughout the organization. If the setup is cost effective, the organization should place the sensors near the choke points on the network. This will help monitor outbound as well as internal host network traffic.
- **Deploying IDS sensors on a single NIC or on multiple data links:** This will lead to an IDS sensor sending the data on the same interface on which it is sensing. This may lead to a possible attack as the interface reports all the data to the centralized database. If an attacker gets access to this infrastructure, they can disable the IDS and prevent further alerts. The attacker can also intercept the data on the interface and alter it. This issue can be resolved by connecting the interface to a dedicated monitoring network.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



General Indications of Intrusions

Intrusion attempts on networks, systems, or file systems can be identified by following some general indicators:

- **File System Intrusions**

  By observing system files, the presence of an intrusion can be identified. System files record the activities of the system. Any modification or deletion of the file attributes or the file itself is a sign that the system has been a target of an attack:

  - If you find new, unknown files/programs on your system, then there is a possibility that the system has been intruded into. The system can be compromised to the extent that it can, in turn, compromise other network systems.
  - When an intruder gains access to a system, he or she tries to escalate privileges to gain administrative access. When the intruder obtains administrator privileges, he/she could change file permissions, for example, from read-only to write.
  - Unexplained modifications in file size are also an indication of an attack. Make sure you analyze all your system files.
  - The presence of rogue suid and sgid files on your Linux system that do not match your master list of suid and sgid files could indicate an attack.
  - You can identify unfamiliar file names in directories, including executable files with strange extensions and double extensions.
  - Missing files are also a sign of a probable intrusion/attack.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **Network Intrusions**

  Similarly, general indications of network intrusions include:

  - A sudden increase in bandwidth consumption
  - Repeated probes of the available services on your machines
  - Connection requests from IPs other than those in the network range, which imply that an unauthenticated user (intruder) is attempting to connect to the network
  - Repeated login attempts from remote hosts
  - A sudden influx of log data, which could indicate attempts at DoS attacks, bandwidth consumption, and DDoS attacks

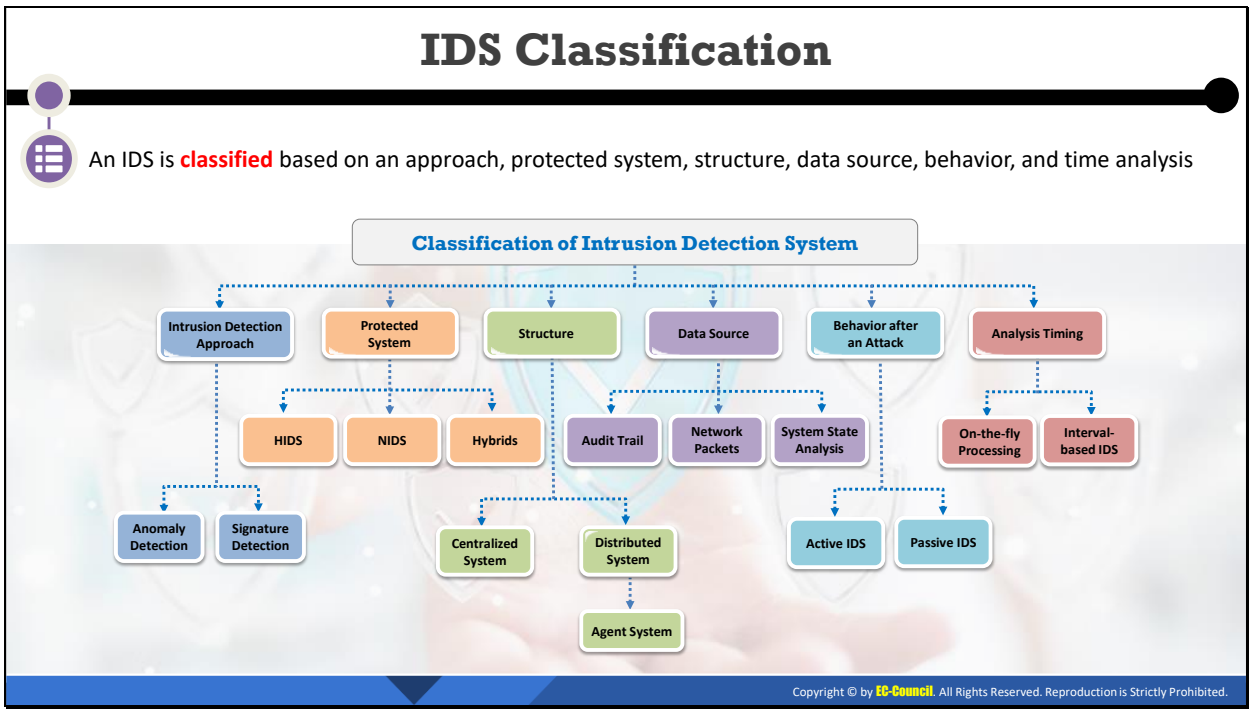
- **System Intrusions**

  Similarly, general indications of system intrusions include:

  - Sudden changes in logs such as short or incomplete logs
  - Unusually slow system performance
  - Missing logs or logs with incorrect permissions or ownership
  - Modifications to system software and configuration files
  - Unusual graphic displays or text messages
  - Gaps in system accounting
  - System crashes or reboots
  - Unfamiliar processes

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



IDS Classification

Generally, an IDS uses anomaly-based detection and signature-based detection methods to detect intrusions. An IDS is classified based on an approach, protected system, structure, data source, behavior, and time analysis.

The classification of IDSs is shown in following figure. This categorization depends on the information gathered from a single host or a network segment, in terms of behavior, based on continuous or periodic feed of information, and the data source.

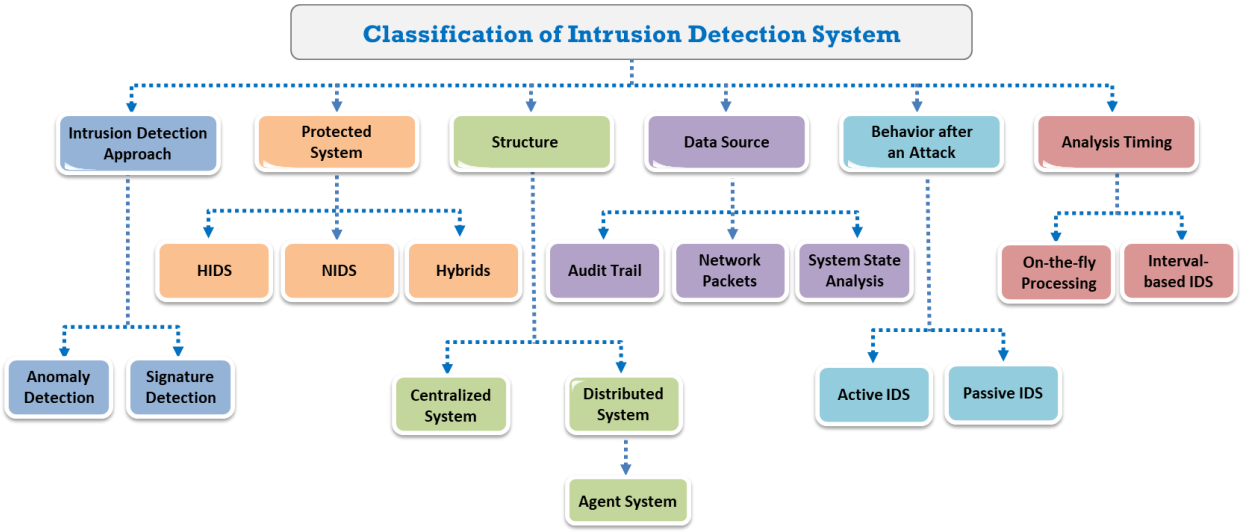
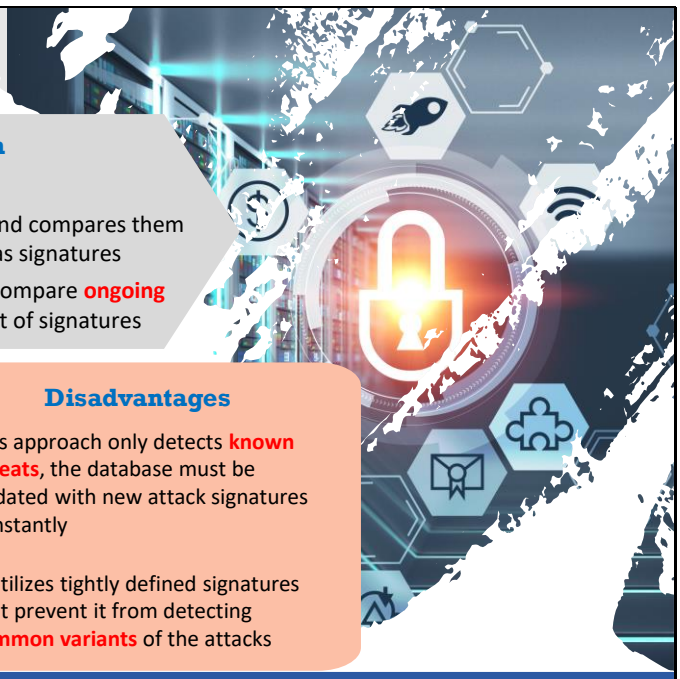


Figure 5.36: Classification of Intrusion Detection System

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Approach-based IDS



Signature-Based Detection

- Known as **misuse detection**
- **Monitors** patterns of data packets in the network and compares them to pre-configured network attack patterns, known as signatures
- This method uses string comparison operations to compare **ongoing activity**, such as a packet or a log entry, against a list of signatures

Advantages

- It detects attacks with minimal false alarms
- It can **quickly** identify the use of a specific tool or technique
- It assists administrators to quickly track any potential **security issues** and initiate incident handling procedures

Disadvantages

- This approach only detects **known threats**, the database must be updated with new attack signatures constantly
- It utilizes tightly defined signatures that prevent it from detecting **common variants** of the attacks

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Approach-based IDS (Cont'd)

Anomaly-based Detection

- In this approach, alarms for **anomalous** activities are generated by evaluating network patterns such as what sort of bandwidth is used, what protocols are used, and what ports and which devices are connected to each other
- An IDS monitors the typical activity for a particular time interval and then builds the **statistics** for the network traffic
- For example: anomaly-based IDS monitors activities for normal Internet bandwidth usage, failed logon attempts, processor utilization levels, etc.

Advantages

- ✓ An anomaly-based IDS identifies **abnormal** behavior in the network and detects the symptoms for attacks without any clear details
- ✓ Information acquired by anomaly detectors is further used to define the signatures for **misuse detectors**

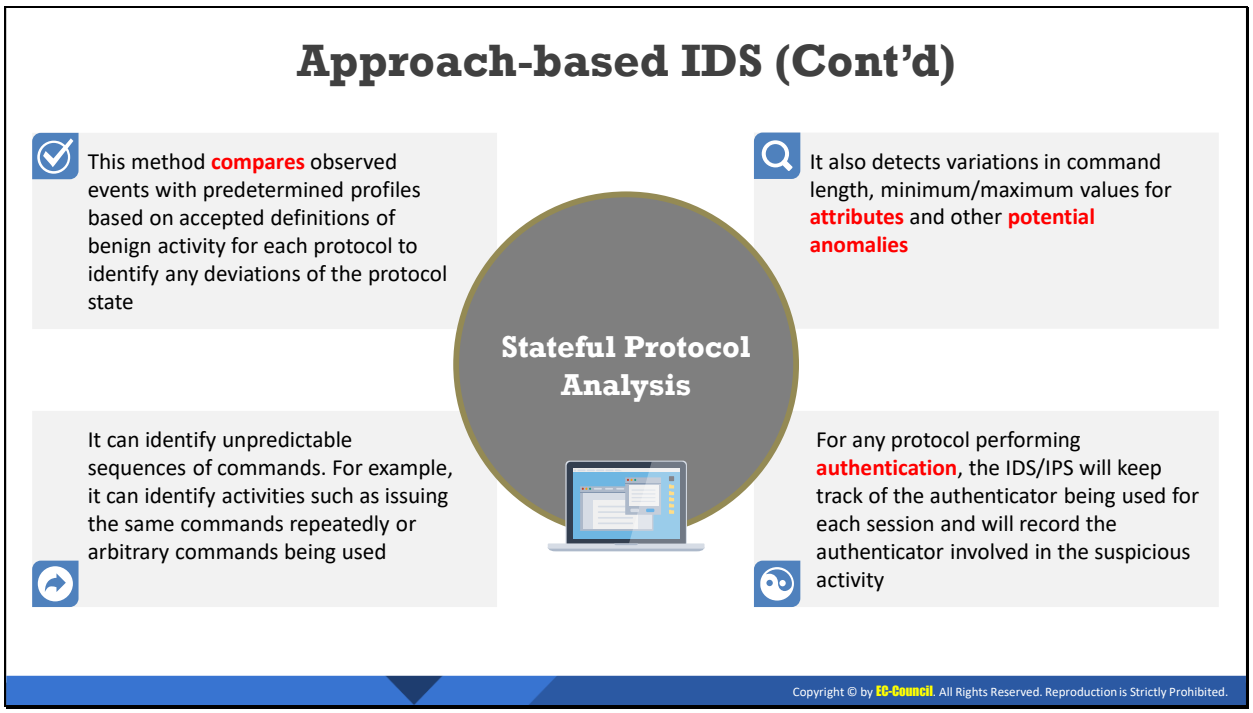
Disadvantages

- ✓ The rate of generating **false alarms** is high due to unpredictable behavior of users and networks
- ✓ The need to create an **extensive set of system events** in order to characterize normal behavior patterns

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Approach-based IDS

Signature-based Detection

It is also known as misuse detection. Monitors patterns of data packets in the network and compares them to pre-configured network attack patterns known as signatures. A signature is a predefined pattern in the traffic on a network. Normal traffic signatures denote normal traffic behavior. However, attack signatures are malicious and are harmful to the network. These patterns are unique, and the attacker uses these patterns to get into the network. This method uses string comparison operations to compare ongoing activity, such as a packet or a log entry, against a list of signatures.

Advantages

- It detects attacks with minimal false alarms.
- It can quickly identify the use of a specific tool or technique.
- It assists administrators to quickly track any potential security issues and initiate incident handling procedures.

Disadvantages

- This approach only detects known threats, the database must be updated with new attack signatures constantly.
- It utilizes tightly defined signatures that prevent it from detecting common variants of the attacks.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Examples of signatures:

- A telnet attempt with a username of 'root', which is a violation of the corporate security policy.
- An operating system log entry with a status code of 645 indicates the host auditing system is disabled.

Anomaly-based Detection

The anomaly-based detection process depends on observing and comparing the observed events with the normal behavior and then detecting any deviation from it. Normal behavior depends on factors such as users, hosts, network connections, and/or applications. These factors are considered only after examining a particular activity over a period of time.

Normal traffic behavior is based on various behavioral attributes such as normal email activity, reasonable number of failed attempts, processor usage, etc. Any activity that does not match normal behavior can be treated as an attack. For example, numerous emails coming from a single sender or a large number of failed login attempts can indicate suspicious behavior. Unlike signature-based detection, anomaly-based detection can detect previously unknown attacks.

In this approach, alarms for anomalous activities are generated by evaluating network patterns such as what sort of bandwidth is used, what protocols are used, and what ports and which devices are connected to each other. An IDS monitors the typical activity for a particular time interval and then builds the statistics for the network traffic. For example: anomaly-based IDS monitors activities for normal Internet bandwidth usage, failed logon attempts, processor utilization levels, etc.

Advantages

- An anomaly-based IDS identifies abnormal behavior in the network and detects the symptoms for attacks without any clear details
- Information acquired by anomaly detectors is further used to define the signatures for misuse detectors

Disadvantages

- The rate of generating **false alarms** is high due to unpredictable behavior of users and networks
- The need to create an **extensive set of system events** in order to characterize normal behavior patterns

Stateful Protocol Analysis

Network communication uses various types of protocols to exchange information on different layers. These protocols define the accepted behavior. Stateful protocol analysis–based IDS detects suspicious activity by analyzing the deviation of specific protocol traffic from its normal behavior. Using this analysis, an IDS can analyze the network, transport, and application layer protocols and traffic against their normal behavior.

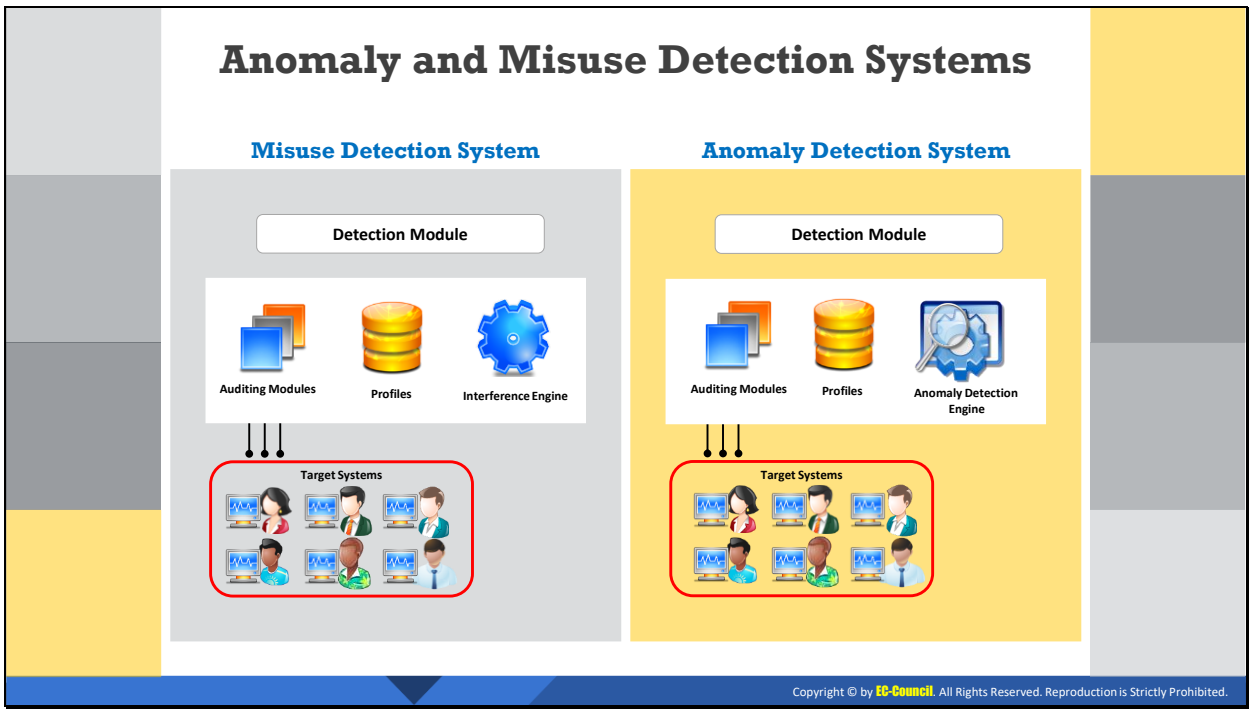
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

Certain IDSs can specify suitable activities for each class of users in accordance with the authenticator information. This method compares observed events with predetermined profiles based on accepted definitions of benign activity for each protocol to identify any deviations of the protocol state. It can identify unpredictable sequences of commands. For example, it can identify activities such as issuing the same commands repeatedly or arbitrary commands being used. It also detects variations in command length, minimum/maximum values for attributes and other potential anomalies. For any protocol performing authentication, the IDS/IPS will keep track of the authenticator being used for each session and will record the authenticator involved in the suspicious activity.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Anomaly and Misuse Detection Systems

Misuse Detection System

In a misuse detection system, first the abnormal behavior system is defined and then the normal behavior. The misuse detection system works differently from an anomaly detection system in that it has a static approach in detecting attacks. Generally, misuse detection systems show a low rate of false positives as the rules are predefined, such as rule-based languages, state transition analysis, expert system, etc.

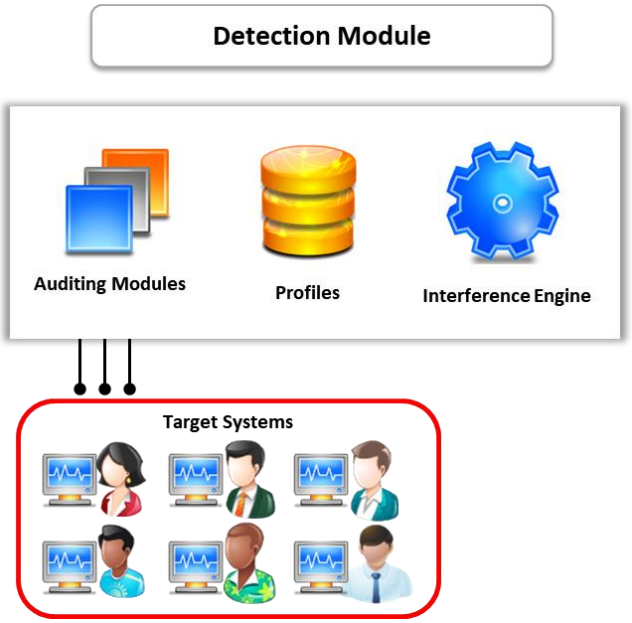


Figure 5.37: Misuse detection system

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Advantages

- More accurate detection than an anomaly detection system
- Fewer false alarms

Disadvantage

- Unable to detect new attacks due to predefined rules

Anomaly Detection System

An anomaly detection system involves detecting intrusions on the network. It uses algorithms to detect discrepancies occurring in a network or system. It categorizes an intrusion as either normal or anomalous. Anomaly intrusion is a two-step process where the first step involves gathering information of how data flows and the second step involves working on that data flow in real time and detecting if the data is normal or not. By implementing this process, an anomaly detection–based IDS protects the target systems and networks that may be vulnerable to malicious activities. Anomalies in the system can be detected through artificial intelligence, neural networks, data mining, statistical method, etc.

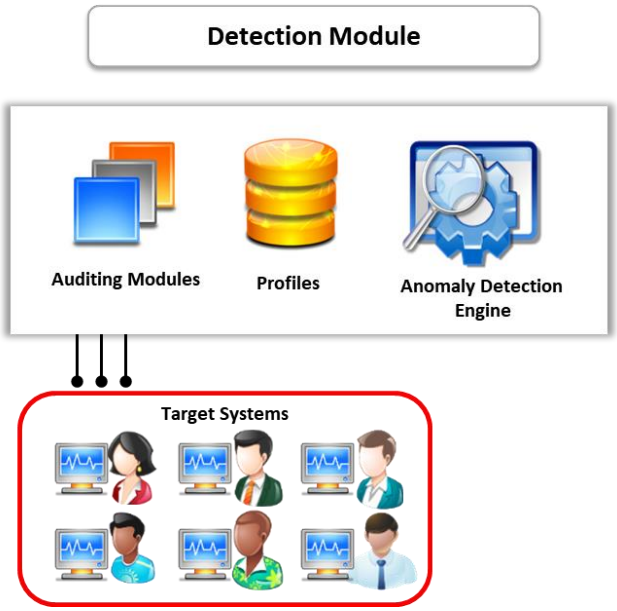


Figure 5.38: Anomaly detection system

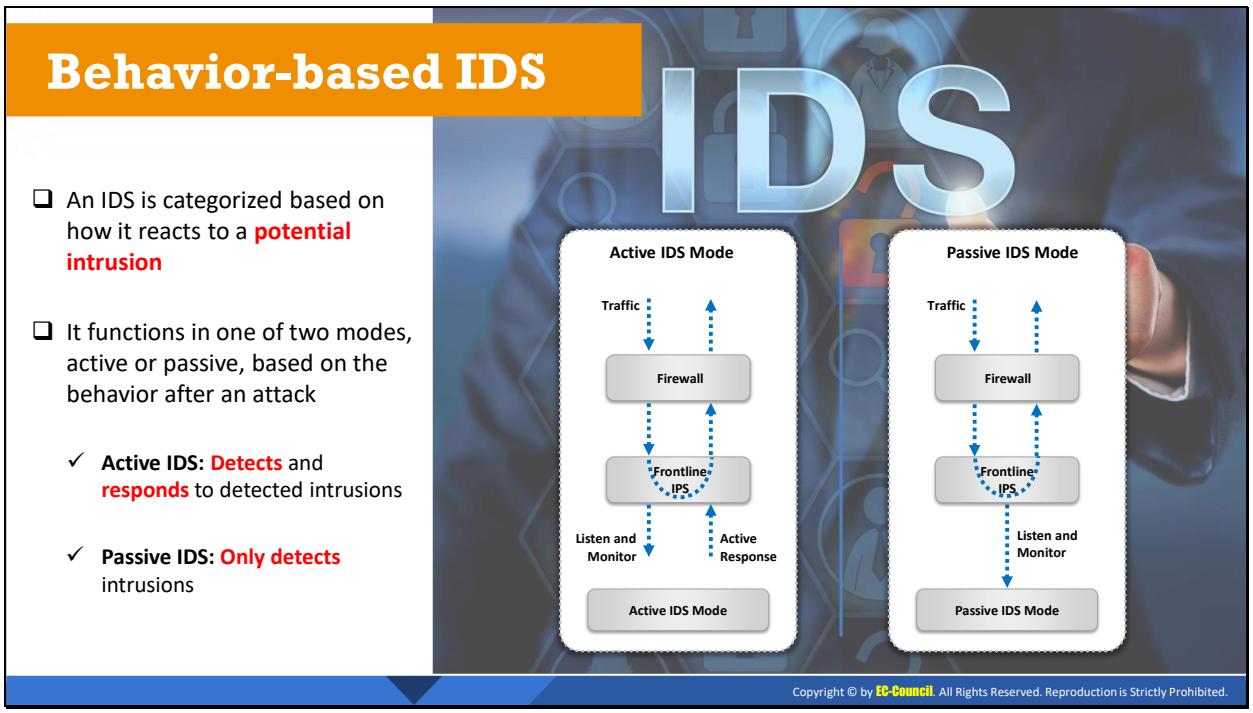
Advantages

- It detects and identifies probes in network hardware, thereby providing early warnings about attacks.
- It has the ability to detect a wide range of attacks in the network.

Disadvantages

- If a legitimate network behavior is not part of the designed model, the system will detect it as anomalous. This increases the number of false positive alerts in the system.
- Network traffic varies and deployment of the same model throughout can lead to a failure in detecting known attacks.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Behavior-based IDS

Behavior-based intrusion detection techniques assume an intrusion can be detected by observing a deviation from normal or expected behavior of the system or users. The model of normal or valid behavior is extracted from reference information collected by various means. The IDS later compares this model with current activity. When a deviation is observed, an alarm is generated.

An IDS is categorized based on how it reacts to a potential intrusion. It functions in one of two modes, active or passive, based on the behavior after an attack.

Active IDS Mode

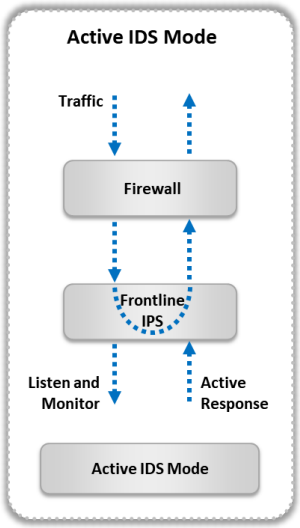


Figure 5.39: Active IDS Mode

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Detects and responds to detected intrusions. An active IDS is configured to automatically block suspected attacks without any intervention from the administrator. Such an IDS has the advantage of providing real-time corrective action in response to an attack. The exact action differs per product and depends on the severity and type of the attack.

Passive IDS Mode

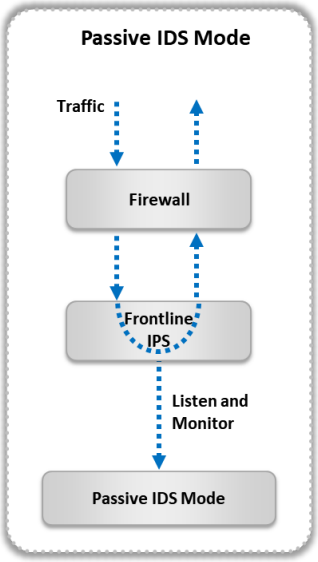
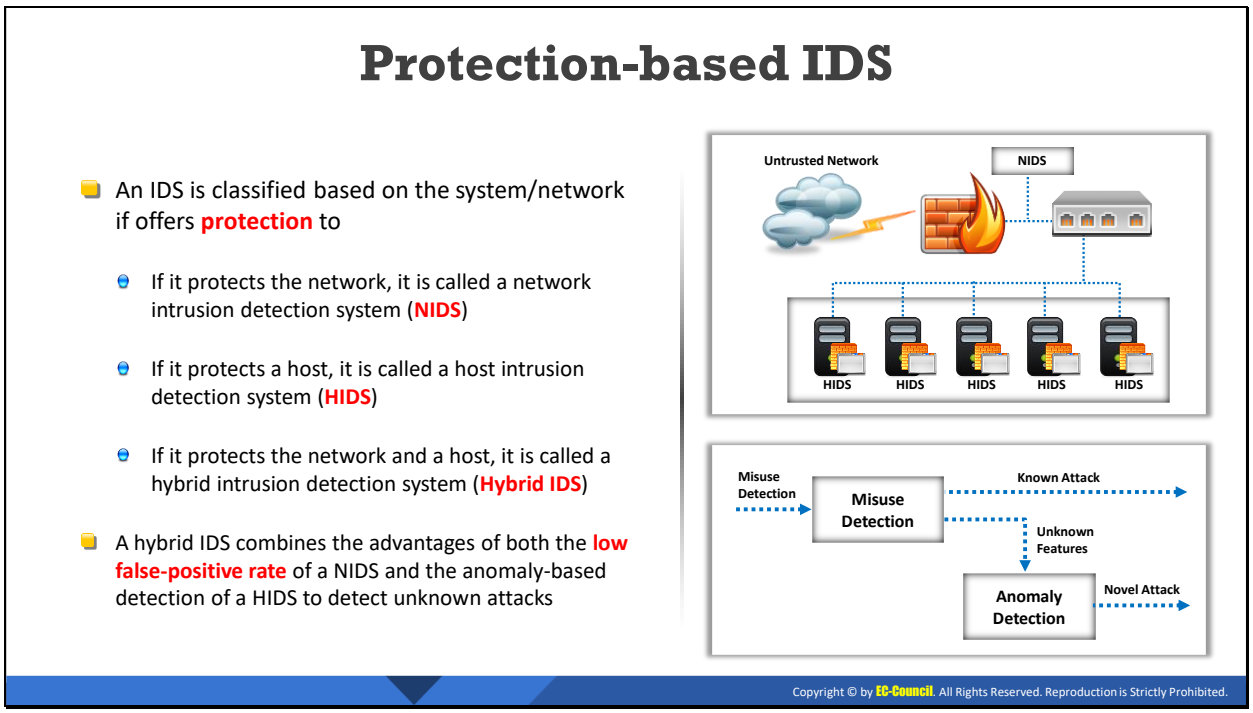


Figure 5.40: Passive IDS Mode

Only detects intrusions. A passive IDS is configured only to monitor and analyze network traffic activity and alert the administrator of any potential vulnerabilities and attacks. This type of IDS is not capable of performing any protective or corrective functions on its own. It merely logs the intrusion and notifies an administrator, through email or pop-ups. A system administrator or someone else will have to respond to the alarm, take appropriate action to halt the attack and possibly identify the intruder.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Protection-based IDS

An IDS can be classified based on the device or network to which it offers protection. There are mainly three types of IDS technologies under this category which includes network intrusion detection systems (NIDS), host intrusion detection systems (HIDS), and hybrid intrusion detection systems (hybrid IDS).

- If it protects the network, it is called a network intrusion detection system (NIDS)
- If it protects a host, it is called a host intrusion detection system (HIDS)
- If it protects the network and a host, it is called a hybrid intrusion detection system (Hybrid IDS)

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

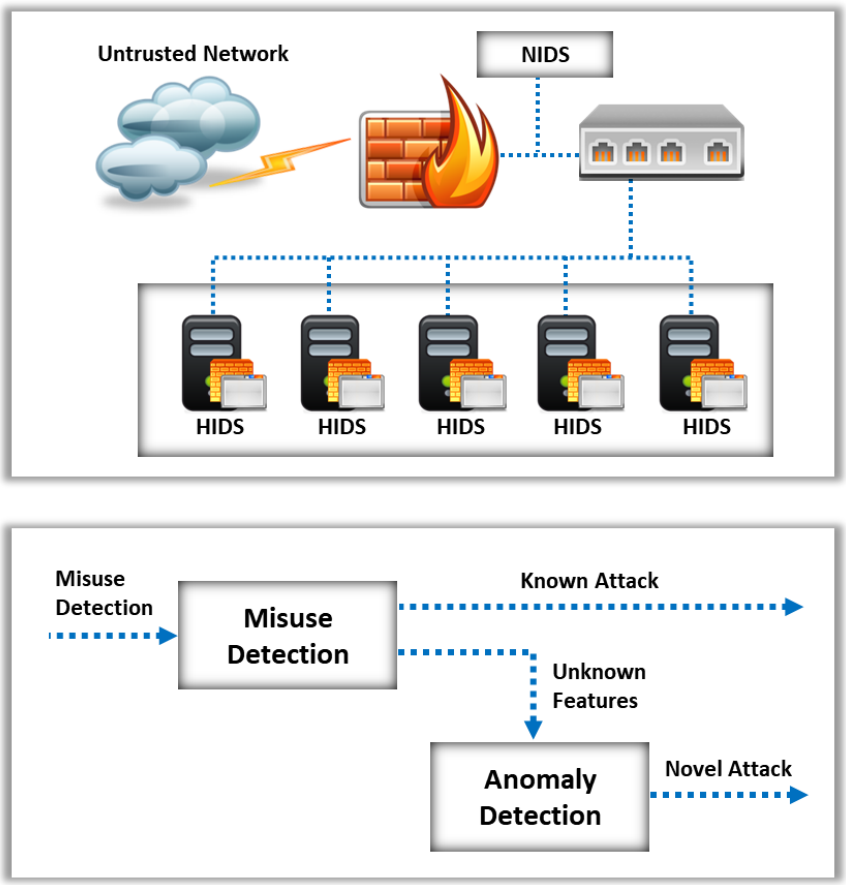


Figure 5.41: Protection-based IDS

Network Intrusion Detection System (NIDS)

NIDS is used to observe the traffic for any specific segment or device and recognize the occurrence of any suspicious activity in the network and application protocols. NIDS is typically placed at boundaries between networks, behind network perimeter firewalls, routers, VPN, remote access servers, and wireless networks.

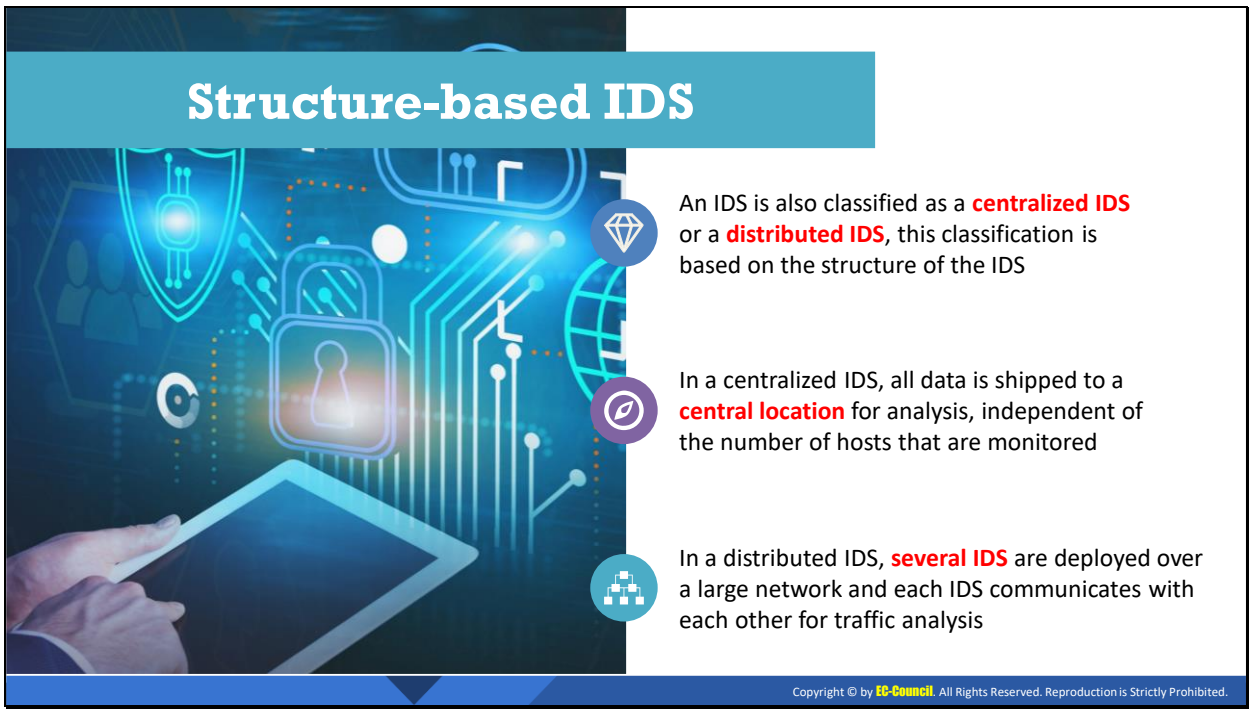
Host Intrusion Detection Systems (HIDS)

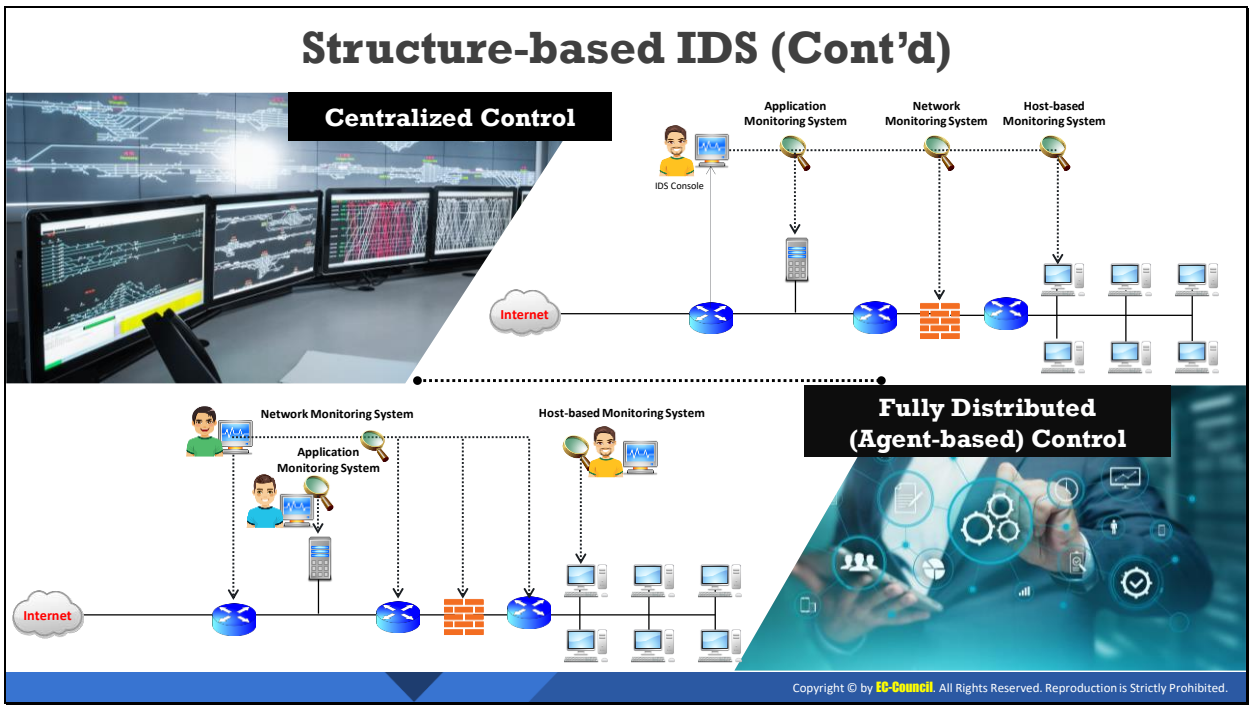
HIDS is installed on a specific host and is used to monitor, detect, and analyze events occurring on that host. It monitors activities related to network traffic, logs, process, application, file access, and modification on the host. HIDS is normally deployed for protecting very sensitive information that is kept on publicly accessible servers.

Hybrid Intrusion Detection Systems (Hybrid IDS)

A hybrid IDS is a combination of both HIDS and NIDS. It combines the advantages of both the low false-positive rate of a NIDS and the anomaly-based detection of a HIDS to detect unknown attacks. It has its agent installed on almost every host in the network, and it has the ability to work online with encrypted networks and storing data on a single host.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets





Structure-based IDS

An IDS is also classified as a **centralized IDS** or a **distributed IDS**, this classification is based on the structure of the IDS

Distributed Structure of an IDS

A distributed intrusion detection system (dIDS) consists of multiple IDSs over a large network. These systems communicate with each other or with a central server that facilitates an

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

advanced network of monitoring, incident analysis, and instant attack data. By having these cooperative agents distributed across a network, network operators can get a broader view of what is occurring on their network as a whole.

dIDS also allows a company to efficiently manage its incident analysis resources by centralizing its attack records and by giving the analyst a way to spot new trends or patterns and identify threats to the network across multiple network segments.

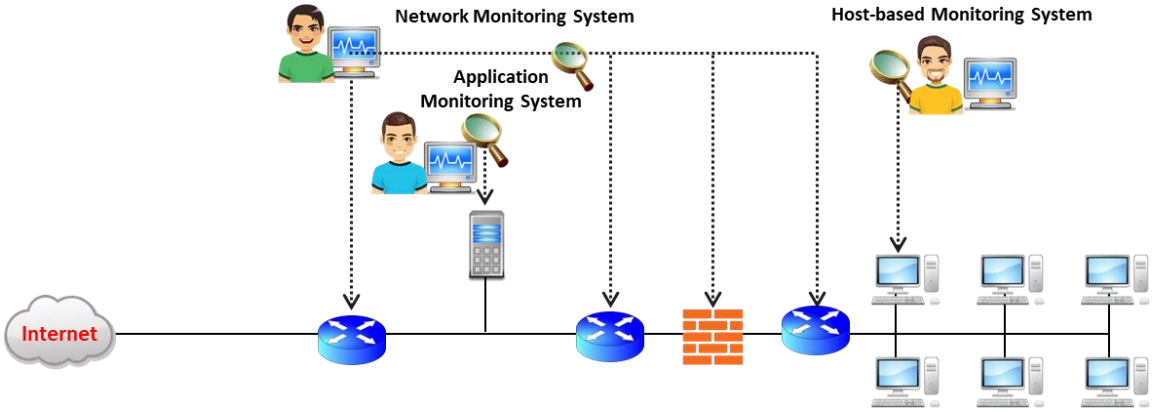


Figure 5.42: Distributed structure of an IDS

Centralized Structure of IDS

In a centralized system, the data is gathered from different sites to a central site and the central coordinator analyzes the data following an intrusion. Such an IDS is designed for centralized systems. In a centralized IDS, data analysis is performed in a fixed number of locations, independent of how many hosts are being monitored. As a result, the centralized structure of an IDS can be harmful in a high-speed network.

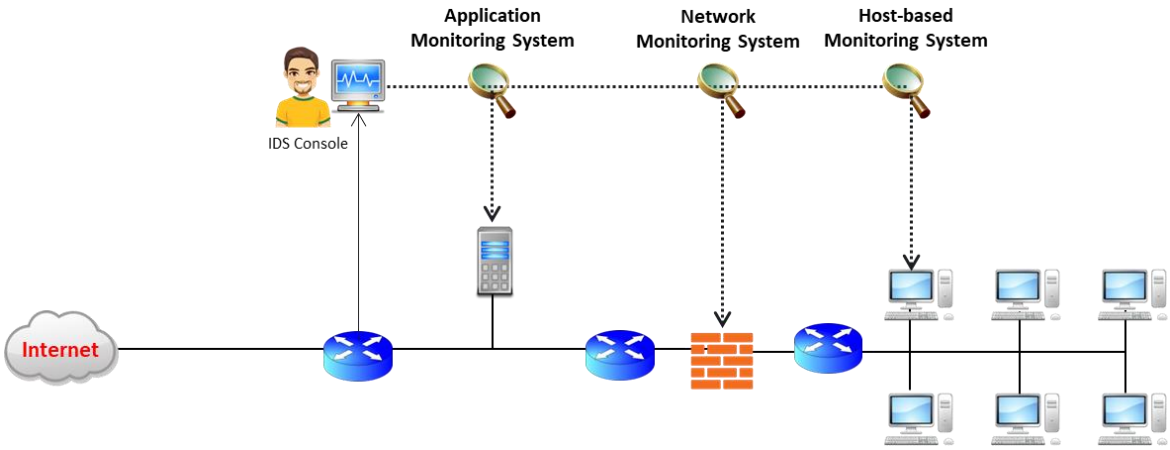
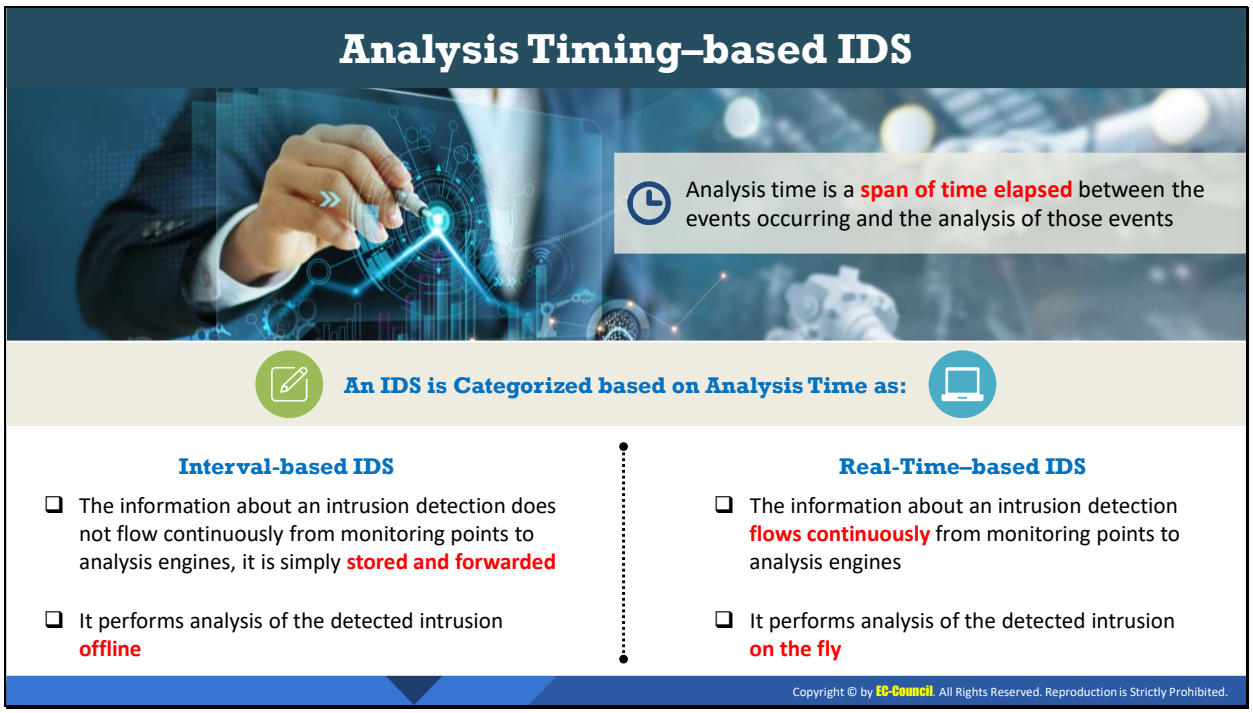


Figure 5.43: Centralized Structure of an IDS

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Analysis Timing–based IDS

Analysis timing refers to the elapsed time between the occurrence of events and analysis of those events. Based on analysis timing, an IDS can be classified into two distinct types: interval-based IDS and real-time–based IDS.

Interval-based IDS

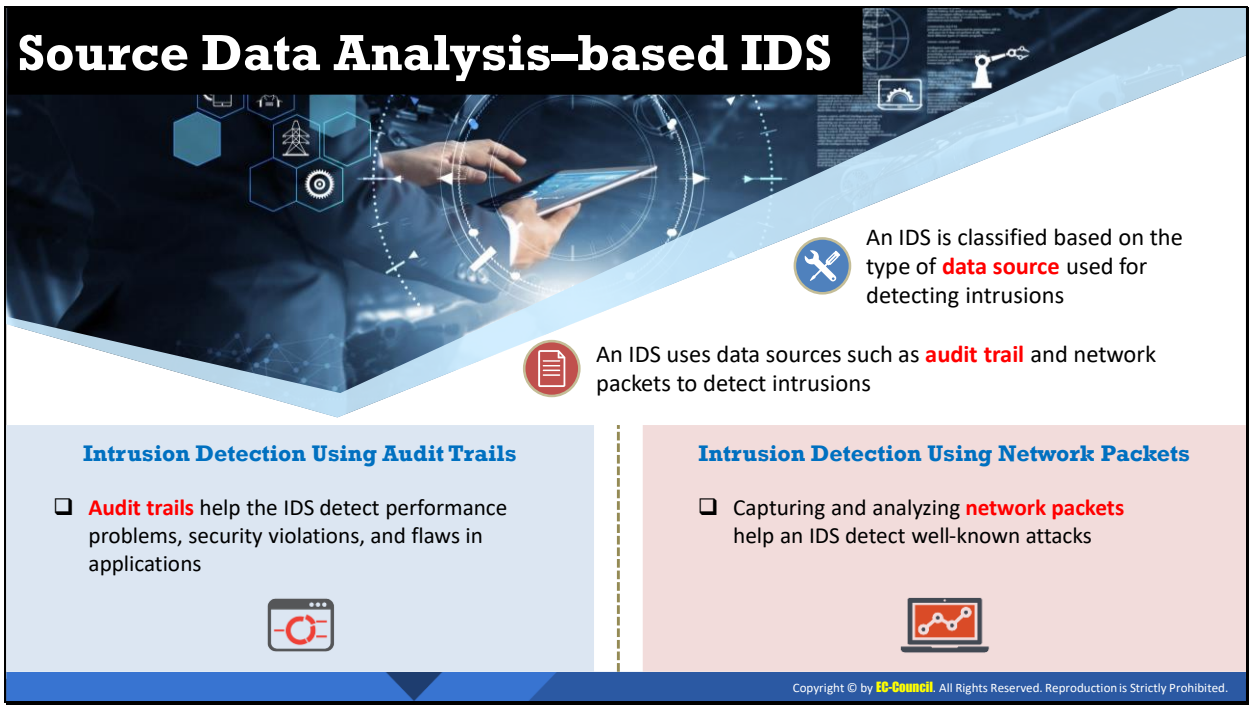
Interval-based or offline analysis refers to the storage of the intrusion-related information for further analysis. This type of IDS checks the status and content of log files at predefined intervals. The information about an intrusion detection does not flow continuously from monitoring points to analysis engines, it is simply stored and forwarded. It performs analysis of the detected intrusion offline. Interval-based IDSs are prohibited from performing an active response. Batch mode was common in early IDS implementations because their capabilities did not support real-time data acquisition and analysis.

Real-time–based IDS

The information about an intrusion detection flows continuously from monitoring points to analysis engines. It performs analysis of the detected intrusion on the fly.

A real-time–based IDS is designed for on-the-fly processing and is the most common approach for a network-based IDS. It operates on a continuous information feed. Real-time–based IDS gathers and monitors information from network traffic streams regularly. The detection performed by this IDS yields results quick enough to allow the IDS system to take action affecting the progress of the detected attack. It can also conduct online verification of events with the help of on-the-fly processing and respond to them simultaneously. An IDS using this type of processing requires more RAM and a large hard drive because of the high data storage required to trace all of the network packets online.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Source Data Analysis–based IDS

An IDS is classified based on the type of data source used for detecting intrusions. An IDS uses data sources such as audit trail and network packets to detect intrusions. Depending on the data source, an IDS can be categorized into two types: intrusion detection using audit trails and intrusion detection using network packets.

Intrusion Detection Using Audit Trails

An audit trail is a set of records that provide documentary evidence of a system's activity using the system and application processes and user activity of systems and applications. Audit trails help the IDS in detecting performance problems, security violations, and flaws in applications. Administrators should avoid storage of audit trail reports in a single file to avoid intruders from accessing the audit reports and making changes.

- Audit systems are used for the following:
  - Watch file access
  - Monitor system calls
  - Record commands run by user
  - Record security events
  - Search for events
  - Run summary reports
- The reasons for performing audit trails are as follows:
  - Identifying the signs of an attack using event analysis
  - Identifying recurring intrusion events

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

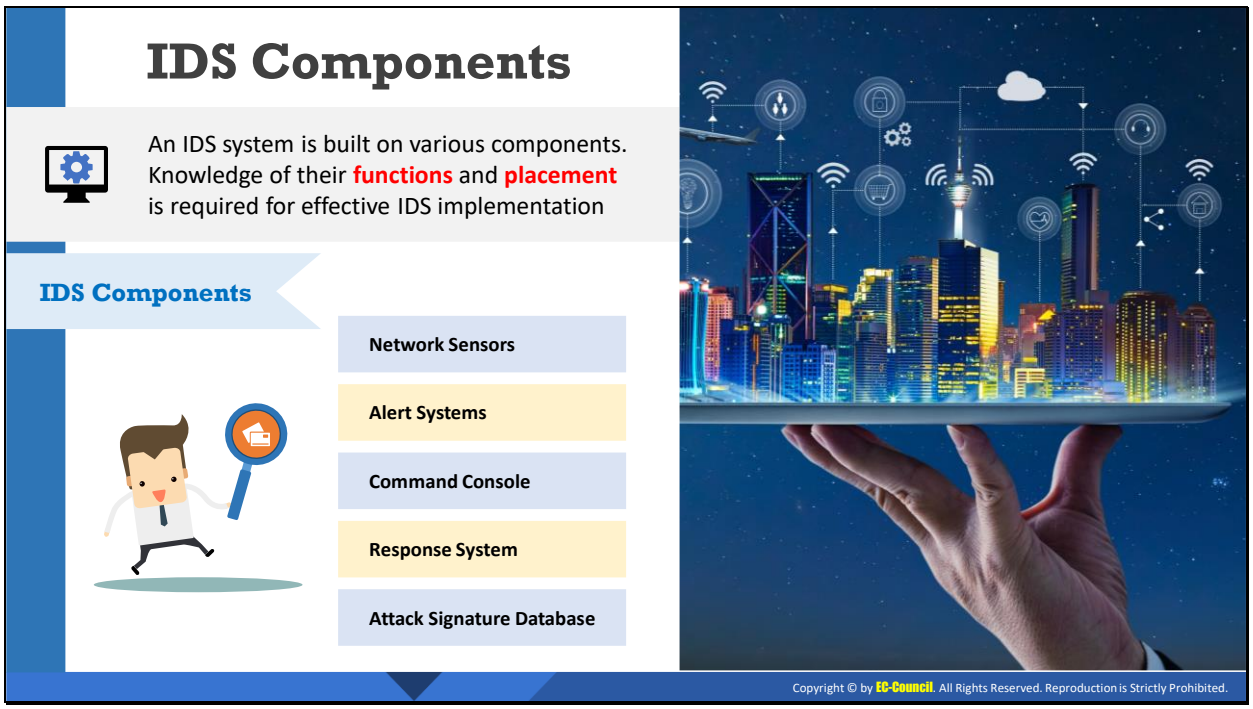
- Identifying system vulnerabilities
- To develop access and user signatures
- To define network traffic rules for anomaly detection-based IDSs
- Provides a form of defense for a basic user against intrusions

Intrusion Detection Using Network Packets

A network packet is a unit of data transmitted over a network for communication. It contains control information in a header and user data. The header of the packet contains the address of the packet's source and its destination; the payload is the body of the packet storing the original content. The header and the payload of a packet can contain malicious content sent by attackers. Capturing these packets before they enter their final destination is an efficient way to detect such attacks.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



IDS Components

An IDS system is built on various components. Knowledge of their functions and placement is required for effective IDS implementation. These components are used to collect information from a variety of systems and network sources, and then analyze the information for any abnormalities. Major components of an IDS are listed below.

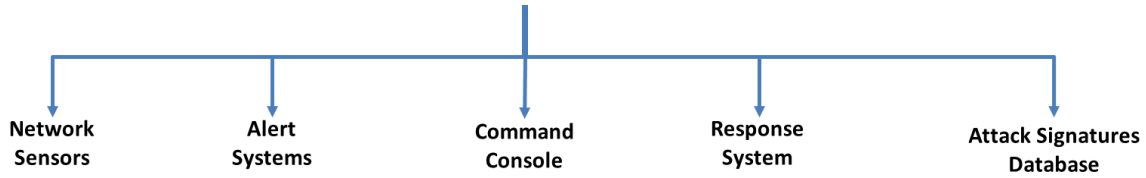
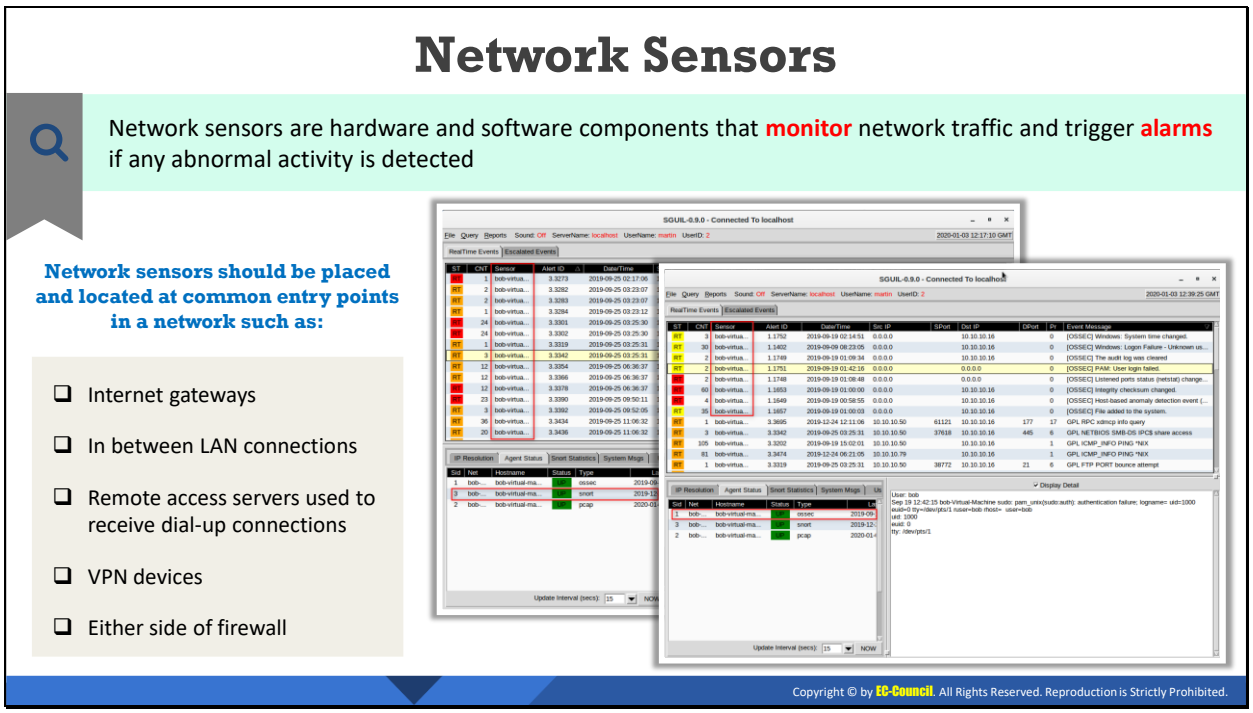


Figure 5.44: IDS Components

- **Network sensors:** These agents analyze and report any suspicious activity.
- **Analyzer:** It analyzes the data collected by the sensors.
- **Alert systems:** These systems trigger alerts when detecting malicious activity.
- **Command console:** It acts as an interface between the user and the IDS.
- **Response system:** An IDS uses this system to initiate countermeasures on detected activities.
- **Database of attack signatures or behaviors:** A list of previously detected signatures stored in a database that assist the IDS in intrusion detection.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Network Sensors

Network sensors are hardware and software components that monitor network traffic and trigger alarms if any abnormal activity is detected. It is a primary data collection point for the IDS. Network sensors collect data from the data source and pass it to the alert systems.

The sensor integrates with the component responsible for data collection such as an event generator. Network sensors determine data collection based on the event generator policy, which defines the filtering mode for event notification information.

The role of the sensor is to filter information and discard any irrelevant data obtained from the event set associated with the protected system, thereby detecting suspicious activities. Sensors check the traffic for malicious packets, trigger an alarm when they suspect a packet is malicious, and then alert the IDS. If an IDS confirms the packet as malicious then the sensors generate an automatic response to block the traffic from the source of the attack.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

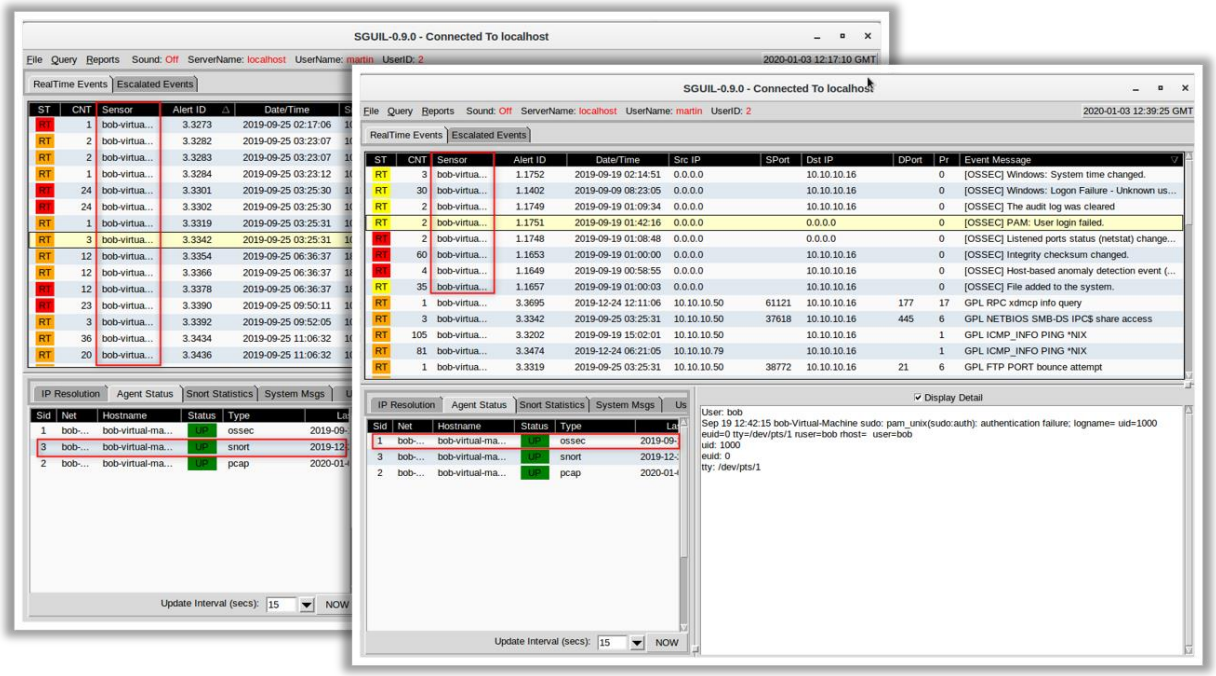


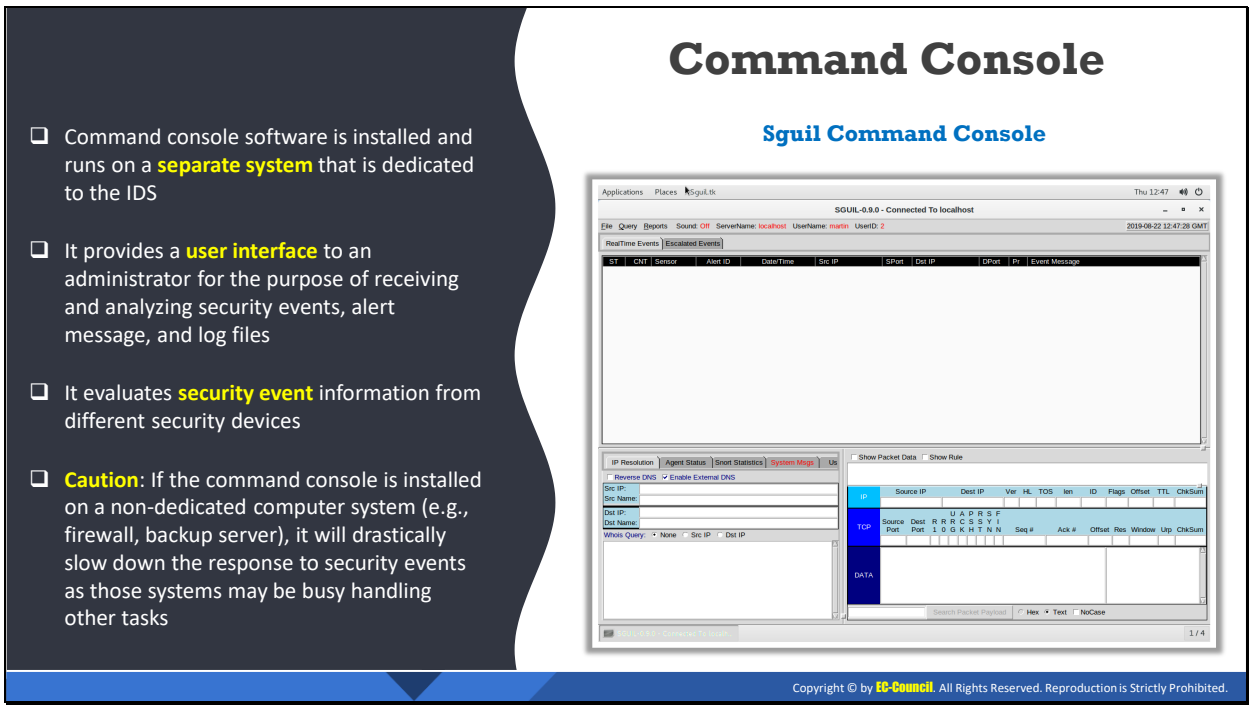
Figure 5.45: Network Sensors Triggering Alarm

Network sensors should be placed and located at common entry points in a network such as:

- Internet gateways
- In between LAN connections
- Remote access servers used to receive dial-up connections
- VPN devices
- Either side of firewall

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Command Console

Command console software is installed and runs on a separate system that is dedicated to the IDS. It provides a user interface to an administrator for the purpose of receiving and analyzing security events, alert message, and log files. The command console evaluates security event information from different security devices.

The IDS collects all the data from security devices and analyzes it using the command console. Administrators use the console to analyze alert messages triggered by the alert system and manage log files. The command console allows administrators in large networks to process large volumes of activities and respond quickly.

An IDS collects information from security devices placed throughout the network and sends it to the command console for evaluation. Installing a command console on the system for other purposes such as backing up files and firewall functions, will make it slow to respond to events. Installing the command console on a dedicated system provides the benefit of a fast response.

Caution: If the command console is installed on a non-dedicated computer system (e.g., firewall, backup server), it will drastically slow down the response to security events as those systems may be busy handling other tasks.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

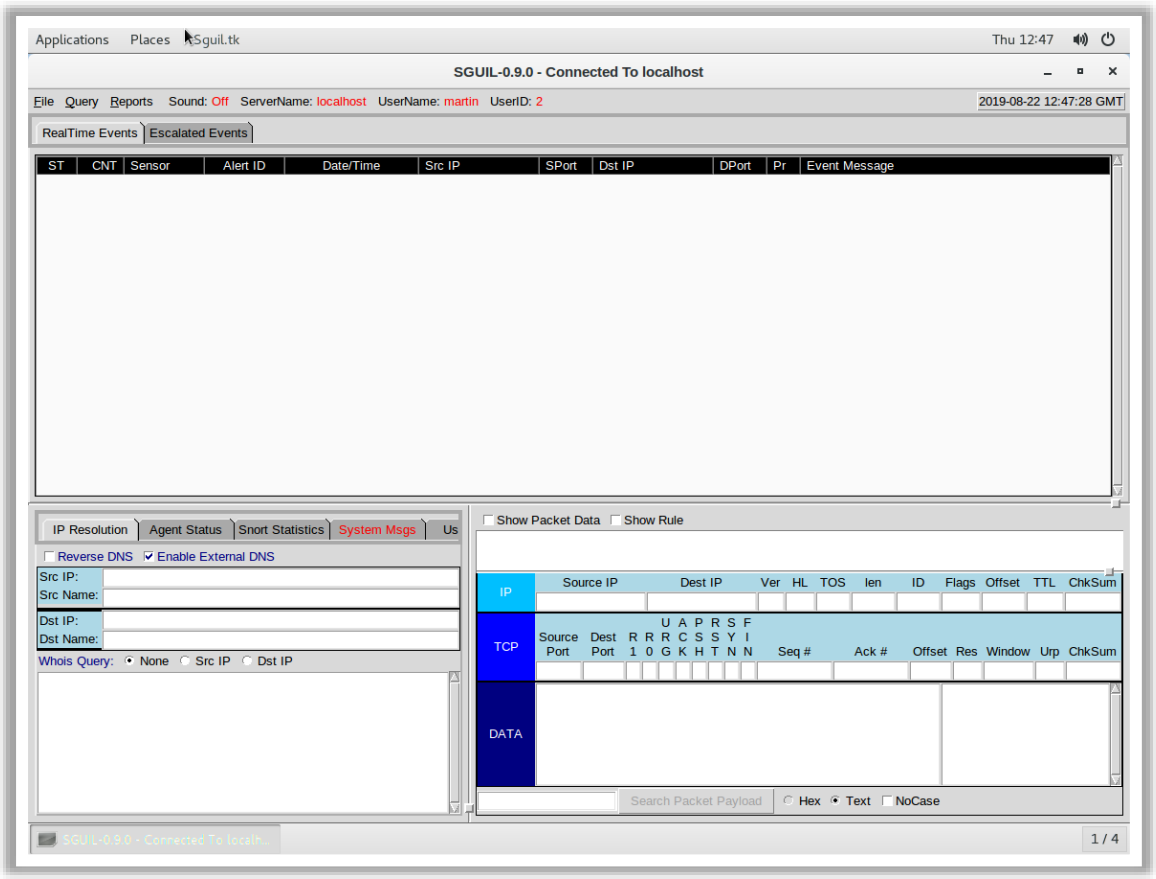
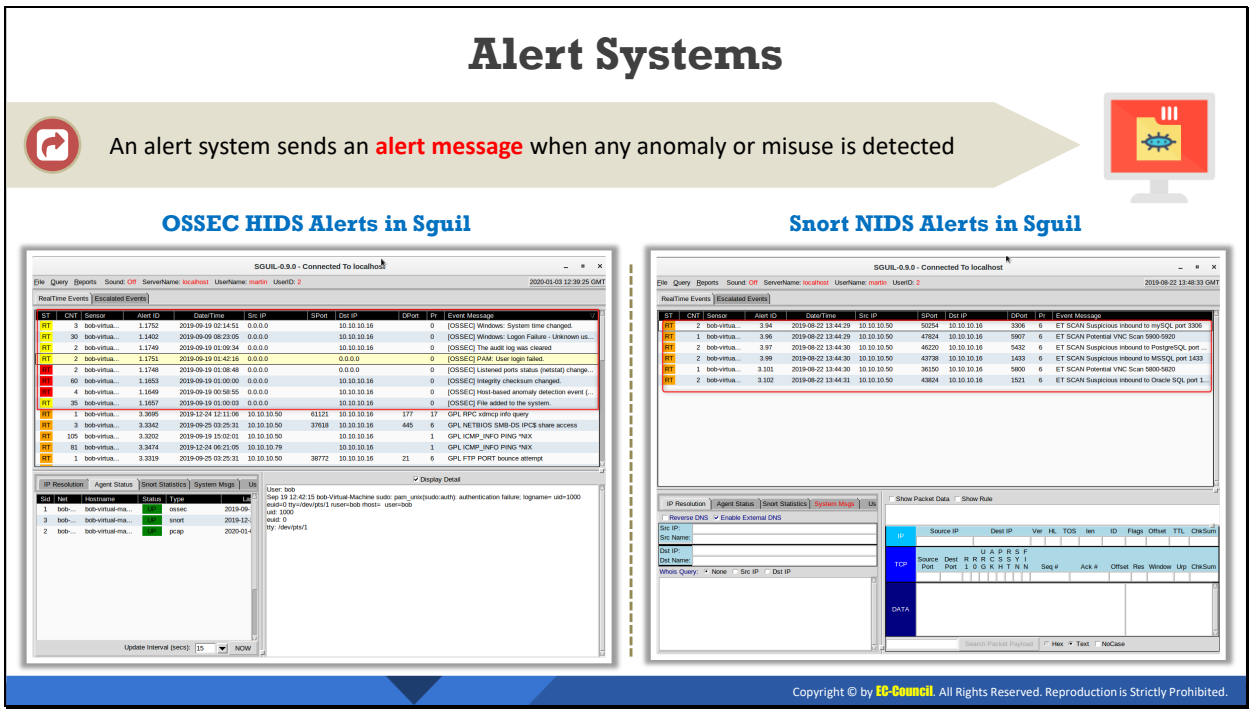


Figure 5.46: Sguil Command Console

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Alert Systems

Alert systems trigger an alert whenever sensors detect malicious activity in the network. The alert communicates to the IDS about the type of malicious activity and its source. The IDS uses triggers to respond to the alert and take countermeasures. An IDS can send alerts using the following methods:

- Pop-up windows
- Email messages
- Sounds
- Mobile messages

When a sensor triggers an alert, there are three possibilities:

- The sensor has correctly identified a successful attack. This alert is most likely relevant and is termed as a true positive.
- The sensor has correctly identified an attack, but the attack failed to meet its objectives. Such alerts are known as non-relevant positive or non-contextual.
- The sensor incorrectly identified an event as an attack. This alert represents incorrect information and is termed as a false positive.

As more IDSs are developed, security professionals would face the task of analyzing an increasing number of alerts resulting from the analysis of different event streams. In addition, IDSs are far from perfect and may produce both false positives and non-relevant positives.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

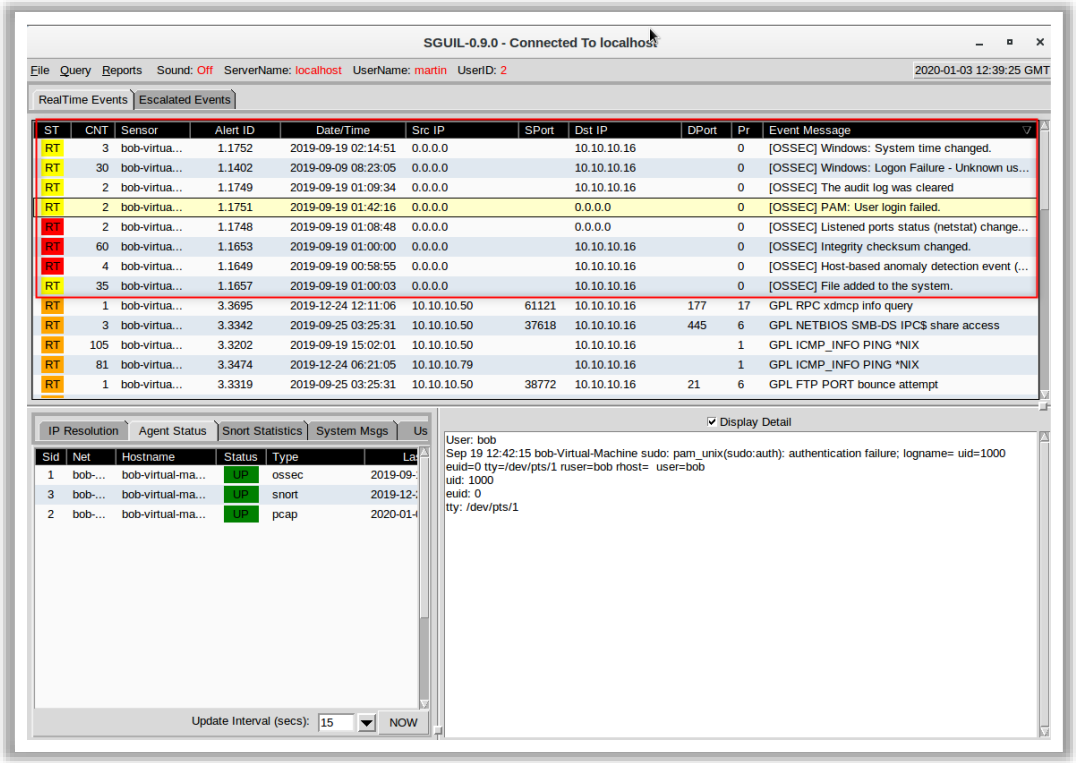


Figure 5.47: OSSEC HIDS Alerts in Sguil

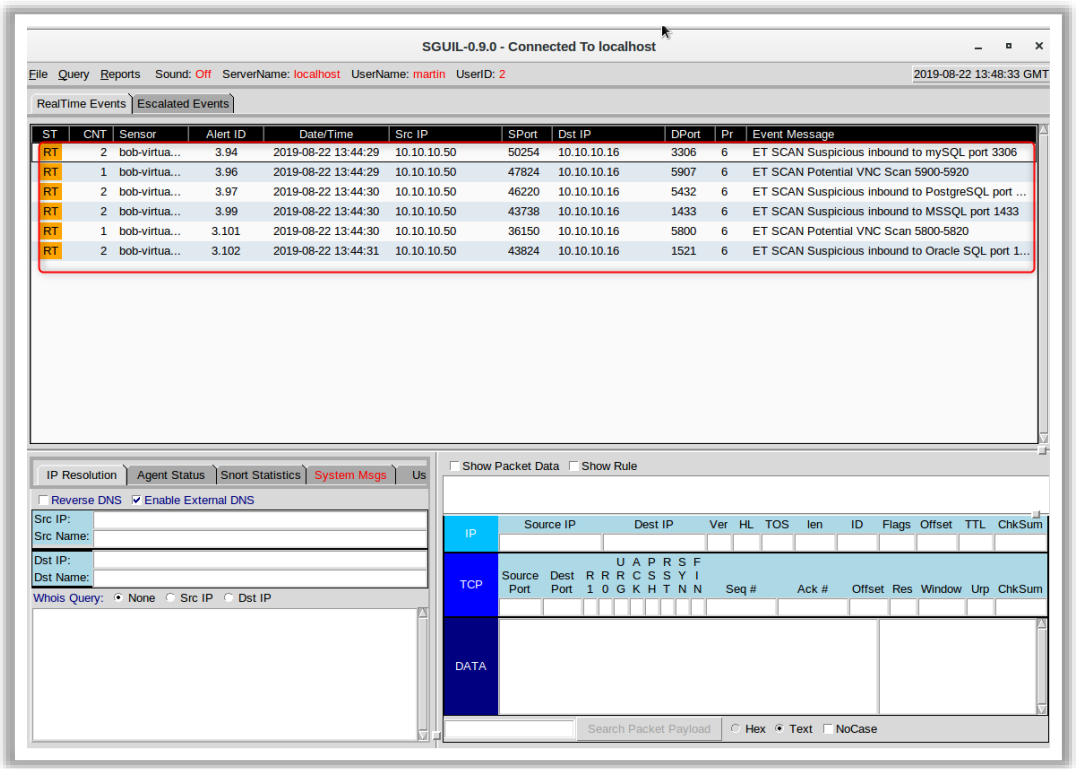
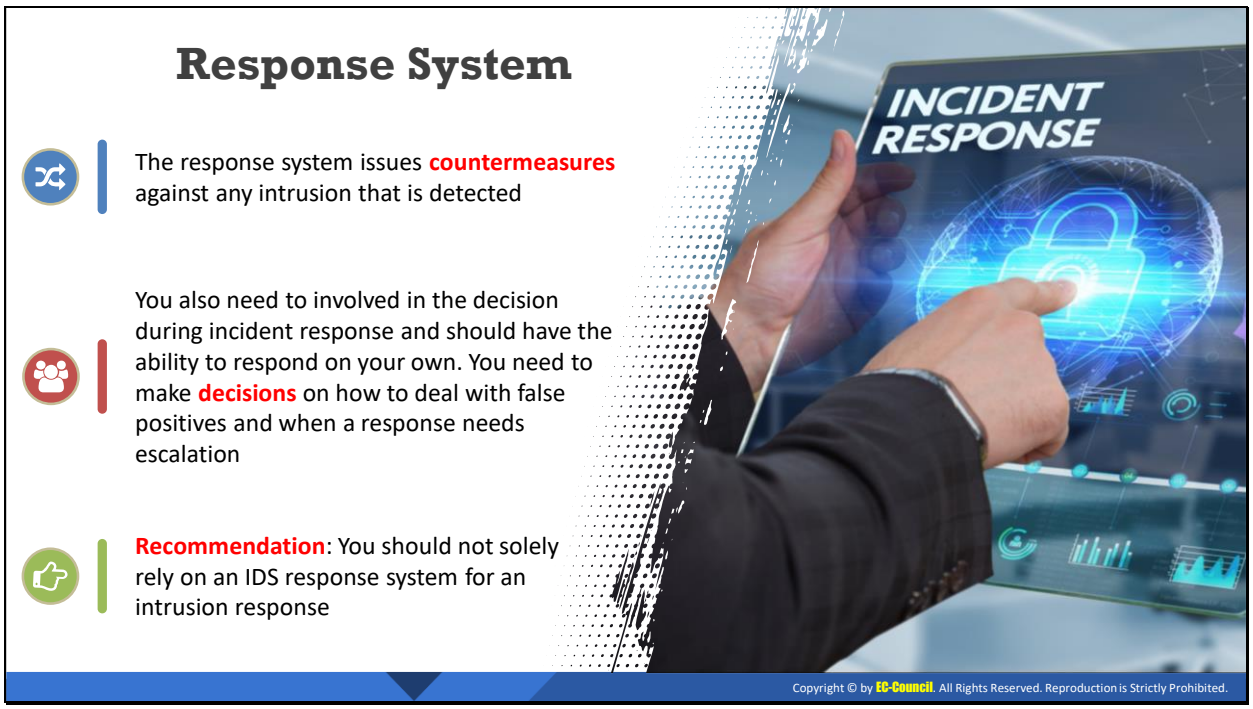


Figure 5.48: Snort NIDS Alerts in Sguil

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Response System

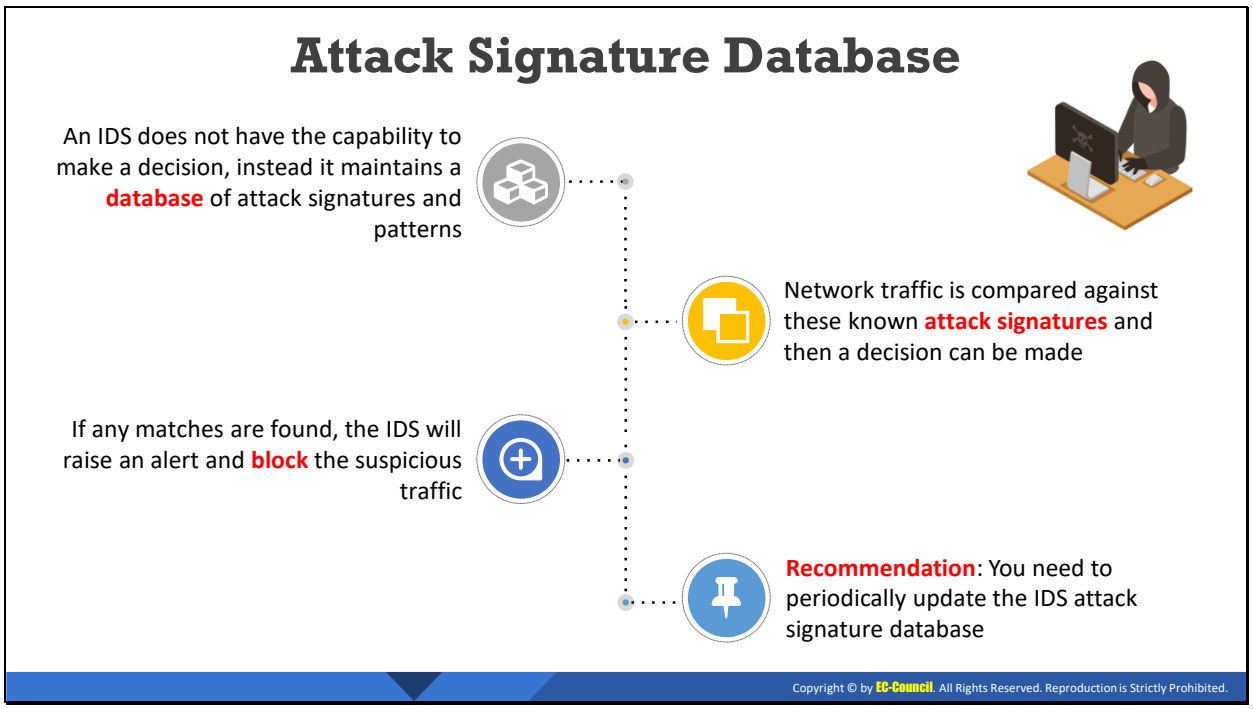
A response system in an IDS is responsible for the countermeasures when an intrusion is detected. These countermeasures include logging out the user, disabling a user account, blocking the source address of the attacker, restarting a server or service, closing connections or ports, and resetting TCP sessions. You also need to involve in the decision during incident response and should have the ability to respond on your own. You need to make decisions on how to deal with false positives and when a response needs escalation.

Security professionals can setup an IDS to allow the response system to take actions against intrusions or they can respond on their own. In the case of false positives, administrators need to respond to allow this traffic into the network without blocking it. Using the response system, administrators can also define the level of counter action an IDS must take to respond to the situation, depending on the severity of the intrusion.

An IDS has the advantage of providing real-time corrective action in response to an attack. It automatically takes action in response to a detected intrusion. The exact action differs per product and depends on the severity and type of attack detected. A common active response is increasing the sensitivity level of the IDS to collect additional information about the attack and the attacker. Another possible active response is making changes to the configuration of systems or network devices such as routers and firewalls to stop the intrusion and block the attacker. Security professionals are responsible for determining the appropriate response and ensuring that the response is executed.

Recommendation: You should not solely rely on an IDS response system for an intrusion response.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



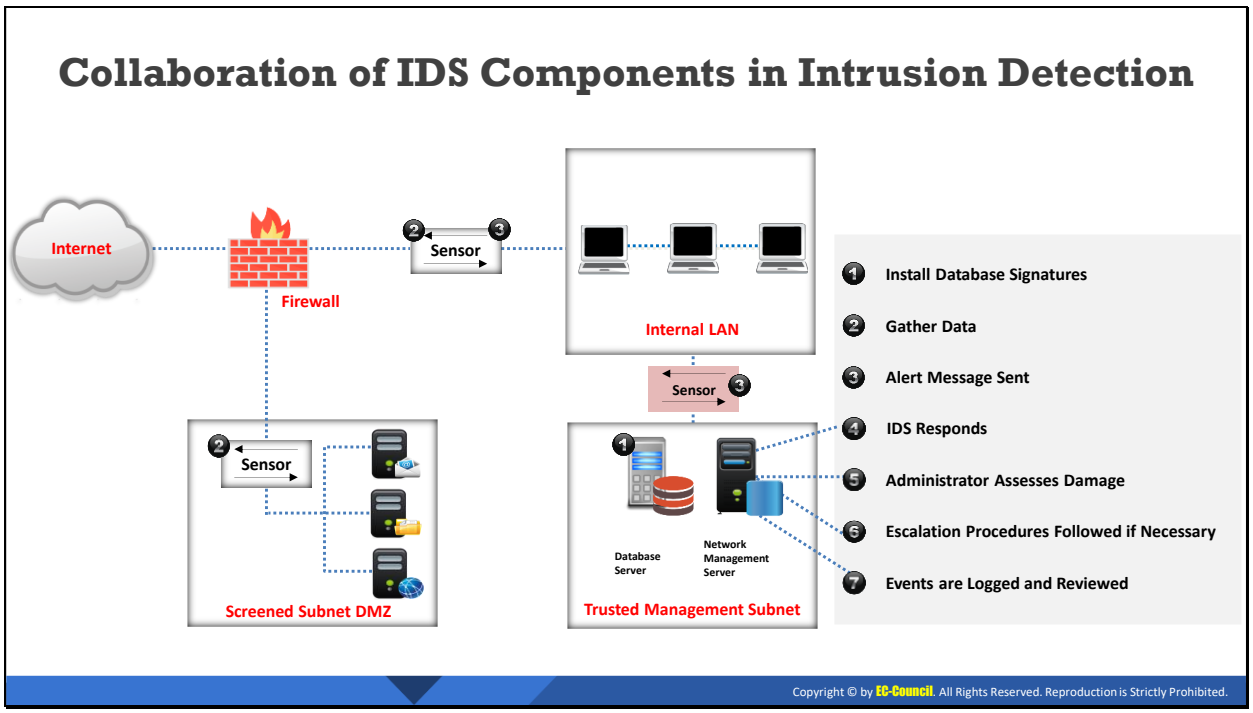
Attack Signature Database

An IDS does not have the capability to make a decision, instead it maintains a database of attack signatures and patterns. Security professionals should exercise their own judgment when evaluating security alerts because an IDS does not have the ability to make these kinds of decisions. However, an IDS can use a list of previously detected signatures, which are stored in the attack signature database, to detect suspicious activity. The IDS compares the signature of packets in the network traffic with the database of known attack signatures. The IDS blocks the traffic if a packet matches a stored signature in the database. Always keep the database updated to detect new types of attacks.

An IDS uses normal traffic logs to match against currently running network traffic to identify suspicious activity. If it identifies unusual traffic activity, it determines the traffic to be suspicious and blocks it before it enters the network.

Recommendation: You need to periodically update the IDS attack signature database.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Collaboration of IDS Components in Intrusion Detection

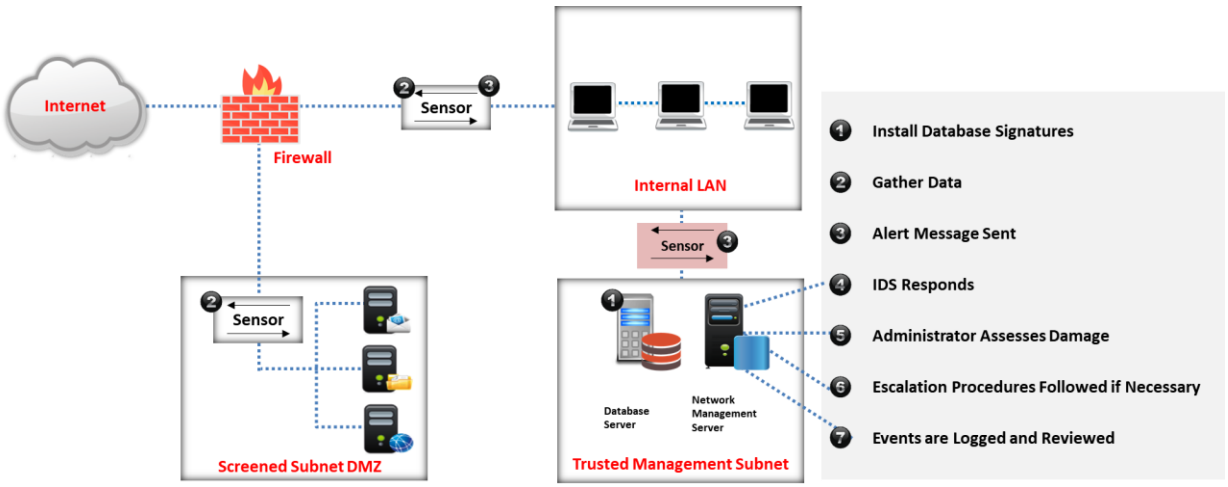


Figure 5.49: Collaboration of IDS Components in Intrusion Detection

Intrusion Detection Steps

An IDS operates in different ways depending on the purpose of the configuration. There is a generalized process for intrusion detection. The steps involved in the process are listed below.

- **Install Database Signatures**

  The first step of intrusion detection occurs before any packets are detected on the network, and it involves installing the database of signatures or user profiles along with the IDS software and hardware. This database helps the IDS compare traffic passing through the network.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **Gather Data**

  The IDS gathers all the data passing through the network using network sensors. The sensors monitor all the packets allowed through the firewall and pass it to the next line of sensors. If it identifies malicious packets, the sensor sends alert messages to the IDS.

- **Alert Message Sent**

  The IDS compares all the packets entering the network with signatures stored in the database. An alert message is transmitted when a packet matches an attack signature or deviates from normal network use. The alert message goes to the IDS command console, where the administrator can evaluate it.

- **IDS Responds**

  When the command console receives an alert message, it notifies the administrator of the alert through a pop-up window, and/or email message, depending on how it is configured for alerts. However, if the administrator configured it to respond automatically, the IDS responds to the alert and takes a counter action such as dropping the packet, restarting the network traffic, and so on.

- **Administrator Assesses the Damage**

  The security professional has to monitor the IDS alerts and determine whether to take any countermeasures or not. The IDS sends alerts depending on the database information and these alerts can include false positives. Administrators need to update the signature database to eliminate false positive alarms.

- **Escalation Procedures (If Necessary)**

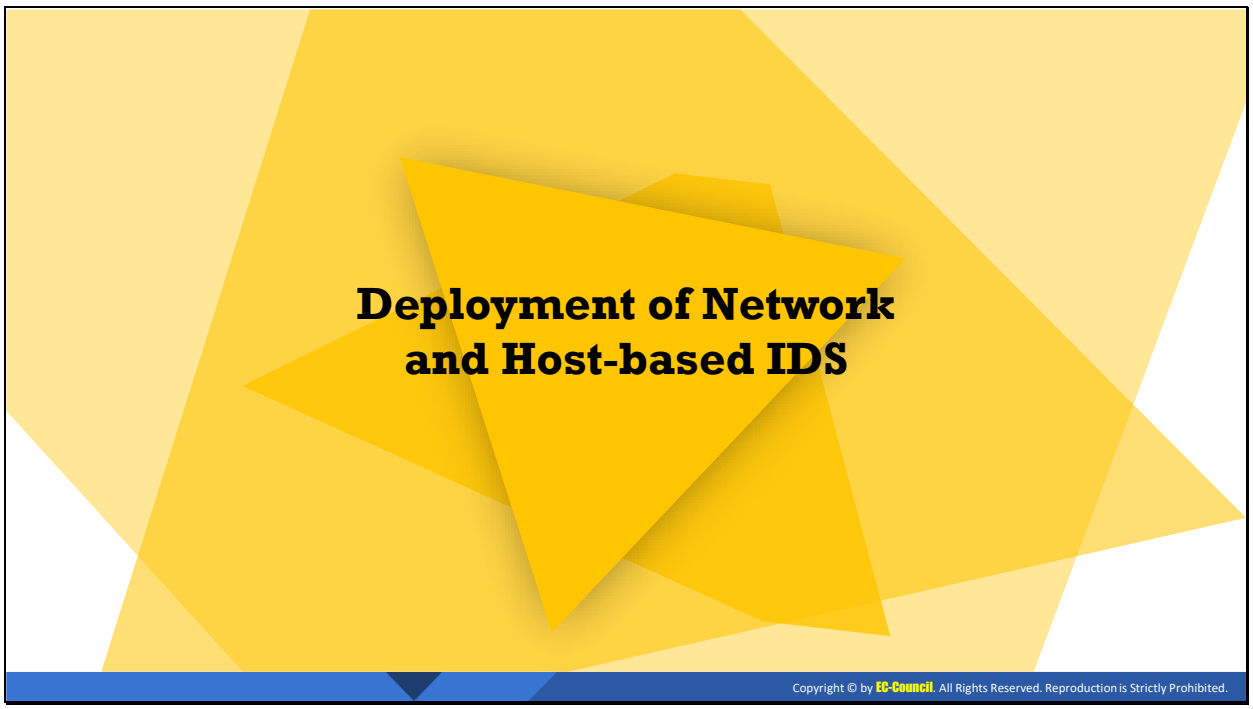
  Escalation procedures are a set of actions written in the security policy and followed if the IDS detects a true positive (attack). These procedures vary depending on the severity of the incident.

- **Events are Logged and Reviewed**

  Security professionals should maintain a log of any intrusion events detected and review them to decide on what countermeasures should be used for future events. These logs can assist security professional in updating the database of attack signatures with new events and in detecting future attacks.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

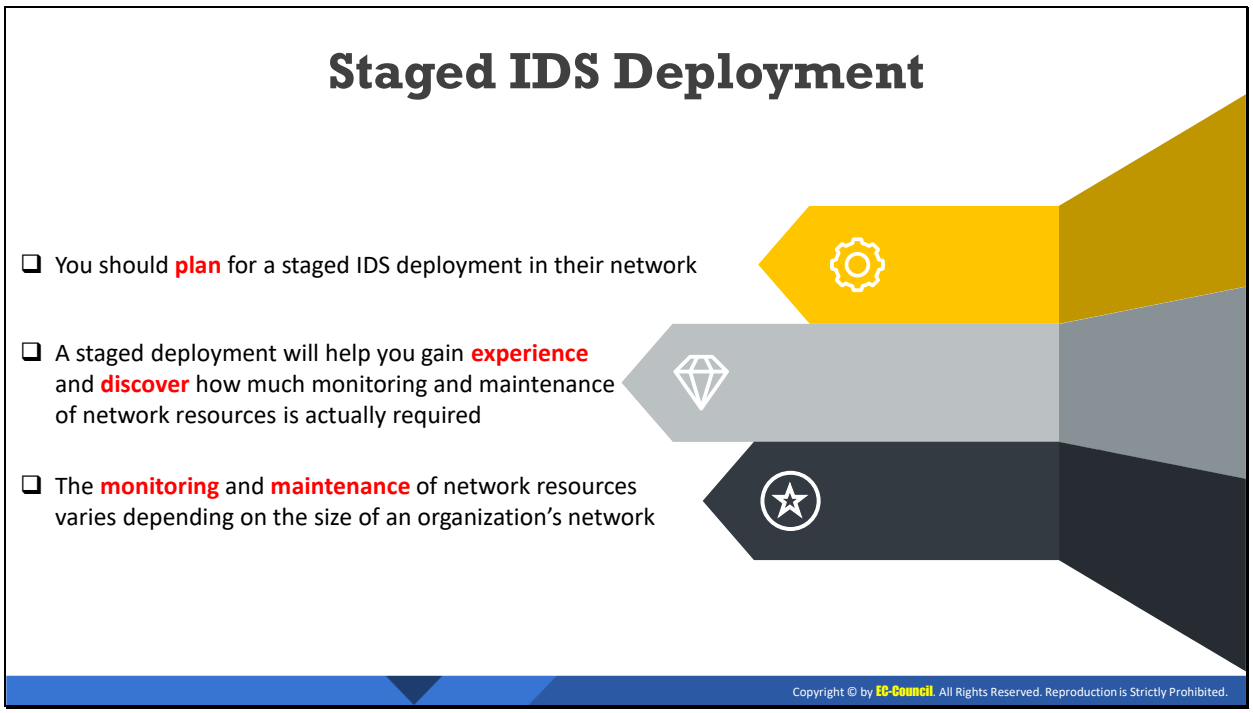
https://t.me/learningnets



Deployment of Network and Host-based IDS

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



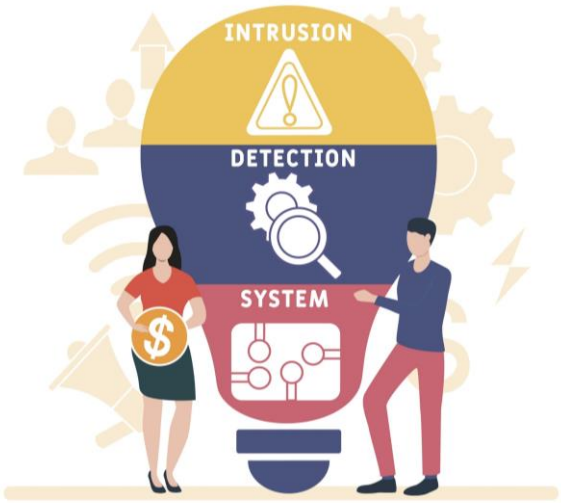
Staged IDS Deployment

Before effectively deploying an IDS, security professionals must understand their network infrastructure and organizational security policies. Then, plan for a staged IDS deployment in the network. A staged deployment will help you gain experience and discover how much monitoring and maintenance of network resources is actually required. The monitoring and maintenance of network resources varies depending on the size of an organization's network.

The organization should consider a staged deployment of an IDS. The initial deployment of an IDS requires high maintenance. Then the organization can think of implementing an IDS at the next stage. The staged deployment helps the organization discover exactly where it needs security from the IDS. Implementing an IDS across the organization's network is advisable when the personnel are able to handle the IDS alerts from different sensors placed at various places. Staged deployment provides administrators enough time to think and get used to the new technology. This staged approach is beneficial to those evaluating and investigating IDS alerts and IDS logs.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Deploying Network-based IDS



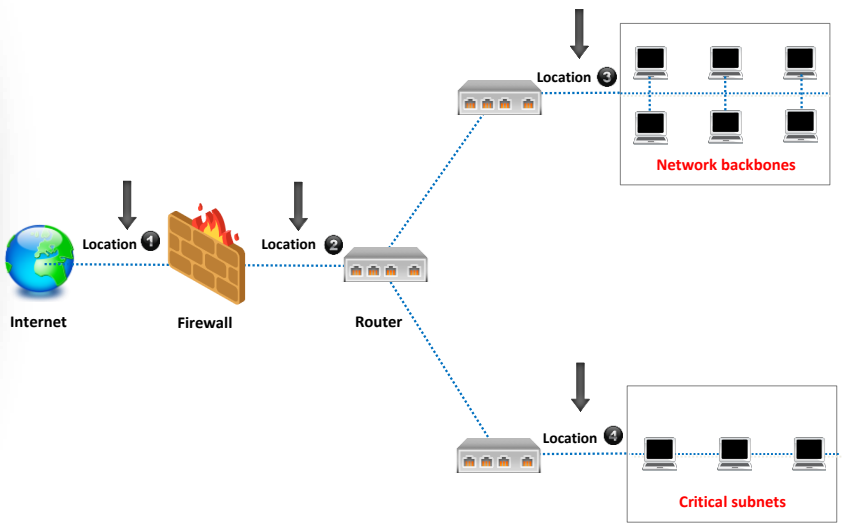
An effective deployment of NIDS requires a lot of attention concerning the **network topology** of the organization

The possible IDS deployment options are categorized based on the location of IDS sensors

Consider all possible **options** and its associated **advantages/disadvantages** when placing a network-based IDS

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

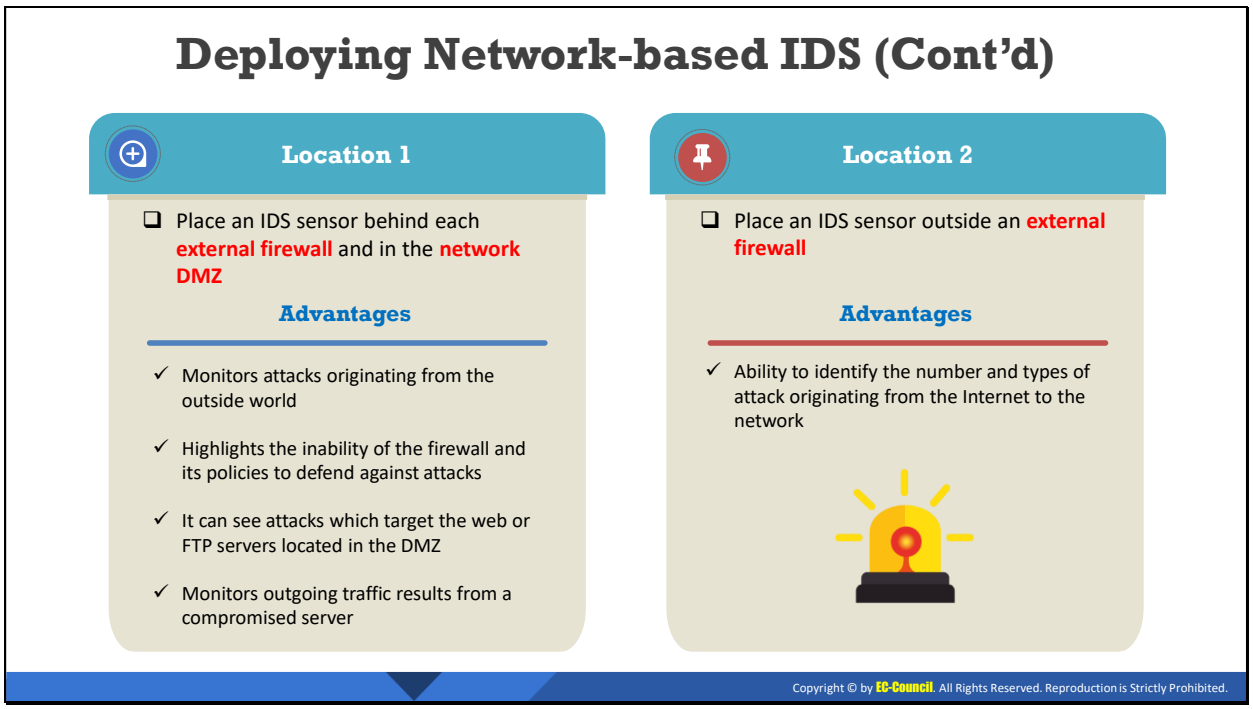
Deploying Network-based IDS (Cont'd)

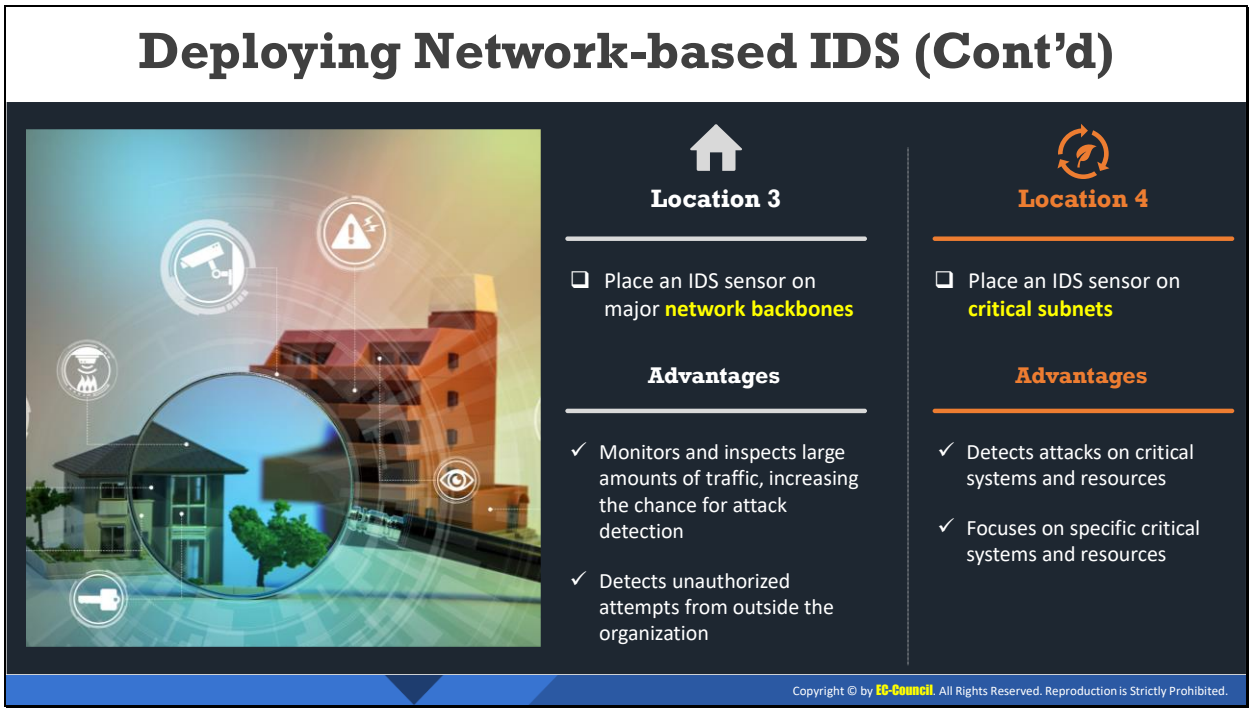


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets





Deploying Network-based IDS

As a NIDS protects multiple hosts from a single location, the security professional can also consider customizing it to provide security for the entire network. An effective deployment of NIDS requires a lot of attention concerning the network topology of the organization. The possible IDS deployment options are categorized based on the location of IDS sensors. The security professional should consider deploying an IDS management console before adding its

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

sensors. Consider all possible options and its associated advantages/disadvantages when placing a network-based IDS.

Security professionals need to deploy IDS sensors incrementally throughout the network. Security professional must consider various factors such as the difference in traffic, logging, reporting, and alerts received when they deploy a new sensor for an IDS.

Security professional should place several network sensors at strategic locations on the network. The positioning of sensors will depend significantly on which kind of network resources need to be monitored for intrusion. Some organizations will want to use the IDS to monitor internal resources such as a sensitive collection of machines or a specific department or physical location. In that case, the most logical place for the IDS sensor will be on the choke point between those systems and the rest of the internal network. Some of the critical common-entry points to place sensors are listed below:

- At Internet gateways
- At connections between LAN connections
- At remote access servers that receive dial-up connections from users
- At VPN devices that connect an internal LAN to an external LAN
- Between subnets that are separated by switches

If an organization is planning to monitor intrusions targeting internal servers such as DNS servers or mail servers, then it must place a sensor inside the firewall on the segment that connects the firewall to the internal network. The logic behind this is that the firewall will prevent a vast majority of attacks aimed at the organization, and regular monitoring of firewall logs will identify them. The IDS on the internal segment will detect some of those attacks that manage to get through the firewall.

If a firewall is in place to protect the network then positioning sensors inside the firewall is more secure than placing a sensor outside the firewall at a position exposed to the Internet. If it is placed outside the firewall, it can become the major focus for attacks. A more secure location to place a sensor is behind the firewall in the DMZ.

Different options for the deployment of sensors in the network are discussed below.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

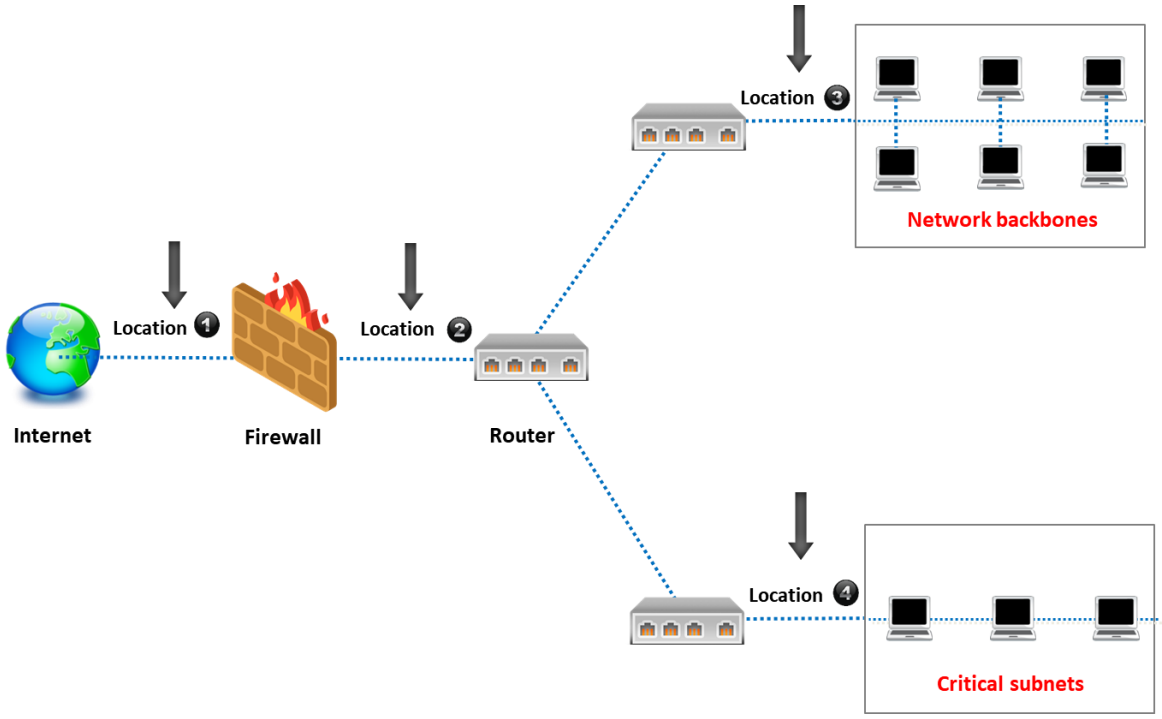


Figure 5.50: Deploying Network-Based IDS

- **Location 1**: Place an IDS sensor behind each external firewall and in the network DMZ. The sensor placed at this location can detect inbound attacks. It can also be configured to detect outbound attacks. The sensor is configured to detect the least sensitive attacks to avoid false alarms. Such a sensor is configured to only log the attack attempts, instead of sending alerts out for them.

  Advantages

  - Monitors attacks originating from the outside world
  - Highlights the inability of the firewall and its policies to defend against attacks
  - It can see attacks which target the web or FTP servers located in the DMZ
  - Monitors outgoing traffic results from a compromised server

- **Location 2**: Place an IDS sensor outside an external firewall. This location is ideal for securing the perimeter network as well as identifying those attacks that bypass the external firewall. The NIDS sensor secures web, FTP, and other servers located on the perimeter of the network. It detects attacks with low to moderate impact in order to avoid the chances of generating false alarms. Any sensor placed here also has the ability to monitor for outbound attacks.

  Advantages

  - Ability to identify the number and types of attack originating from the Internet to the network

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **Location 3**: Place an IDS sensor on major **network backbones.** The sensor placed at this location is used to secure the internal network of the organization. It detects an attack may have bypassed the internal firewall. A sensor at this location is capable of detecting both inbound and outbound attacks. Such a sensor is configured to detect medium to high impact level attacks.

  Advantages

  - Monitors and inspects large amounts of traffic, increasing the chance for attack detection
  - Detects unauthorized attempts from outside the organization

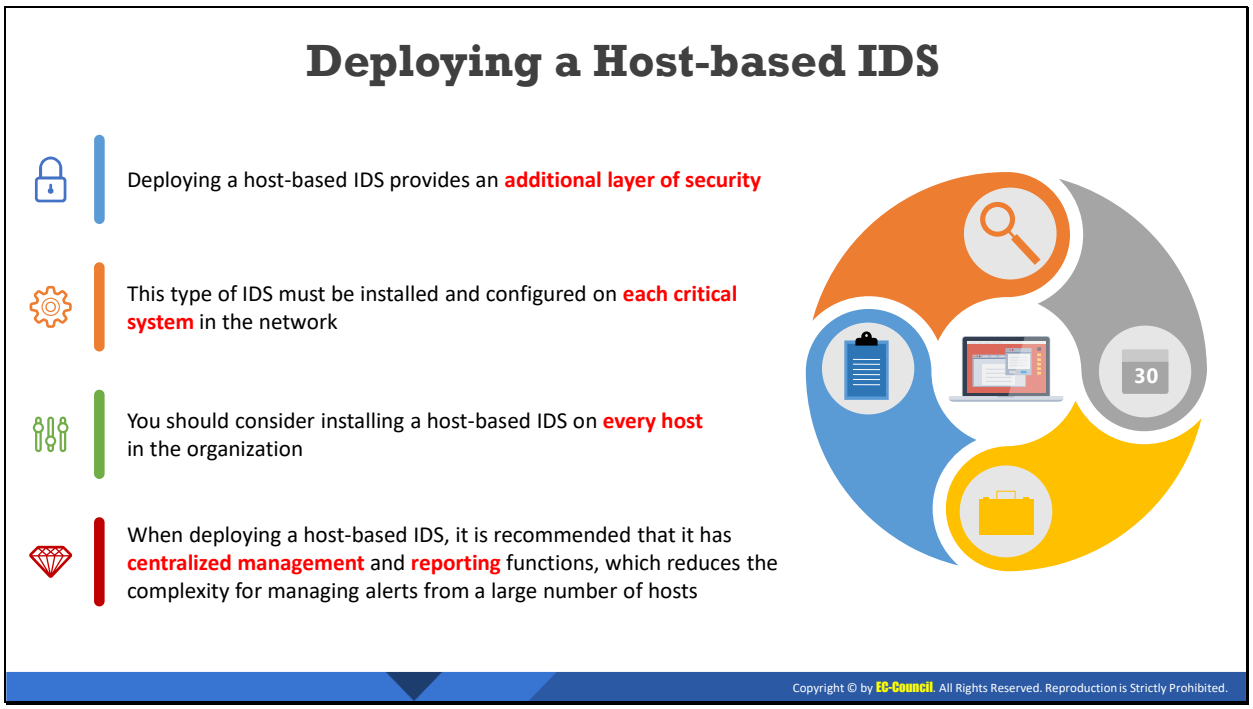
- **Location 4**: Place an IDS sensor on critical subnets. The sensor at this location is used to protect sensitive hosts in the network, including critical servers. It is capable of detecting both inbound and outbound attacks. Such a sensor is configured to detect high impact level attacks.

  Advantages

  - Detects attacks on critical systems and resources
  - Focuses on specific critical systems and resources

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



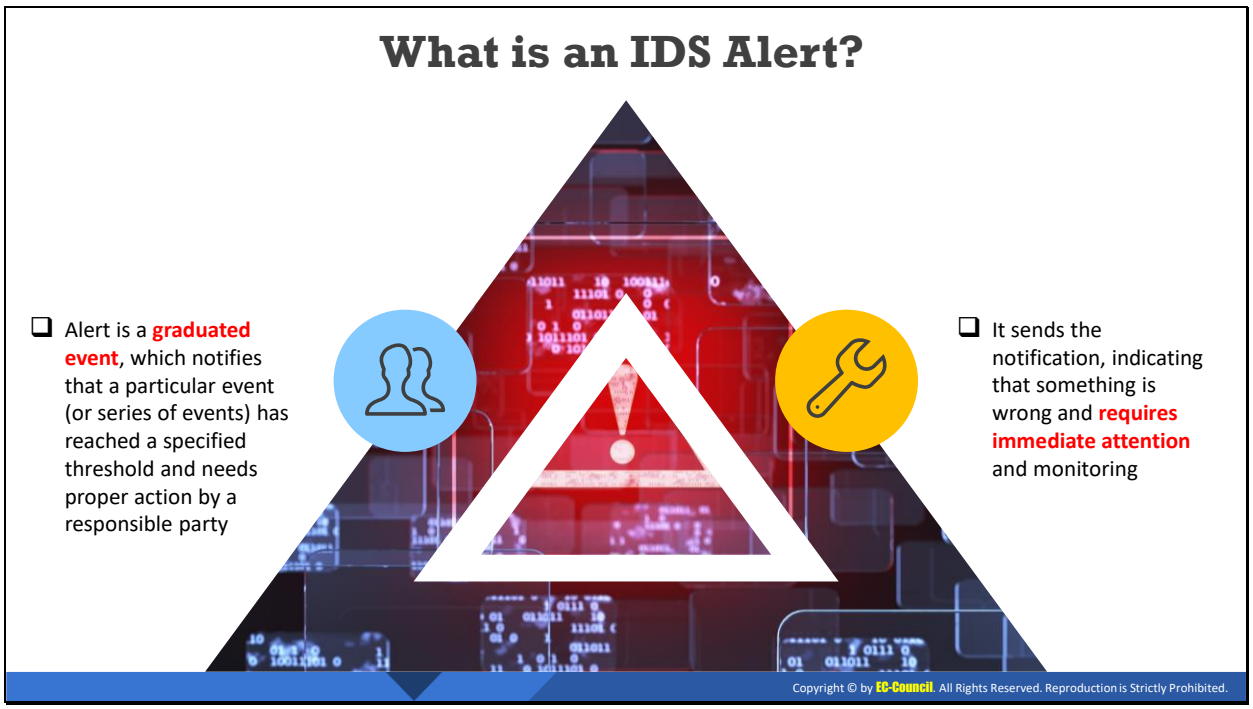
Deploying a Host-based IDS

Deploying a host-based IDS provides an additional layer of security. This type of IDS must be installed and configured on each critical system in the network. You should consider installing a host-based IDS on every host in the organization. When deploying a host-based IDS, it is recommended that it has centralized management and reporting functions, which reduces the complexity for managing alerts from a large number of hosts.

Host-based IDS (HIDS) deployment is done with proper planning and care, as deploying these on a large-scale environment has the potential to generate numerous false alarms, which can get quite difficult to manage. Initial deployment of a HIDS is done on critical servers only. Security professionals must consider implementing an IDS management console before adding additional hosts.

If security professional comfortably manages the HIDS on critical servers at the initial stage, then and only then they can consider deploying the HIDS on all remaining hosts in the network. This allows security professional to provide security at the individual host level. However, deploying HIDS on every host on the network is quite expensive and requires additional software and maintenance, especially in case of a wide-scale HIDS deployment.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



What is an IDS Alert?

An alert is a graduated event that notifies that a particular event (or series of events) has reached a specified threshold and needs appropriate action by a responsible party. It generates incidents and/or issue tickets, indicating that something is wrong and requires immediate attention and monitoring. This alerting can be done in many ways such as sending emails, producing alerts on the desktop, etc. An alert may contain details such as what kind of event, duration of that event, when it occurred, where it occurred, in which device, and what OS or version is it running on.

Alerts are the domain of security devices and security-related systems. However, this is not fixed. For example, IDS/IPS analyzes all inbound network traffic and decides whether a specific connection is allowed or not, based on packet content. If it is identified that a specific connection is malicious, then it will take predefined actions or generate alerts to notify the users.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Types of IDS Alerts

An IDS generates four types of alerts: True Positive, False Positive, False Negative, and True Negative.

- **True Positive (Attack - Alert)**: A true positive is a condition that occurs when an event triggers an alarm and causes the IDS to react as if a real attack is in progress. The event may be an actual attack, in which case an attacker attempts to compromise the network, or it may be a drill, in which case security personnel use hacker tools to test a network segment.
- **False Positive (No attack - Alert)**: A false positive occurs if an event triggers an alarm when no actual attack is in progress. It occurs when an IDS treats regular system activity as an attack. False positives tend to make users insensitive to alarms and weaken their reactions to actual intrusion events. While testing the configuration of an IDS, administrators use false positives to determine whether the IDS can distinguish between false positives and real attacks.
- **False Negative (Attack - No Alert)**: A false negative is a condition that occurs when an IDS fails to react to an actual attack event. This condition is the most dangerous failure, as the purpose of an IDS is to detect and respond to attacks.
- **True Negative (No attack - No Alert)**: A true negative is a condition that occurs when an IDS identifies an activity as acceptable behavior, and the activity is acceptable. A true negative means successfully ignoring acceptable behavior. It is not harmful, as the IDS performs as expected in this case.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Characteristics of Good IDS Solutions

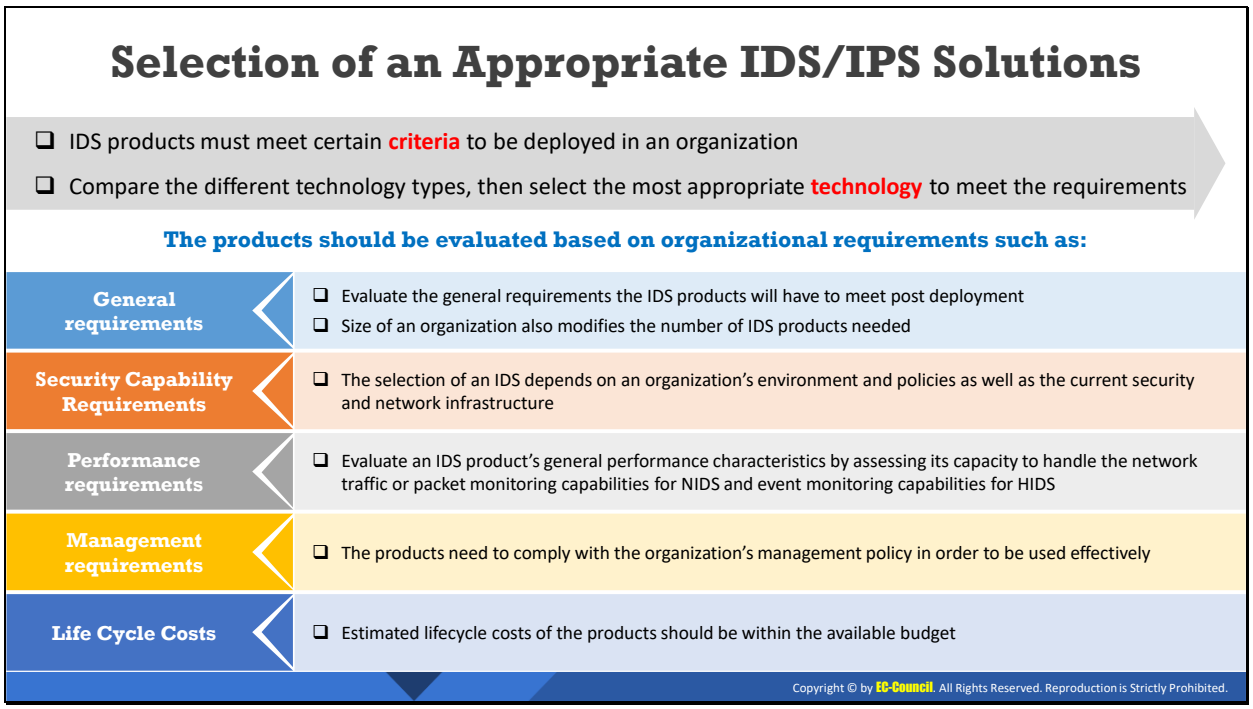
An ideal IDS should have the following characteristics:

- Organizations should have an IDS that can run without or with minimal human intervention. The configuration of the system monitors and detects all suspicious activities on the host system. However, administrators should have all the privileges in auditing and monitoring for this to work.
- Even if the host system fails or crashes, the IDS should still function reliably. It is advisable to configure the IDS so it is fault tolerant and does not require a reconfiguration or reboot every time the host system fails. In addition, it should be capable of monitoring itself to avoid any damage.
- An IDS should provide features for halting and blocking attacks. These attacks can occur from any application or software. This also involves alerting the security professional through online, mobile, or email notification. The method of notification depends on the configuration setup by the administrator.
- By having information gathering capabilities, an IDS helps a security professional detect the type of attack, source of the attack, and the effects the attack caused in the network. Gathering evidence for a cyber-forensic investigation is one of the required characteristics of an IDS.
- In large organizations, an IDS is built with a fail-safe feature to help hide itself in the network. This feature helps create a fake network to attract intruders to as well as for analyzing the possibilities of different types of attacks. It also helps in vulnerability analysis of the network.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- Not easily deceived. An IDS should be able to detect changes in the files of the system or network. The file checker feature in an IDS notifies the security professional if the intruder made any sort of alteration to the files. The IDS should report every activity that has occurred on the network as this aids the security professional when analyzing vulnerabilities and rectifying them.
- Tailored to specific system needs. When recursive changes occur in the network, an IDS should be adaptable to these changes. This also includes adapting different defense mechanisms for every different system in the network.
- Minimal overhead on the system. The configuration of an IDS should be such that it does not cause overheads in the network or system.
- Resistant to subversion.
- Observe deviations from normal behavior.
- Copes with dynamic system behavior.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Selection of an Appropriate IDS/IPS Solutions

IDS products must meet certain criteria to be deployed in an organization. An organization should compare the different technology types and then select the most appropriate technology to meet its requirements. The products should be evaluated based on organizational requirements such as the following:

- **General requirements:** An organization must have a clear baseline of the requirements for an IDS product. IDS solutions may differ in terms of features and services. The organization must determine which IDS product will best suit their requirements. For example, there are situations where a single IDS product may not satisfy the requirements of an organization. This scenario encourages the use of multiple IDS products. Wireless IDS products have certain general requirements such as a method of detecting anomalies and a process of connecting to other components, which determine whether the product can satisfy the company's requirements. Evaluate the general requirements of the IDS products to meet post deployment. The number of IDS products needed also depends on the size of the organization.
- **Security capability requirements:** The selection of an IDS depends on an organization's environment and policies as well as the current security and network infrastructure. It is crucial to meet these as the product will be used in conjunction with other security controls.

  Organizations should evaluate IDS security capability requirements as a baseline for creating a specific set of criteria. This is achieved by accounting for the organization's environment, security policies, and network infrastructure. It is important to check and confirm the security capabilities of an IDS product. An IDS product that does not meet the required security capabilities is of no use as a security control, and a security

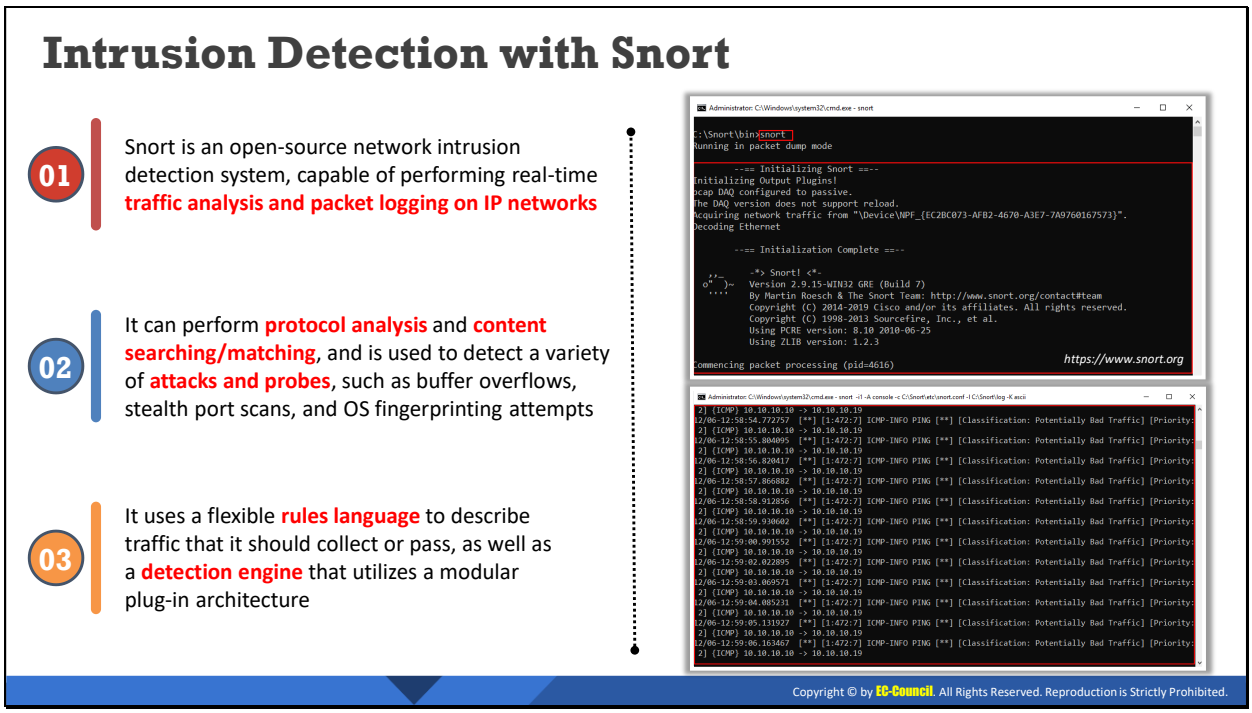
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

professional must select a different product or use that product in combination with another security control. The IDS product should feature security capabilities such as information gathering, logging, detection, and prevention.

- **Performance requirements:** Evaluate IDS products based on their general performance characteristics.
  - **Network-based IDS (NIDS)**: This type of IDS has the ability to monitor and handle network traffic.
  - **Host-based IDS (HIDS)**: This type of IDS has the ability to monitor a certain number of events per second.

  Security professionals should evaluate an IDS product's general performance characteristics by assessing its capacity to handle network traffic or its packet monitoring capabilities for NIDS and event monitoring capabilities for HIDS.
- **Management requirements:** The products need to comply with the organization's management policy to offer sufficient performance. If the product does not comply with the company's policy, it would be difficult to handle it and make it work effectively.
- **Lifecycle costs:** IDS products are environment-specific, and it can be a tedious task for organizations to quantify the cost of IDS solutions. The cost of the IDS product should be proportional to the available budget of the organization. Estimated lifecycle costs of the selected IDS products should be in the range of the available funding. Selecting an IDS based on cost is difficult as the environment, security, and other networking criteria are likely to affect the cost.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Intrusion Detection with Snort

Source: *https://www.snort.org*

Snort is an open-source network intrusion detection system capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis and content searching/matching, and it is used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, and OS fingerprinting attempts. It uses a flexible rules language to describe traffic that it should collect or pass, as well as a detection engine that uses a modular plug-in architecture.

Uses of Snort:

- Straight packet sniffer such as tcpdump
- Packet logger (useful for network traffic debugging, etc.)
- Network intrusion prevention system

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

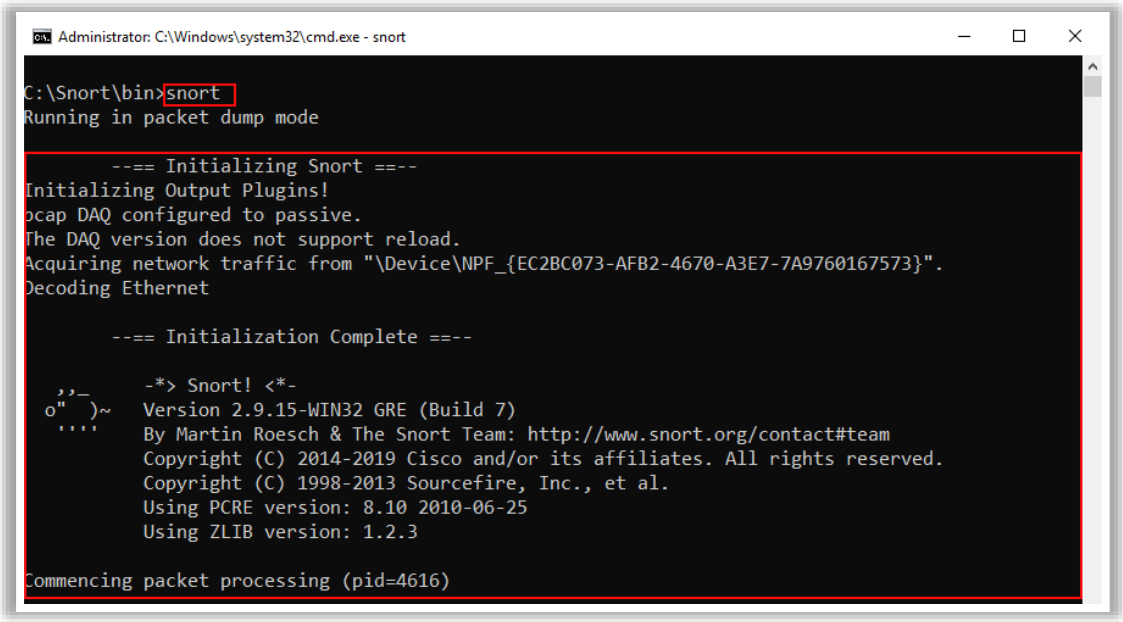


Figure 5.51: Screenshot of Snort

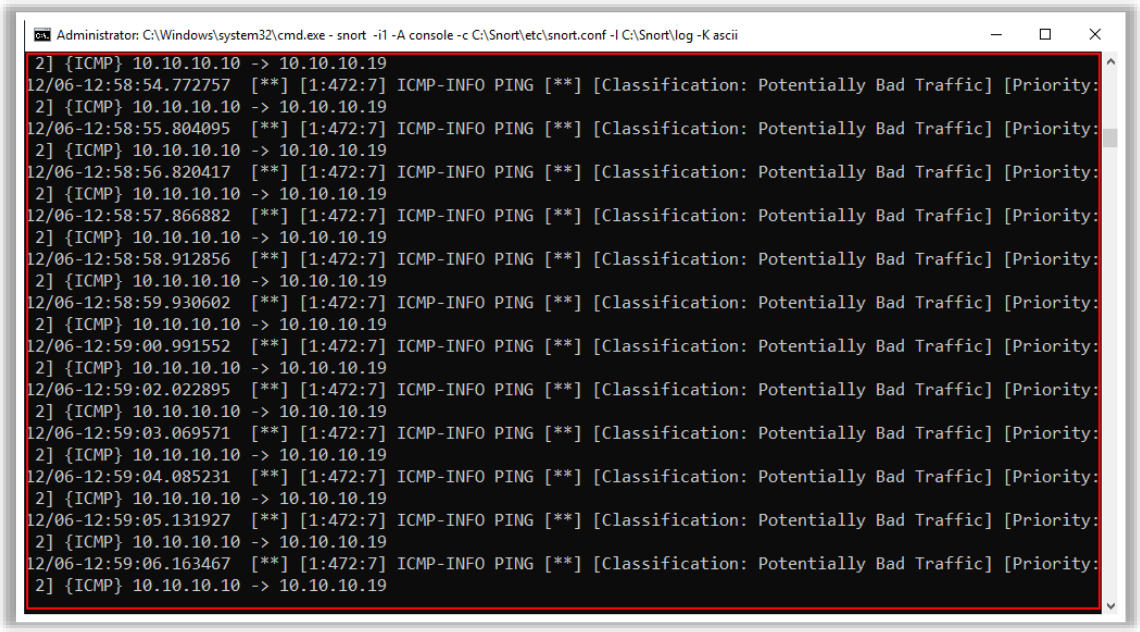
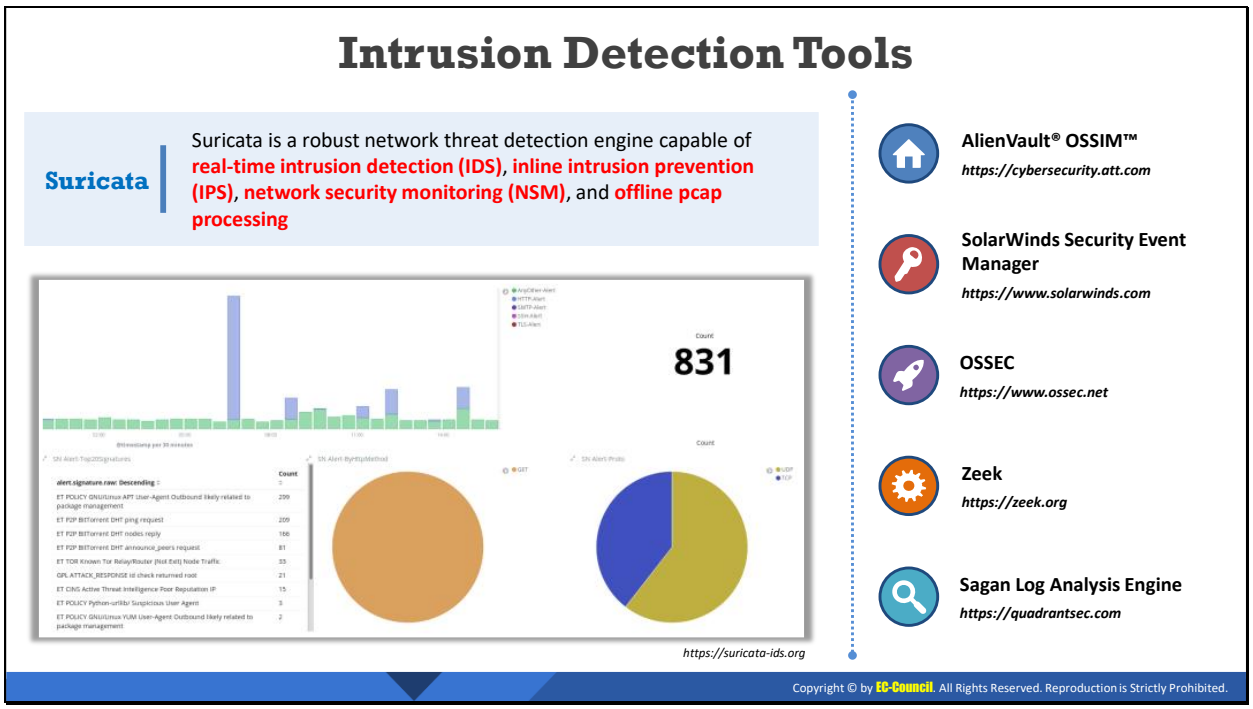


Figure 5.52: Snort output

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Intrusion Detection Tools

Intrusion detection tools detect anomalies. These tools, when running on a dedicated workstation, read all network packets, reconstruct user sessions, and scan for possible intrusions by looking for attack signatures and network traffic statistical anomalies. Moreover, these tools offer real-time, zero-day protection from network attacks and malicious traffic, and they prevent malware, spyware, port scans, viruses, DoS, and DDoS from compromising hosts.

- **Suricata**

  Source: *https://suricata-ids.org*

  Suricata is a robust network threat detection engine capable of real-time intrusion detection (IDS), inline intrusion prevention (IPS), network security monitoring (NSM), and offline pcap processing. It inspects the network traffic using powerful and extensive rules and a signature language, and it provides powerful Lua scripting support for the detection of complex threats. With standard input and output formats such as YAML and JSON, integrations with existing tools such as SIEMs, Splunk, Logstash/Elasticsearch, Kibana, and other databases become effortless.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

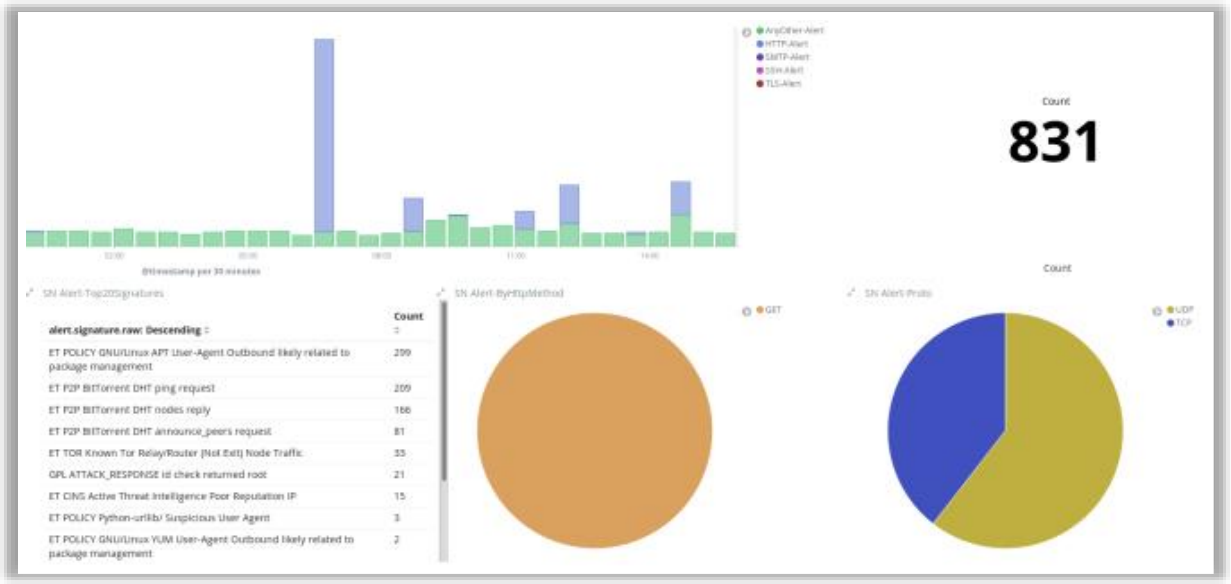


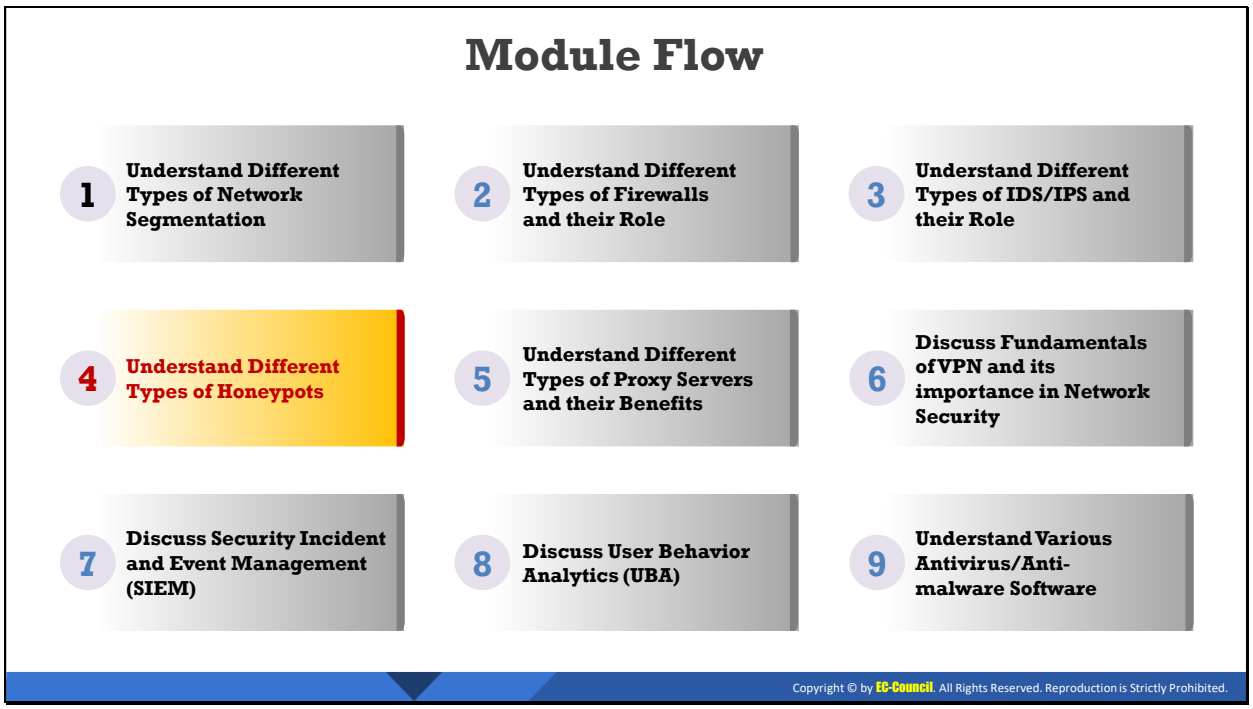
Figure 5.53: Screenshot of TippingPoint

Some additional intrusion detection tools are listed below:

- AlienVault® OSSIM™ (*https://cybersecurity.att.com*)
- SolarWinds Security Event Manager (*https://www.solarwinds.com*)
- OSSEC (*https://www.ossec.net*)
- Zeek (*https://zeek.org*)
- Sagan Log Analysis Engine (*https://quadrantsec.com*)

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

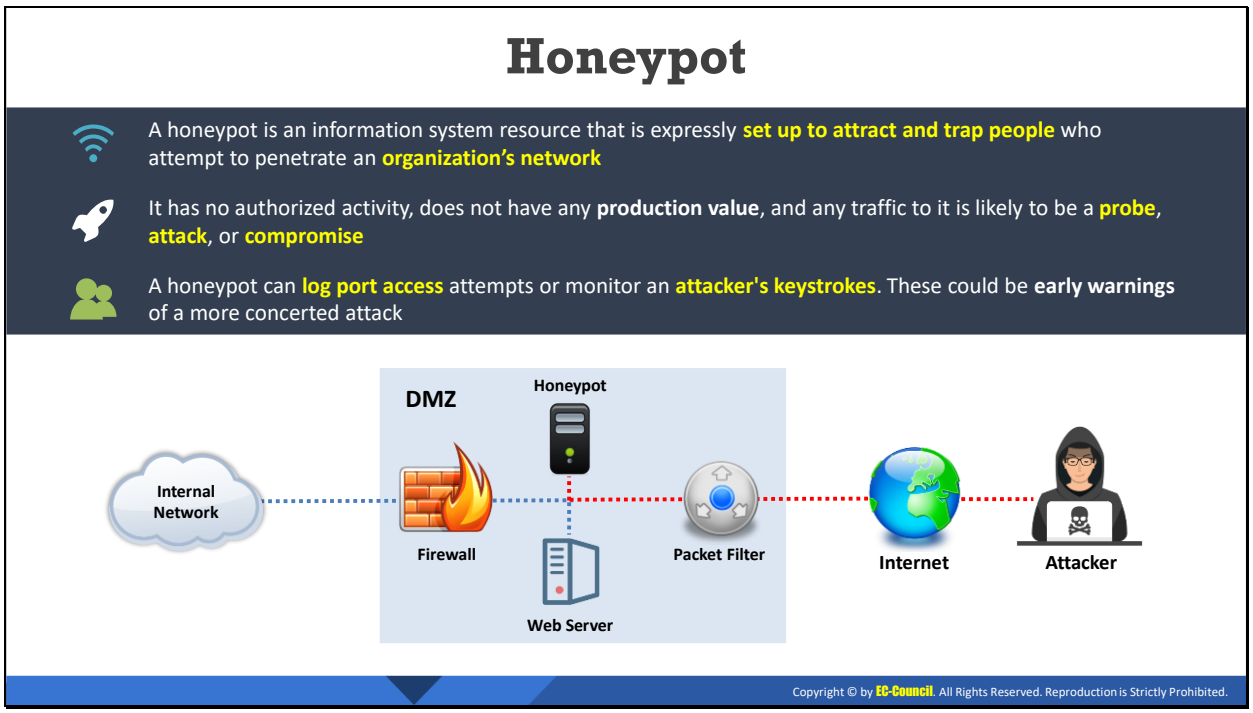
https://t.me/learningnets



Understand Different Types of Honeypots

Honeypots allow security professionals to defend against attacks that even a firewall cannot prevent. Honeypots provide increased visibility and an additional layer of security against both internal and external attacks. This section provides an understanding of different types of honeypots and honeypot tools.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Honeypot

A honeypot is a computer system on the Internet intended to attract and trap those who attempt unauthorized or illicit utilization of the host system to penetrate an organization's network. It is a fake proxy run to frame attackers by logging traffic through it and then sending complaints to the victims' ISPs. It has no authorized activity or production value, and any traffic to it is likely a probe, attack, or compromise. Whenever there is any interaction with a honeypot, it is most likely to be malicious. Honeypots are unique; they do not solve a specific problem. Instead, they are a highly flexible tools with many different security applications. Honeypots help in preventing attacks, detecting attacks, and information gathering and research. A honeypot can log port access attempts or monitor an attacker's keystrokes; these could be early warnings of a more concerted attack. It requires a considerable amount of effort to maintain a honeypot.

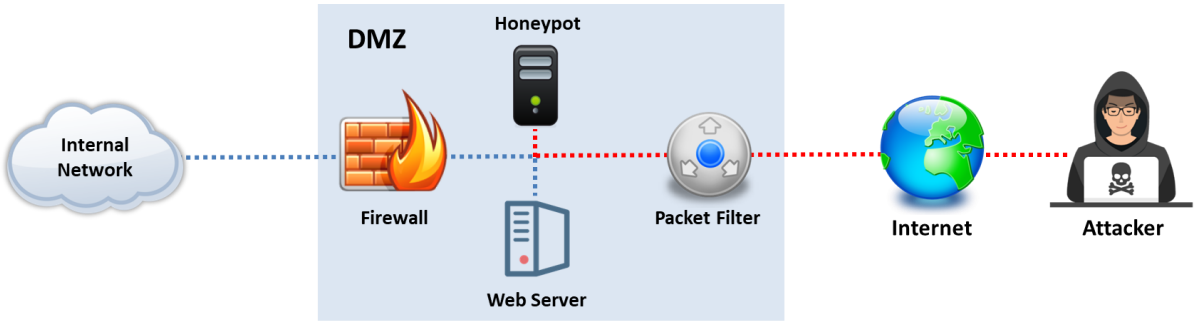


Figure 5.54: Example of Honeypot

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Types of Honeypots

Classification of Honeypots based on their design criteria

Low-interaction Honeypots

- These honeypots simulate only a **limited number of services** and applications of a target system or network

Medium-interaction Honeypots

- These honeypots simulate a **real operating system**, applications, and services of a target network

High-interaction Honeypots

- These honeypots **simulate all services** and applications of a target network

Pure Honeypots

- These honeypots emulate the **real production network** of a target organization

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Honeypots (Cont'd)

Classification of honeypots based on their deployment strategy

Production Honeypots

- Are deployed inside the production network of the organization along with other production servers
- As they are deployed internally, they also help to find out internal flaws and attackers within an organization

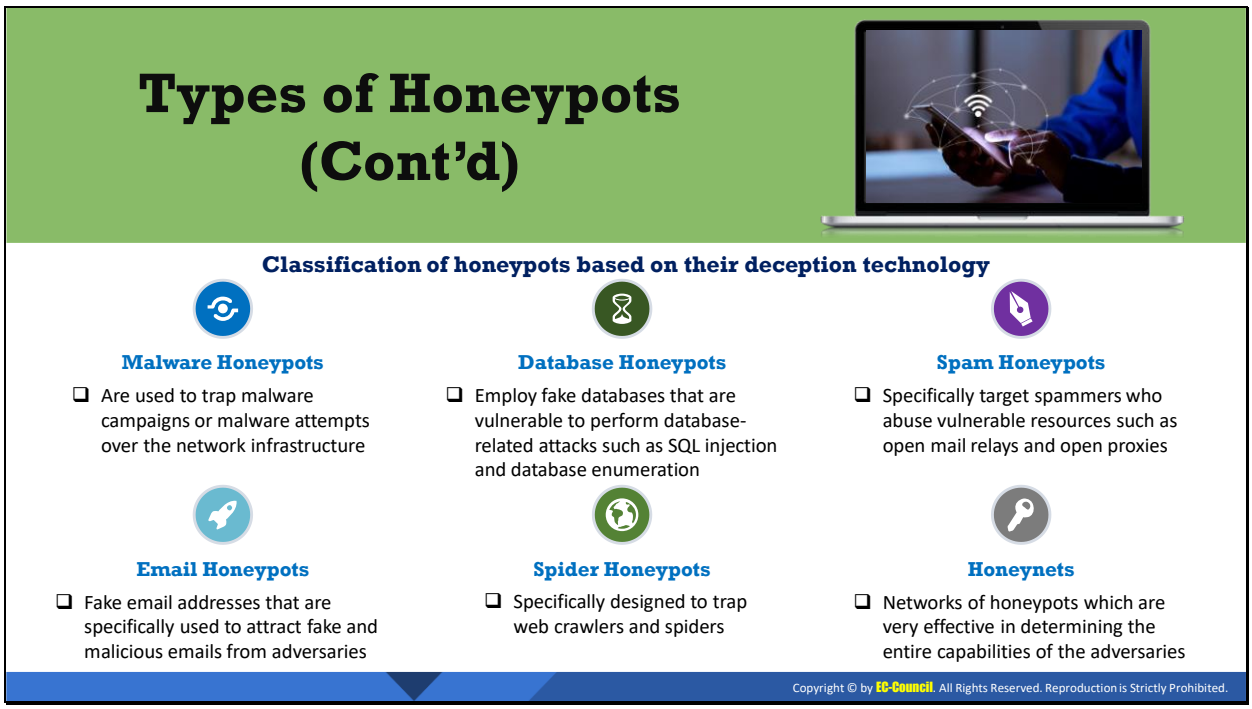
Research Honeypots

- Are high-interaction honeypots primarily deployed by research institutes, governments, or military organizations to gain detailed knowledge about the actions of intruder

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Types of Honeypots

Honeypots are classified into the following types based on their design criteria:

- **Low-interaction Honeypots**

  Low-interaction honeypots emulate only a limited number of services and applications of a target system or network. If the attacker does something that the emulation does not expect, the honeypot will simply generate an error. They capture limited amounts of information, i.e., mainly transactional data, and some limited interactions. These honeypots cannot be compromised completely. They are set to collect higher-level information about attack vectors such as network probes and worm activities. Some examples are KFSensor, and Honeytrap.

- **Medium-interaction Honeypots**

  Medium-interaction honeypots simulate a real OS as well as applications and services of a target network. They provide greater misconception of an OS than low-interaction honeypots. Therefore, it is possible to log and analyze more complex attacks. These honeypots capture more useful data than low-interaction honeypots. They can only respond to preconfigured commands; therefore, the risk of intrusion increases. The main disadvantage of medium-interaction honeypots is that the attacker can quickly discover that the system behavior is abnormal. Some examples of medium-interaction honeypots include HoneyPy, Kojoney2, and Cowrie.

- **High-Interaction Honeypots**

  Unlike their low- and medium-interaction counterparts, high-interaction honeypots do not emulate anything; they run actual vulnerable services or software on production systems with real OS and applications. These honeypots simulate all services and

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

applications of a target network. They can be completely compromised by attackers to gain full access to the system in a controlled area. They capture complete information about an attack vector such as attack techniques, tools, and intent. The honeypotized system is more prone to infection, as attack attempts can be carried out on real production systems.

A honeynet is a prime example of a high-interaction honeypot. It is neither a product nor a software solution that a user installs. Instead, it is an architecture—an entire network of computers designed to attack. The idea is to have an architecture that creates a highly controlled network with real computers running real applications, in which all activities are monitored and logged.

"**Bad guys**" find, attack, and break into these systems through their own initiative. When they do, they do not realize that they are in a honeynet. Without the knowledge of the attackers, all their activities and actions, from encrypted SSH sessions to email and file uploads, are captured by inserting kernel modules into their systems.

At the same time, the honeynet controls the attacker's activity. Honeynets do this by using a honeywall gateway, which allows inbound traffic to the victim's systems but controls the outbound traffic using intrusion prevention technologies. This gives the attacker the flexibility to interact with the victim's systems but prevents the attacker from harming other non-honeynet computers.

- **Pure Honeypots**

  Pure honeypots emulate the real production network of a target organization. They cause attackers to devote their time and resources toward attacking the critical production system of the company. Attackers uncover and discover the vulnerabilities and trigger alerts that help network administrators to provide early warnings of attacks and hence reduce the risk of an intrusion.

Honeypots are classified into the following types based on their deployment strategy:

- **Production Honeypots**

  Production honeypots are deployed inside the production network of the organization along with other production servers. Although such honeypots improve the overall state of security of the organization, they effectively capture only a limited amount of information related to the adversaries. Such honeypots fall under the low-interaction honeypot category and are extensively employed by large organizations and corporations. As production honeypots are deployed internally, they also help to find out internal flaws and attackers within an organization.

- **Research Honeypots**

  Research honeypots are high-interaction honeypots primarily deployed by research institutes, governments, or military organizations to gain detailed knowledge about the actions of intruders. By using such honeypots, security analysts can obtain in-depth information about how an attack is performed, vulnerabilities are exploited, and attack techniques and methods are used by the attackers. This analysis, in turn, can help an

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

organization to improve attack prevention, detection, and security mechanisms and develop a more secure network infrastructure.

The main drawback of research honeypots is that they do not contribute to the direct security of the company. If a company is looking to improve its production infrastructure, it should opt for production honeypots.

Honeypots are classified into the following types based on their deception technology:

- **Malware Honeypots**

  Malware honeypots are used to trap malware campaigns or malware attempts over the network infrastructure. These honeypots are simulated with known vulnerabilities such as outdated APIs, vulnerable SMBv1 protocols, etc., and they also emulate different Trojans, viruses, and backdoors that encourage adversaries to perform exploitation activities. These honeypots lure the attacker or malware into performing attacks, from which the attack pattern, malware signatures, and malware threat actors can be identified effectively.

- **Database Honeypots**

  Database honeypots employ fake databases that are vulnerable to perform database-related attacks such as SQL injection and database enumeration. These fake databases trick the attackers by making them think that these databases contain crucial sensitive information such as credit card details of all the customers and employee databases. However, all the information present in the database is fake and simulated. Such databases lure the attacker to perform attacks, with their vulnerabilities; from the attacks, the attack pattern and the threat actor's TTP's towards database attacks can be identified effectively.

- **Spam Honeypots**

  Spam honeypots specifically target spammers who abuse vulnerable resources such as open mail relays and open proxies. Basically, spam honeypots consist of mail servers that deliberately accept emails from any random source from the Internet. They provide crucial information about spammers and their activities.

- **Email Honeypots**

  Email honeypots are also called email traps. They are nothing but fake email addresses that are specifically used to attract fake and malicious emails from adversaries. These fake email IDs will be distributed across the open Internet and dark web to lure threat actors into performing various malicious activities to exploit the organization. By constantly monitoring the incoming emails, the adversary's deception techniques can be identified by the administrators and internal employees can be warned to avoid falling into such email traps.

- **Spider Honeypots**

  Spider honeypots are also called spider traps. These honeypots are specifically designed to trap web crawlers and spiders. Many threat actors perform web crawling and

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

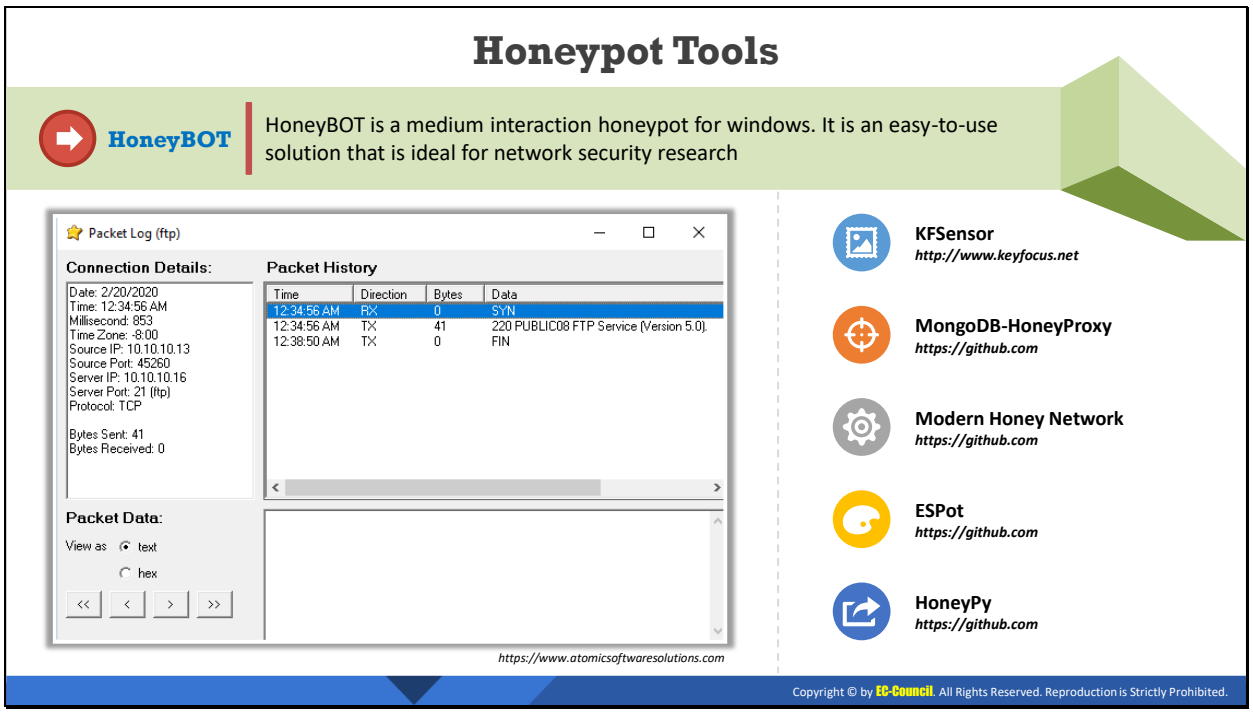
spidering to extract important information from web applications. Such crucial information includes URLs, contact details, directory details, etc. Spider honeypots are employed to trap such adversaries. A fake website will be emulated and presented as a legitimate one. Threat actors attempting to perform web crawling on such traps will be identified and blacklisted.

- **Honeynets**

  Honeynets are networks of honeypots. They are very effective in determining the entire capabilities of the adversaries. Honeynets are mostly deployed in an isolated virtual environment along with a combination of vulnerable servers. The various TTPs employed by different attackers to enumerate and exploit networks will be recorded, and this information can be very effective in determining the complete capabilities of the adversary.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Honeypot Tools

Honeypots are security tools that allow the security community to monitor attackers' tricks and exploits by logging all their activity so that it can respond to such exploits quickly before the attacker can misuse or compromise the system.

- **HoneyBOT**

  Source: *https://www.atomicsoftwaresolutions.com*

  HoneyBOT is a medium interaction honeypot for windows. A honeypot creates a safe environment to capture and interact with unsolicited traffic on a network. HoneyBOT is an easy-to-use solution that is ideal for network security research or as part of an early-warning IDS.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

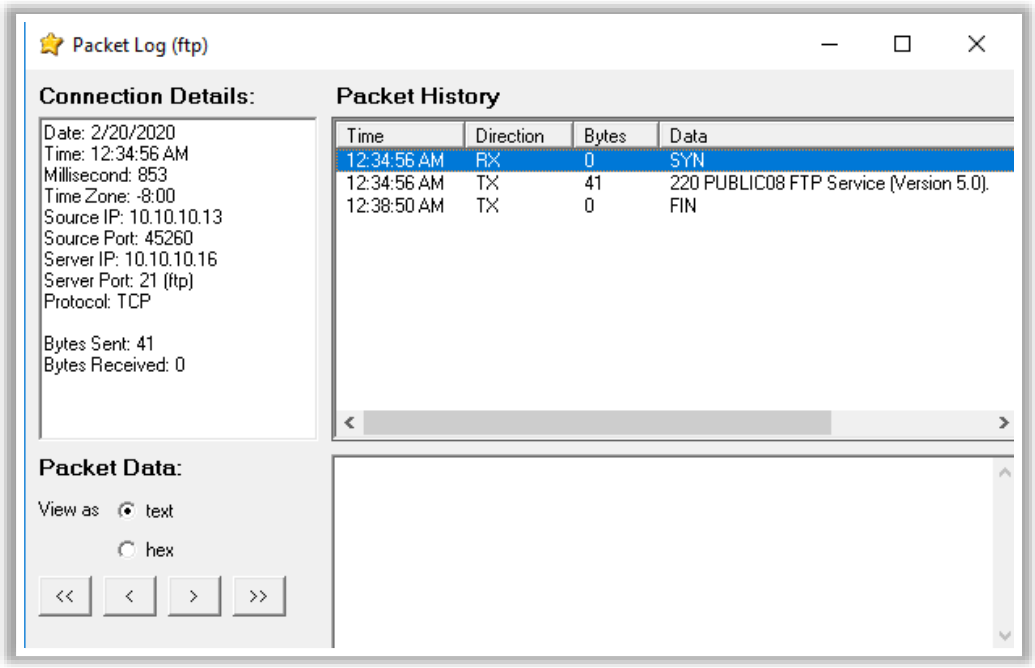
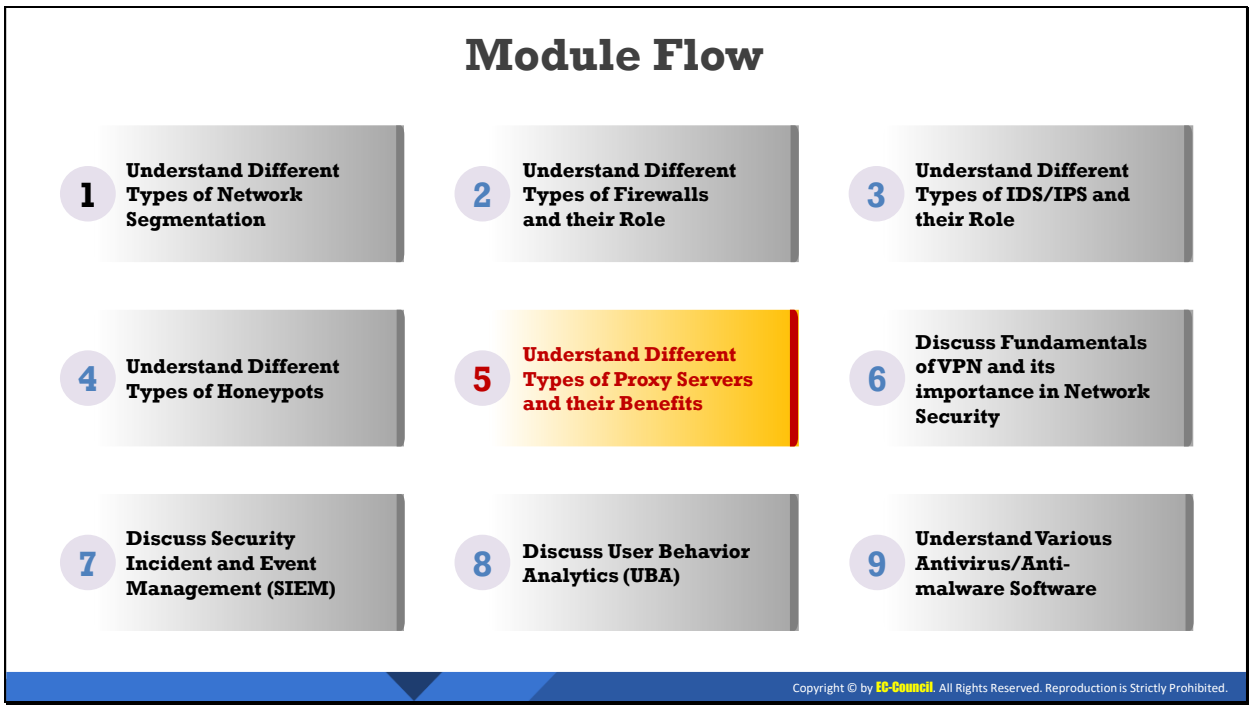


Figure 5.55: Screenshot of HoneyBOT

Some additional honeypot tools are listed below:

- KFSensor (*http://www.keyfocus.net*)
- MongoDB-HoneyProxy (*https://github.com*)
- Modern Honey Network (*https://github.com*)
- ESPot (*https://github.com*)
- HoneyPy (*https://github.com*)

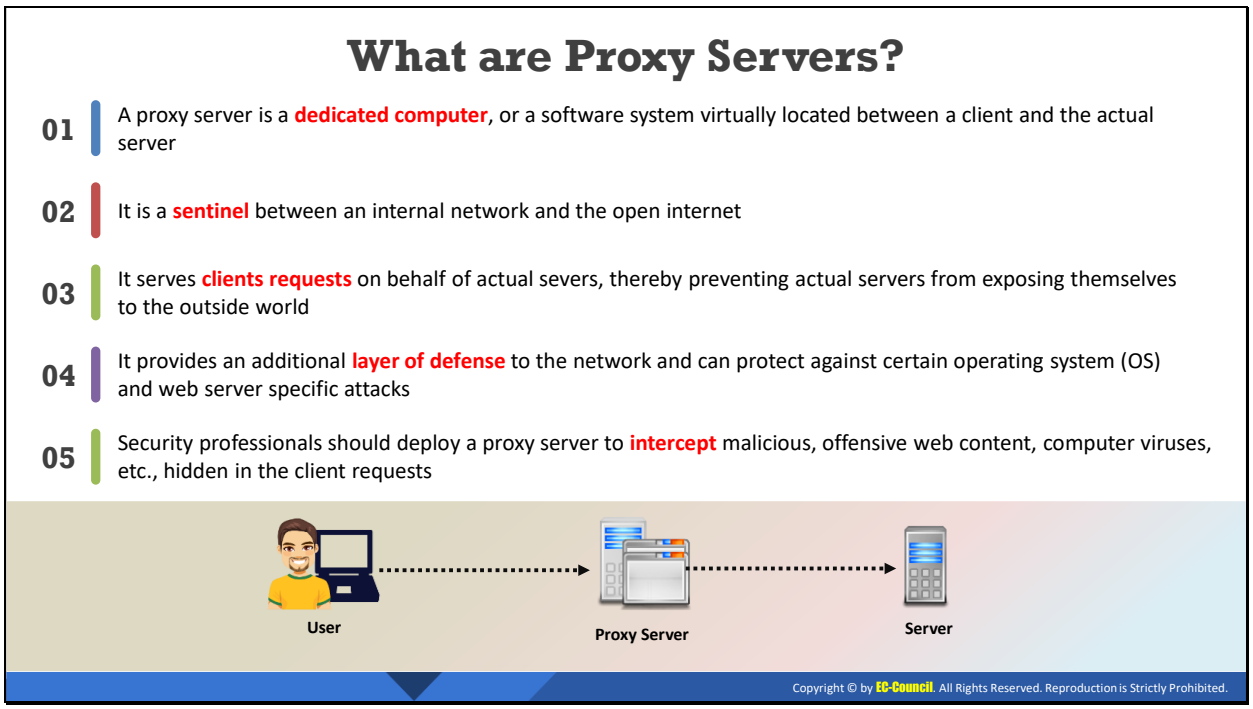
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Understand Different Types of Proxy Servers and their Benefits

Proxy servers play an important role in securing the servers connected to the Internet. They provide an additional layer of the security to the servers and reduce the probability of an attack on the servers. This section discusses proxy servers, their benefits, and types of proxy servers.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



What are Proxy Servers?

A proxy server is an application that can serve as an intermediary when connecting with other computers. Security professionals should deploy a proxy server to intercept malicious, offensive web content, computer viruses, etc., hidden in the client requests.

A proxy server is used:

- As a firewall and to protect the local network from outside attacks.
- To anonymously surf the web (to some extent).
- To filter out unwanted content such as ads or "unsuitable" material (using specialized proxy servers).
- To provide some protection against hacking attacks.

How do proxy servers work?

When a user uses a proxy for requesting a particular web page on an actual server, the proxy server receives it. It then sends this request to the actual server on behalf of the user's request—it mediates between the user and the actual server to send and respond to the request.

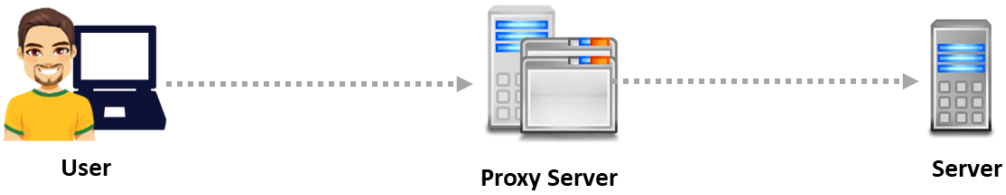


Figure 5.56: Working of Proxy

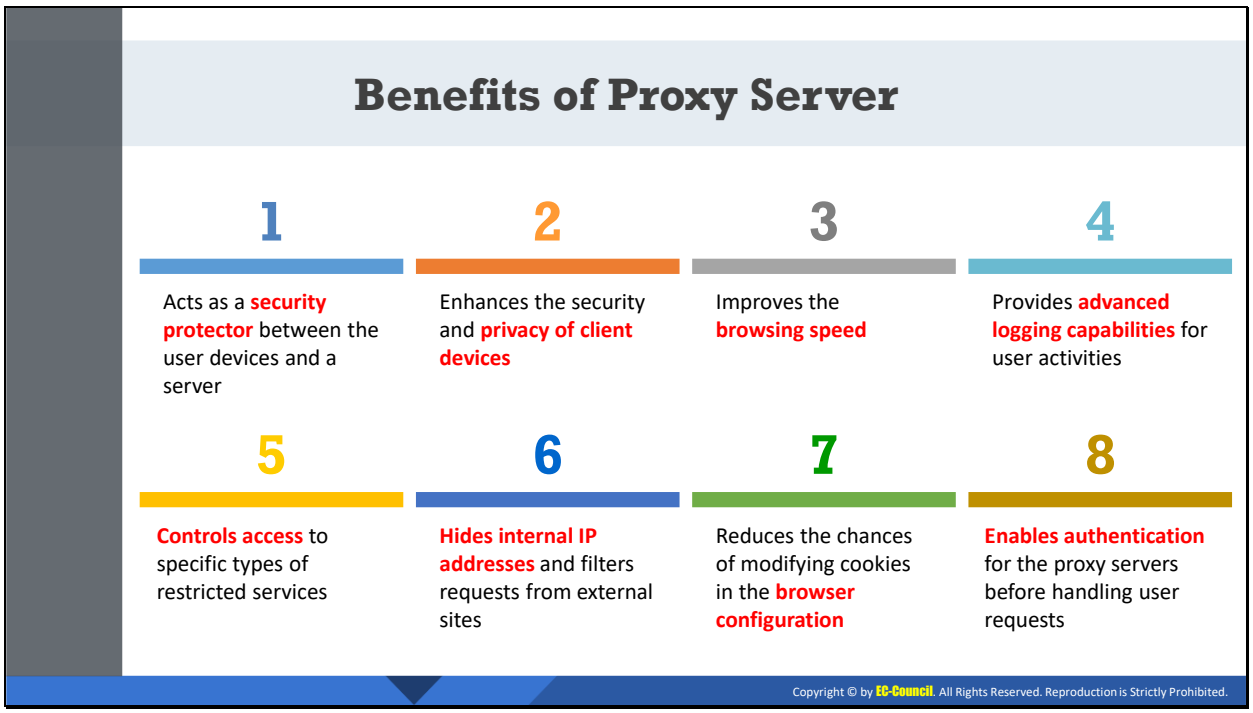
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

A proxy server improves security, administrative control, and caching services. It is also used for evaluating the network traffic and maintaining user confidentiality.

Proxy servers in an organization help in maintaining security and administrative controls. However, attackers use proxy servers to hide their presence on the internet.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

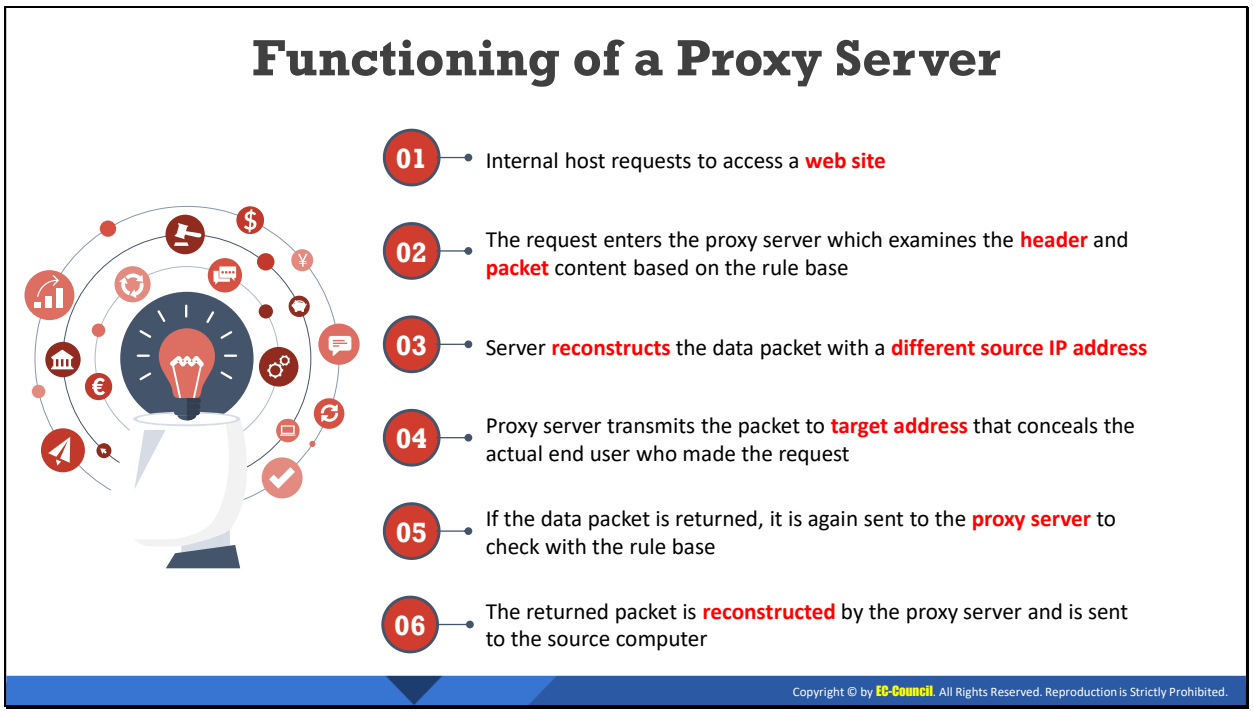


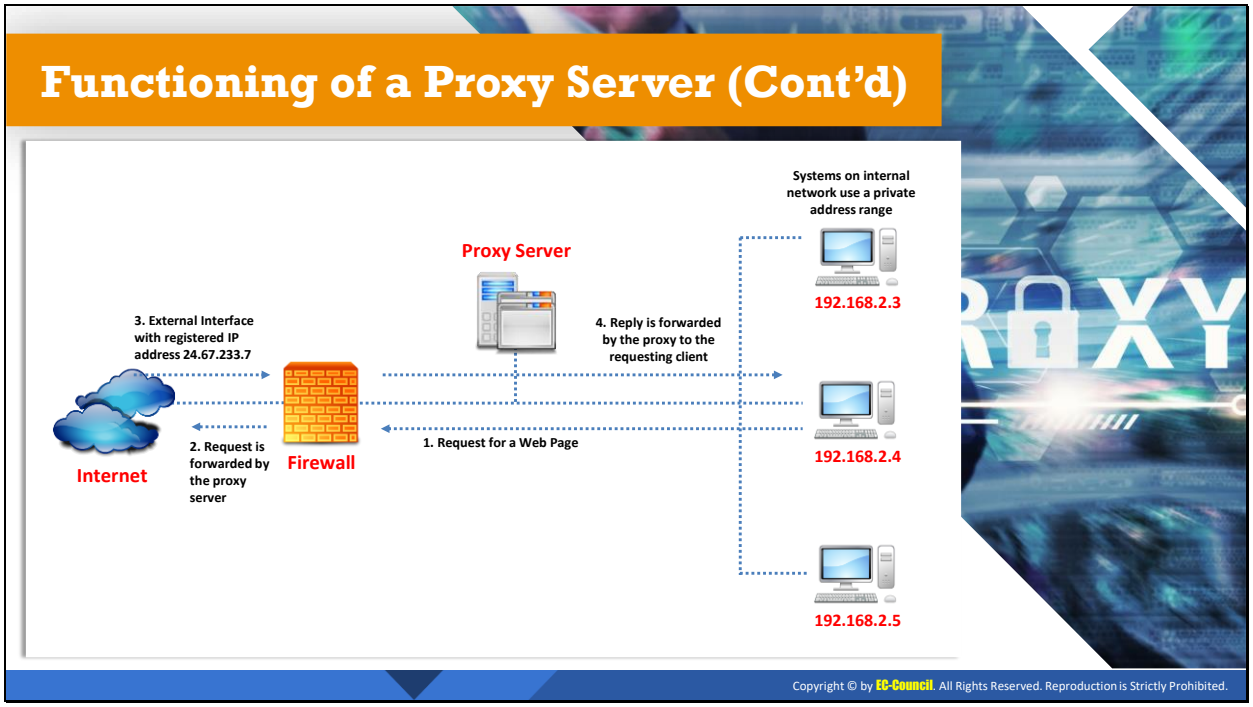
Benefits of Proxy Server

The following are the benefits of using a proxy server while accessing a network:

- It acts as a security protector between the user devices and a server.
- It enhances the security and privacy of client devices.
- It improves the browsing speed.
- It provides advanced logging capabilities for user activities.
- It is used for controlling the access to specific types of restricted services.
- It helps the organization to hide its internal IP address.
- It reduces the chances of modifying cookies in the browser configuration and protects from any kind of malware.
- It filters requests from external sites.
- It improves the delivery of the requested web pages to the users.
- It enables authentication for the proxy servers before handling user requests and services.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets





Functioning of a Proxy Server

- The client first requests a web page and recognizes the server that contains the web page.
- The request for the web page is passed on to the proxy server, which checks the packet with its set of conventions for this service and decides whether the request is to be granted.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- Once the proxy has made the decision to allow the request, a new packet is created with the source IP address of the proxy server.
- This new packet is the request for the web page from the proxy server. The web server receives the request and returns the web page to the requesting host.
- When the proxy receives the web page, it verifies its rules to determine whether this page is to be allowed.
- Once the decision is made to proceed, the proxy creates a new packet with the web page as the payload and sends it to the original client.
- This type of service significantly increases the security of the network, as no packets can travel directly from the client to the server.

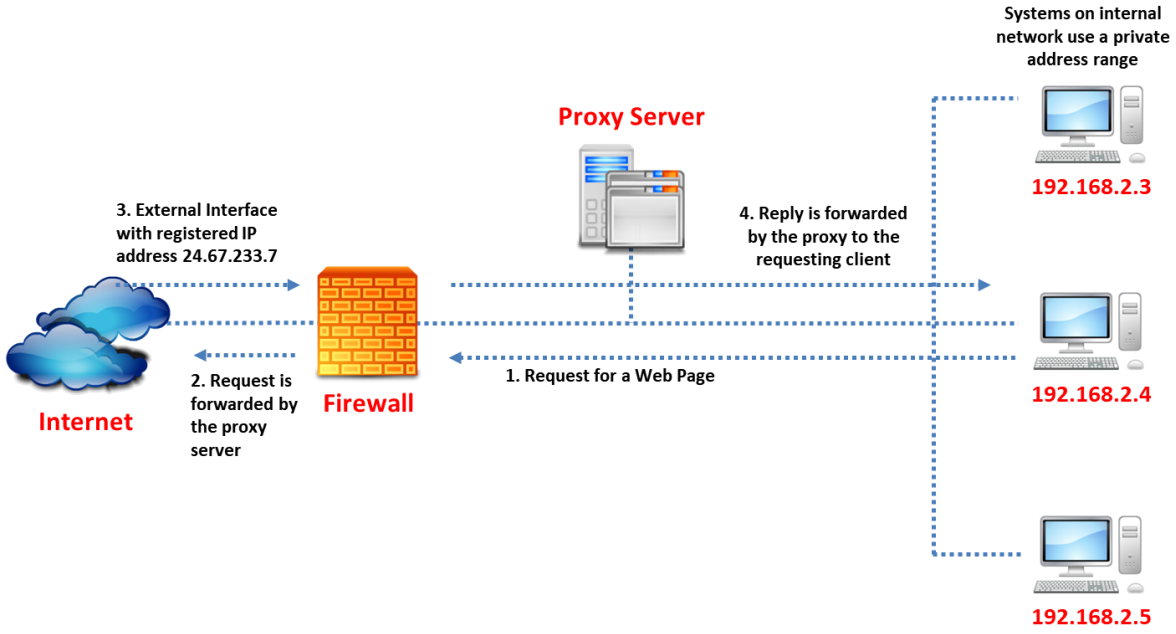
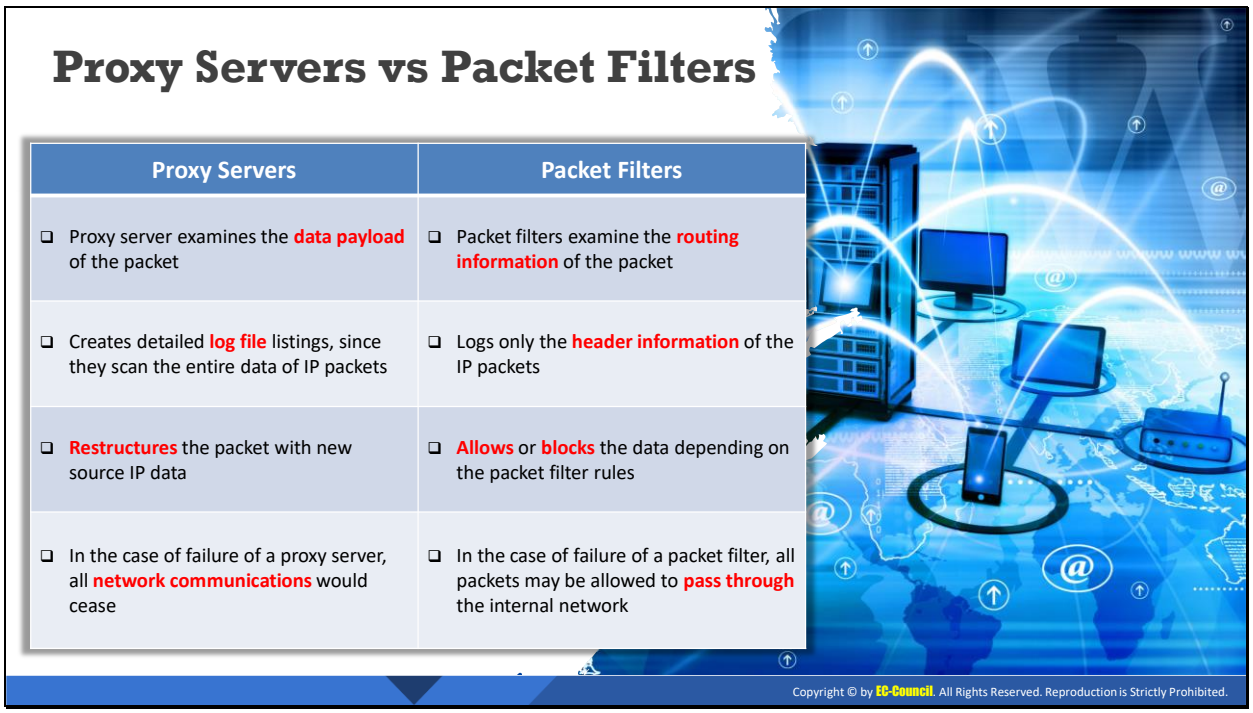


Figure 5.57: Functioning of a Proxy Server

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Proxy Servers vs Packet Filters

Proxy servers and packet filters are used together in a firewall and work in the application layer of the OSI model. They mainly differ in terms of the inspection of different parts of IP packets and the way they act on them.

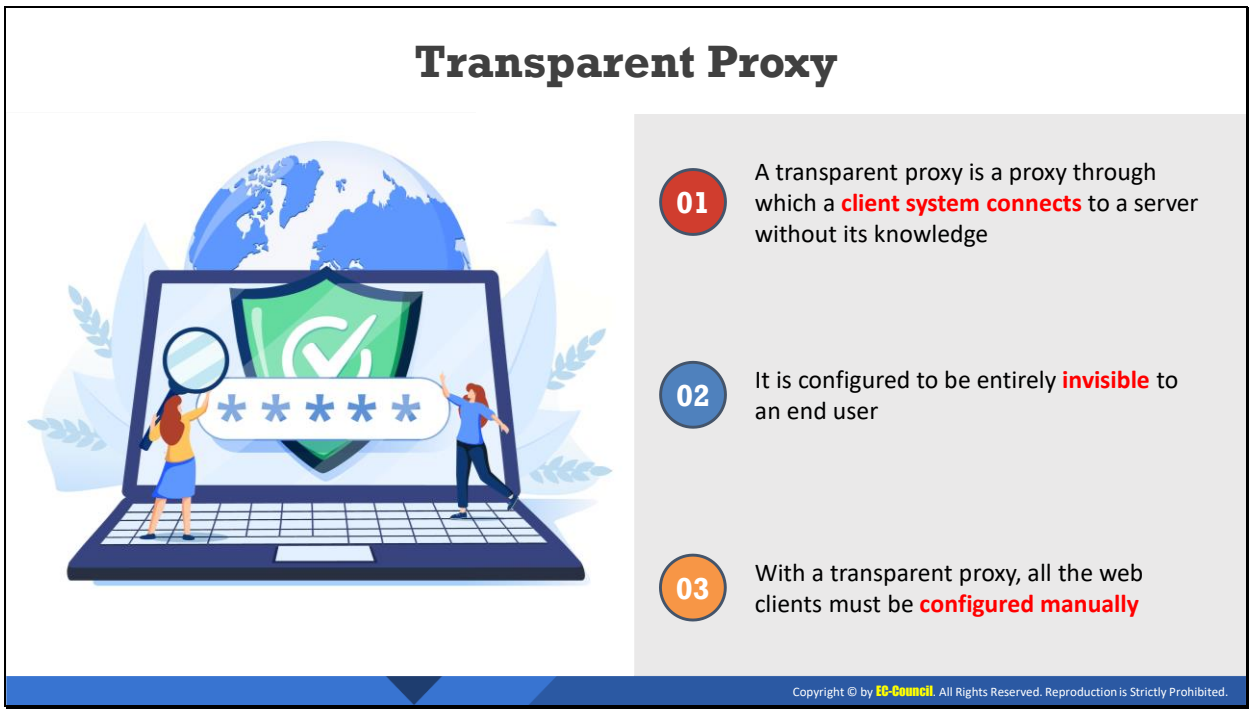
- A proxy server creates detailed log file listings because they scan the entire data part of the IP packets, whereas a packet filter logs only header information of the IP packets.
- A packet filter simply allows the data packet to pass through to the destination if it matches the packet filter rules. On the other hand, a proxy server restructures the packet with new source IP data.
- In the case of failure of a proxy server, all network communications would cease, whereas in the case of packet filter failure, all packets may be allowed to pass through to the internal network.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Types of Proxy Servers

Discussed below are various types of proxy servers.

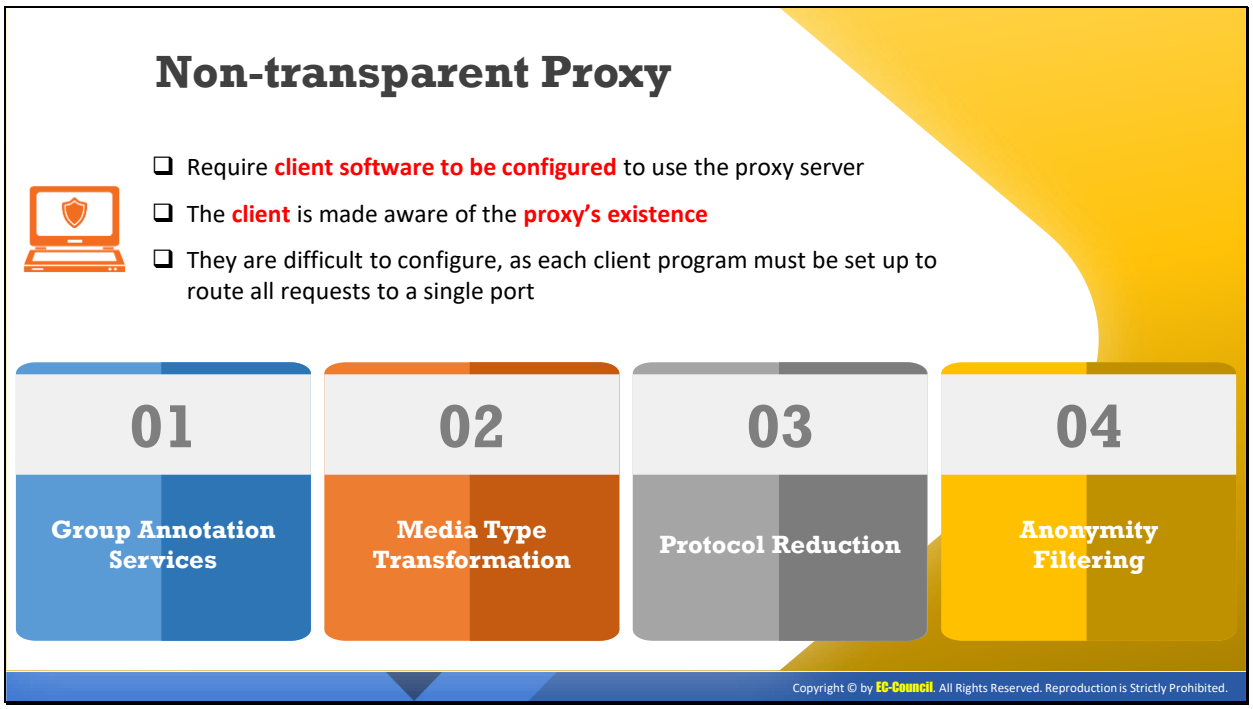
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Transparent Proxy

A transparent proxy is a proxy through which a client system connects to a server without its knowledge. It is configured to be entirely invisible to an end user. It is placed between two networks, similar to a router. A firewall tracks the outgoing traffic and directs it to a specific computer, such as a proxy server. Network administrators need not configure the client's software with transparent proxies. With a transparent proxy, all the web clients must be configured manually.

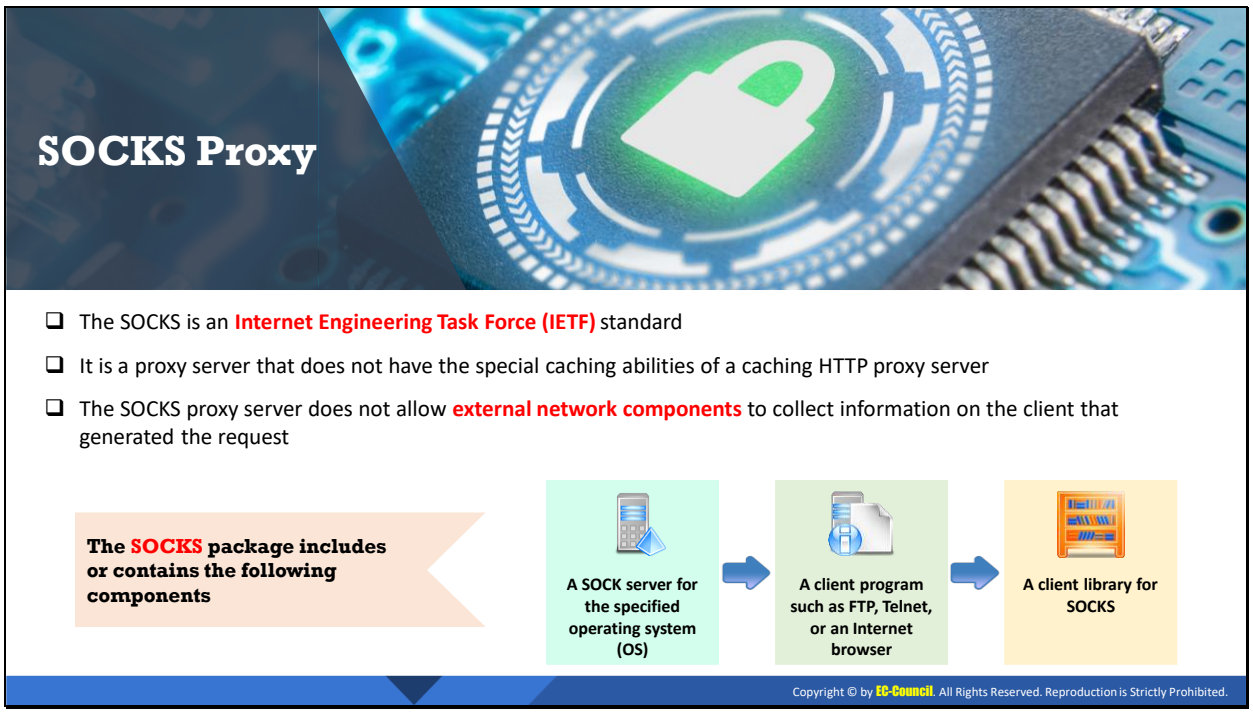
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Non-transparent Proxy

Non-transparent proxies are also known as explicit proxies and require client software to be configured to use the proxy server. Non-transparent proxies are difficult to configure, as each client program must be set up to route all requests to a single port. However, these proxies provide a greater level of security than other types. A non-transparent proxy is one that modifies a request or response, and the client is made aware of the proxy's existence. The entire requested URL is sent to the proxy that has the host name. It provides added services to the user agent such as group annotation services, media-type transformation, protocol reduction, and anonymity filtering.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



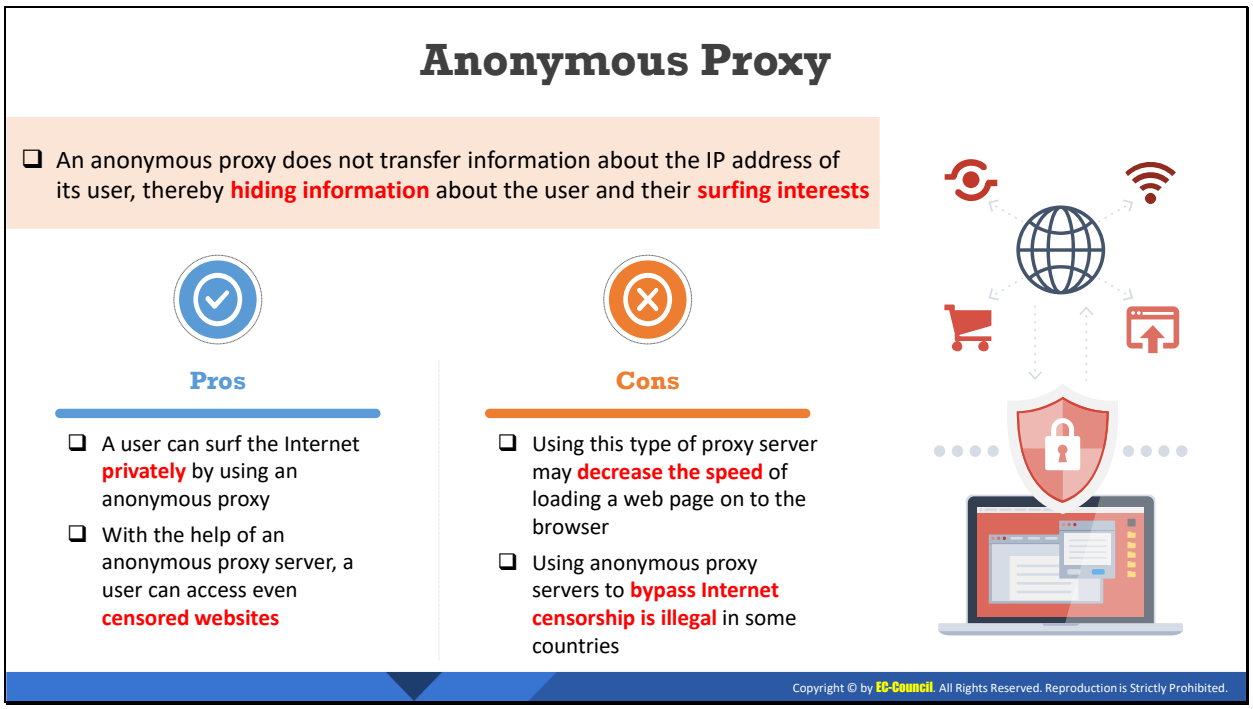
SOCKS Proxy

SOCKS, an Internet Engineering Task Force (IETF) standard, is a proxy server that does not have the special caching abilities of a caching HTTP proxy server. The SOCKS protocol internally uses "sockets," which help track all the individual connections of clients. The function of a SOCKS server is to handle all clients' requests inside the organization's firewall; based on the requested Internet destination or user identification, it allows or rejects connection requests. If the requested connection is valid, then it "binds" the request, and information is exchanged with the usual protocol (e.g., HTTP). The SOCKS proxy server does not allow external network components to collect information on the client that generated the request.

The SOCKS package contains the following components:

- A SOCK server for the specified operating system (OS)
- A client program such as FTP, Telnet, or an Internet browser
- A client library for SOCKS

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Anonymous Proxy

An anonymous proxy does not transfer information about the IP address of its user, thereby hiding information about the user and their surfing interests. A user can surf the Internet privately by using an anonymous proxy. With the help of an anonymous proxy server, a user can access even censored websites. The use of this type of proxy server may decrease the speed of loading a web page on to the browser. Further, the use of anonymous proxy servers to bypass Internet censorship is illegal in some countries.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Reverse Proxy

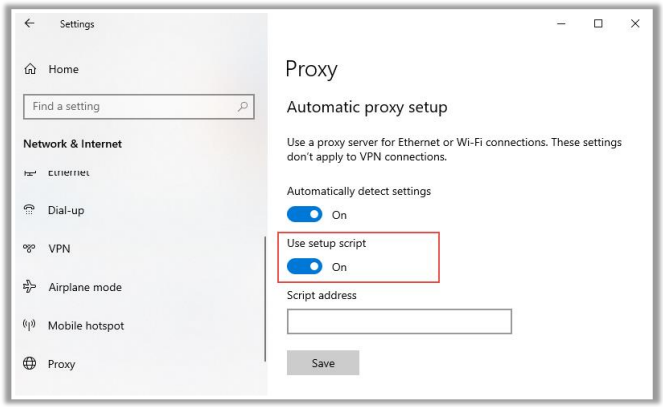
A reverse proxy is usually situated closer to the server(s) and will only return a configured set of resources. It can optimize content by compressing it to speed up loading. The client is unaware of the presence of a reverse proxy. A reverse proxy server is an intermediate server that is located between a client and the actual web server.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

How to Configure Proxy Server

Configuring Automatic Proxy Setup in Windows 10

Step 1	Open Windows Settings by pressing the **Windows key** and **I** together
Step 2	Click **Network & Internet → Proxy**
Step 3	Check if the "**Automatically detect settings**" toggle button is **On**
Step 4	Windows runs an automatic check by default
Step 5	If Windows detects PAC file, set the "**Use Setup Script**" toggle button to **On**
Step 6	Type **proxy.certifiedhacker.com** in the "**Script Address**" field
Step 7	Click **Save** to implement the changes and use the Internet through the proxy

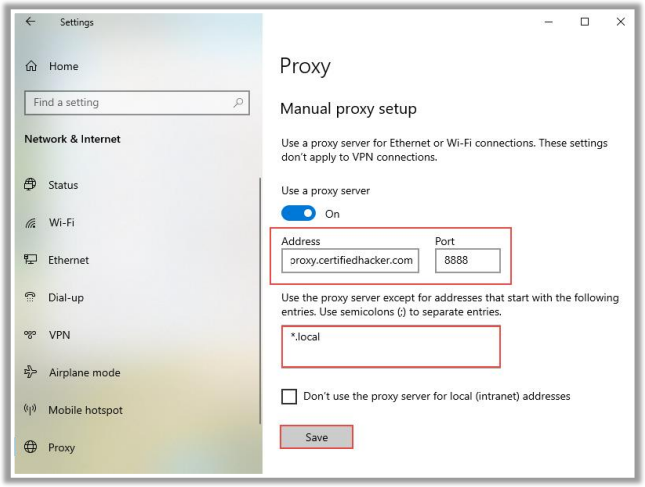


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

How to Configure Proxy Server (Cont'd)

Step 1	Open the Windows settings menu by pressing the **Windows key** and **I** together
Step 2	Click **Network & Internet → Proxy**
Step 3	Automatic proxy setup window opens. Scroll down to "**Manual proxy setup**" and set the "**Use a Proxy Server**" toggle button to **On**
Step 4	Type **proxy.certifiedhacker.com** in the address field and **8888** in the port field
Step 5	Type ***.local** in the field below the address and port fields to exempt the use of a proxy server
Step 6	Click **Save** to implement the changes and use the proxy in Windows 10

Configuring Manual Proxy Setup in Windows 10



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

How to Configure Proxy Server (Cont'd)

Configuring Proxy Setup in Google Chrome

Step 1

Open the Google Chrome browser and select "**Settings**" in the toolbar

Step 2

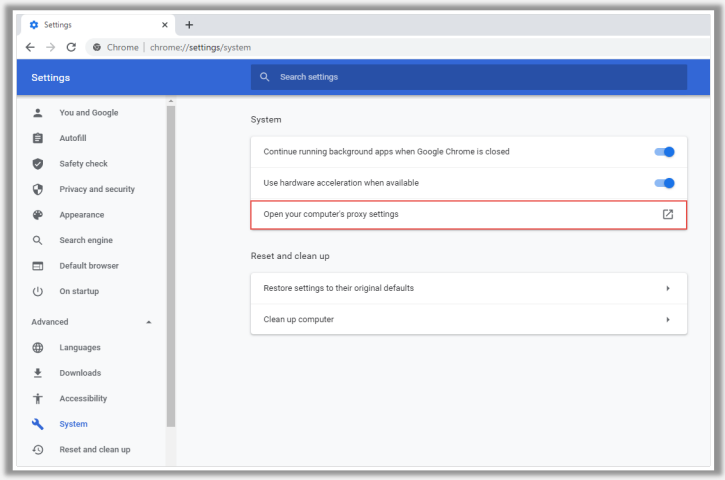
Scroll down on the page and Click **Advanced → System**

Step 3

The **System** window opens. Click "**Open your computer's proxy settings**"

Step 4

The proxy server settings window opens. Follow the instructions to configure the proxy



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

How to Configure Proxy Server (Cont'd)

Configuring Proxy Setup in Microsoft Edge

Step 1

Open the Microsoft Edge browser and click "**Settings**" from the menu displayed on the top-right corner

Step 2

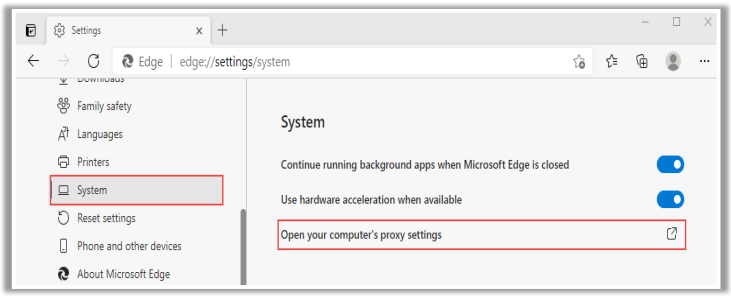
Scroll down on the page and click "**System**"

Step 3

The **System** window opens. Click "**Open your computer's proxy settings**"

Step 4

The proxy server setup window opens. Follow the instructions to configure the proxy server



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

How to Configure Proxy Server

A proxy server acts as a gateway between a user and the Internet and can perform many functions such as virus scanning, secure communication, and fast data transmission; further, it maintains the privacy of online identity.

The following are the different ways to set up a proxy server in Windows 10, Google Chrome, and Microsoft Edge.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

Configuring Automatic Proxy Setup in Windows 10

- **Step 1**: Open Windows Settings by pressing the Windows key and I together.

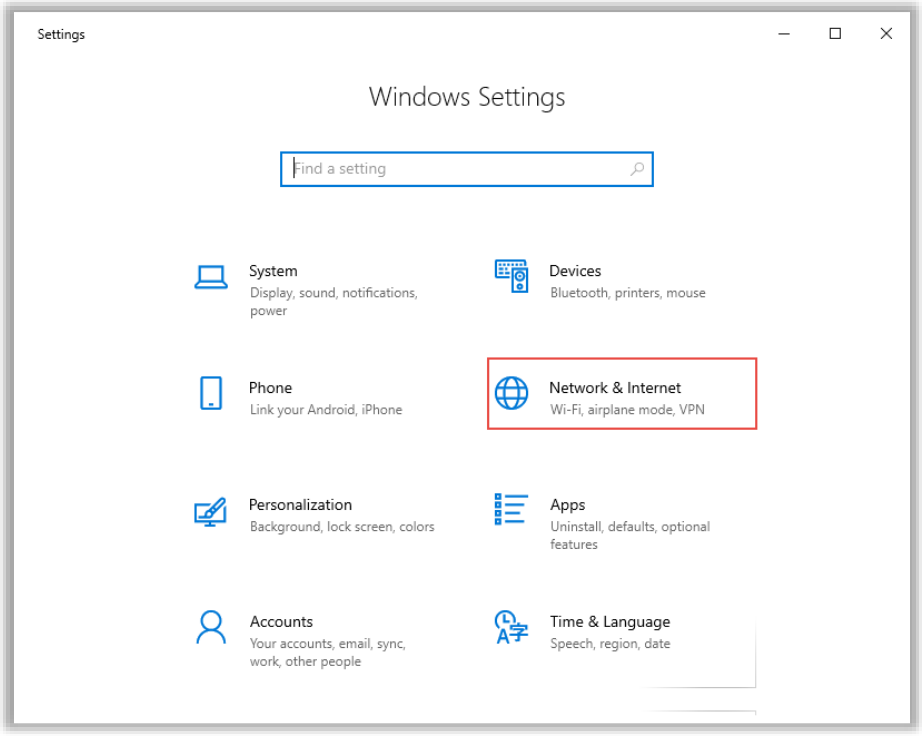


Figure 5.58: Screenshot showing Windows Settings in Windows 10

- **Step 2**: The Windows Settings box appears. Click **Network & Internet → Proxy**.

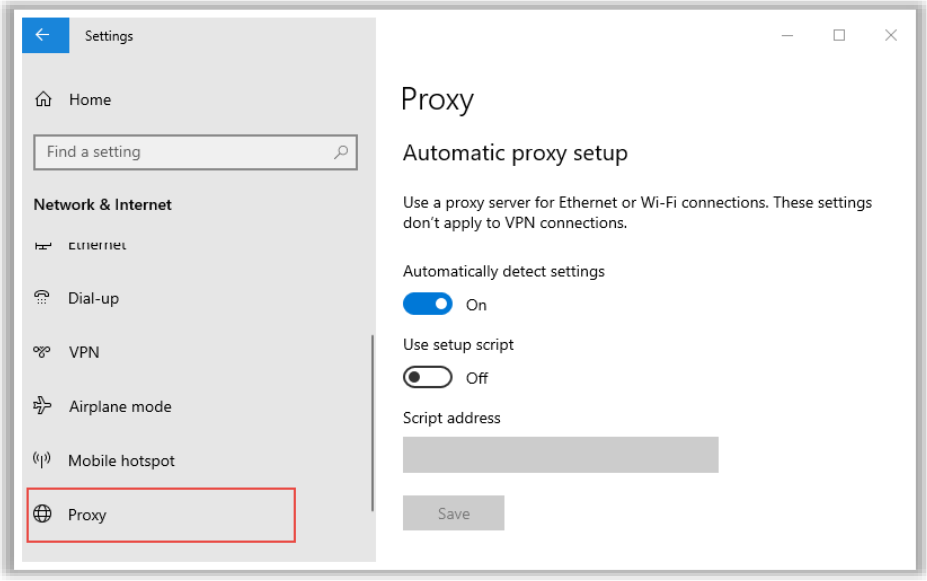


Figure 5.59: Screenshot displaying proxy settings in Windows 10

- **Step 3**: An automatic proxy setup window opens. Ensure that the "**Automatically detect settings**" toggle button is **On**.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **Step 4**: Windows runs an automatic check by default to check whether an automatic proxy server setup has been implemented previously on the network and provides the name and instructions to follow.
- **Step 5**: If Windows detects the Proxy Auto-Configuration (PAC) file, set the "**Use Setup Script**" toggle button to **On**.

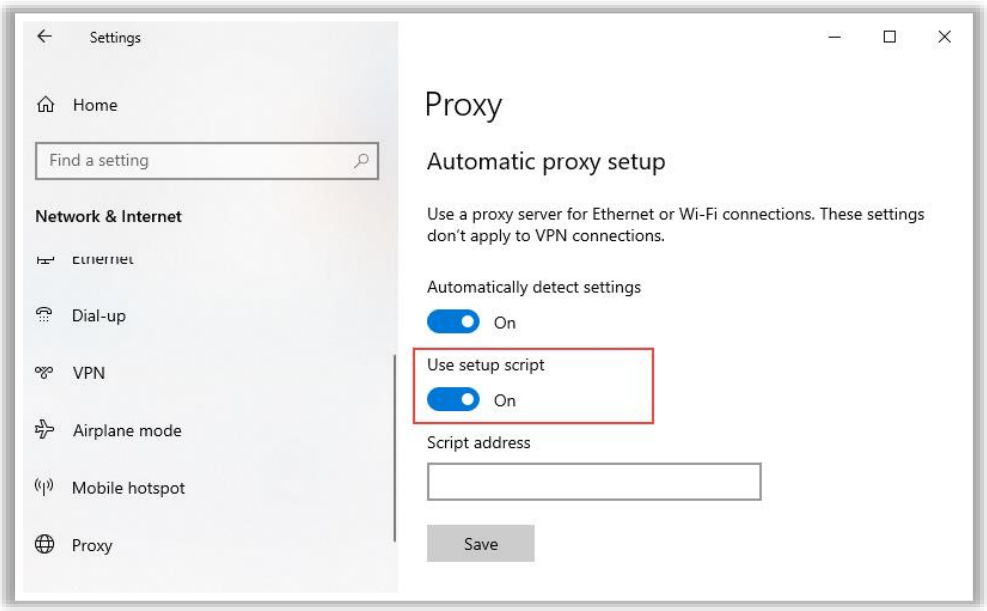


Figure 5.60: Screenshot displaying automatic proxy setup in Windows 10

- **Step 6**: Type **proxy.certifiedhacker.com** in the "**Script Address**" field.
- **Step 7**: Click **Save** to implement the changes and use the Internet through the proxy.

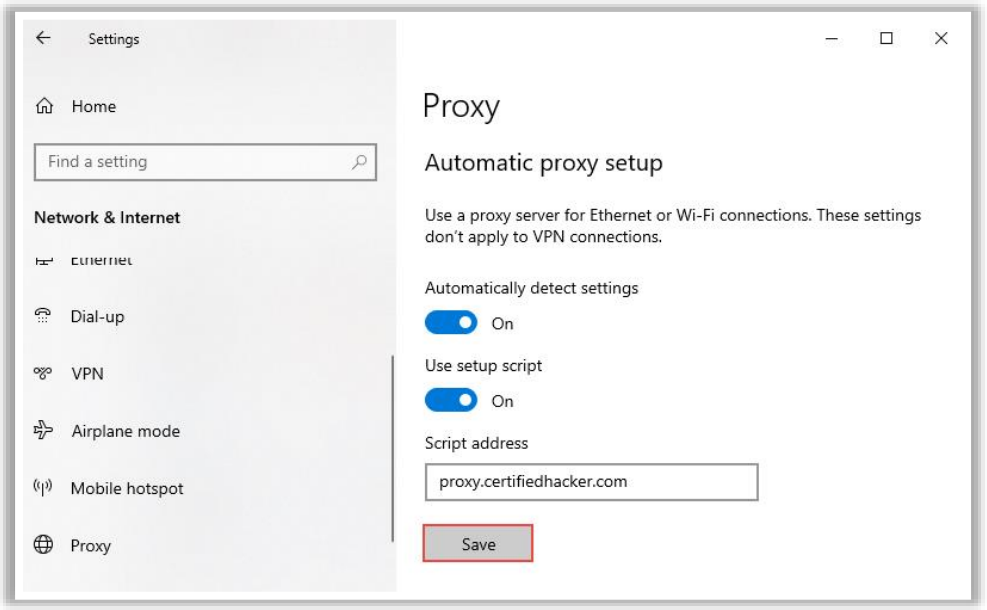


Figure 5.61: Screenshot showing the configuration of automatic proxy setup

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Configuring Manual Proxy Setup in Windows 10

- **Step 1**: Open Windows Settings by pressing the **Windows key** and **I** together.
- **Step 2**: The Windows Settings box appears. Click **Network & Internet → Proxy**.

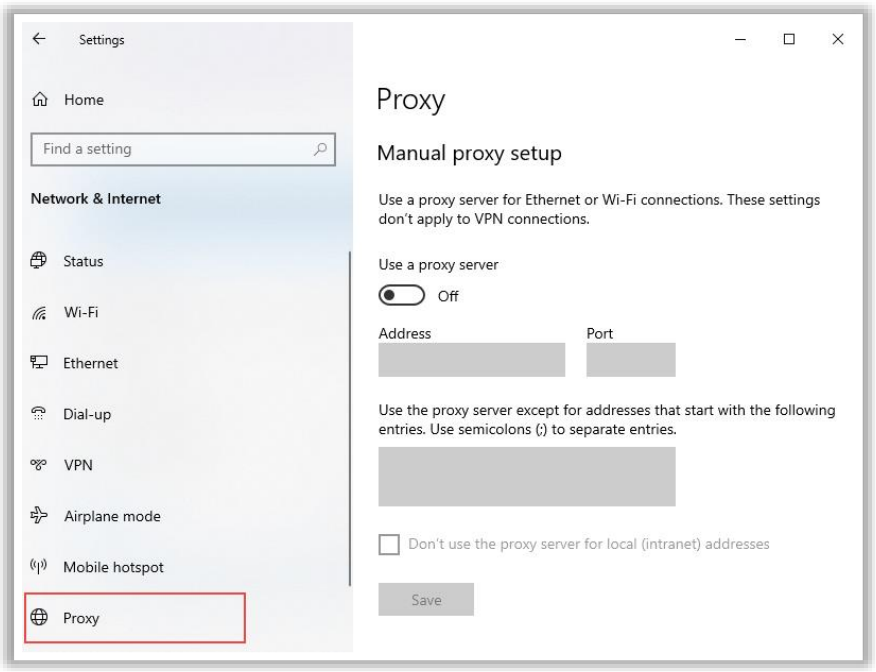


Figure 5.62: Screenshot showing manual proxy setup

- **Step 3**: Automatic proxy setup window opens. Scroll down to "**Manual proxy setup**" and set the "**Use a Proxy Server**" toggle button to **On**.

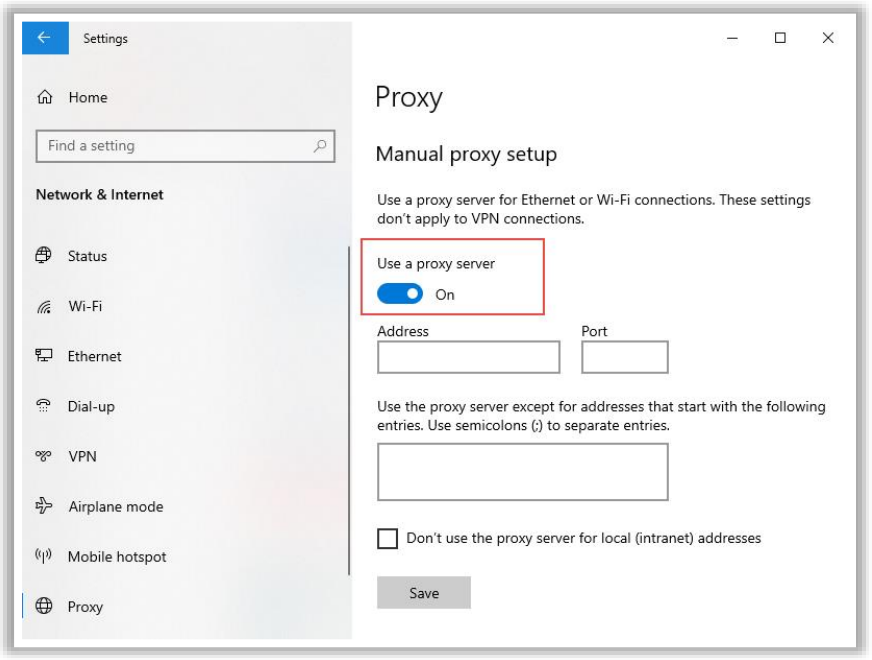


Figure 5.63: Screenshot showing the configuration of manual proxy setup

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **Step 4**: Type **proxy.certifiedhacker.com** in the address field and **8888** in the port field.

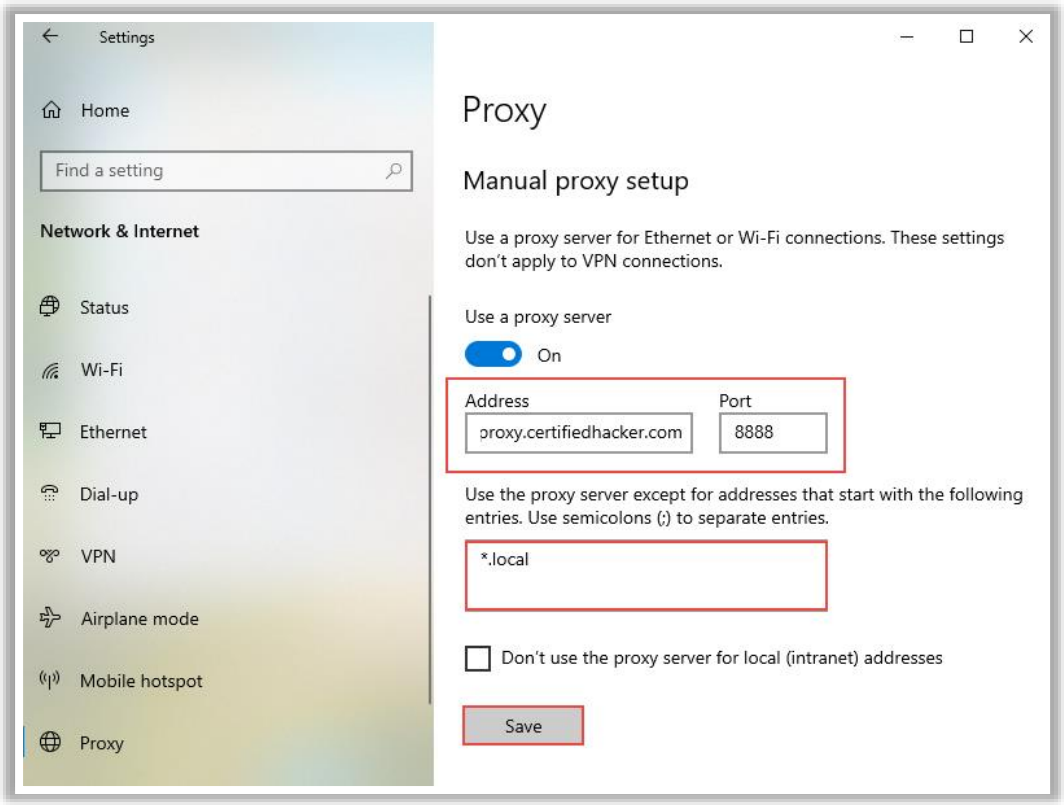


Figure 5.64: Screenshot showing the text to be entered in the address and port field for configuring manual proxy setup

- **Step 5**: Type ***.local** in the field below the address and port fields to exempt the use of a proxy server.
- **Step 6**: Click **Save** to implement the changes and use the proxy in Windows 10.

Configuring Proxy Setup in Google Chrome

- **Step 1**: Open the Google Chrome browser and select **Settings** in the toolbar.
- **Step 2**: Scroll down on the page and Click **Advanced → System**.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

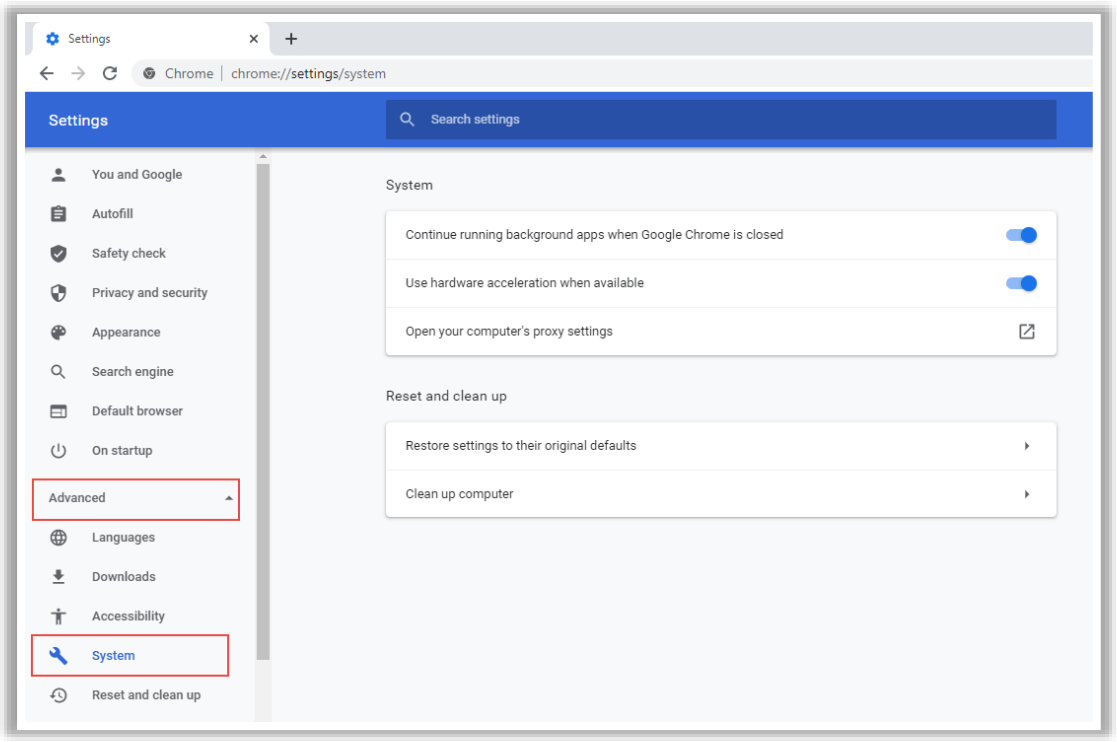


Figure 5.65: Screenshot displaying proxy setup in Google Chrome

- **Step 3**: The **System** window opens. Click "**Open your computer's proxy settings**."

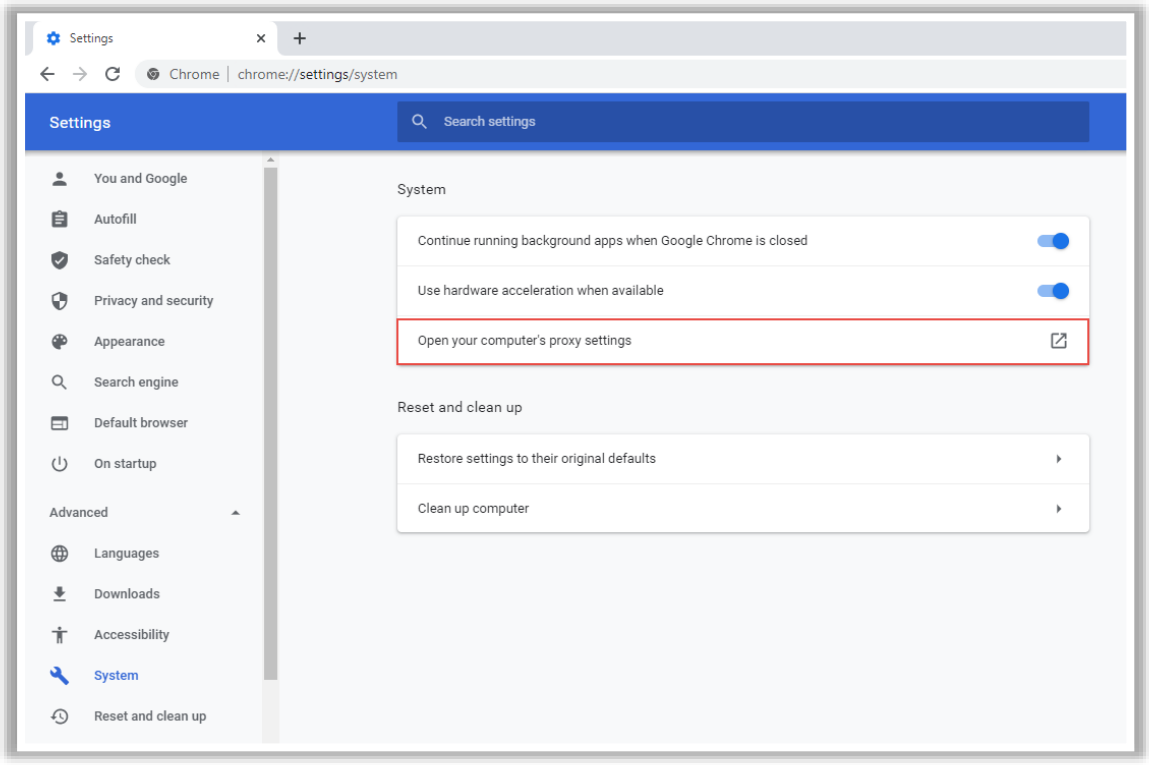


Figure 5.66: Screenshot displaying the option to open the computer's proxy settings in Google Chrome

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **Step 4**: The proxy server settings window opens. Follow the instructions to configure the proxy.

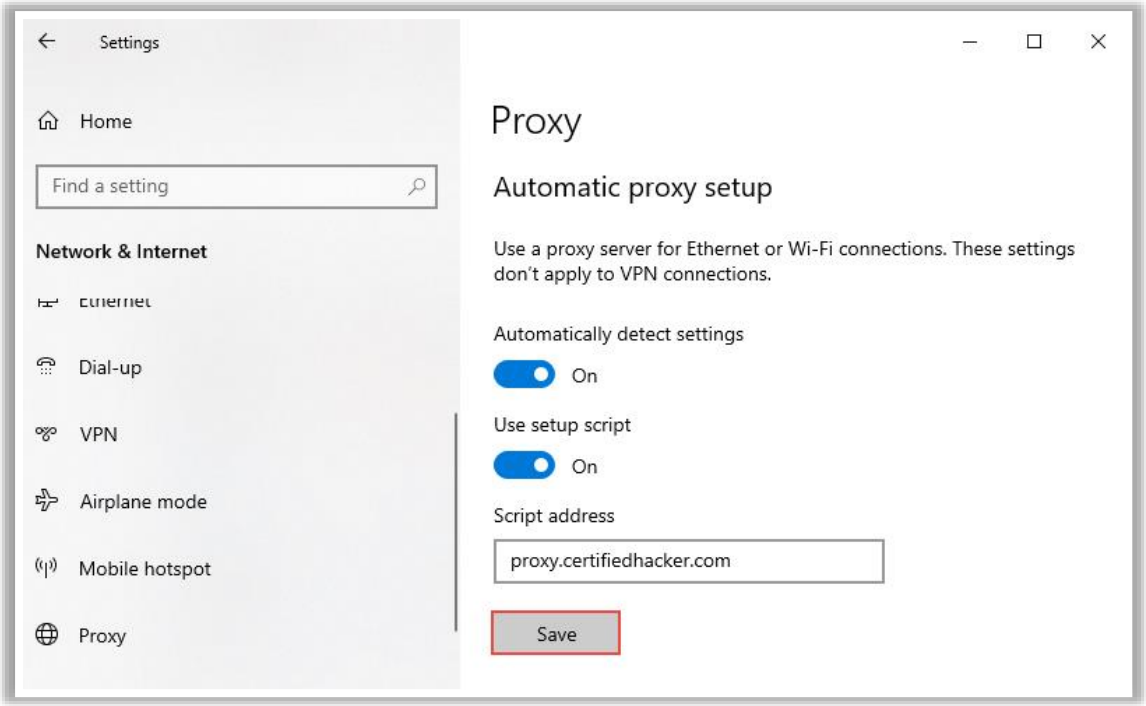


Figure 5.67: Screenshot displaying proxy setup in Windows opened through Google Chrome

Configuring Proxy Setup in Microsoft Edge

- **Step 1**: Open the Microsoft Edge browser and click **Settings** from the menu displayed on the top-right corner.
- **Step 2**: Scroll down on the page and click **System**.
- **Step 3**: The **System** window opens. Click "**Open your computer's proxy settings**."

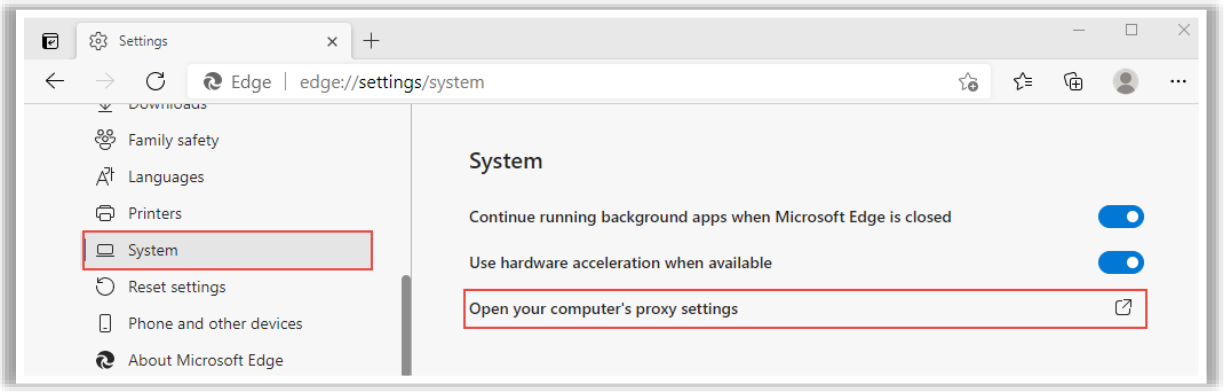


Figure 5.68: Screenshot displaying proxy setup in Microsoft Edge

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **Step 4**: The proxy server setup window opens. Follow the instructions to configure the proxy server either automatically or manually.

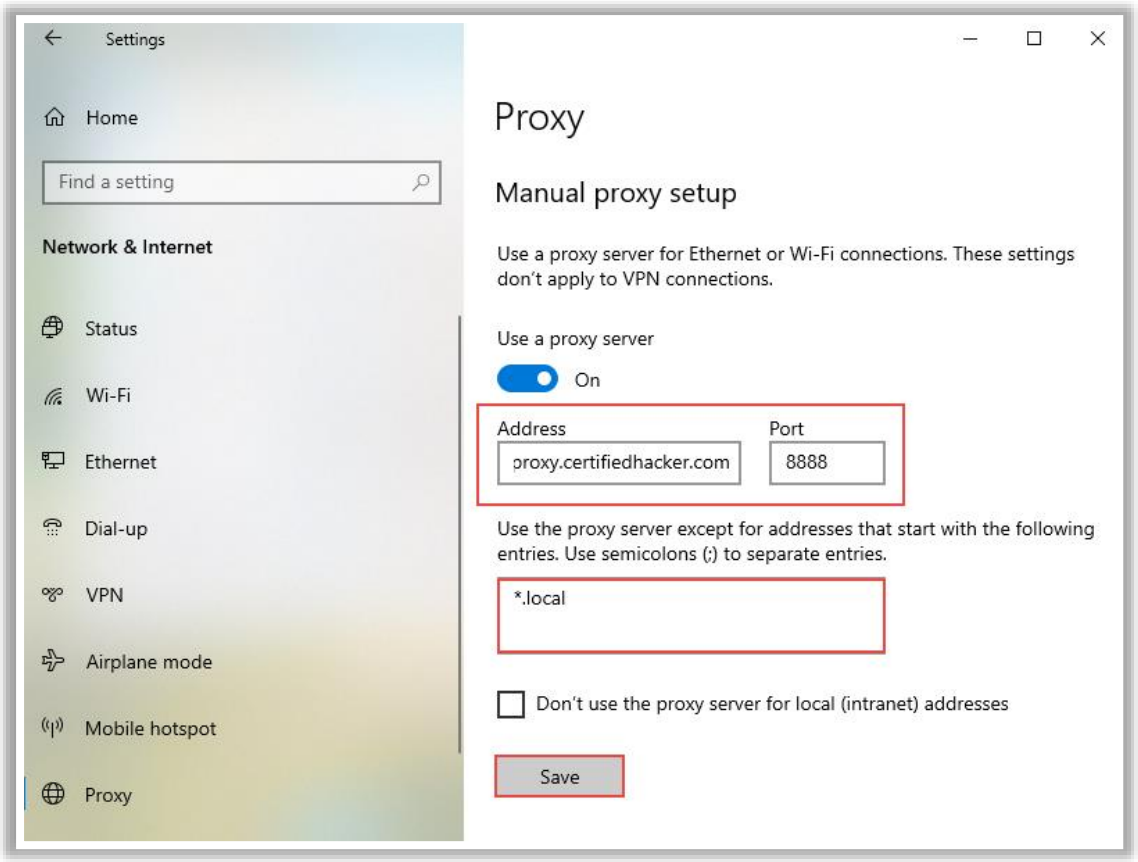
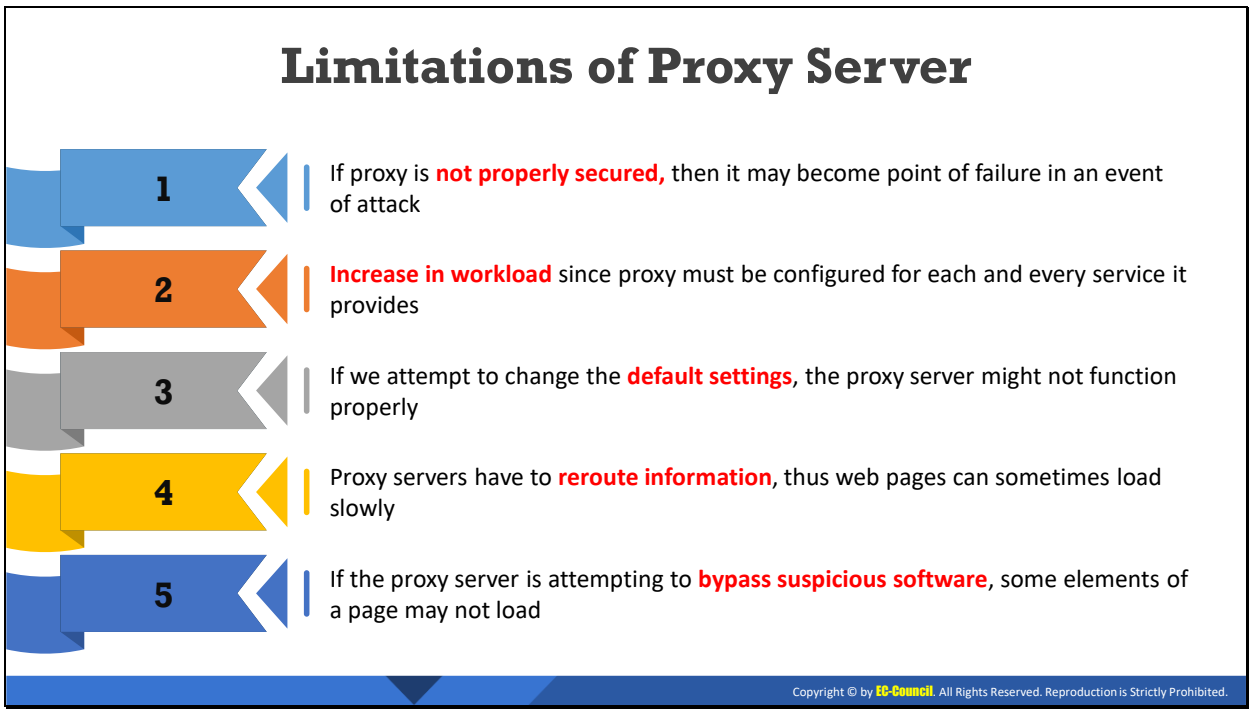


Figure 5.69: Screenshot displaying proxy setup in Windows opened through Microsoft Edge

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Limitations of Proxy Server

The following are some of the limitations of proxy servers.

- **Single Point of Failure**

  An issue with a proxy server is the creation of a single point of failure. If the entire organization uses the same proxy, that machine is quite critical and should be configured properly. A common mistake is forgetting that a proxy is insecure. Although a proxy server protects the internal network, any interface directly connected to the Internet is wide open to attack. Organizations should ensure that the proxy is used in conjunction with other security mechanisms, such as a packet filter, to decrease the possibility of a direct intrusion attack on the proxy.

- **A Proxy for Each Service**

  The proxy must be configured for each service. A network that allows numerous types of services in both directions can create considerable work. For supplementary services, it is important that the proxy server remains securely configured. The workload is high because the proxy must be configured for each and every service it provides.

- **Default Configurations**

  When implementing a proxy, it is recommended to avoid the use of the default configurations. Take time to follow the rules and restrictions. If some default settings are changed, the proxy server might not function properly.

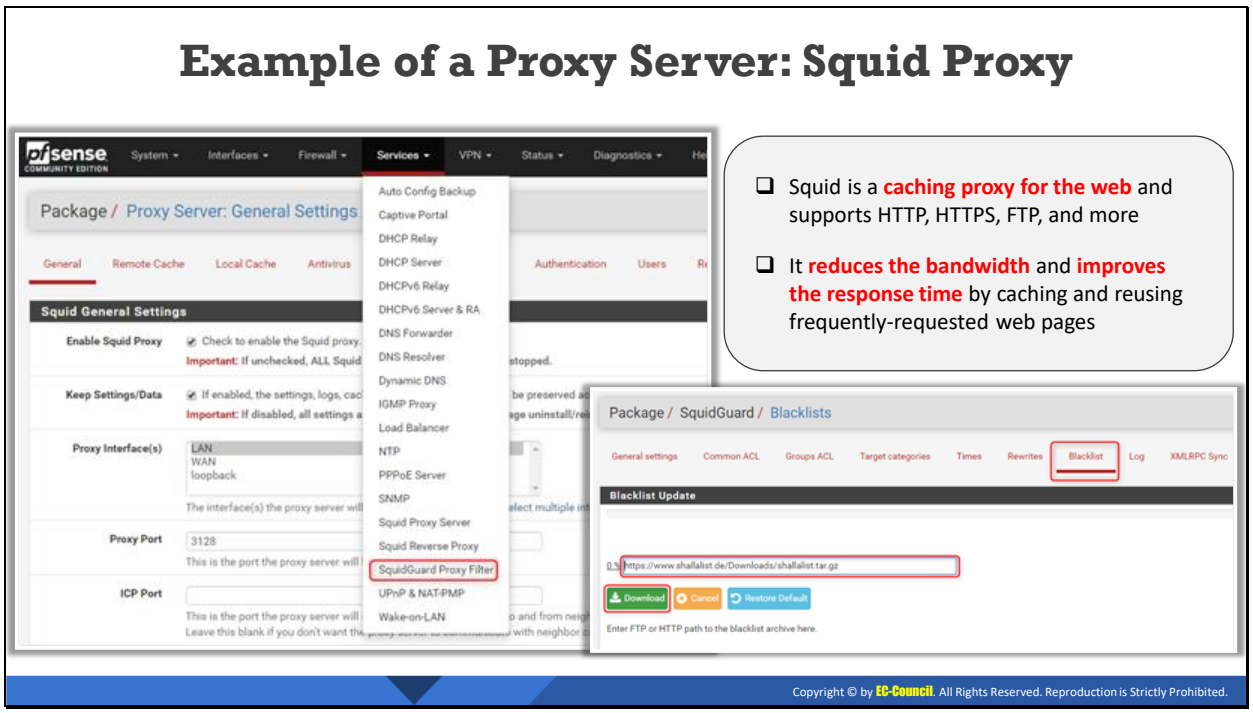
- Proxy servers have to reroute information; thus, web pages can occasionally load slowly.
- If the proxy server is attempting to bypass suspicious software, some elements of a page may not load.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- As personal information is passed through an external server that could be accessed by intruders, data security can be compromised.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Example of a Proxy Server: Squid Proxy

Source: *http://www.squid-cache.org*

Squid is a caching proxy for the web and supports HTTP, HTTPS, FTP, and more. It reduces the bandwidth and improves the response times by caching and reusing frequently-requested web pages. Squid has extensive access controls and is a great server accelerator. It runs on most available operating systems, including Windows and is licensed under the GNU general public license (GNU GPL).

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

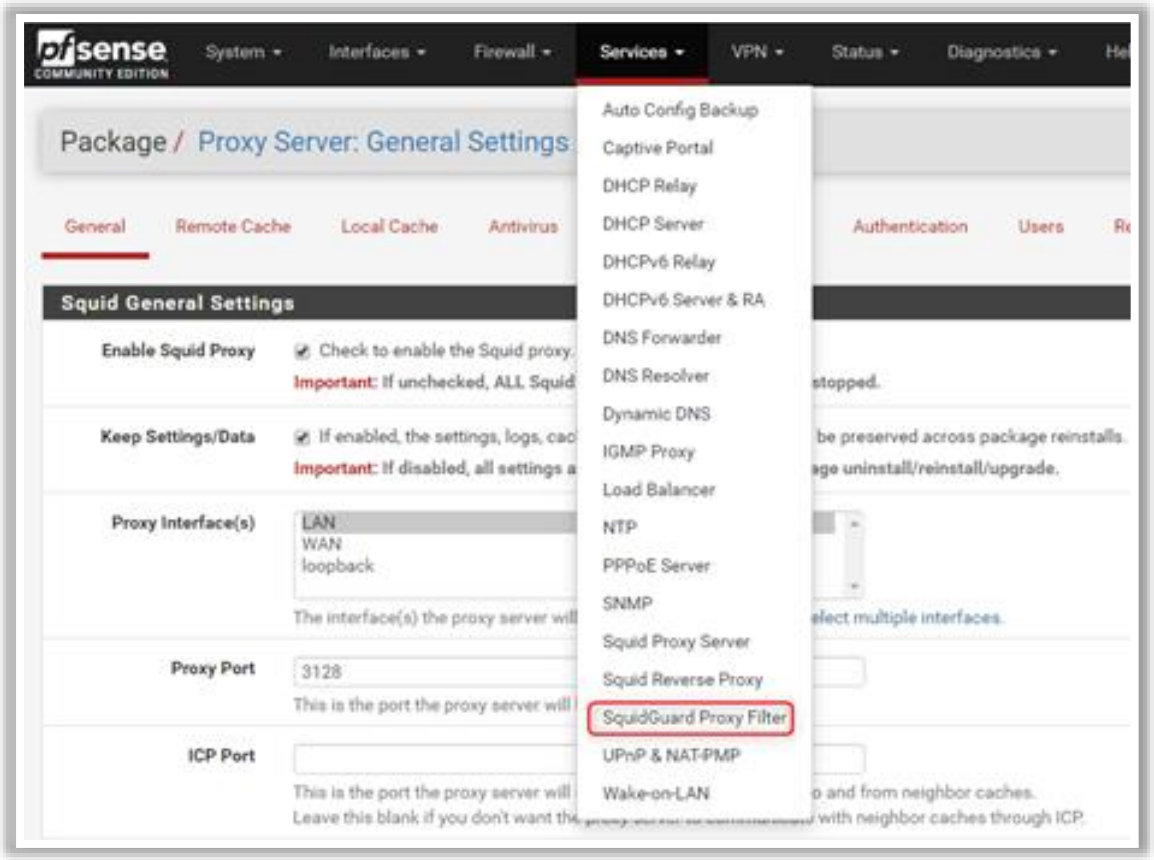


Figure 5.70: Screenshot of Squid Proxy

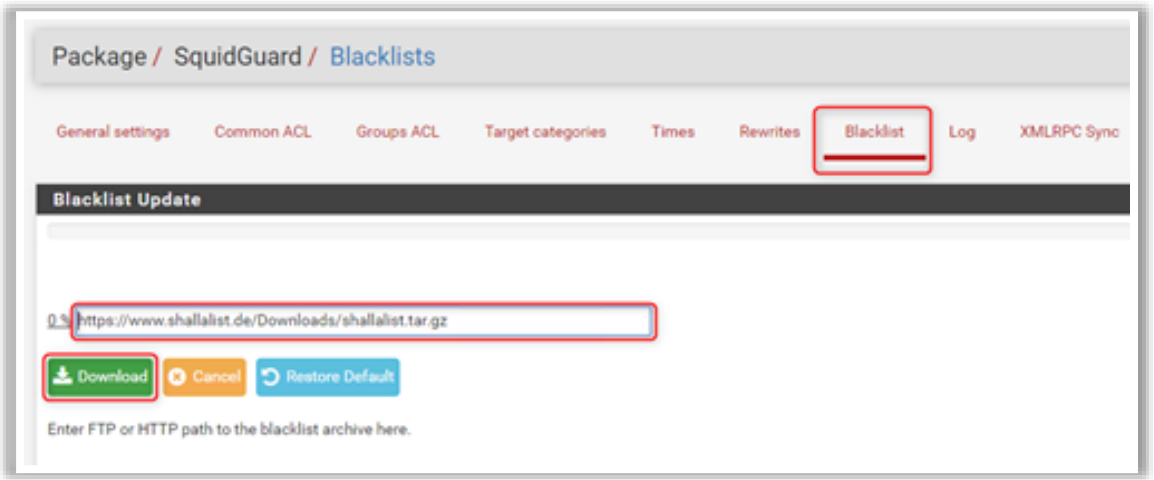
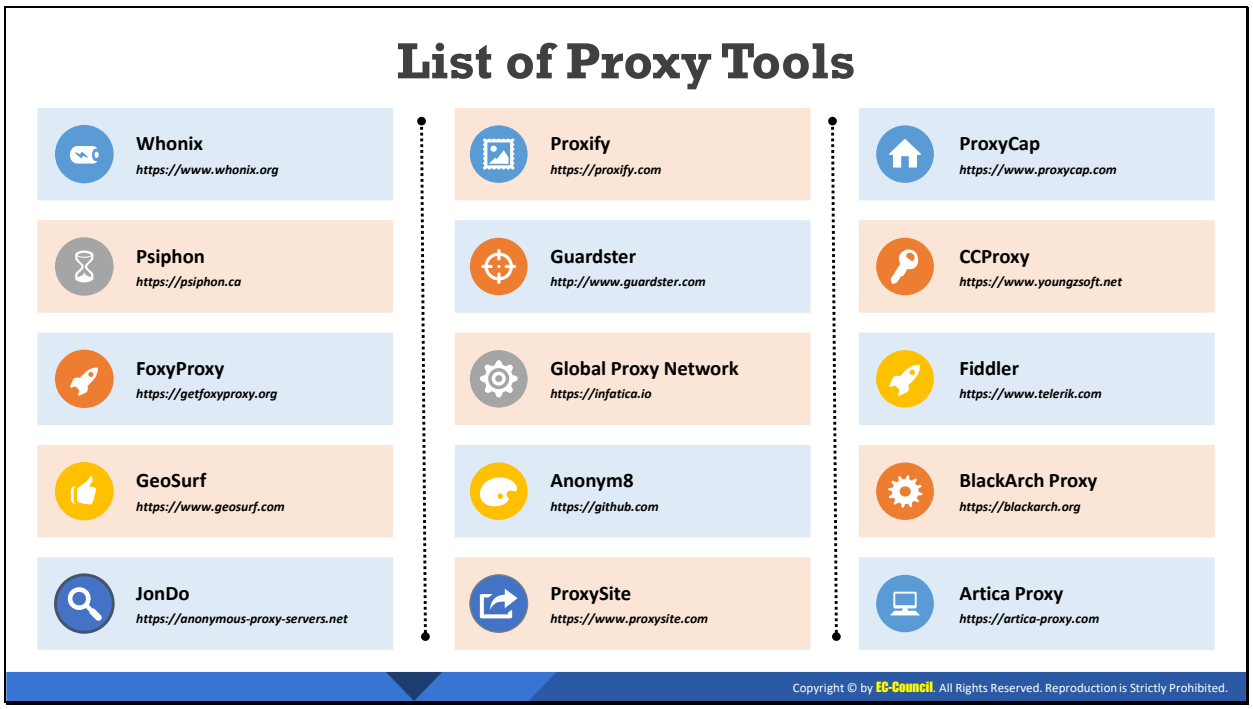


Figure 5.71: Screenshot of Squid Proxy

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

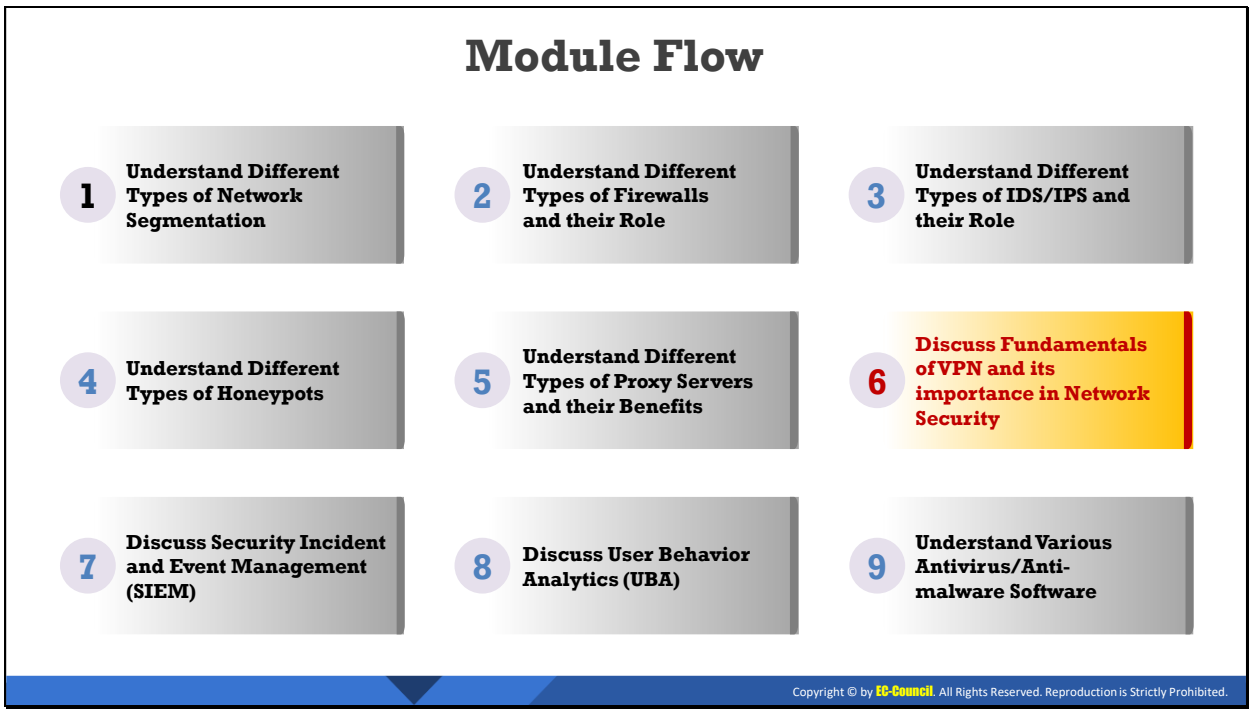


List of Proxy Tools

Some of proxy tools are listed below:

- Whonix (*https://www.whonix.org*)
- Psiphon (*https://psiphon.ca*)
- FoxyProxy (*https://getfoxyproxy.org*)
- GeoSurf (*https://www.geosurf.com*)
- JonDo (*https://anonymous-proxy-servers.net*)
- Proxify (*https://proxify.com*)
- Guardster (*http://www.guardster.com*)
- Global Proxy Network (*https://infatica.io*)
- Anonym8 (*https://github.com*)
- ProxySite (*https://www.proxysite.com*)
- ProxyCap (*https://www.proxycap.com*)
- CCProxy (*https://www.youngzsoft.net*)
- Fiddler (*https://www.telerik.com*)
- BlackArch Proxy (*https://blackarch.org*)
- Artica Proxy (*https://artica-proxy.com*)

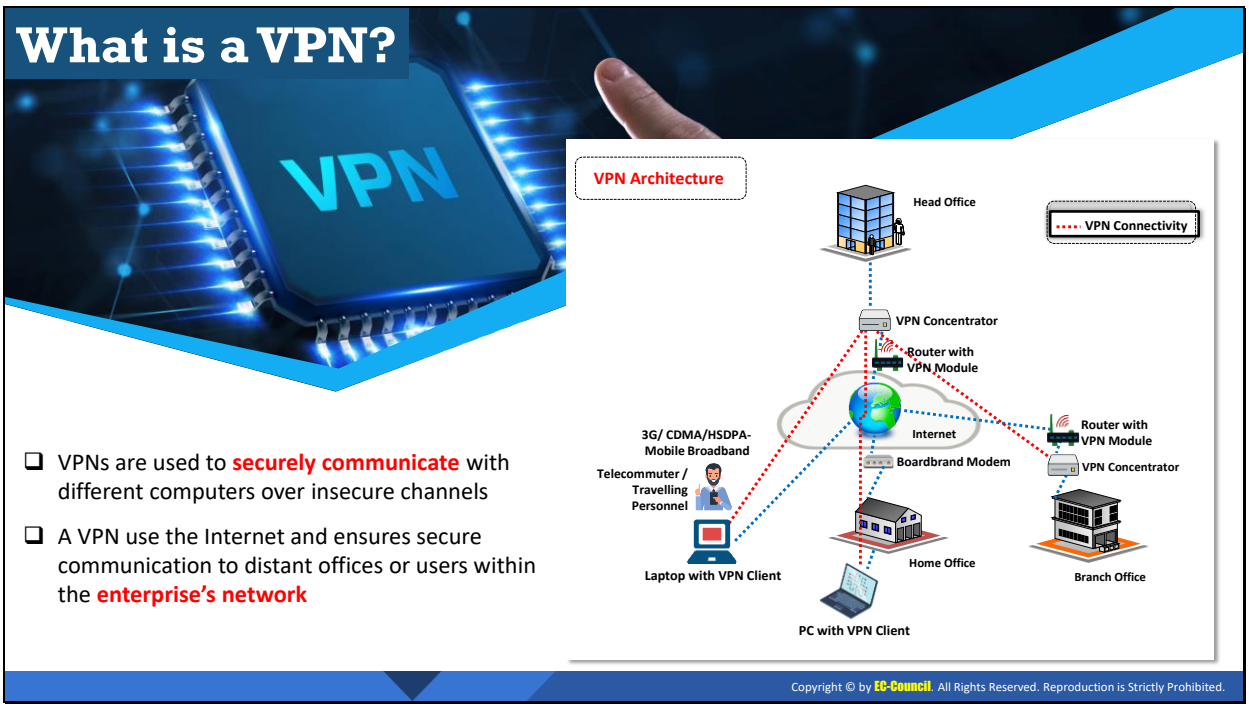
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Discuss Fundamentals of VPN and its importance in Network Security

VPN technology helps organizations protect the communication between their corporate private networks spread across the public Internet. It provides privacy and secures the communication between these networks through encrypted tunnels that transmit data between a remote user and corporate network. This section explains the fundamentals of VPN and its importance in securing networks.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



What is a VPN?

Most organizations have offices at different locations around the world. Consequently, there is a need for establishing a remote connection between these offices. Previously, remote access was established through leased lines with the help of dial-up telephone links such as ISDN, DSL, cable modem, satellite, and mobile broadband. However, establishing remote connections with these leased lines is quite expensive, and the costs increase as the distance between the offices increases.

To overcome the drawbacks of conventional remote access technologies, organizations are adopting virtual private networks (VPNs) to provide remote access to their employees and distant offices.

A VPN offers an attractive solution for security professionals to connect their organization's network securely over the Internet. VPN is used to connect distant offices or individual users to their organization's network over a secure channel.

VPN uses a tunneling process to transport encrypted data over the Internet. IPsec is the most common protocol used in VPN at the IP level. VPN ensures data integrity by using a message digest and protects data transmission from being tampered with. VPN guarantees quality of service (QoS) through service-level agreements (SLAs) with the service provider.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

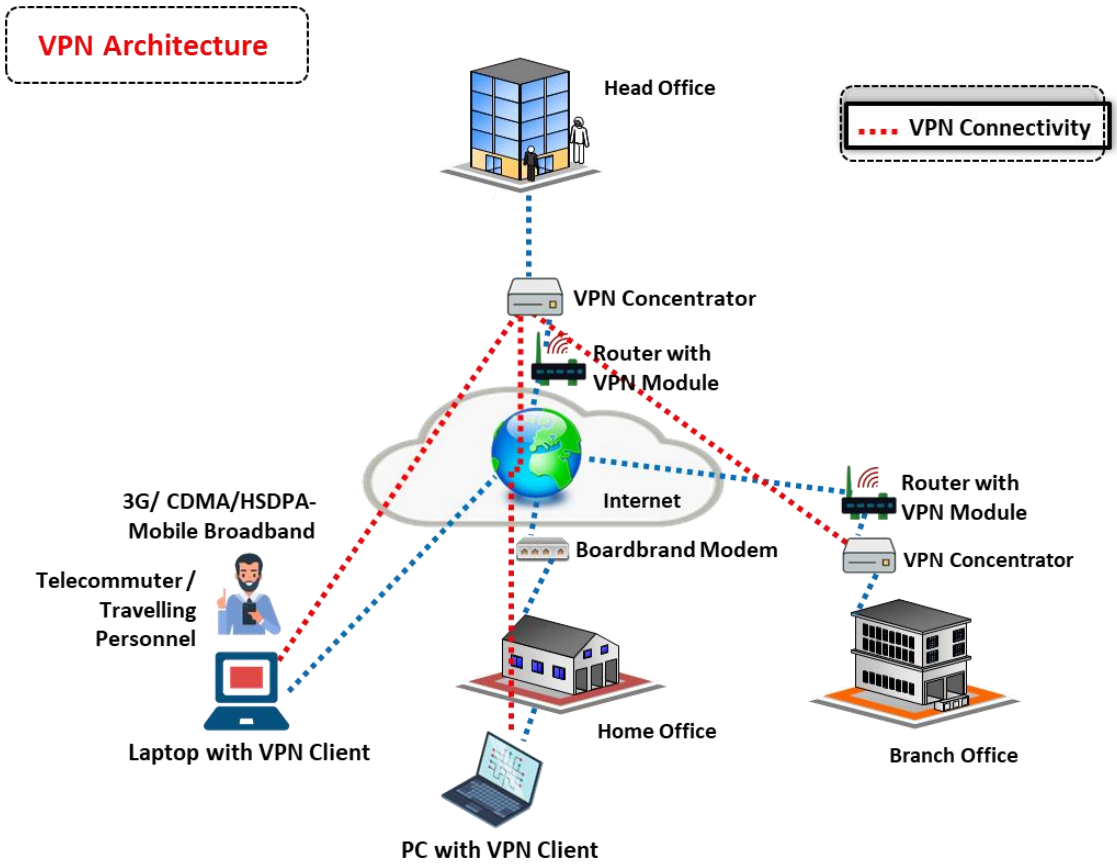


Figure 5.72: VPN architecture

- **Typical Features of VPN**
  - VPN establishes a connection between a remote system and a LAN across an intermediary network such as the Internet.
  - VPNs allow cheap long-distance connections over the Internet because both end points require a local Internet link, which serves as a free long-distance carrier.
  - VPN uses tunneling or encapsulation protocols.
  - VPNs use encryption to provide a secure connection to a remote network over the Internet and protects the communication.
  - VPNs provide virtual access to the physical network, and the experience is similar to the case where the user is physically located in the office.
- **Advantages of VPNs**
  - VPNs are inexpensive.
  - They provide a framework for corporate intranets and extranets.
  - VPN ensures secured data transfer.
  - VPN allows the user to access both web applications and websites in complete anonymity.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **Disadvantages of VPNs**
  - Designing and implementing a VPN is a complex issue that requires experts for configuration.
  - Reliability depends on the chosen service provider.
- **VPN Architecture**

  A certain set of protocols and standards must be followed while establishing a VPN architecture. Security professionals should decide the scope, implementation, and deployment of the VPN and perform continuous network monitoring to ensure the security of a VPN. They should be continuously aware of the overall architecture and scope of the VPN.
- **Protocols Used in Deploying a VPN**

  To deploy VPNs, there are two primary options: IPsec and SSL. Each protocol has its own unique advantages and is utilized depending on the requirement of the user or the organization's IT processes.
- **IPsec VPN**

  IPsec-based VPN is the deployment solution most commonly used by organizations. It is a set of protocols and standards developed by the Internet Engineering Task Force (IETF) for secure communication on the IP layer. It ensures the security of each packet in communication by encrypting and authenticating them. IPsec connections are established using pre-installed VPN client software, which mainly focuses on company-managed desktops.
  - **Advantages**
    - IPsec VPNs can support all IP-based applications through an IPsec VPN product.
    - They offer tremendous versatility and customizability through the modification of the VPN client software.
    - Organizations can control the VPN client functions by using the APIs in IPsec client software.
    - They ensure the secure exchange of IP packets between remote networks or hosts and an IPsec gateway located at the edge of the organization's private network.

  The three basic applications of IPsec VPNs (associated with business requirements) are as follows.
  - **Remote-access VPNs:** These allow individual users, such as telecommuters, to connect to a corporate network. This application creates an L2TP/PPTP session protected by IPsec encryption.
  - **Intranet VPNs:** These help in connecting branch offices to the corporate headquarters, creating a transparent intranet.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- **Extranet VPNs:** These allow companies to connect with their business partners (for example, suppliers, customers, and joint ventures).

- **SSL VPN (Web-based)**

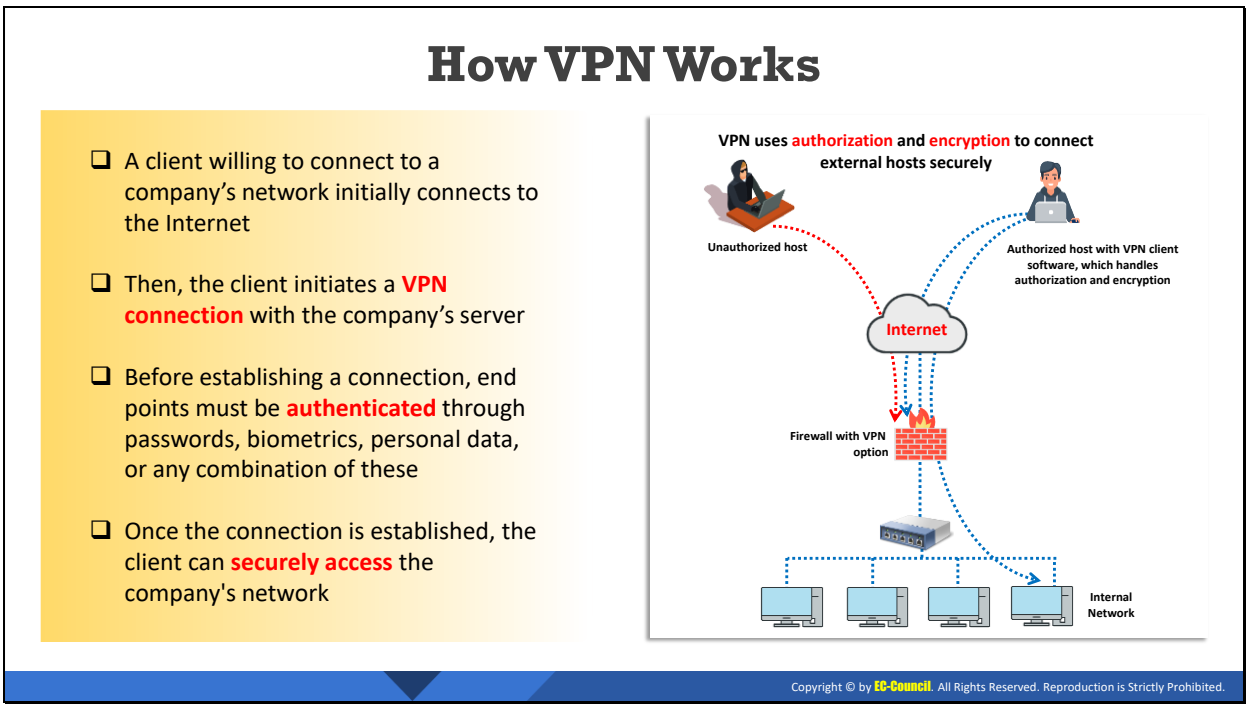
  SSL-based VPNs provide remote-access connectivity using a web browser and its native SSL encryption, irrespective of the location. SSL does not require any special client software to be pre-installed and is capable of any type of connectivity. The connectivity ranges from company-managed desktops to non-company-managed desktops, such as employee-owned PCs, contractor-owned PCs, or business partner desktops. It helps in reducing desktop software maintenance as it downloads software dynamically whenever needed.

  - **Advantages**

    - It offers additional features such as easy connectivity from non-company-managed desktops and requires little or no desktop software maintenance.
    - It provides accessibility to the SSL library and access to TCP port 443.
    - It works wherever the user can gain access to HTTPS websites such as Internet banking, secure webmail, or intranet sites.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



How VPN Works

A VPN enables a secured connection over the Internet from a public network to a private network placed at a distant site. All the network traffic in a VPN is encrypted and passes through a virtual secure tunnel placed between the client and VPN server.

All the packets passing through a VPN are encrypted or decrypted with respect to inbound or outbound traffic. The packets are encrypted at the client side and decrypted at the VPN server. A client willing to connect to a company's network initially connects to the Internet. Then, the client initiates a VPN connection with the company's server. Before establishing a connection, end points must be authenticated through passwords, biometrics, personal data, or any combination of these. Once the connection is established, the client can securely access the company's network.

For example, when a client with a VPN connection enabled browses Youtube.com, the outbound traffic is encrypted at the client side. The encrypted data are then sent to the nearest VPN server, which passes the data to the gateway server. At the gateway server, the data are decrypted and sent to the server hosting Youtube.com. When Youtube.com sends a reply request, the VPN server performs the reverse process on the outbound traffic.

A VPN closely monitors any insecure networks. It creates a new IP address for an encrypted packet, concealing the real IP address; this prevents attackers from finding the real IP address from which the packets were sent.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

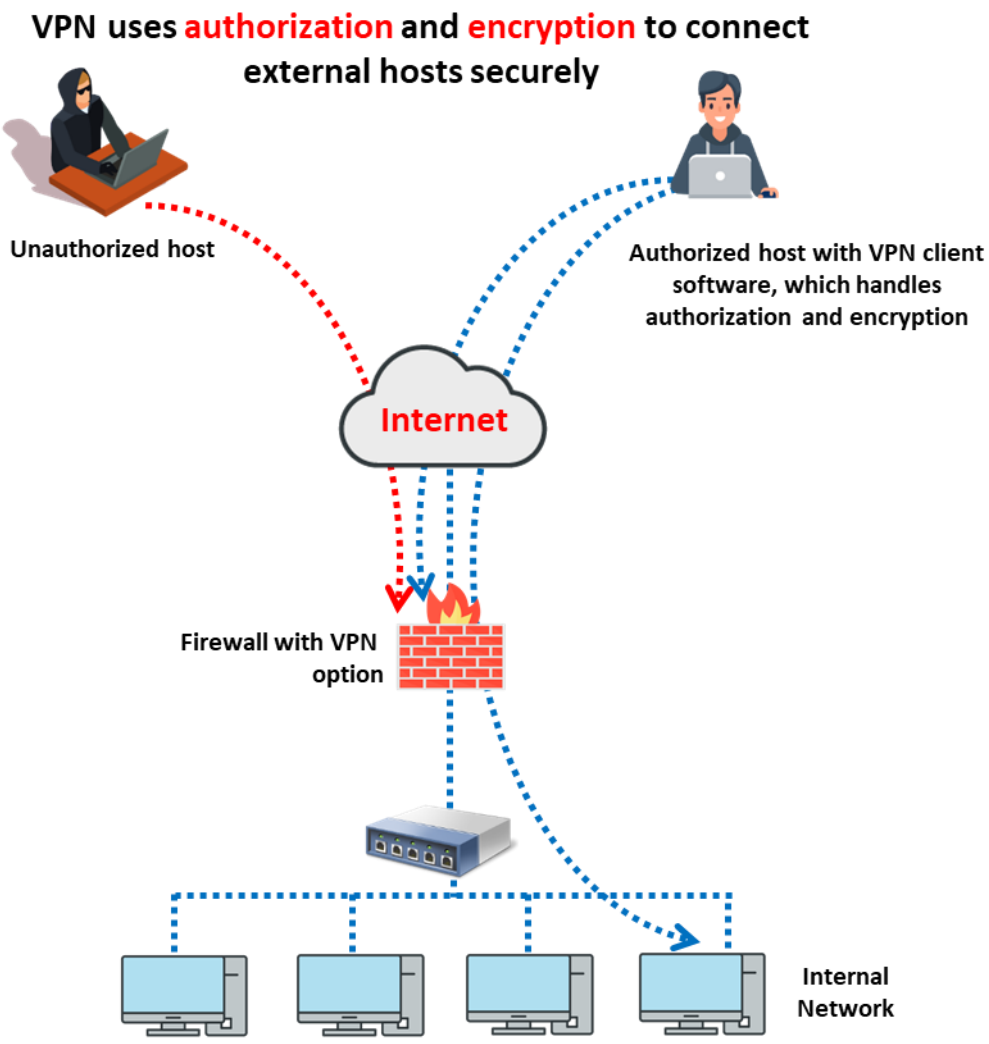
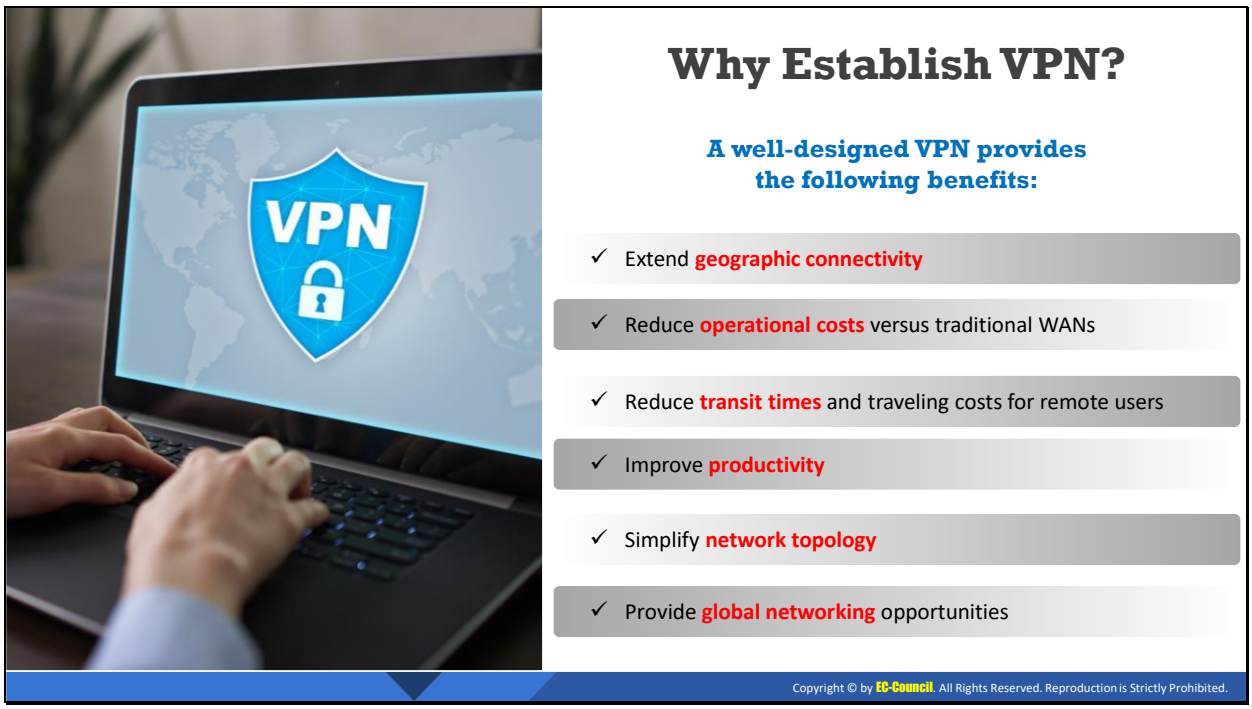


Figure 5.73: Working of VPN

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Why Establish VPN?

The easy accessibility of sensitive data over the Internet poses a serious security threat to organizations. Attackers easily exploit and gain access to sensitive information sent over an unsecured public network such as the Internet. A VPN ensures reliable communication through an encrypted tunnel, preventing attackers from gaining access to the organization's information. A well-designed and well-implemented VPN can provide the following benefits:

- It enables a secured connection across multiple geographical locations.
- It saves time and expenditure for employees as it allows the sharing of information between a corporate office and regional offices.
- It enhances the level of output for remote users.
- It improves the security of data by concealing the IP address from attackers.
- It handles multiple connections simultaneously and provides the same quality of service for each connection.
- It has the ability to provide a secure connection to large enterprises.
- The implementation of a VPN increases the bandwidth and efficiency of the network.
- Maintenance costs are low.
- It reduces transit times and traveling costs for remote users.
- It improves productivity and simplifies network topology.
- It provides global networking opportunities and telecommuter support.
- It has a faster return on investment (ROI) than a conventional WAN.

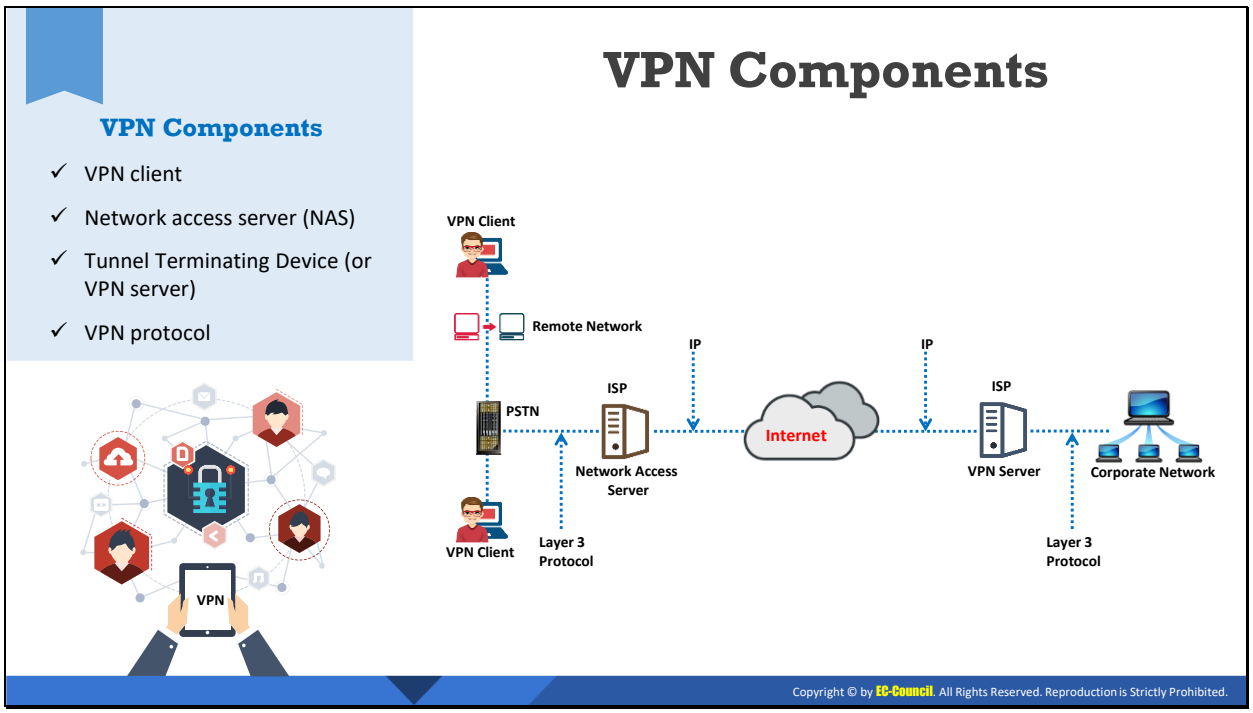
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

This encrypted traffic proves beneficial when a user connects their system to Wi-Fi networks in public places. The encryption makes it difficult for eavesdroppers in the network to identify the encrypted data.

A VPN allows users to access servers across the world, making it easy for them to access all types of content. With a VPN, users need not face restrictions such as geo-blocking while browsing. A VPN allows the user to stay anonymous without sharing their device information in the network. By hiding such data, a VPN prevents websites from spying on or monitoring the user. To avoid excessive monitoring from third-party websites or attackers, users should install a VPN for safe browsing.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



VPN Components

The VPN architecture consists of four main components.

- **VPN client:** It is a computer that initiates a secure remote connection to a VPN server.
- **Network access server (NAS):** Also called a media gateway or a remote-access server (RAS), the NAS is responsible for setting up and maintaining each tunnel in a remote-access VPN. Users need to connect to the NAS to use a VPN.
- **Tunnel terminating device (or VPN server):** It is a computer that accepts VPN connections from VPN clients.
- **VPN protocol:** It includes VPN-specific protocols used to manage tunnels and encapsulate private data. It includes the use of PPTP and L2TP protocols, along with IPsec.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

The following diagram shows the use of various VPN components in a remote-access VPN:

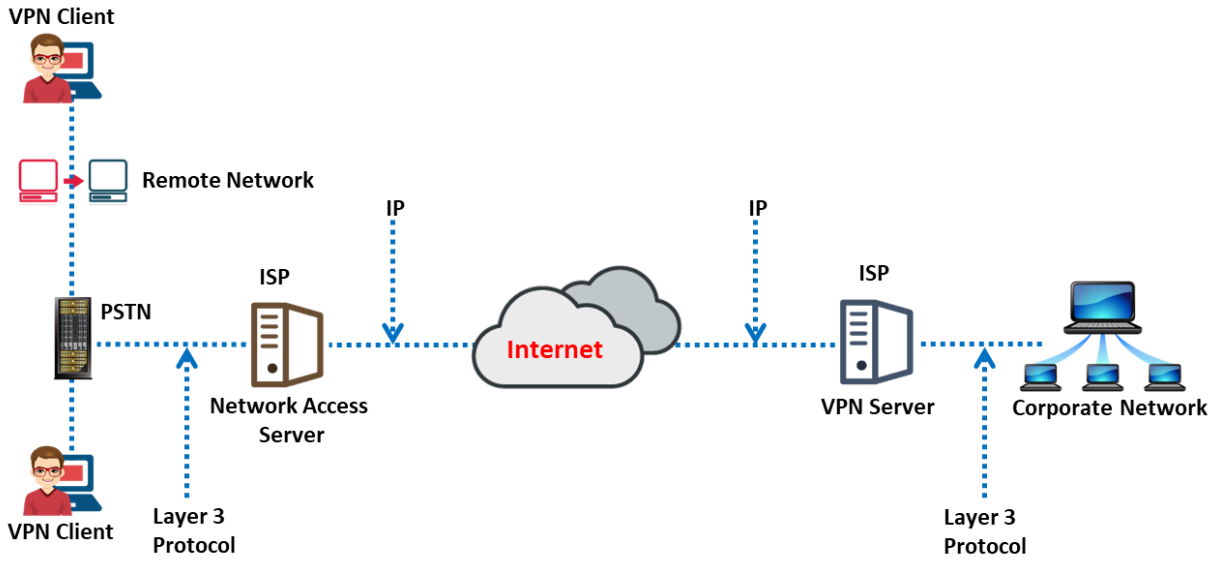
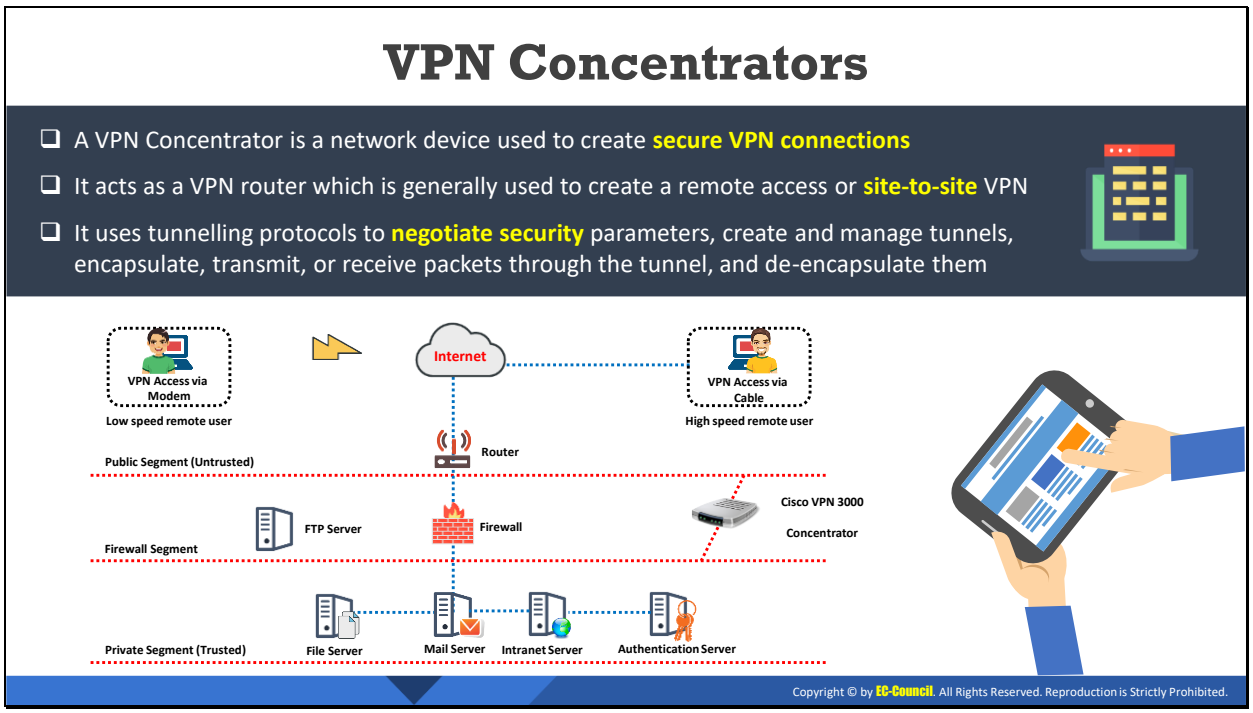


Figure 5.74: VPN components in a remote-access VPN

A typical remote-access VPN connection is established as follows:

- The remote user propagates a PPP connection with an ISP's NAS through a PSTN.
- The packets sent by the user are sent to the tunnel connecting the NAS and VPN server after authenticating the user.
- The packet is encrypted before placing it in the tunnel.
- The location of the VPN server depends on the model used for the VPN implementation.
- The VPN server accepts the packet from the tunnel, decrypts it, and sends it to the final destination.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



VPN Concentrators

VPN concentrators normally enhance the security of the connections made through a VPN. They are generally used when a single device needs to handle a large number of VPN tunnels. They are best used for developing a remote-access VPN and site-to-site VPN.

VPN concentrators implement the security of tunnels using tunneling protocols. These protocols manage the following:

- Flow of packets through the tunnel
- Encryption and decryption of packets
- Creation of tunnels

A VPN concentrator works in two ways:

- Receives plain packets at one end, encrypts at the other end, and forwards the packet to the final destination
- Receives encrypted packets at one end, decrypts at the other end, and forwards the packet to the final destination

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

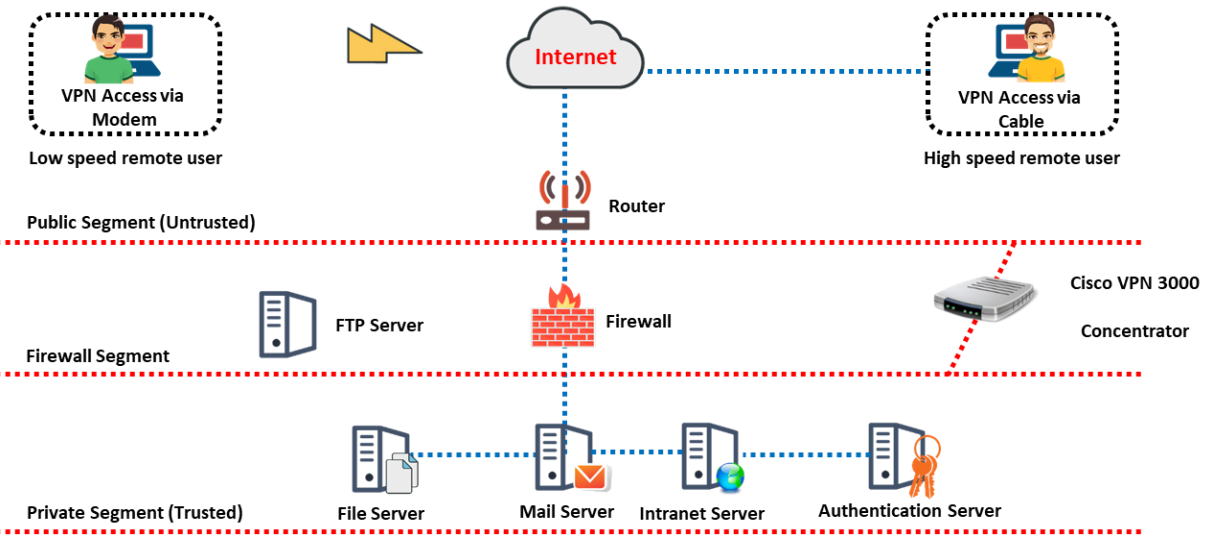
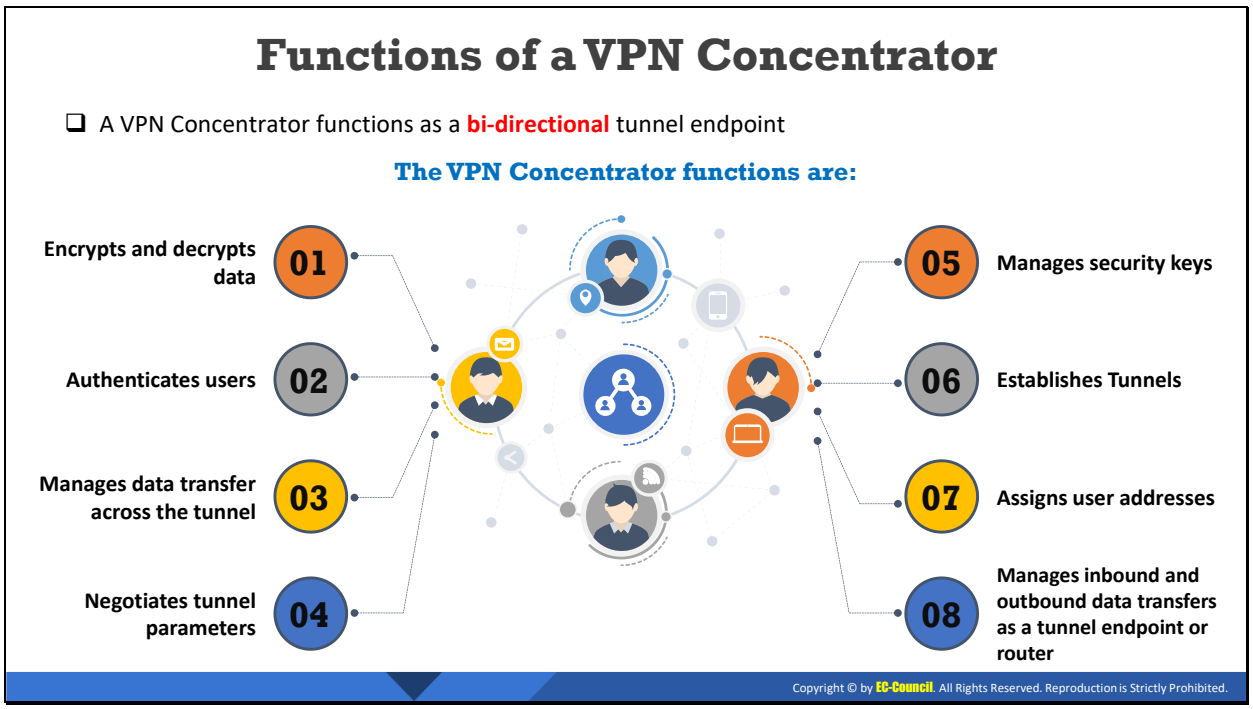


Figure 5.75: VPN concentrator

In the figure, the VPN concentrator is placed in parallel with the firewall supporting two remote users who have a slow and fast Internet speed, respectively. If the VPN is placed behind the firewall, the implementation requires additional configuration changes and is vendor-dependent.

VPN concentrators provide a high level of security for SSL and IPsec VPN architectures. A normal VPN tunnel requires IPsec to be implemented on the network layer of the OSI model. A major benefit of using a VPN concentrator is that the client is considered to be present outside the network and can access the network as if it is connected.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

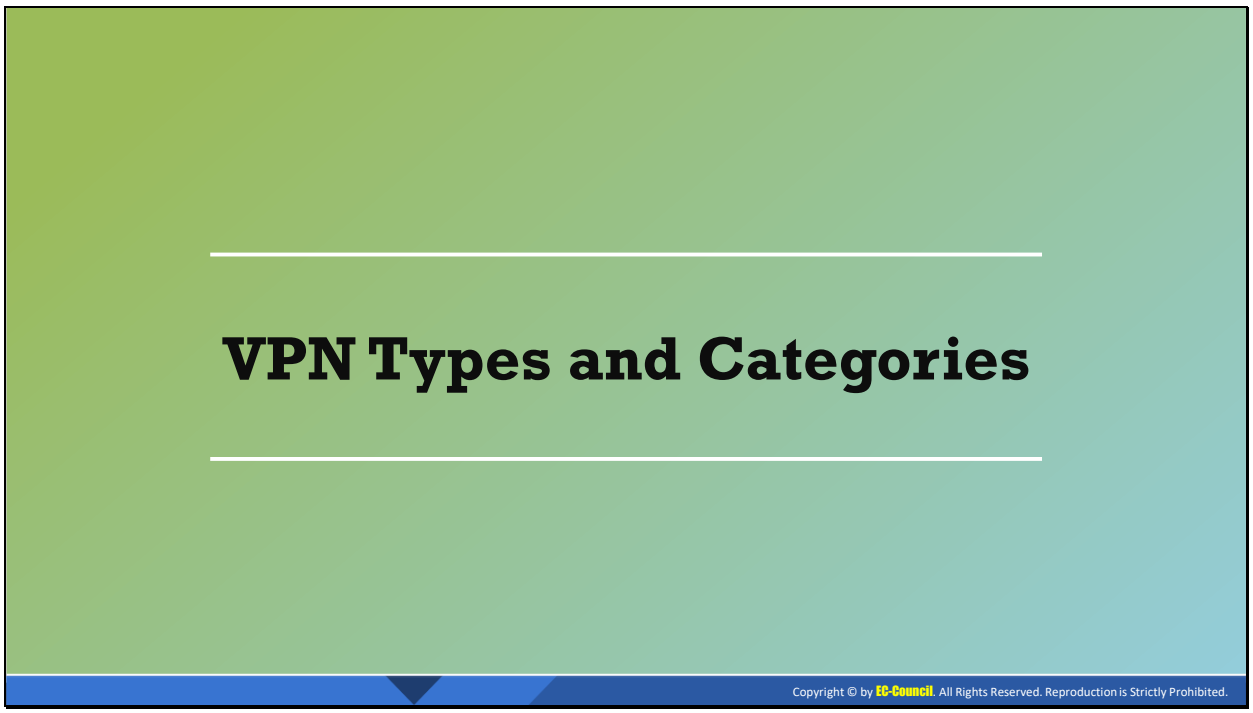


Functions of a VPN Concentrator

A VPN Concentrator functions as a bi-directional tunnel end point. A VPN concentrator adds more security controls to the router, improving the security of the communication. The functions of a VPN concentrator are as follows.

- **Data encryption:** The VPN concentrator encrypts the data. Being bi-directional, it initially encrypts the plain packets it receives and later decrypts them at the end of the tunnel, before sending them to the destination. It manages security keys.
- **Managing tunnels:** By adding the features of advanced data and network security, a VPN concentrator has the ability to create and manage large VPN tunnels. These tunnels ensure data integrity among systems. It negotiates tunnel parameters.
- **User authentication:** A VPN concentrator authenticates users at either the computer level or the user level. Authentication at the computer level is performed using the Layer 2 Tunneling Protocol (L2TP), whereas authentication at the user level is performed using the Point-to-Point Tunneling Protocol (PPTP).
- **Traffic handler:** A VPN concentrator routes the tunneled and non-tunneled traffic depending on the server configuration. It simultaneously handles traffic of a corporate network as well as Internet resources. It manages inbound and outbound data transfers as a tunnel end point or router. It assigns user addresses.

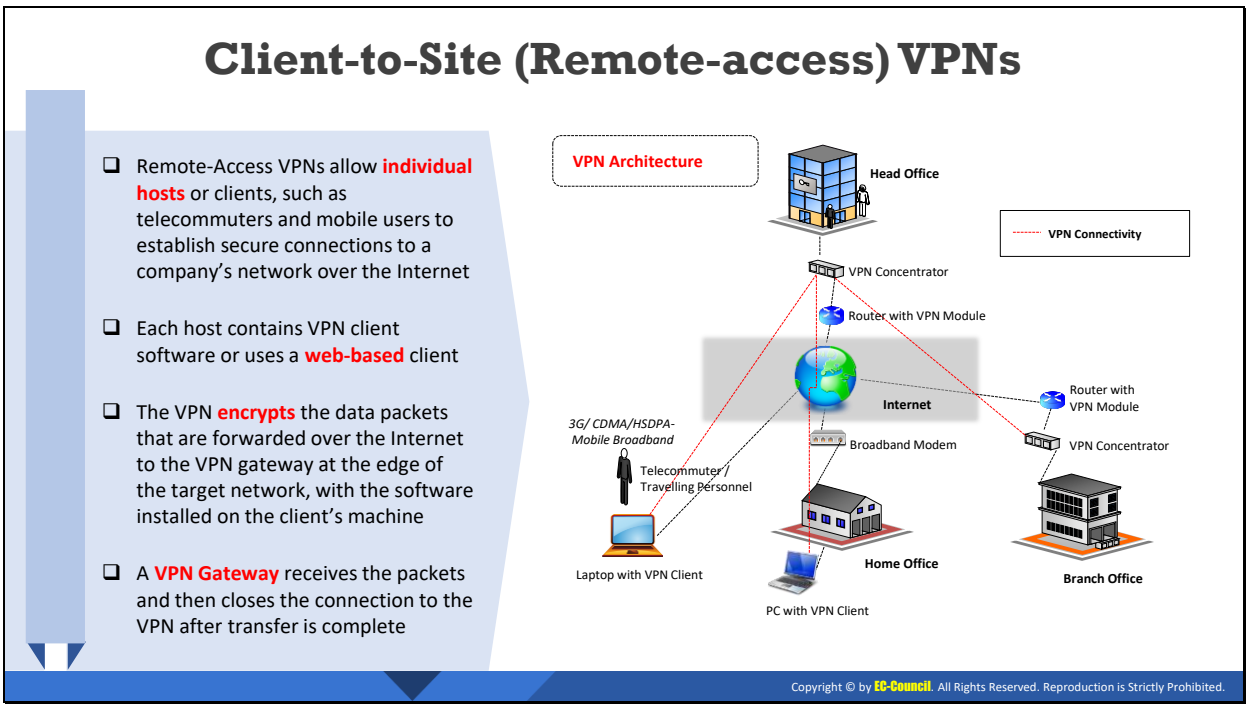
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



VPN Types and Categories

This sub-section explains different types of VPN and their categories.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Client-to-Site (Remote-access) VPNs

Remote-access VPNs allow individual hosts or clients such as telecommuters and mobile users to establish secure connections to a company's network over the Internet. This allows the users to access the information provided in the private network. An older name for a remote-access VPN is a virtual private dial-network (VPDN), in which a dial-up configuration is required for the connection to a server.

Every host using a remote-access VPN must have the VPN client software installed; this software wraps and encrypts the data before the host sends any traffic over the Internet to a VPN gateway. After reaching the gateway, the data are unwrapped, decrypted, and passed over to the final destination in a private network. The gateway performs the reverse process to send data packets back to the user.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

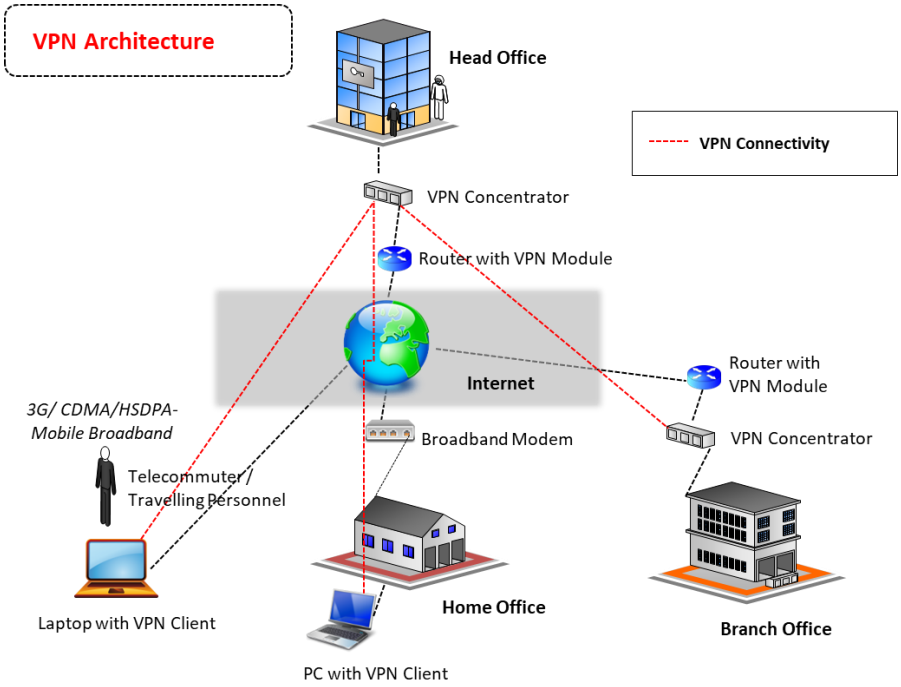


Figure 5.76: Remote-access VPN

A remote-access VPN consists of two types of components.

- **Network access server (NAS) or remote-access server (RAS)**: NAS is required while users are accessing a VPN. A separate authentication process is involved while authenticating users accessing a VPN.
- **Client software**: Users accessing a VPN from their own network need to install software that helps create and manage the VPN connection.

VPN client software and a VPN gateway are required for the hosts supporting a remote-access VPN. Most VPN gateways support only IPsec while maintaining VPN services.

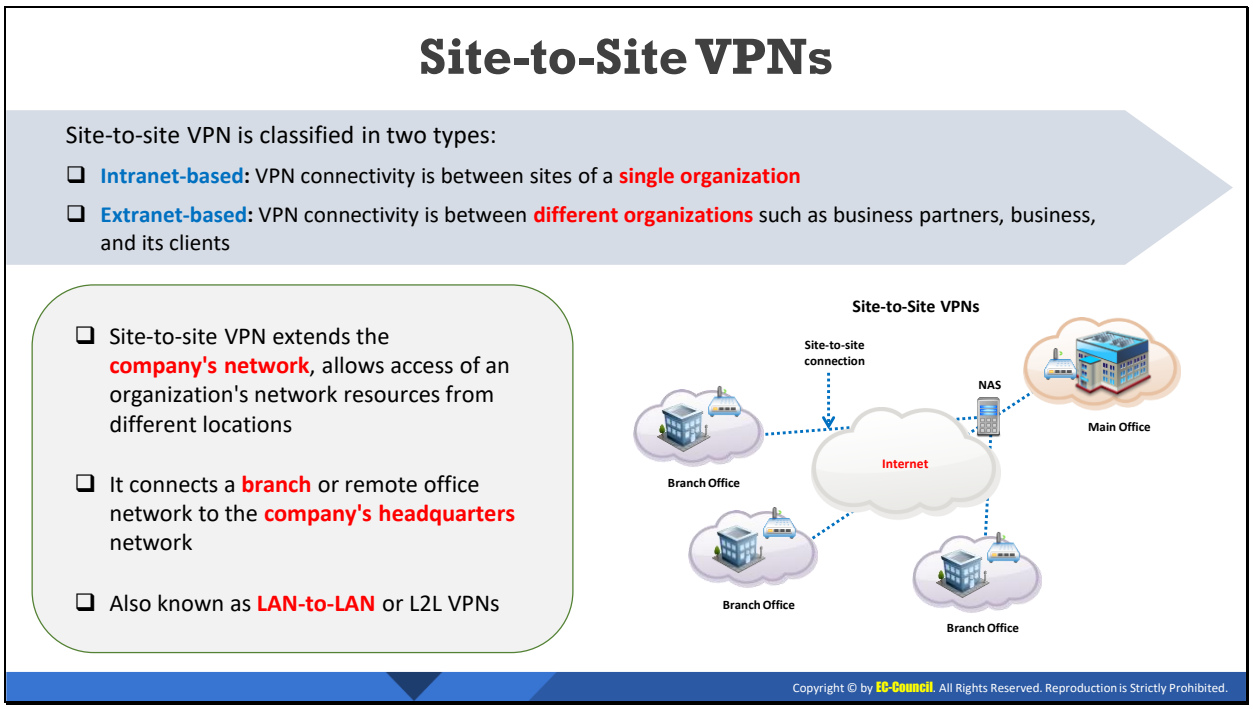
Advantages

- Remote-access VPNs minimize the connection cost for the users.
- The encryption of data packets provides an added security layer. This hides the IP address of the packets and prevents attackers from accessing the packets.
- Remote-access VPNs can handle a large number of users. The VPN provides the same service even if more users are added to the VPN network.
- Remote-access VPNs allow the sharing of files from a remote location.

Disadvantages

- Computers without any antivirus installed pose a threat to the VPN connection.
- Implementing many VPN connections simultaneously may affect the bandwidth of the network.
- It is time-consuming to accessing files and applications over the Internet.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Site-to-Site VPNs

A site-to-site VPN helps connect different networks. For example, the branch offices of an organization can be connected to the main campus through a site-to-site VPN. The main differentiation between a remote-access VPN and a site-to-site VPN is that a site-to-site VPN does not require any client software. The entire traffic is sent through a VPN gateway that encrypts the data packets passing through it.

In a site-to-site VPN, the outbound traffic passes through a tunnel to the VPN gateway. The data packets in the outbound traffic are encrypted at the gateway and passed to the tunnel over the Internet. The traffic is sent to the nearest gateway to the target location. The nearest gateway decrypts the data packets and then forwards them to the final destination.

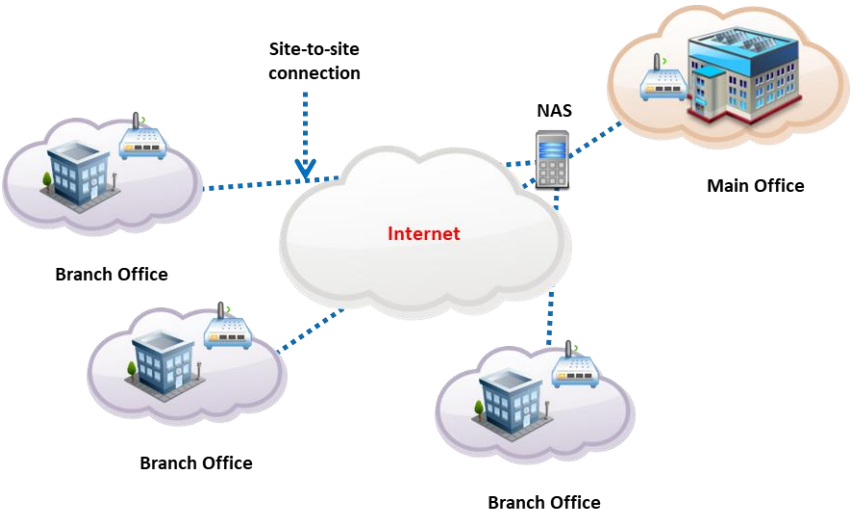


Figure 5.77: Site-to-site VPN

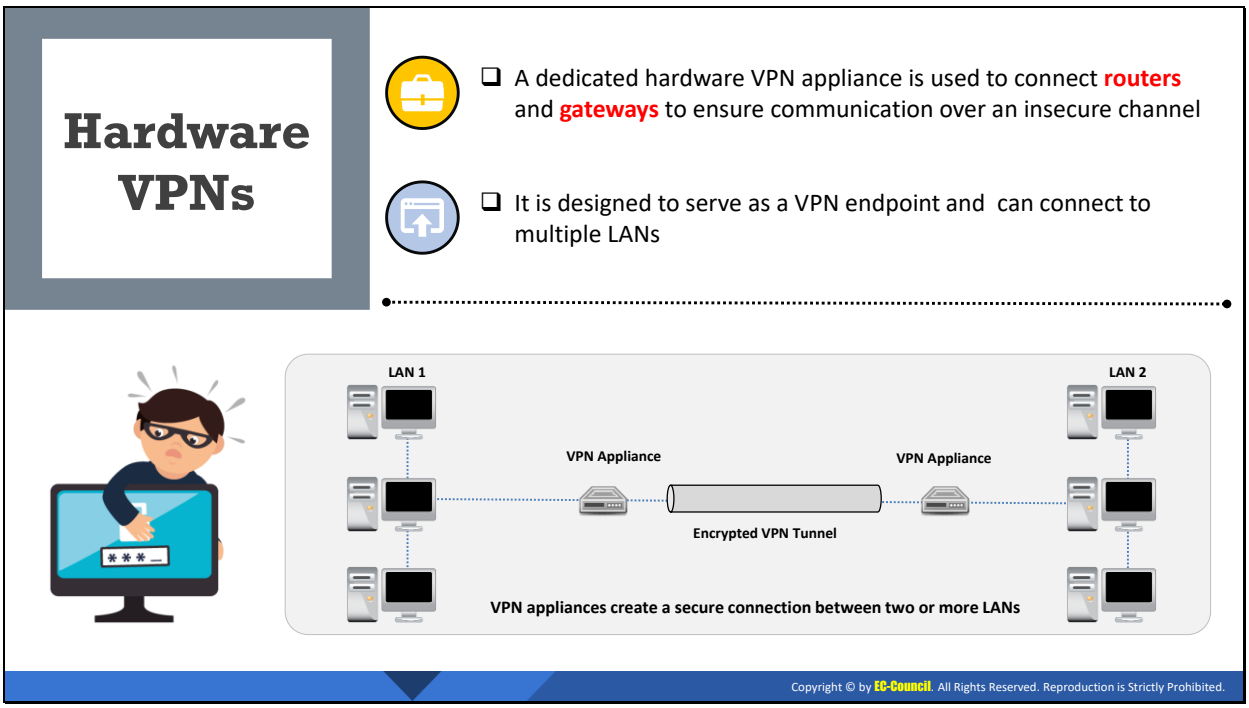
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

There are two types of site-to-site VPNs.

- **Intranet-based:** In this type, VPN connectivity is between the sites of a single organization. It creates an intranet VPN to connect each individual LAN to a single WAN.
- **Extranet-based:** In this type, VPN connectivity is between different organizations such as business partners, businesses, and clients. An extranet VPN connects every single LAN of an organization. The extranet VPN configuration prevents any access to an intranet VPN.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Hardware VPNs

Hardware-based VPNs are separate devices that consist of individual processors and hardware firewalls. They easily manage the authentication and encryption of data packets. The main advantage of using a hardware-based VPN is that they provide more protection than the software variant.

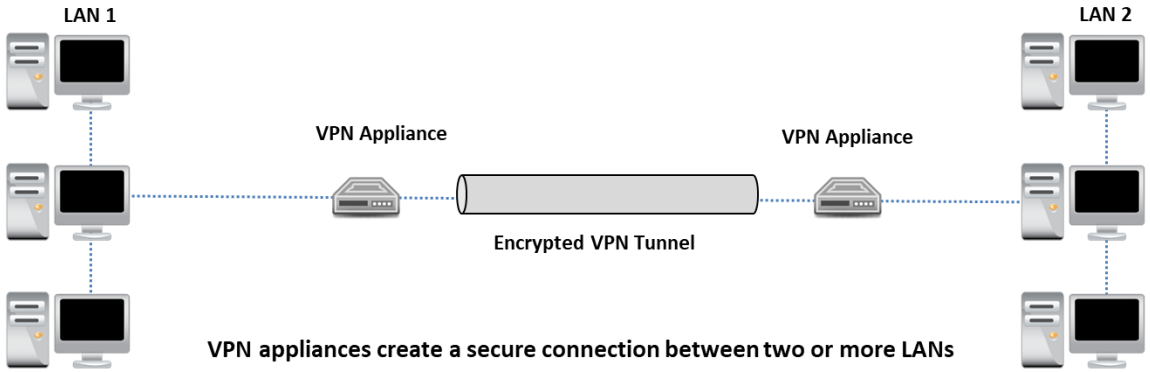


Figure 5.78: Hardware VPN

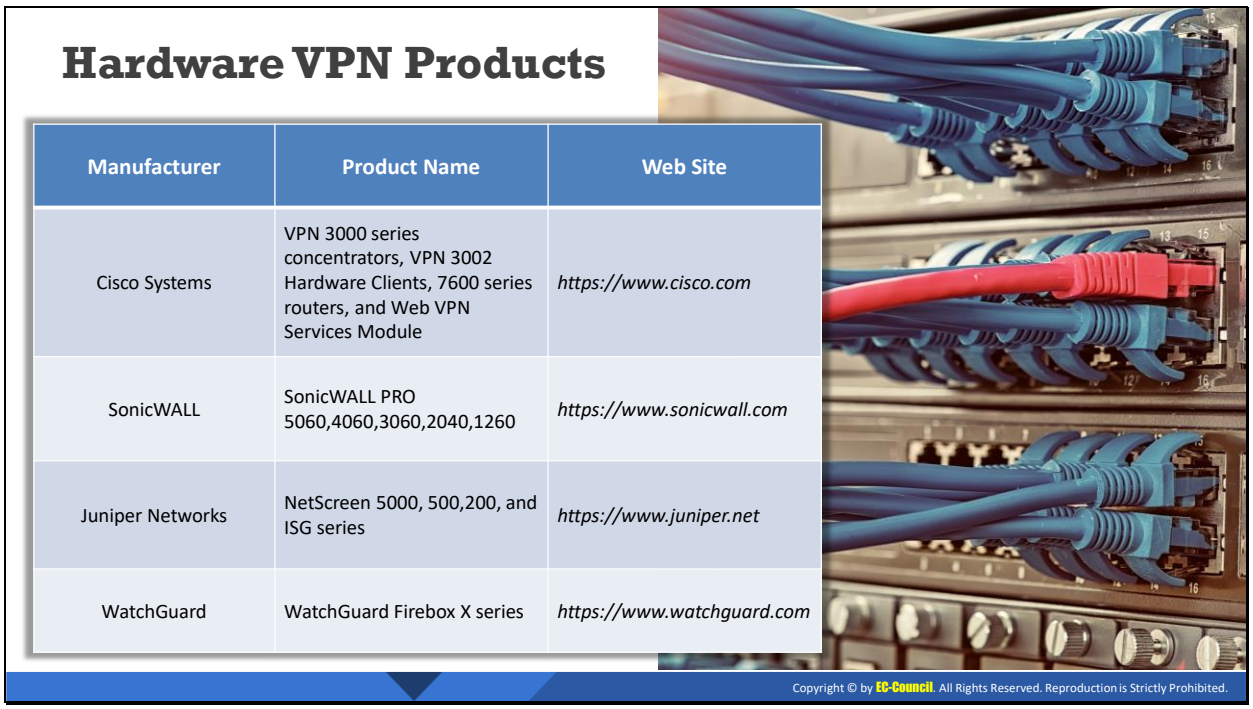
Advantages

- A hardware VPN provides load balancing, especially for large client loads.

Disadvantages

- It is more expensive than a software VPN.
- It is more useful for large business organizations than for smaller ones.
- It has low scalability.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

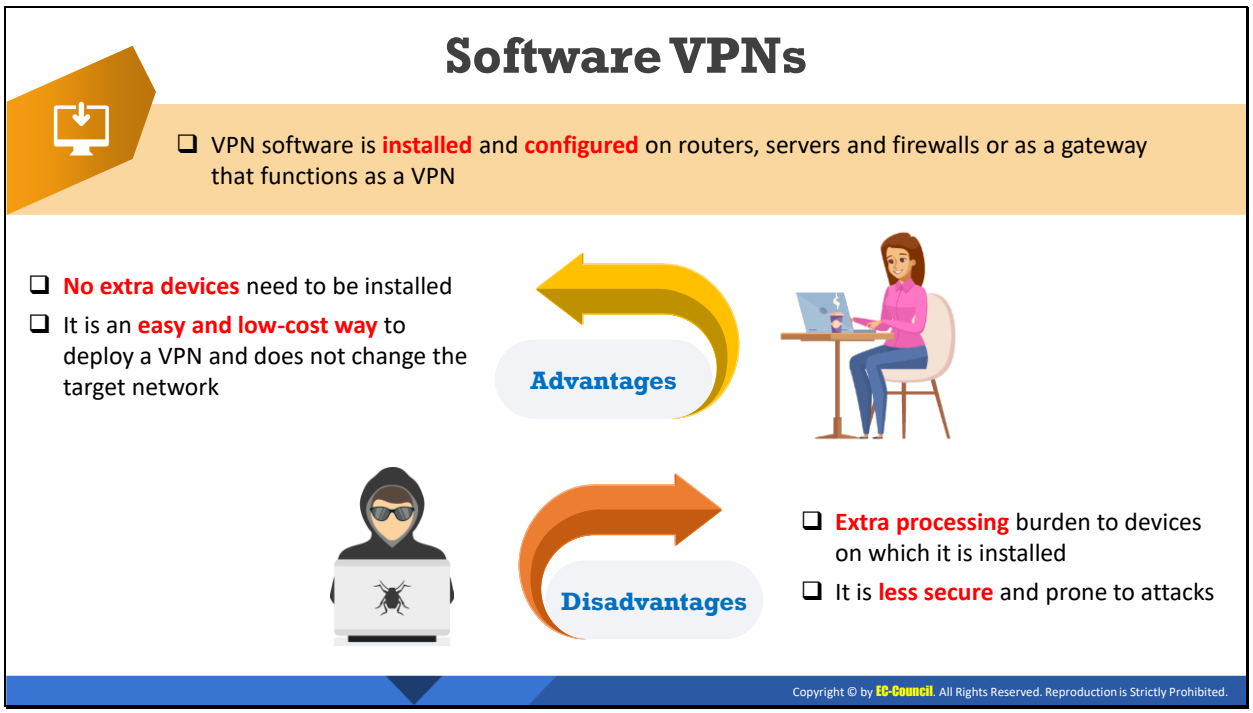


Hardware VPN Products

Manufacturer	Product Name	Web Site
Cisco Systems	VPN 3000 series concentrators, VPN 3002 Hardware Clients, 7600 series routers, and Web VPN Services Module	*https://www.cisco.com*
SonicWALL	SonicWALL PRO 5060, 4060, 3060, 2040, 1260	*https://www.sonicwall.com*
Juniper Networks	NetScreen 5000, 500, 200, and ISG series	*https://www.juniper.net*
WatchGuard	WatchGuard Firebox X series	*https://www.watchguard.com*

Table 5.3: Hardware VPN products

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Software VPNs

VPN software is installed and configured on routers, servers, and firewalls or as a gateway that functions as a VPN. Software-based VPNs are best suited for network traffic management and when the same party does not manage the VPN end points. Traffic management is performed using a tunneling process depending on the protocol and address of the traffic. Hardware encryption accelerators are used to improve the performance of the network.

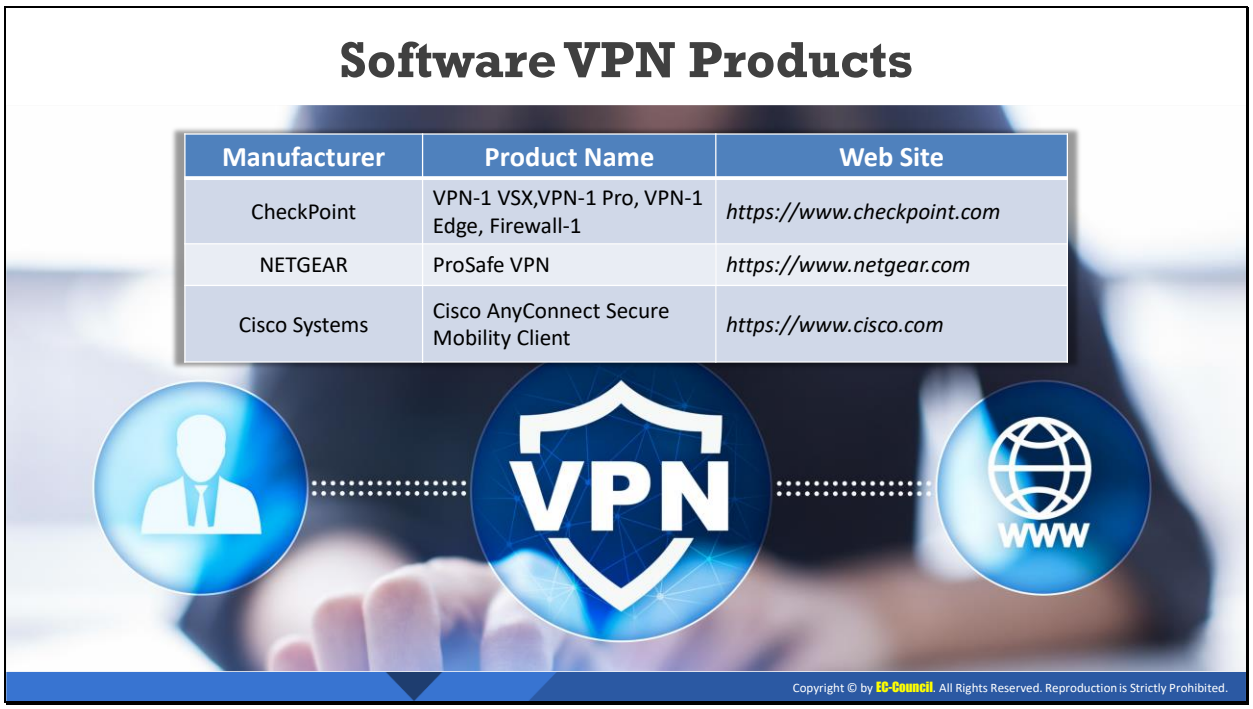
Advantages

- A software VPN minimizes the cost of additional hardware purchases.
- It is easy and inexpensive to deploy and does not change the target network.
- It has high scalability.

Disadvantages

- It causes increased processing tasks for devices implementing the VPN.
- Security is an issue; a software VPN is prone to attacks as they need to share the server with other servers and OSes.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

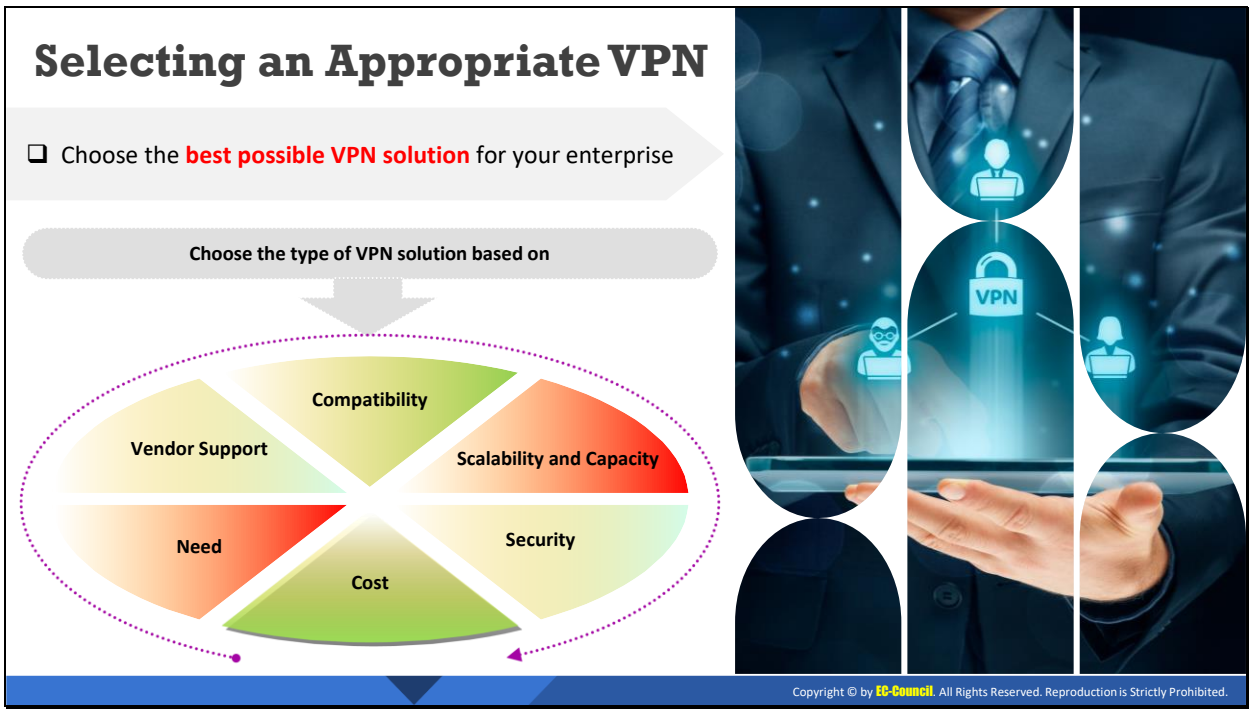


Software VPN Products

Manufacturer	Product Name	Web Site
CheckPoint	VPN-1 VSX, VPN-1 Pro, VPN-1 Edge, Firewall-1	*https://www.checkpoint.com*
NETGEAR	ProSafe VPN	*https://www.netgear.com*
Cisco Systems	Cisco AnyConnect Secure Mobility Client	*https://www.cisco.com*

Table 5.4: Software VPN products

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Selecting an Appropriate VPN

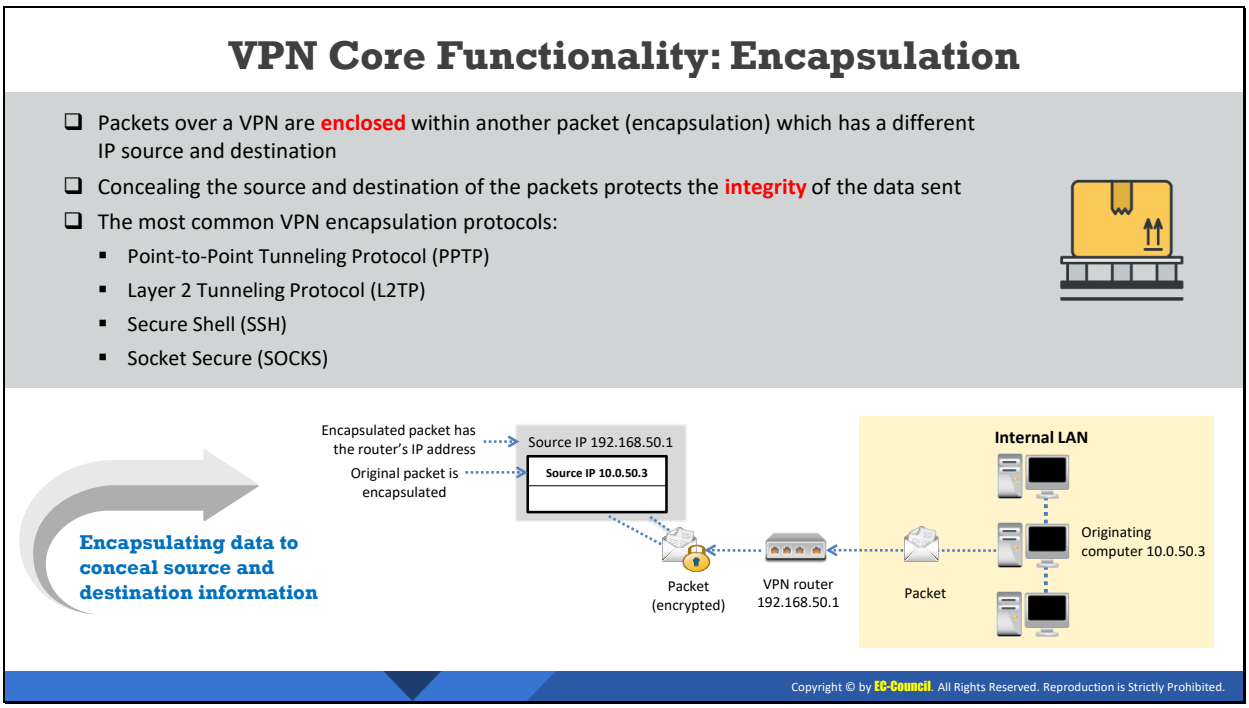
The selection of an appropriate VPN depends on many factors such as cost, protocols, and technical issues. The following are a few factors to consider while selecting a VPN.

- **Compatibility**: The organization should consider the compatibility of the selected VPN within the organization's network and determine whether it is possible to adopt the selected VPN. Selecting and implementing a VPN that is not compatible will add extra expenditure and cause security issues.
- **Scalability**: Increasing the number of employees working for an organization is a common trend. As the number of employees increases, the configured VPN needs to accommodate the new employees. The inability to handle an increasing number of users adversely affects the performance of the network. The organization must select a VPN that can handle any number of users at any time without affecting the performance of the network.
- **Security**: Security is an important factor while selecting a VPN. The following are the two major criteria in selecting a VPN.
  - **Authentication**: Organizations need to select an appropriate authentication method depending on the type of network on which the VPN is implemented.
  - **Encryption**: Organizations should be highly alert regarding the encryption process for the selected VPN. Some VPNs do not provide direct encryption, allowing attackers to gain information from the network.
- **Capacity**: Organizations need to foresee the number of users joining it in the future and then select the VPN accordingly.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **Cost**: An organization should consider cost as a factor while selecting VPNs.
- **Need**: The need for a VPN depends on the requirements of an organization. Requirements such as the need for remote employees to access the network or encrypted traffic rules must be considered. Each organization is different, and these differences will decide the appropriate VPN choice.
- **Vendor support**: The following are the two factors to consider in vendor support.
  - The first factor is the number of servers and their location. The VPN should be selected according to the location of the vendor server and the activities performed.
  - Does the vendor limit connections, use bandwidth throttling, or restrict service? VPNs that control bandwidth, reduce Internet speeds, or limit them in any way should not be used in an organization. Moreover, care should be taken while dealing with the protocols and services running in the network. The organization must decide whether the existing services and protocols running are actually required.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



VPN Core Functionality: Encapsulation

Encapsulation is the method through which protocols have separate functions to communicate among each other by hiding the data. Data vulnerability increases if the data do not pass through a secure channel. When data are transmitted using VPN tunneling, the data are encapsulated to ensure security. Encapsulation relies on various technologies and protocols such as GRE, IPsec, L2F, PPTP, and L2TP.

The packets sent over a VPN are enclosed within another packet (encapsulation), which has a different IP source and destination. Concealing the source and destination of the packets protects the integrity of the data sent. The VPN tunnel acts as a path between the source and destination. To send the encapsulated data securely, it is necessary to establish a tunnel. All the data packets travelling through the tunnel are encapsulated at the source point and de-encapsulated at the destination point. To send the data to the destination point, a tunnel data protocol is created. The information in the data packet is called a payload. The tunnel data protocol encapsulates the payload within the header containing the routing information. Once the server receives the payload, it discards the header, de-encapsulates the payload, and sends it to the destination.

All data packets transmitted through a VPN network are encapsulated using a VPN base or a carrier protocol. The encapsulated data packet is then sent through the tunnel and later de-encapsulated at the receiver's end.

For example, a TCP/IP packet encapsulated with an ATM frame is hidden within the ATM frame. Upon receiving the ATM frame, the encapsulated packet is de-encapsulated to extract the TCP/IP packet.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

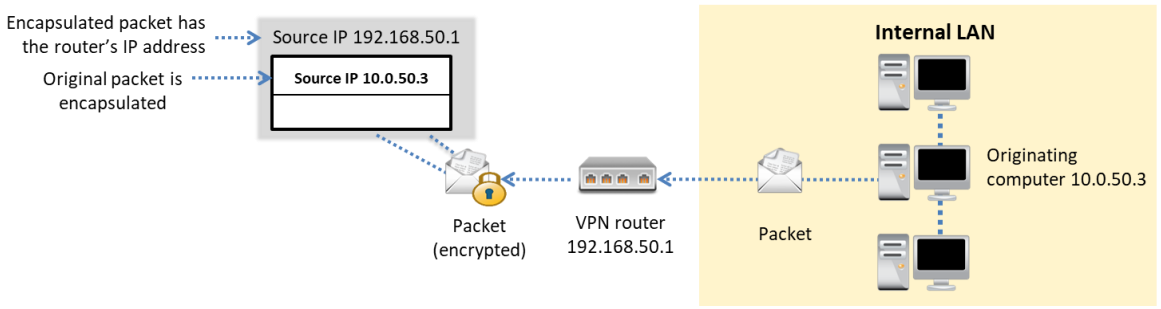


Figure 5.79: VPN encapsulation

The main goal is to provide an extra layer of security to each packet travelling across the Internet. These protocols define the way packets are sent and received by the ISP.

Types of VPN Tunneling

- **Voluntary tunneling:** In voluntary tunneling, the client machine sets up a virtual connection to the target tunnel server. Voluntary tunneling can be setup only when there is an existing connection between the client and server.
- **Compulsory tunneling:** In compulsory tunneling, the client machine is not the tunnel end point. A remote-access server configures and creates the tunnel. A dial-up access server acts as the tunnel end point.

Advantages of VPN Tunneling

- VPN tunneling allows the deployment of a VPN in a public network.
- It is a cost-effective method, as a dedicated network is not required.

The following are the VPN encapsulation protocols:

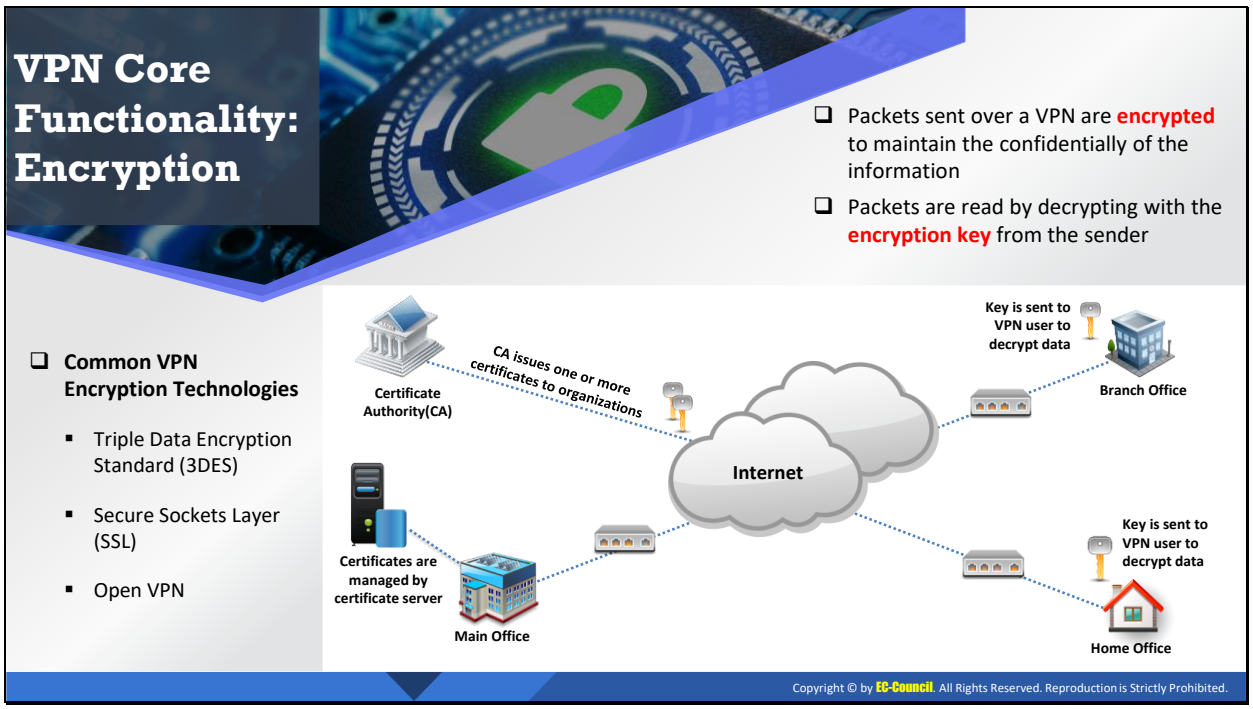
- **Point-to-Point Tunneling Protocol (PPTP):** This protocol allows multiprotocol encryption and encapsulates the IP header that is directed across the Internet. Used in both remote and site-to-site VPN connections, PPTP manages tunneling using a TCP connection and encapsulates PPP frames in IP datagrams.
- **Layer 2 Tunneling Protocol (L2TP):** L2TP permits multiprotocol encryption and data transfer across any medium supporting point-to-point delivery. L2TP is installed using the TCP/IP protocol. Encapsulation uses L2TP and consists of the following two layers.
  - **L2TP encapsulation:** The PPP frame is encapsulated using an L2TP header and a UDP header.
  - **IPsec encapsulation:** The L2TP message after the first layer is encapsulated using IPsec, which encapsulates the security payload header, IPsec authentication trailer, and a final IP header.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **Secure Shell (SSH):** SSH is a connection-oriented service that uses public-key cryptography to authenticate a remote user. It includes the following two types of features:
  - Port forwarding
  - Secure tunneling
- **Socket Secure (SOCKS):** SOCKS enables clients to communicate with Internet servers through firewalls. SOCKS is employed on proxy servers.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



VPN Core Functionality: Encryption

A VPN uses encryption to provide an additional layer of security to data transmitted over the VPN. Encryption plays an important role when sensitive data in an organization are transferred over the Internet. All data that enter the VPN tunnel are encrypted, and decryption is performed as soon as the data reach the end of the tunnel. An encryption key is used in the process of encryption and decryption. Encryption disables monitoring, logging, or tampering of the data in an organization.

Encryption helps secure the data passing through the network. The sender encrypts the data passing through the network, and the receiver decrypts the data. No encryption is required on the communication link between a dial-up client and the internal service provider, as the process of encryption occurs between the VPN client and VPN server.

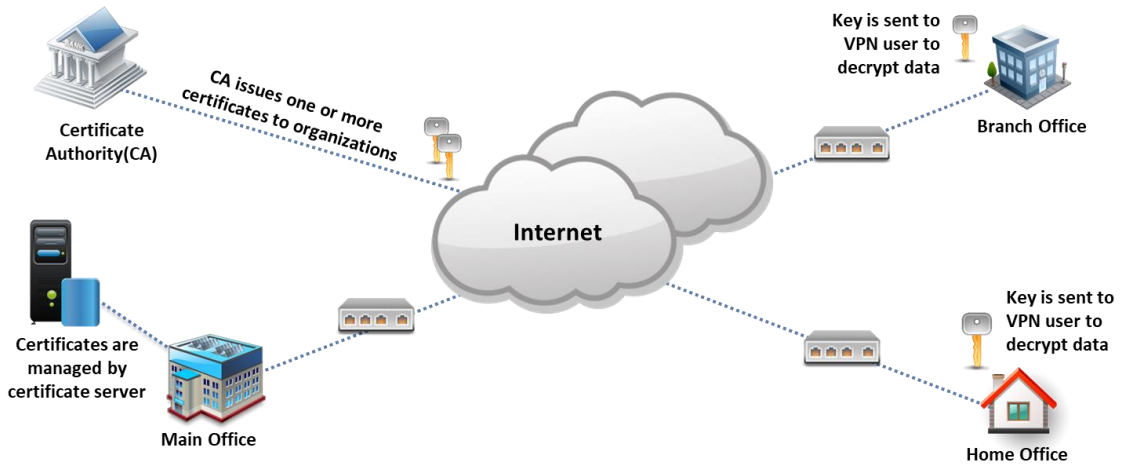


Figure 5.80: VPN encryption

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

In VPN encryption, both the sender and the receiver must have a common encryption key that is sent along with the data. If a packet traveling through the VPN connection does not have the keys associated with it, then it is of no use to the computer. There are many mechanisms to determine the length of the encryption key. The encryption of messages using the same key enables the easy interpretation of the encrypted data. The administrator can always select the encryption keys used for a connection.

In end-to-end encryption, the encryption occurs between the client application and server. IPsec is used with an end-to-end connection once a remote-access connection is established. IPsec works as follows:

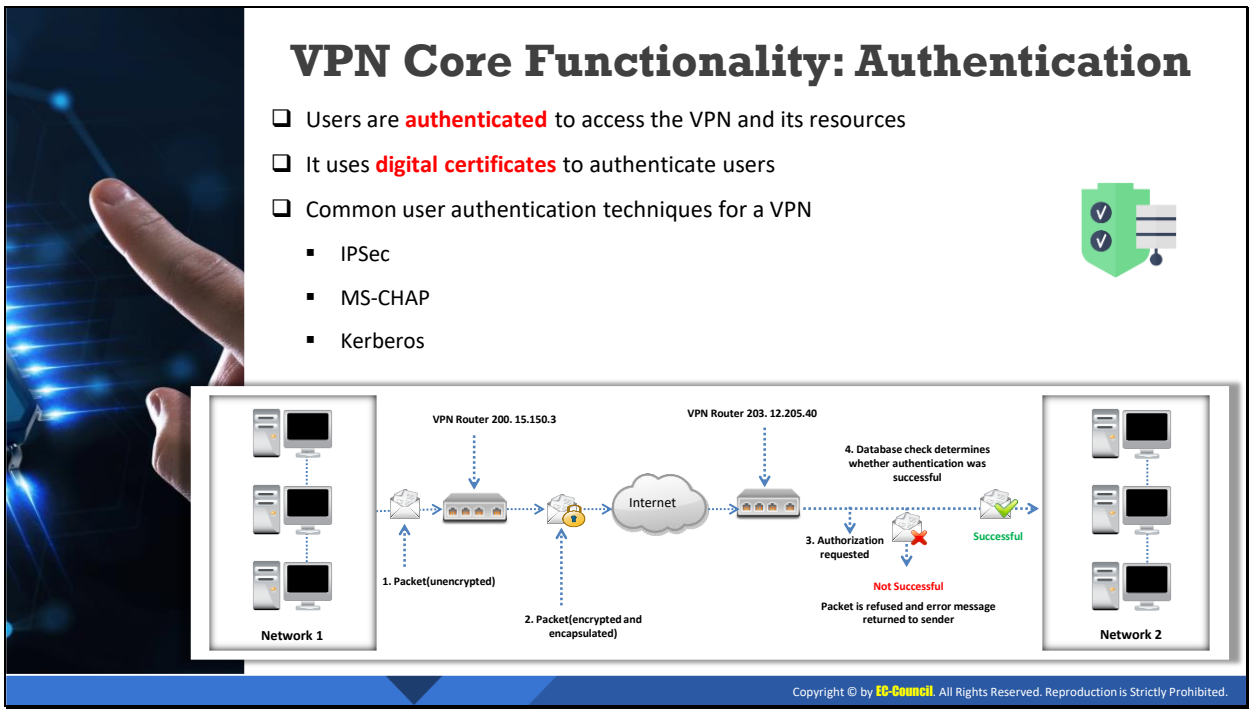
- A packet is encrypted using an encryption key. The key is known only to the sender and the receiver.
- An encapsulation header, a sub-protocol, conceals the sensitive information of the packets including the sender's identity.

VPN Encryption Technologies

- **Triple DES algorithm:** It is a 64-bit block of data that processes each block three times with a 56-bit key. 3DES eliminates the chances of breaking the encryption key.
- **Secure Socket Layer (SSL):** SSL is a secure technology that enables communication between a server and client. SSL technology enables the secure transmission of credit card numbers, login credentials, etc. over the Internet.
- **Open VPN:** It is an open-source VPN and works with the SSL protocol.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



VPN Core Functionality: Authentication

Authentication is an integral part of VPN technology, as the hosts receiving VPN communication must ensure the authenticity of the hosts initiating and sending the VPN connections. Users must be authenticated to access the VPN and its resources, and authentication uses digital certificates. A VPN employs the following three types of authentication.

- **User authentication:** In this type of authentication, the VPN employs the mutual authentication concept. The VPN server authenticates the VPN client to check whether the client has the permission to connect. Moreover, the VPN client can authenticate a VPN server for proper permissions.
- **Computer authentication with L2TP/IPsec:** Remote-access computers are authenticated for proper permissions using IPsec and L2TP/IPsec.
- **Data authentication and integrity:** All L2TP/IPsec packets sent are included with a cryptographic checksum based on the encryption key. Only the sender and the receiver know this checksum. This is to ensure that the data sent are not manipulated during transit.

Authentication Techniques Used in VPN

- **IPsec Family**
  - **Internet Protocol Security (IPsec):** All application traffic is secured using the IP network. IPsec conducts session authentication and data packet authentication for any two securely connected entities. IPsec ensures a secure connection between two networks or remote networks to the main network.
  - **Layer 2 Tunneling Protocol (L2TP):** This protocol initiates a connection between two L2TP connections. L2TP is always combined with IPsec to confirm security.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **Kerberos**

  Kerberos consists of a record of clients and their private keys. Only the client and Kerberos know the details of the private key, and Kerberos generates session keys that encrypt the messages between two clients.

- **Password Authentication Protocol (PAP)**

  PAP uses a cleartext authentication mechanism for authenticating users. It sends a username and password as per the NAS request. The NAS receives the username and password in cleartext, which implies that the NAS receives the details in an unencrypted form. This makes it easy for attackers to establish a connection with the NAS to acquire all the information.

- **Shiva Password Authentication Protocol (SPAP)**

  SPAP is a reversible encryption mechanism that is more secure than PAP. SPAP plays its role when a Shiva client attempts to access a server. However, this authentication mechanism is less secure than the Challenge Handshake Authentication Protocol (CHAP) or Microsoft CHAP (MS-CHAP).

- **Challenge Handshake Authentication Protocol (CHAP)**

  CHAP is more secure than PAP and uses an encryption authentication technique, which transmits a password representation instead of an actual password during the authentication process. The server sends a challenge message to the client to authenticate users. Users respond with a hash value created using a hash algorithm. The server then compares this hash value with its own calculation of the hash. If they match, then authentication is acknowledged. The remote client creates a hash of the session ID, challenge, and password. It uses the MD-5 one-way hashing algorithm.

- **Microsoft CHAP (MS-CHAP)**

  MS-CHAP uses a remote-access server to send a session identifier and a challenge string to the remote-access client. The client, in turn, sends an encrypted form of the identifier and challenge string to the server. This encrypted form is irreversible.

- **Extensible Authentication Protocol (EAP)**

  With EAP, the data for authentication are compared against an authentication database server. The EAP authentication protocol allows new plug-ins to be added at the client and server.

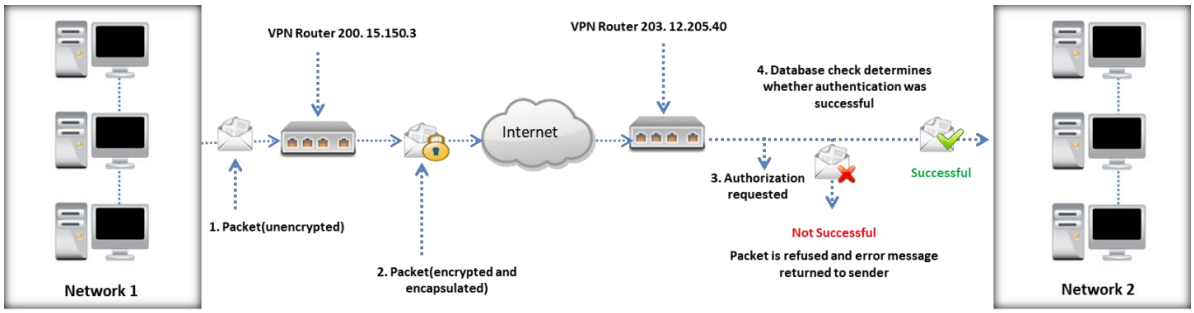
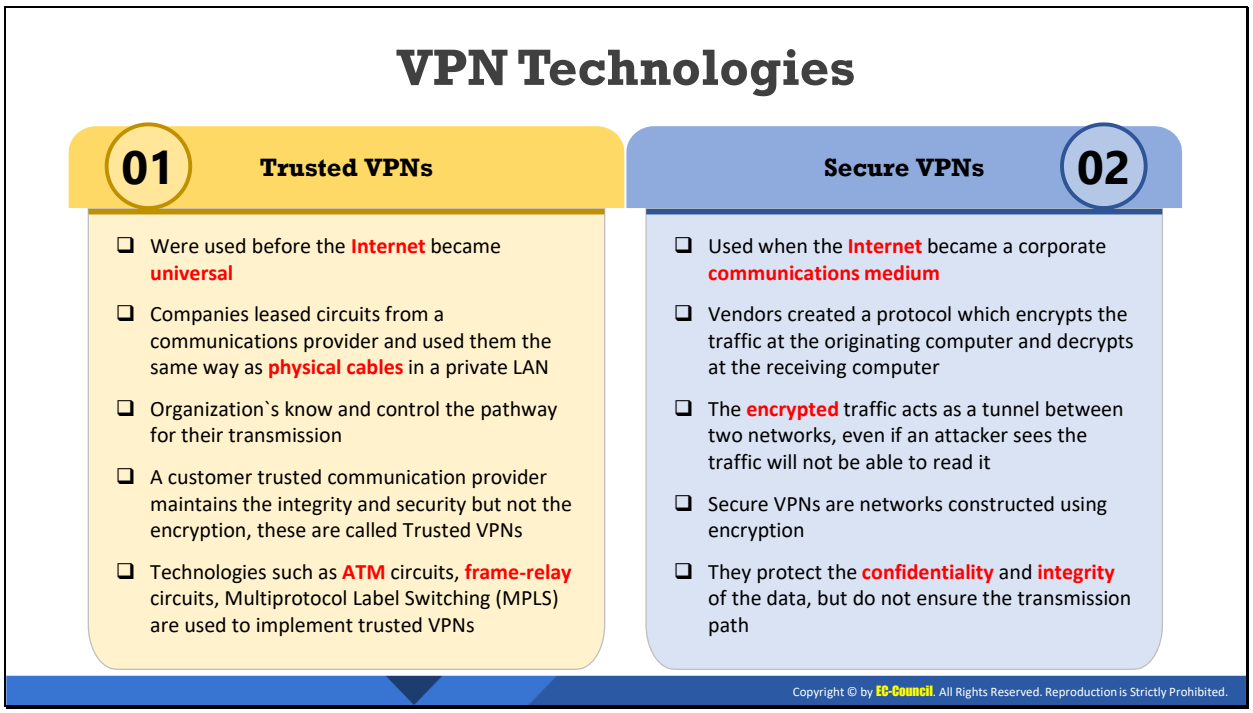
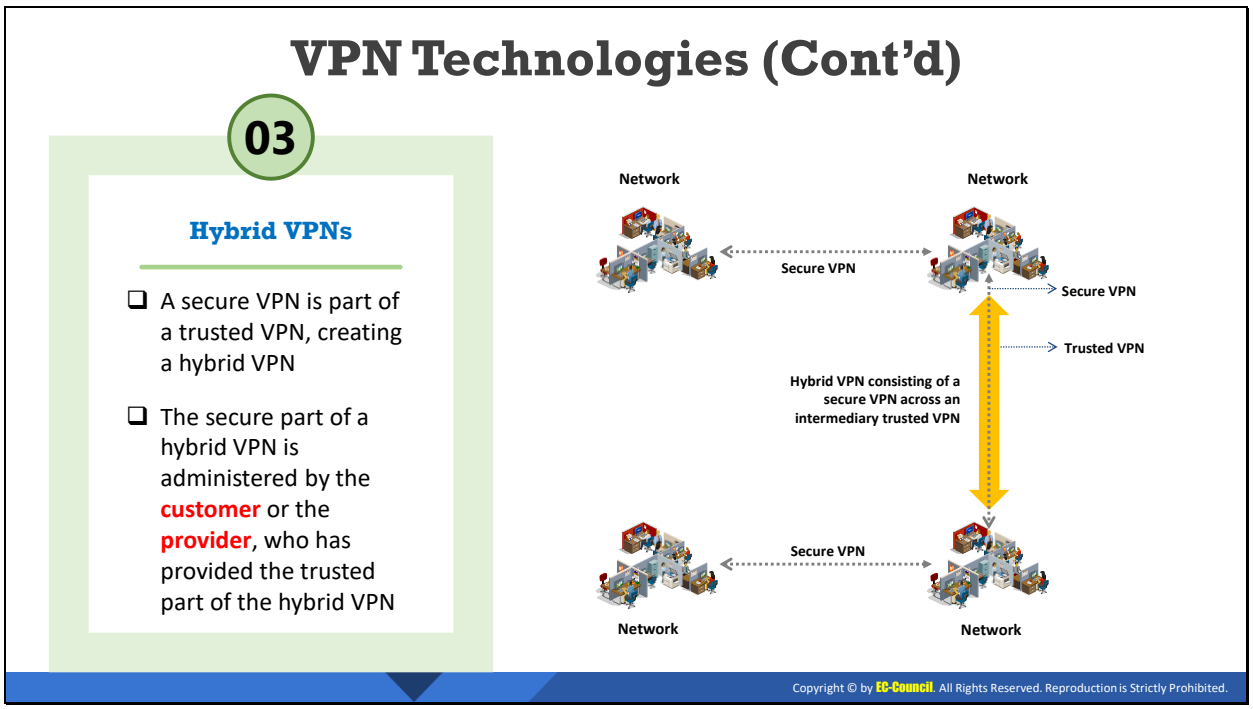


Figure 5.81: VPN authentication

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets





VPN Technologies

VPN technology enables organizations to connect mobile and remote users with network access and also to connect separate branches of the same organization to a single network. The following are common technologies used to deploy VPNs for secure data transmission.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Trusted VPN

Even before the popularity of the Internet, service providers provided customers with specific circuits that could not be used by anyone else. Companies leased circuits from a communications provider and used them in the same manner as physical cables in a private LAN. Organizations know and control the pathway for their transmission. This gave customers privacy and the ability to have their own IP addresses and policies. To provide security measures and avoid sniffing of the data, VPN providers are entrusted to maintain circuit integrity. This type of VPN is called a trusted VPN. The technologies used for implementing trusted VPNs over an IP network are Asynchronous Transfer Mode (ATM) circuits, frame relay circuits, and MLPS.

ATM and frame relay operate at layer 2 of the OSI model, and MLPS operates in between the data link layer and network layer. The requirements for a trusted VPN are as follows:

- Any changes in the path of a VPN can be made only by a trusted VPN.
- All routing and addressing methods need to be described before creating a trusted VPN.
- Only a VPN provider can inject, change, or delete the data in the path of a VPN.

Secure VPN

Secure VPNs are used when the Internet became a corporate communications medium. The main goal behind implementing a secure VPN is to ensure complete security of the data in transit. In a secure VPN, all the data packets sent through the tunnel undergoes an encryption process at one end of the tunnel and decryption process at the other end. This thwarts any attempt from an attacker to obtain data in transit. Secure VPNs protect the confidentiality and integrity of the data but do not ensure the transmission path. The main requirements for secure VPNs are as follows:

- All the data packets in the traffic are encrypted and authenticated before sending to the client.
- The client and server need to be in a mutual understanding before initiating the connection between each other.
- The security of the connection must be confirmed by unauthorized users.

Hybrid VPN

Hybrid VPNs are those with trusted VPNs as part of secure VPNs. They implement different network components of an organization simultaneously to confirm security at very low costs. A security professional takes extra time in differentiating between the data transfer among the trusted VPNs that are part of the secured VPNs. The secure part of a hybrid VPN is administered by the customer or the provider of the trusted part of the hybrid VPN. The main requirements for hybrid VPNs are as follows:

- There should be clear differentiation between the trusted VPN and secure VPN.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

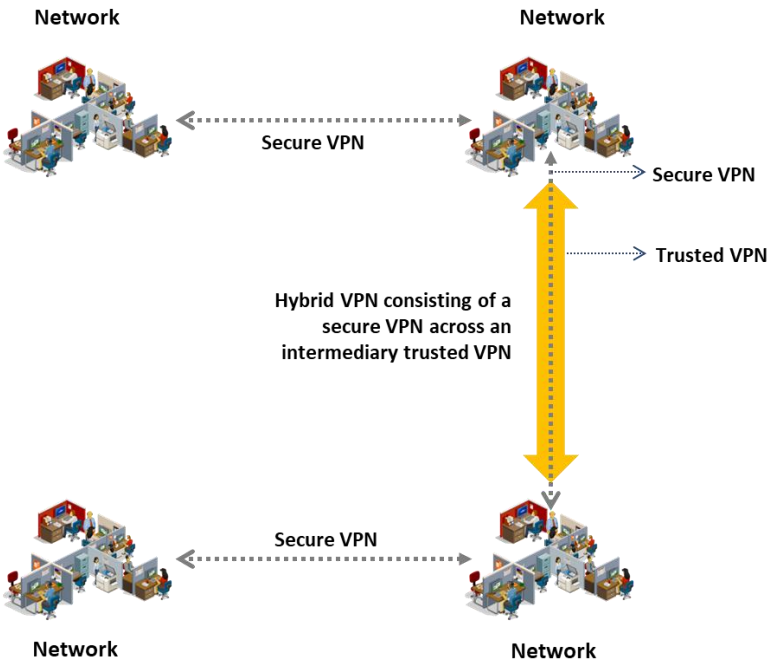
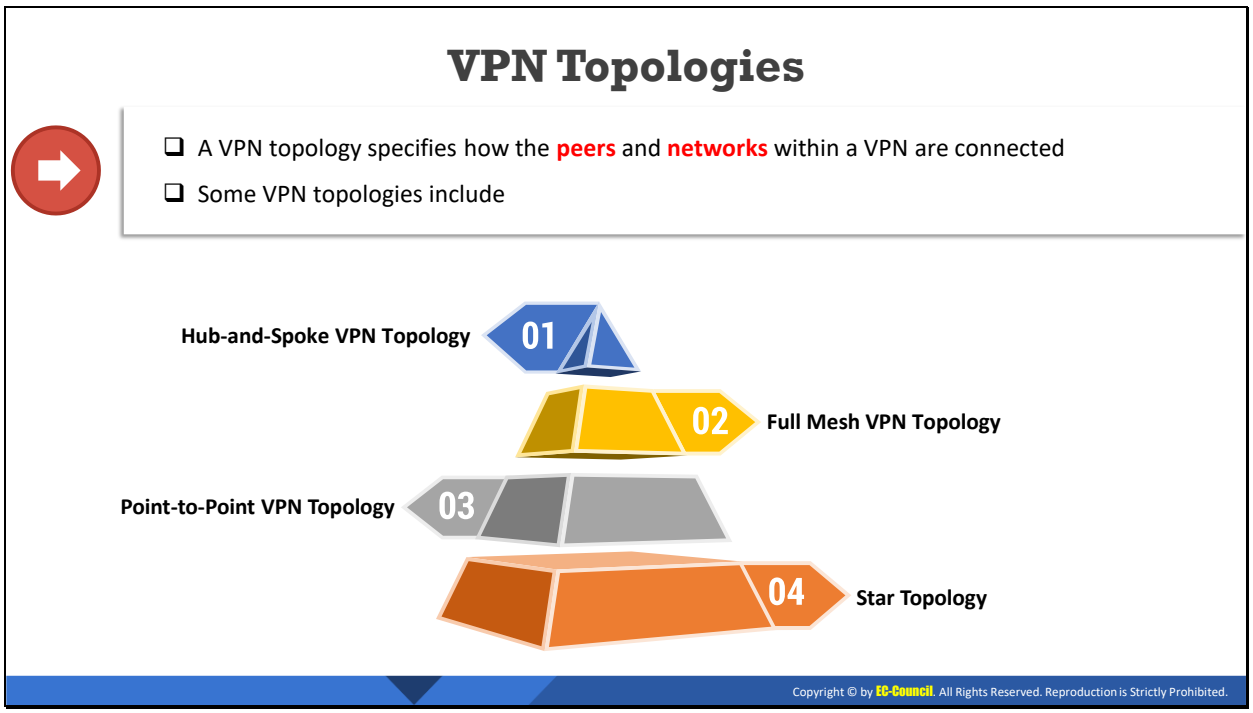


Figure 5.82: Hybrid VPN

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



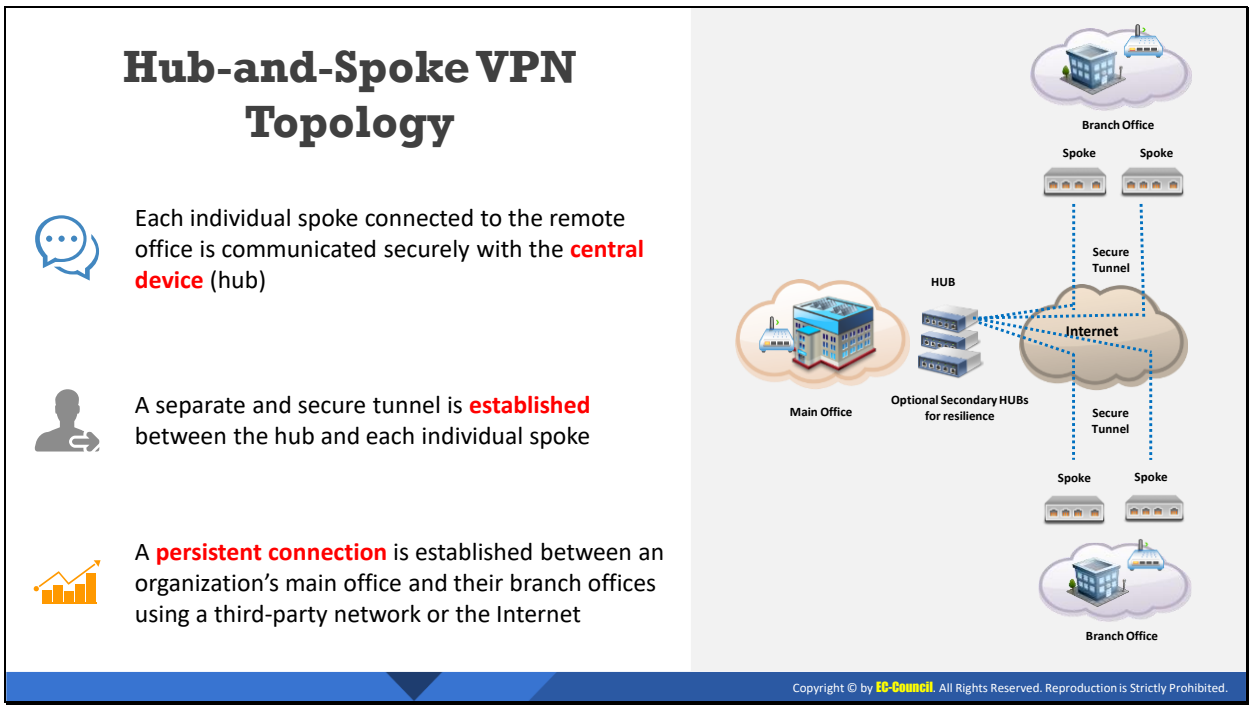
VPN Topologies

A VPN topology mainly deals with the specifications of how nodes in a network are connected and how they communicate with the other nodes. A VPN enables companies in a different networks to communicate with each other with data sharing. VPN topologies enable an organization to design the way they communicate with other networks. The following are the different VPN topologies:

- Hub-and-spoke
- Point-to-point
- Full mesh
- Star

It is important to note that the selection of topologies depends on the requirements of the organization. For example, a star topology is best suited in environments where the company needs to share information with another company located in a different network. A mesh topology is best suited for an intranet.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Hub-and-Spoke VPN Topology

In hub-and-spoke technology, the main organization is considered the hub, and its remote offices are considered the spokes. The spokes access the VPN through the hub. This topology is mainly used in banking and international organizations. The hub controls the following two types of communication:

- Communication between a spoke and hub
- Communication between spokes

This topology is used to represent an intranet VPN connecting an organization's main office to its regional offices. The hubs facilitate the sharing of large amounts of data. There are separate tunnels for data transfer between the hub and a spoke. All data transfers occur through the hub. The hub-and-spoke topology can become a multilevel topology depending on the growth of the network.

In a multi-site network, the central hub controls the data transfer or is considered the gateway for the remote sites to communicate with each other. For example, a cell-phone tower in an area is the hub, and all the mobile devices in and around the cell-phone tower are the spokes. A security professional must always thoroughly study the hub-and-spoke technology in their network.

Advantages

- The hub-and-spoke topology is relatively less expensive and easy to repair when one of the spokes fails.
- Bonded circuits between the hub and a spoke increase the flexibility of the network.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- This topology offers enhanced security, as each device in the network is separated from others through a single connection to the hub.
- This topology provides high performance, centralization, and simplicity.

Disadvantages

- Any issue in the hub can affect the connection between the hub and a spoke and the connection between different spokes.

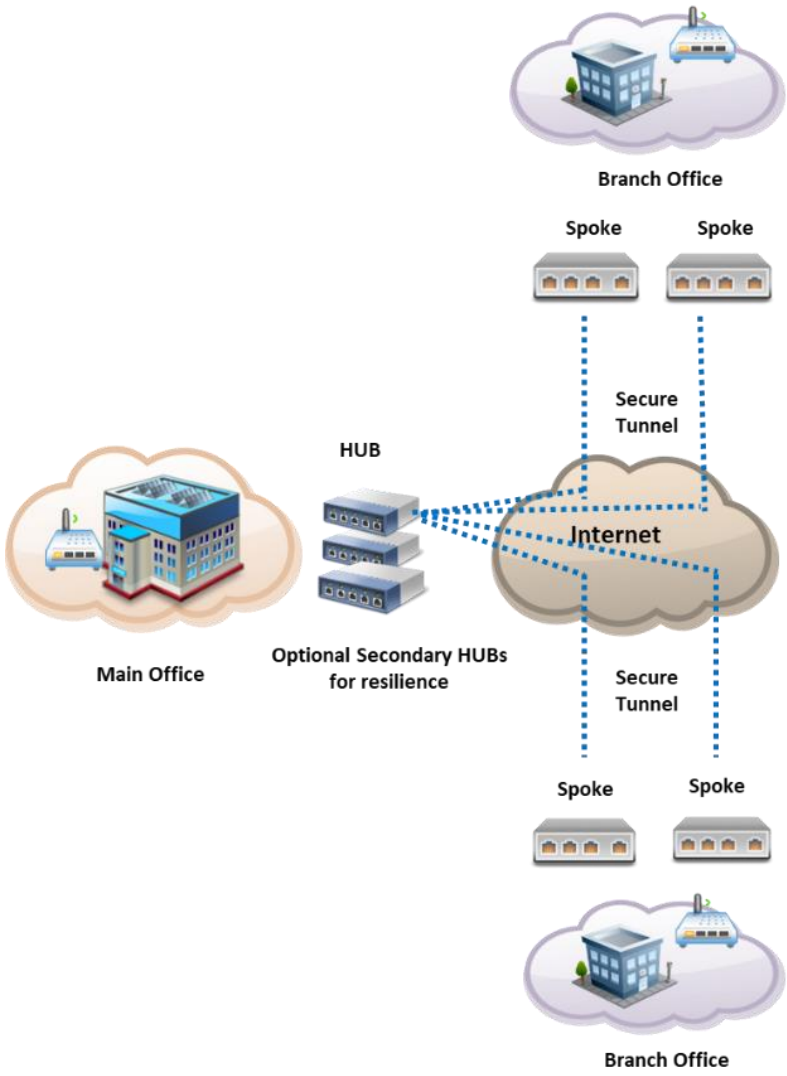


Figure 5.83: Hub-and-spoke VPN topology

The figure clearly illustrates the hub-and-spoke topology. In the figure, each spoke at the branch offices establishes a secured connection with the hub at the main office. These secured connections are established across the Internet. The main office can have more than one hub at a time, but only one hub is used to connect to each spoke. The other hubs are kept as backup hubs for flexibility.

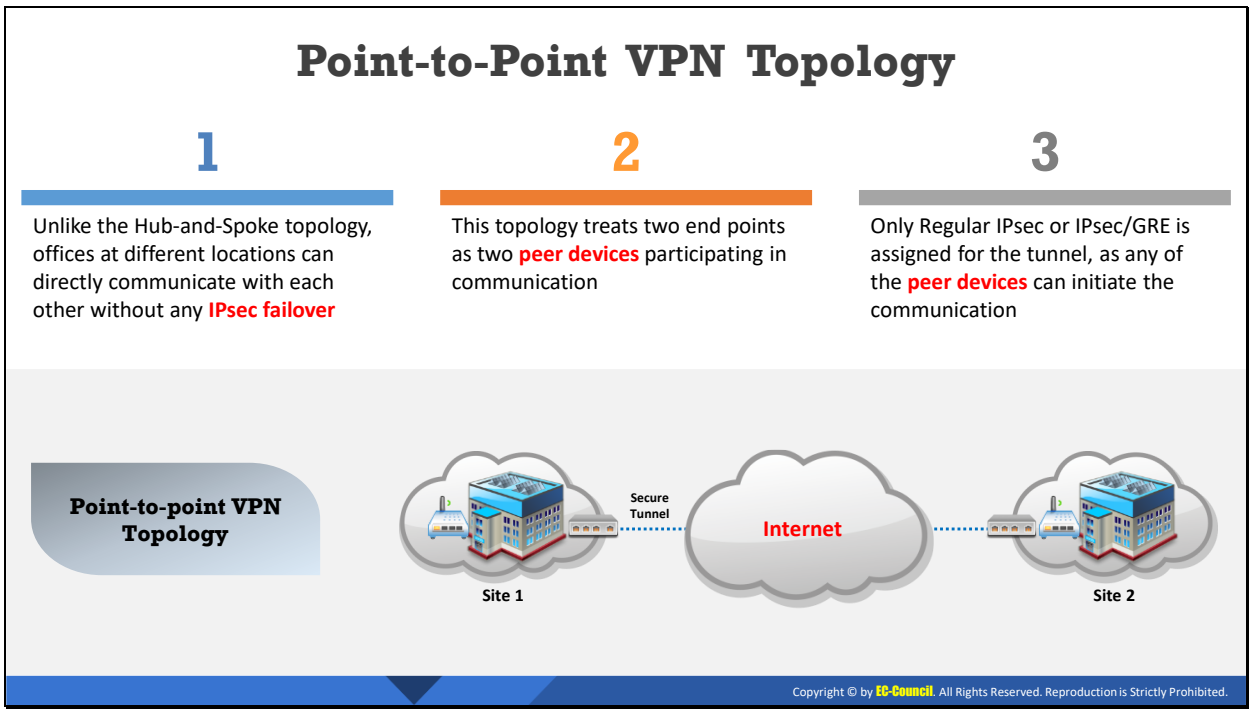
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

This topology works well if the traffic is between the hub and spoke, rather than between spokes or remote sites. This is because traffic between two spokes needs to pass through the hub before being forwarded to the respective spoke. This increases the chance of a bottleneck at the hub due to increased spoke-to-spoke connections. All IPsec technologies can be used in this topology.

If the hub faces any connection issue, IPsec failover transfers the connection to a backup hub to be used by all spokes. It is possible to configure multiple hubs as the main hub.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Point-to-Point VPN Topology

In a point-to-point topology, any two end points are considered as peer devices that can communicate with each other. Any of the devices can be used to initiate the connection. Unlike a hub-and-spoke topology, offices at different locations can directly communicate with each other without any IPsec failover. The IPsec technology assigned can be either IPsec or IPsec/GRE.

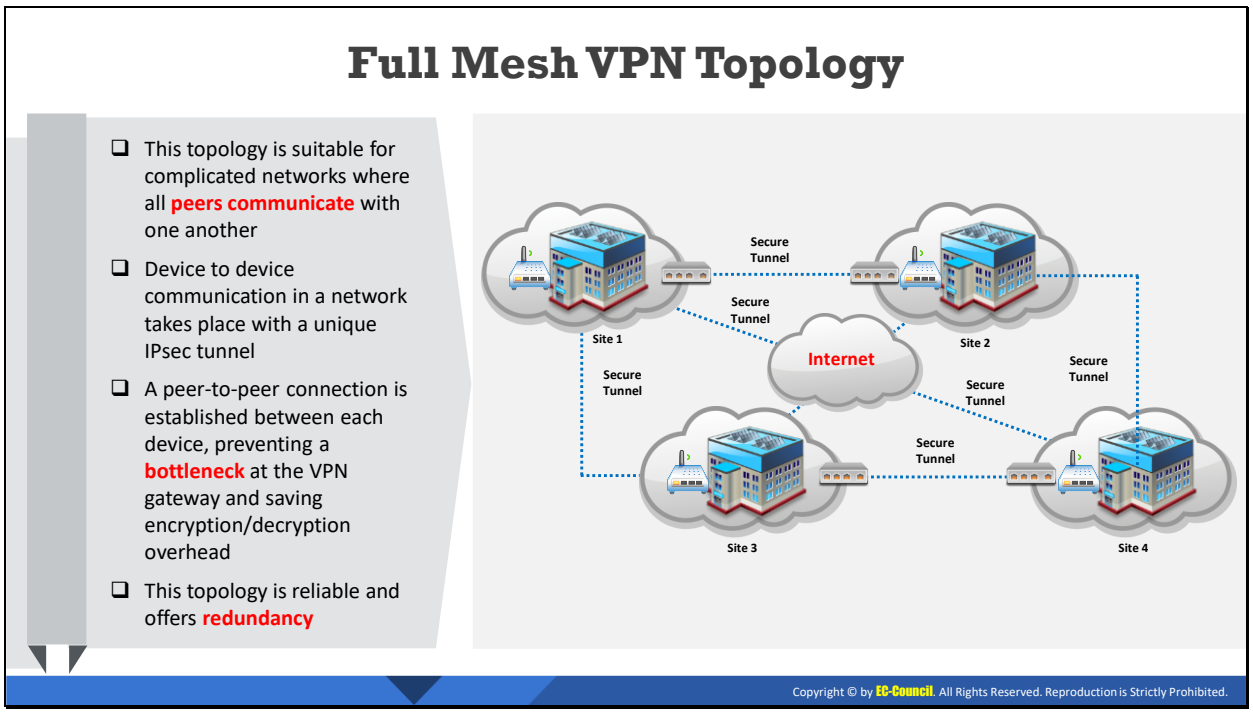
Regular IPsec point-to-point VPNs are commonly configured and known as extranets. This is where a connection is established between a device in a regularly managed network and an unmanaged device in the service provider's network.

The major features of the point-to-point topology are as follows:

- Easy routing of data, which need to pass through only one router
- Optimal routing between customer sites
- Introduces encryption and authentication to confirm the integrity of packets in transit
- Uses a tunneling process to capture data packets with normal IP packets for forwarding over IP-based networks

Figure 5.84: Point-to-point VPN topology

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Full Mesh VPN Topology

In a fully meshed VPN network, all peers can communicate with each other, making it a complex network. This topology is suitable for complicated networks where all peers communicate with one another. This topology allows all the devices in the network to communicate directly with each other through an IPsec tunnel. A peer-to-peer connection is established between each pair of devices, preventing a bottleneck at the VPN gateway and saving encryption/decryption overhead. A fully meshed VPN can implement normal IPsec, IPsec/GRE, and GET VPN technologies.

Advantages

- Any failure on one of the devices does not affect the entire network.
- It is very reliable and offers redundancy.
- It prevents any kind of block at the gateway.

Disadvantages

- It increases the number of devices connected to the network, making it difficult to manage.
- There are chances of redundancy in network connections.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

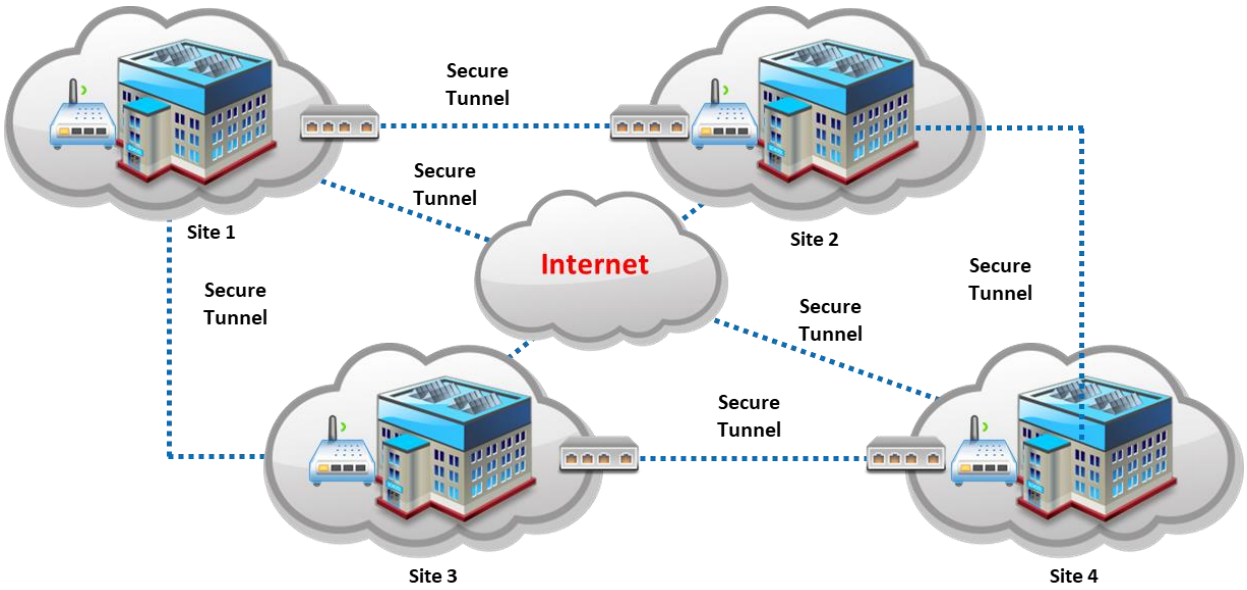
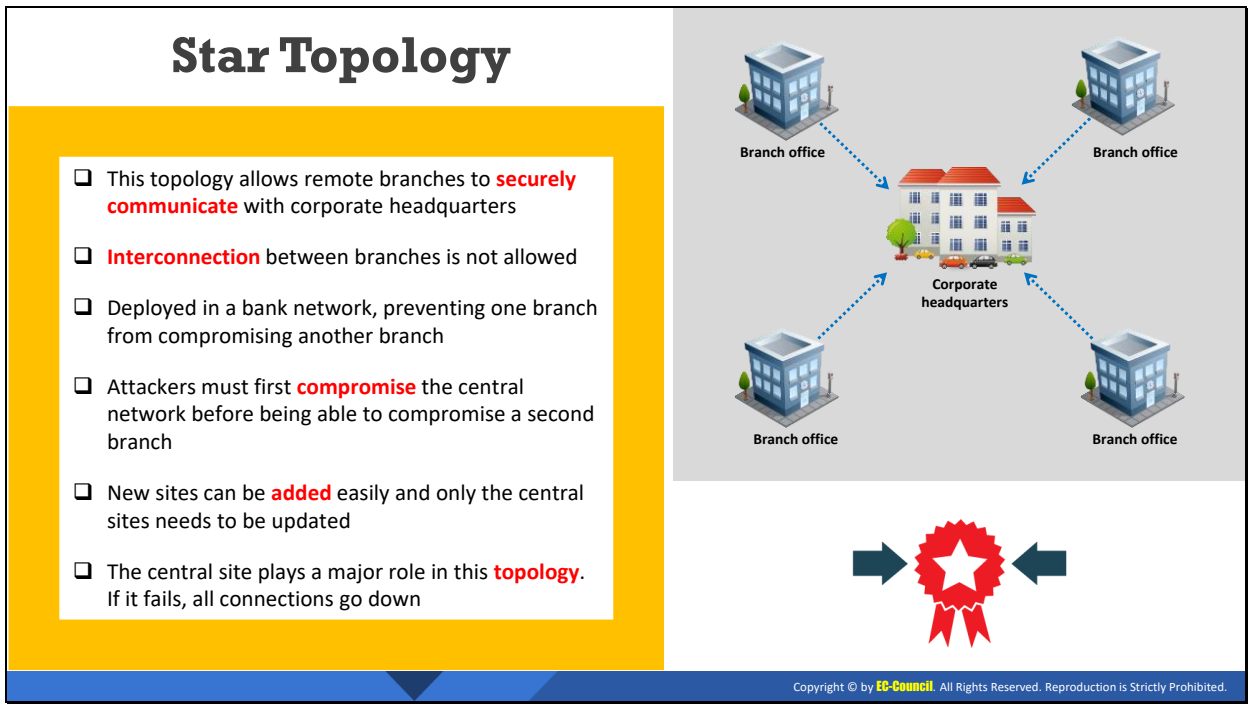


Figure 5.85: Full mesh VPN topology

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Star Topology

This is the most commonly used topology in organizations. In this topology, all the remote offices communicate with the corporate office, but communication between the remote offices is denied. Each device on the network is connected to a central hub that manages the traffic through the network.

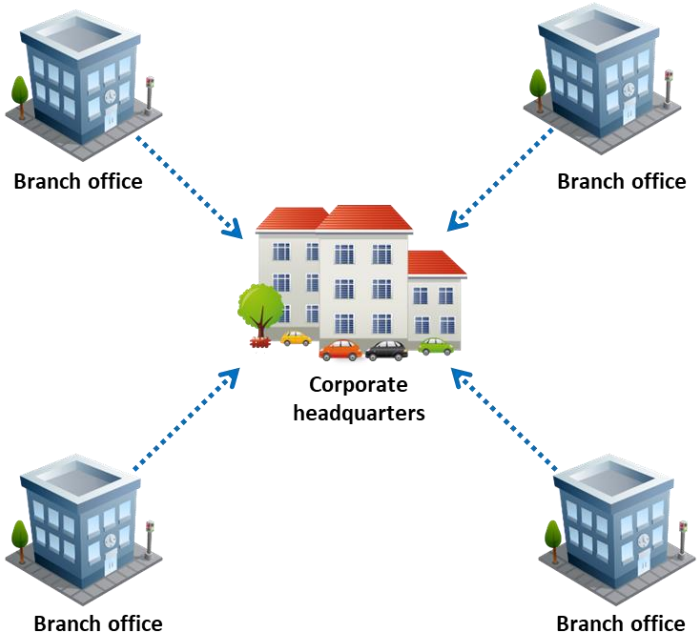


Figure 5.86: Star topology

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

In the figure, all the branch offices can communicate with each other through the corporate headquarters. However, in this topology, no two branch offices can initiate a separate communication, as these are allowed only through the corporate network.

Advantages

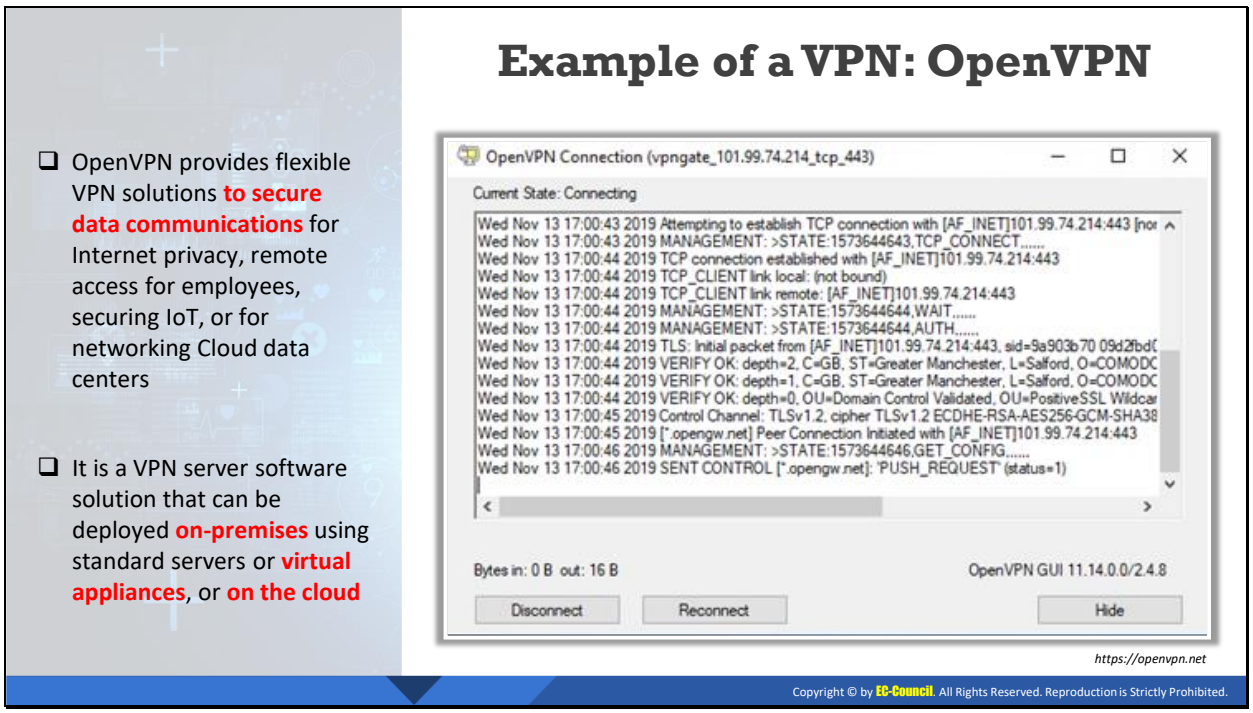
- It is most suitable for financial infrastructure, as a compromise on one system does not compromise another branch without detection.
- Any attack on branch offices can be performed only through the main branch. Any manipulation in the network can be easily detected by security professionals.
- It is easy to add and remove new branch offices to the main office without affecting the neighboring sites. However, it is mandatory to update the main site regarding the addition or removal of sites.

Disadvantages

- Any failure in the central site affects the communication of all other sites.
- No two sites can communicate with each other directly.
- Adding more sites to the network can affect the capacity of the main site.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Example of a VPN: OpenVPN

Source: *https://openvpn.net*

OpenVPN provides flexible VPN solutions to secure data communications for Internet privacy, remote access for employees, securing IoT, or for networking cloud data centers. It is a VPN server software solution that can be deployed on premises using standard servers or virtual appliances; it can also be deployed on the cloud.

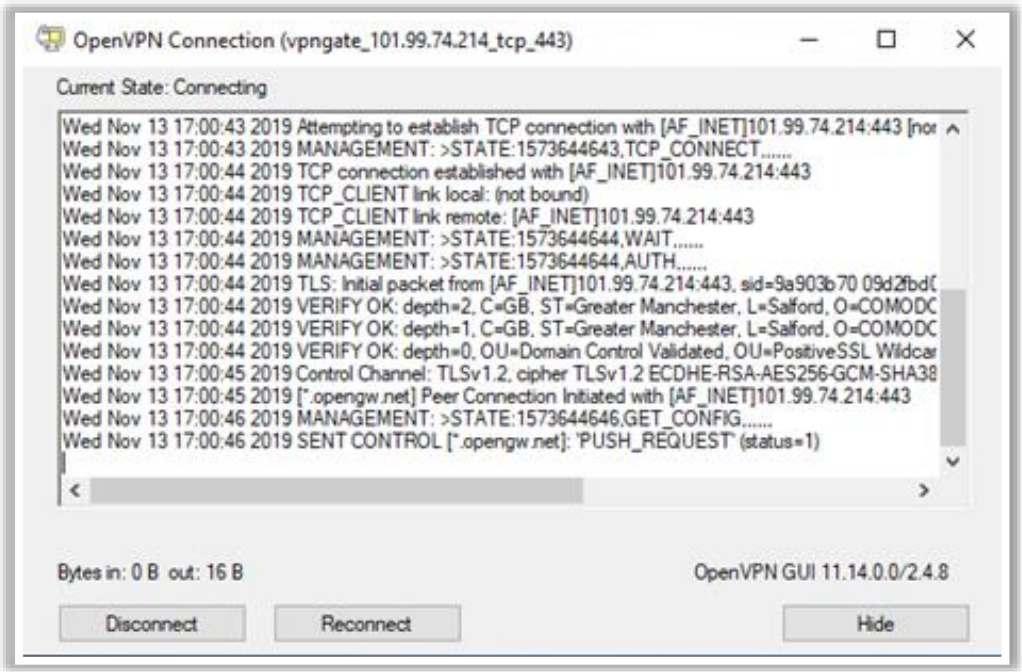
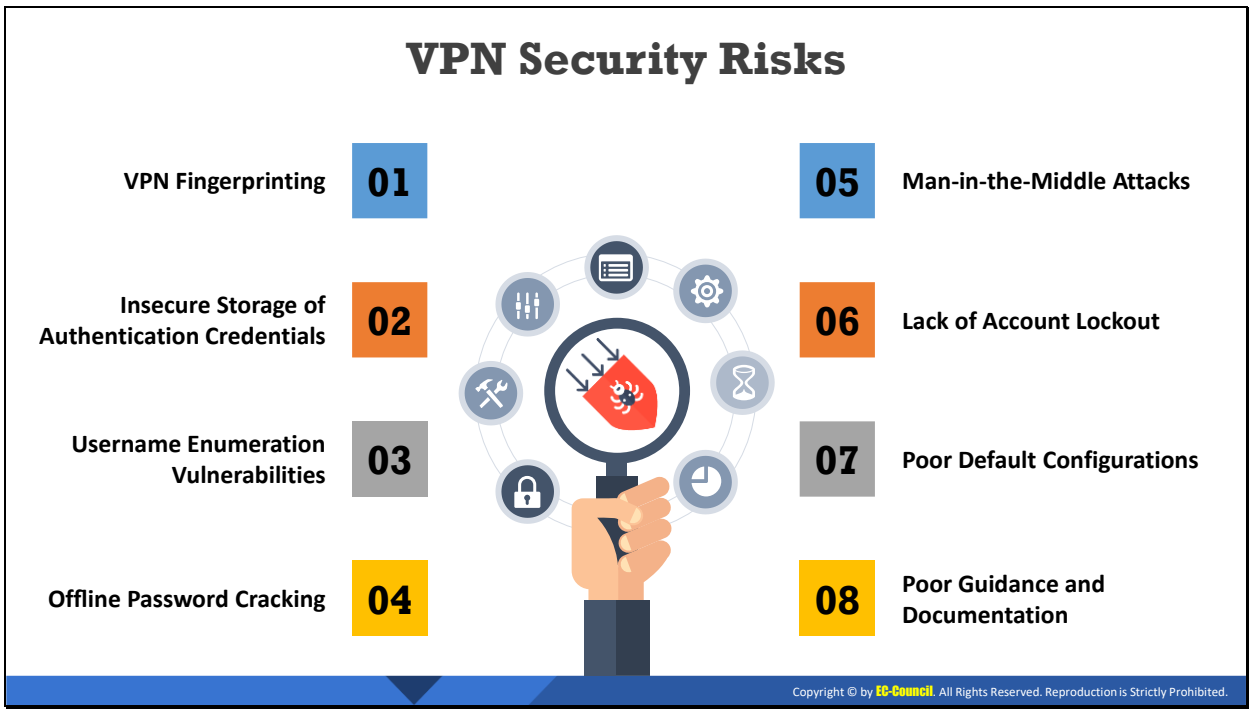


Figure 5.87: Screenshot of OpenVPN

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



VPN Security Risks

Discussed below are the various VPN-related security risks.

- **VPN Fingerprinting**

  The VPN fingerprinting technique allows the attacker to access useful information such as the type of connections implemented, devices used, and OSes deployed. Some systems, such as Cisco PIX and Nortel Contivity, potentially reveal crucial data such as the general type of devices deployed for building the network, while other systems display software version details.

- **Insecure Storage of Authentication Credentials**

  Certain security issues occur if the credentials are not stored and protected appropriately. These security issues are due to an insecure method of storing authentication credentials by VPN clients.

  The following are common VPN issues with authentication and credentials:

  - Storing the username unencrypted in a file or a registry
  - Storing the password in a scrambled form
  - Storing credentials in plaintext in memory
  - Weak registry or file permissions for stored credentials

- **Username Enumeration Vulnerabilities**

  Many remote-access VPNs use the IKE aggressive mode with a pre-shared key authentication method. The client sends an IKE packet to the VPN server, which

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

responds using another IKE packet. These packets contain several payloads; the identity payload contains the username, and the hash payload contains the password.

An attacker can confirm the difference between valid and invalid usernames from their computational differences. Furthermore, an attacker can guess the correct password using the IKE aggressive mode and easily uncover the hash from the VPN server. This hash can be used with a brute-force attack to obtain the password.

- **Offline Password Cracking**

  Offline password cracking is one of the most common flaws of a VPN. An attacker can crack a password offline by gaining access to the password hashes. Once the attacker obtains the user credentials, they can easily gain hash access from the VPN server. Simple passwords containing simple words can increase the frequency of password cracking.

- **Man-in-the-middle Attacks**

  Attackers may use insecure authentication protocols such as IKE to perform man-in-the-middle attacks on a VPN. In this type of attack, an attacker intercepts the communication between the client and server and obtains the client's authentication to the server. Man-in-the-middle attacks occur during data transfer through the VPN and allow an attacker to intercept, insert, delete, and modify messages; reflect messages back to the sender; replay old messages; and redirect messages.

- **Lack of Account Lockout**

  The main aim of using the account lockout feature is to restrict the number of login attempts to a certain limit. If a user keeps attempting to login beyond the limit, the account is automatically locked out. This feature prevents password cracking attacks such as brute forcing and dictionary attacks. Attackers can take advantage of the lack of an account lockout feature to gain account credentials, and the lack of such a feature reduces the security of the account.

- **Poor Default Configurations**

  Almost all organizations have an automated configuration setup. However, if the organization uses the default configuration for the VPN, attackers may exploit these default configurations to compromise the security of the VPN. The default configurations support many ciphers and modes, ESP, and AH. An attacker with access to the client machine can prompt the end user to use a weaker cipher, which will make the attack easier. The end user may not notice that the cipher and configuration was changed, because the VPN will continue to function normally.

- **Poor Guidance and Documentation**

  Poor guidance can lead to security vulnerabilities in the configuration and implementation of a VPN. An incorrect implementation provides an opportunity for attackers to gain access to the VPN.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

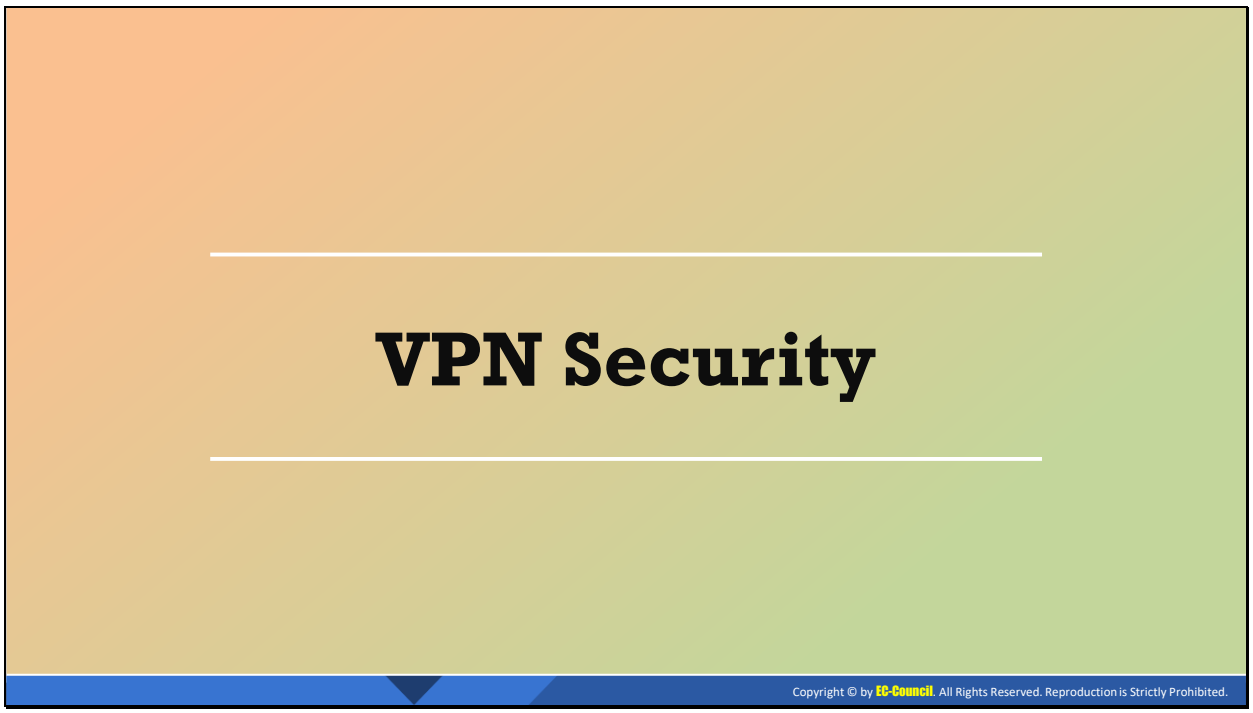
https://t.me/learningnets

The following are situations where this guidance is required:

- Using weak ciphers such as export-grade or single DES, which can be cracked easily
- Using weak key authentication techniques such as a pre-shared key with the IKE aggressive mode, which sends the username and vulnerable offline password to crack if a valid username is identified
- Choosing the AH protocol, which does not encrypt VPN traffic

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

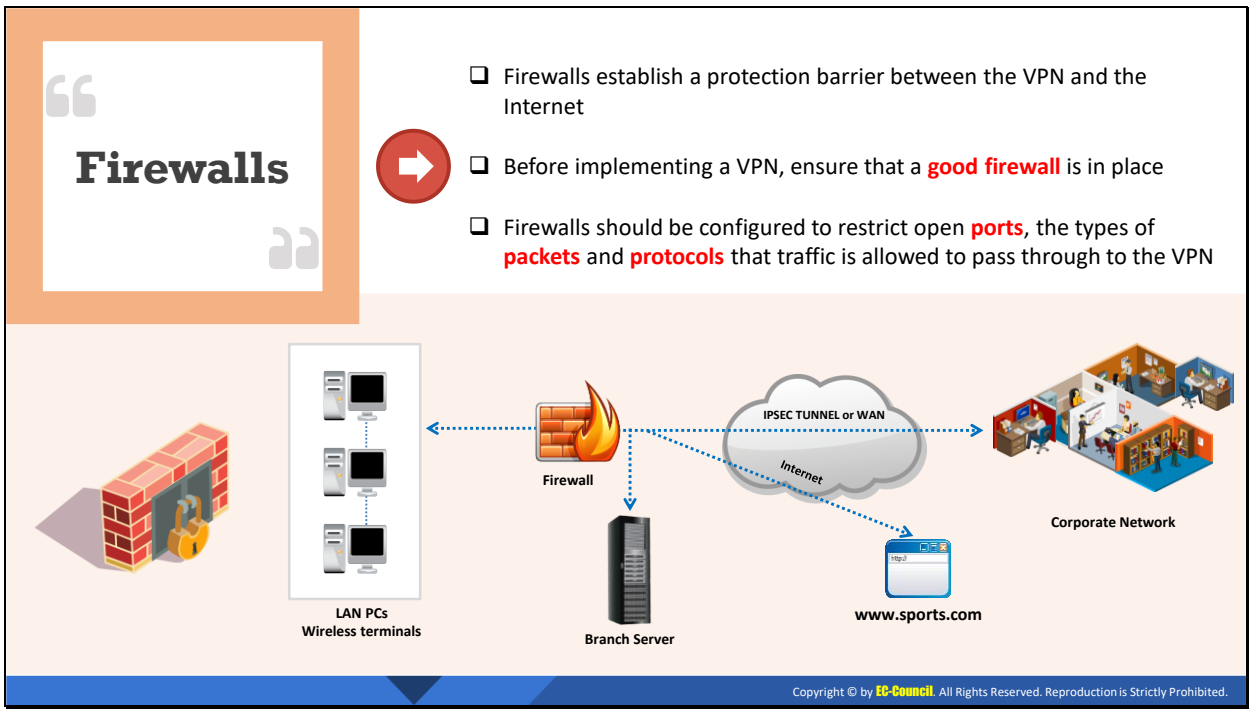
https://t.me/learningnets



VPN Security

This sub-section discusses various VPN security measures.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Firewalls

Firewalls establish a protection barrier between the VPN and the Internet. Before implementing a VPN, ensure that a good firewall is installed. A firewall can allow or deny the flow of data through the network. Firewalls should be configured to restrict open ports as well as the types of packets and protocols that are allowed to pass through to the VPN. They are also used to terminate VPN sessions. Firewalls generally help in protecting the network from attackers. Firewalls can be used in the following two ways with a VPN.

- The VPN server is connected to the Internet, and the firewall is located between the VPN server and intranet.
  - Here, packet filters are added to allow only VPN traffic to and from the IP address of the VPN server.
- A firewall is attached to the Internet, and the VPN server is located between the firewall and intranet.
  - Here, the firewall has input and output filters on the Internet interface to maintain traffic and the passage of traffic to the VPN server.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

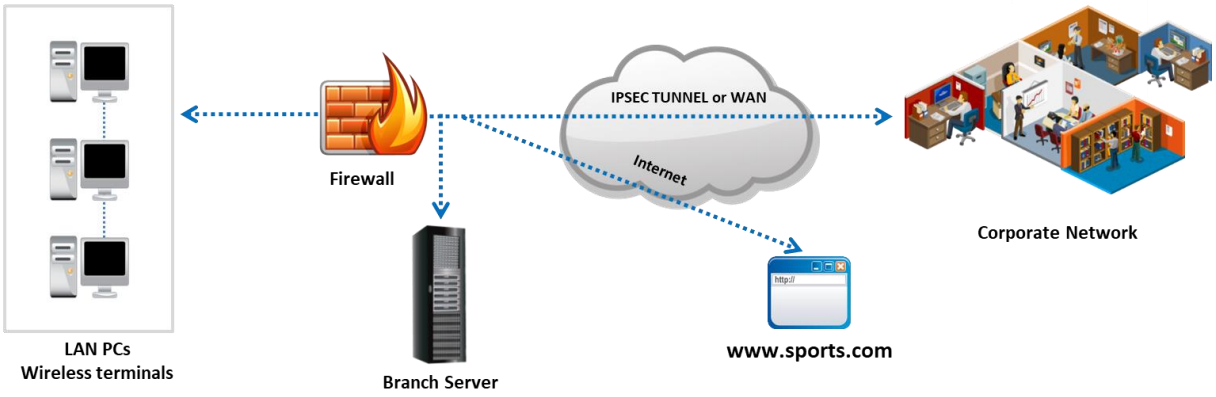
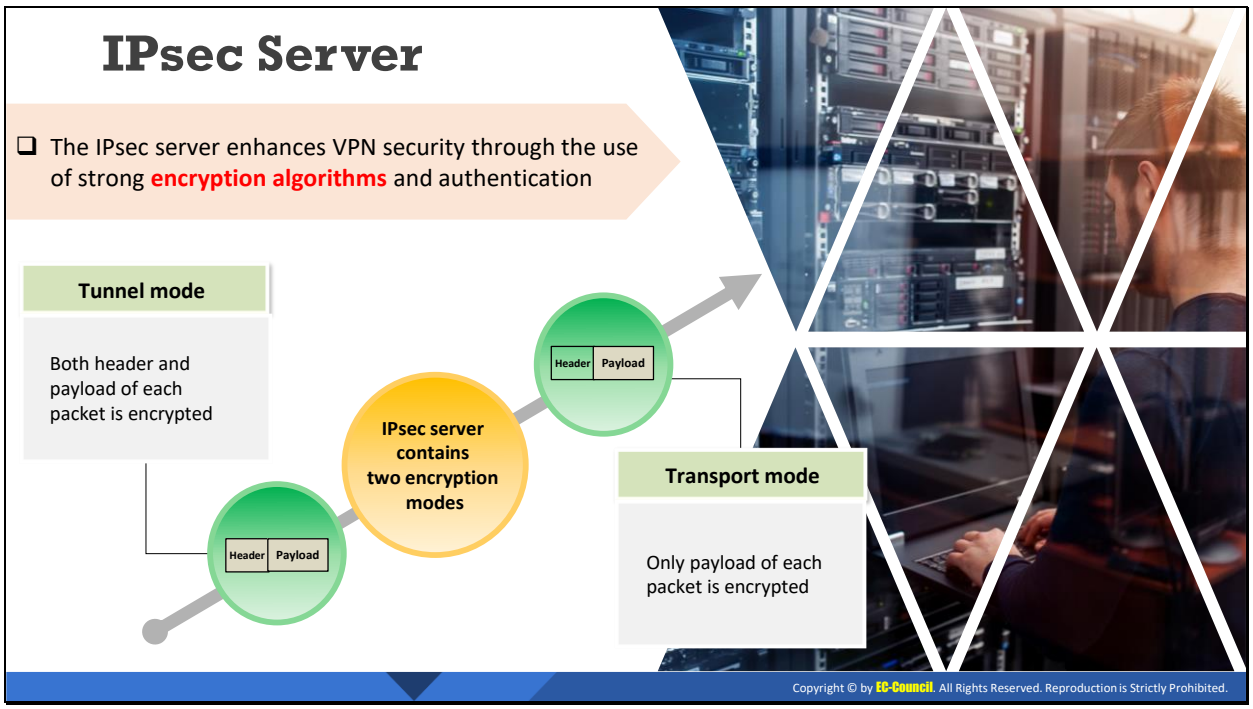


Figure 5.88: Depiction of a firewall in VPN security

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



IPsec Server

An IPsec server has the following two types of encryption modes.

- **Transport Mode**

  This is the default mode for an IPsec server. These are generally used for end-to-end communication between a server and a client. In the transport mode, IPsec encrypts the IP payload through an authentication header (AH) or encapsulating security payload (ESP) header. The IP payloads can be TCP segments (containing a TCP header and TCP segment data), UDP messages (containing a UDP header and message data), or ICMP messages (containing an ICMP header and ICMP message data).

  AH does not generally encrypt the data and only provides authentication, integrity, and anti-replay protection. From an AH, it is possible to read the data, but it denies any kind of change to the data. AH assesses the integrity check value (ICV) over the source and destination address; therefore, it cannot be utilized to traverse NATs. ESP traverses NATs as it does not utilize the outermost address value for ICV calculation. When AH and ESP are used together, then the ESP will be applied first, followed by AH, which authenticates the entire new packet.

  - **AH in transport mode:** The AH can be used individually or along with ESP. The AH header protects the entire packet. In the transport mode, a new IP header is not created before the data packet; rather, a copy of the original IP header is placed with minor changes in the protocol ID. Hence, it fails to provide complete protection to all the fields in the IP header. AH is recognized in the new IP header with an IP protocol ID of 51.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

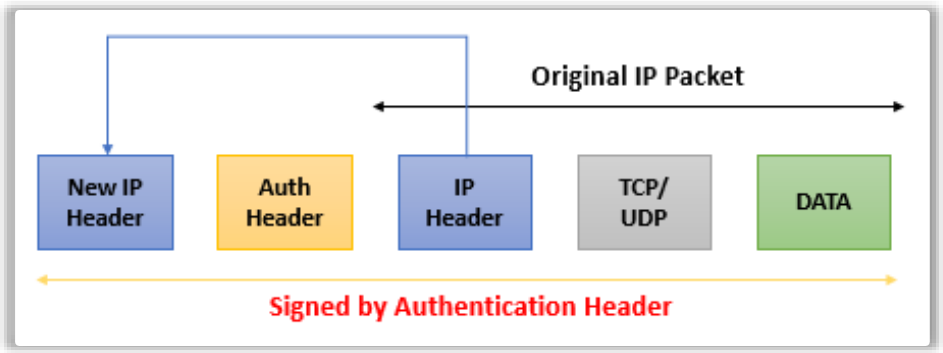


Figure 5.89: AH in the transport mode

- **ESP in transport mode:** The original IP header is moved to the front position. Placing the sender's IP header at the front position by making minor changes to the protocol ID will prove that the transport mode will not protect or encrypt the original IP header, and the ESP will be recognized in the new IP header with an IP protocol ID of 50.

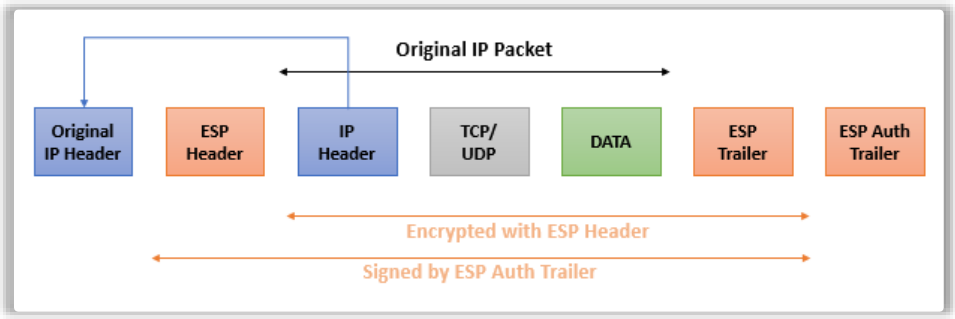


Figure 5.90: ESP in the transport mode

- **Tunnel Mode**

  In the tunnel mode, IPsec encrypts both the IP payload and the header to protect an entire IP packet by encapsulating it with an AH or ESP header and an additional IP header. This mode is useful for protecting traffic between different networks and is primarily used for interoperability with gateways.

  The tunnel mode of IPsec is generally implemented in configurations such as gateway-to-gateway, server-to-gateway, and server-to-server configurations. The IPsec tunnel mode is useful in protecting traffic while it is passing through untrusted networks.

  - **AH in tunnel mode**: The AH header can be used individually or along with ESP. It defends the entire packet. However, AH does not safeguard all the fields of the new IP header in case of some change in transit. Nevertheless, it safeguards everything that does not change in transit. AH is recognized in the new IP header with an IP protocol ID of 51.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

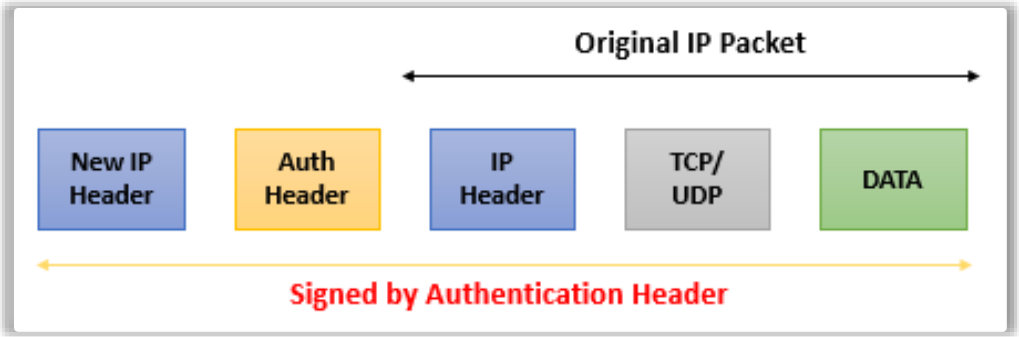


Figure 5.91: AH in the tunnel mode

- **ESP in tunnel mode**: ESP is recognized in the new IP header with an IP protocol ID of 50.

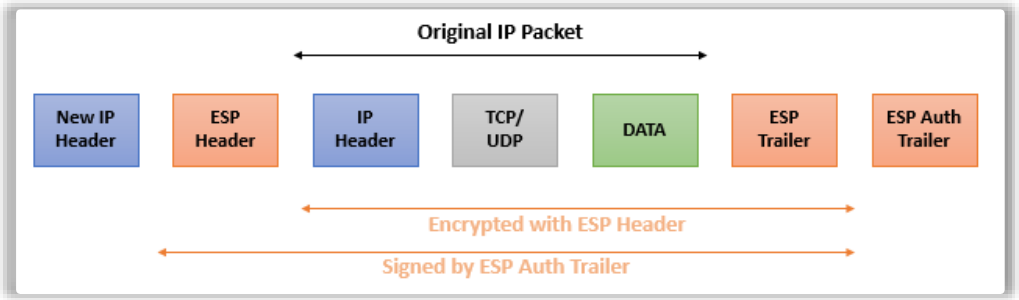
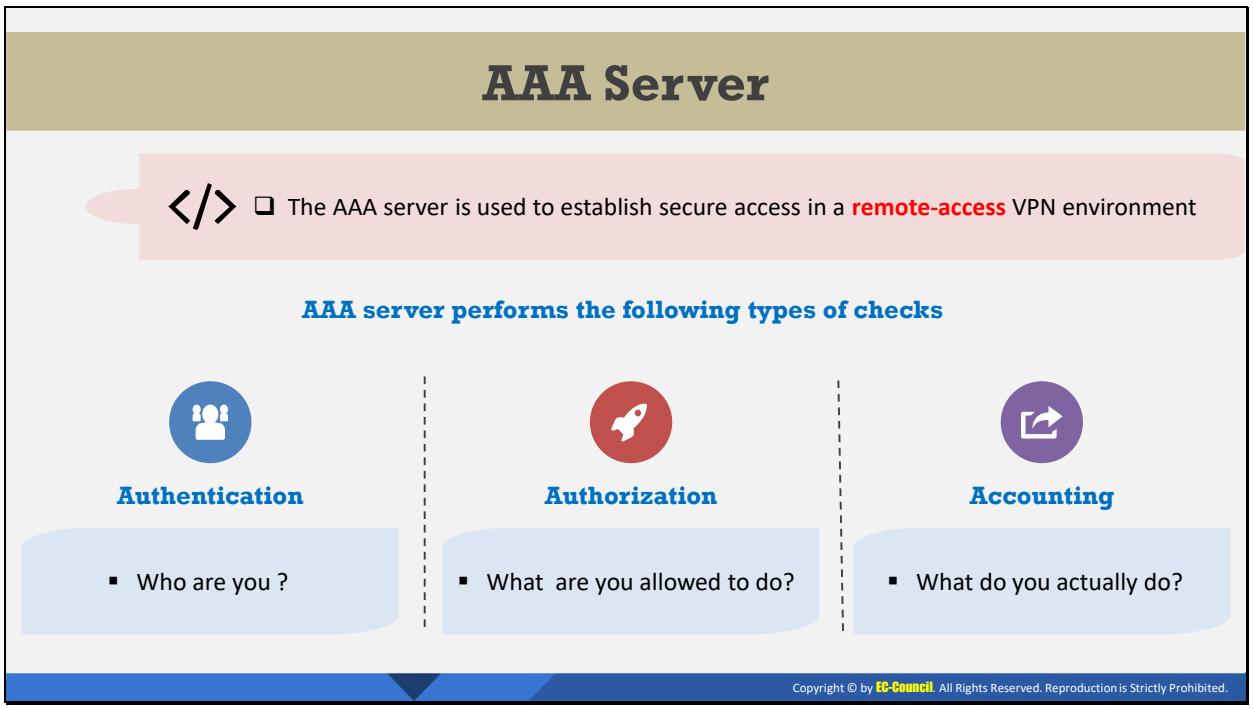


Figure 5.92: ESP in the tunnel mode

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



AAA Server

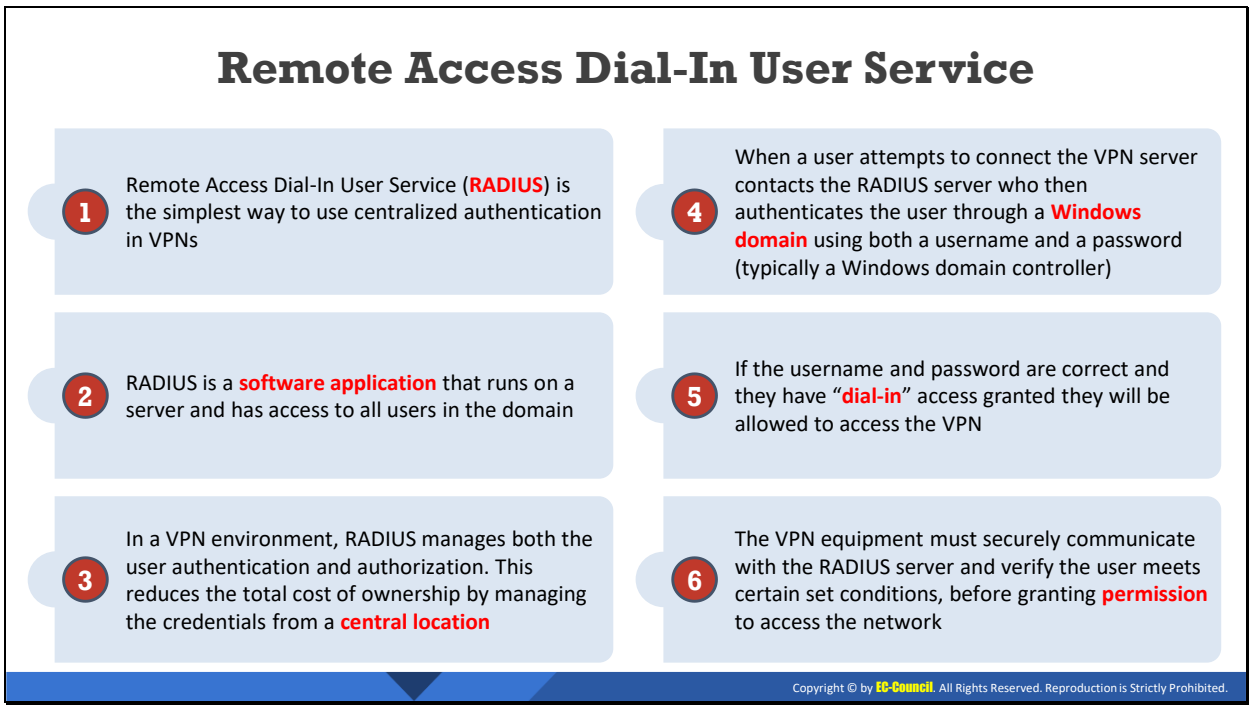
Authentication, authorization, and accounting (AAA) provides additional secure access in a remote-access environment. An AAA server provides users an extra layer of protection and control when compared to an access-control list (ACL) alone. An ACL enables outside users to access Telnet in the DMZ network. AAA grants permits to only a few users for accessing the application after proper authorization and authentication have occurred. This can be implemented using the following:

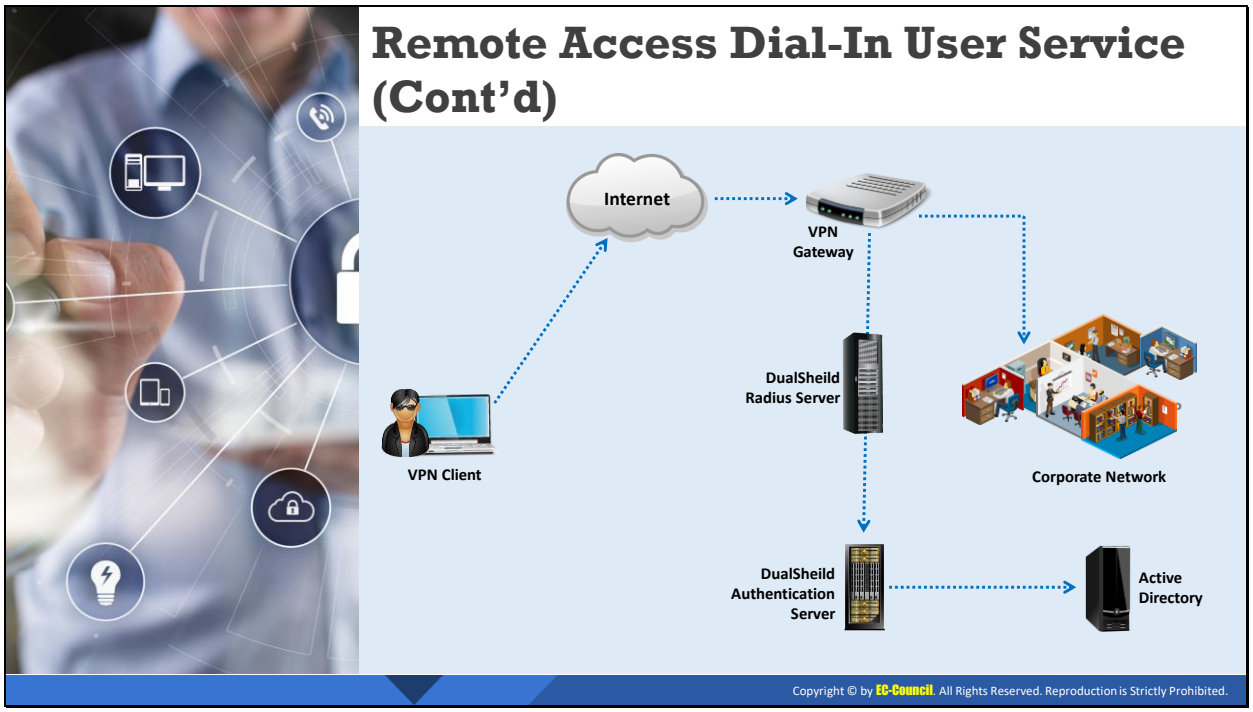
- **Who you are** (authentication) is established by verifying user credentials such as the username and password.
- **What you are allowed to do** (authorization) is verified to offer access controls such as management commands, network access, and VPN access.
- **What do you actually do** (accounting) refers to the type of traffic the users access through the VPN. This option tracks traffic that passes through the VPN and records all user activity.

The following are the authentication protocols used for an AAA server:

- RADIUS
- TACACS+
- RSA SecurID
- Windows NT
- Kerberos
- LDAP

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets





Remote Access Dial-In User Service

Remote Authentication Dial-In User Service (RADIUS) is the simplest method to use centralized authentication in VPNs. RADIUS is a client/server protocol that authenticates and authorizes dial-in-users to access the system or device. It is a software application that runs on a server and has access to all users in the domain. RADIUS maintains profiles in their databases that enable the remote servers to share the data as well as a centralized administration of data.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Companies using a VPN network implement RADIUS for data authentication. This reduces the total cost of ownership because the credentials are managed from a central location.

In RADIUS, the VPN server interacts with the RADIUS server once the user attempts a connection. The RADIUS server authenticates the user with their credentials. The user is granted access if and only if the user provides the correct credentials and has dial-in access. The RADIUS server sends a RADIUS message to the RADIUS client in response to the request for authentication. The VPN equipment must securely communicate with the RADIUS server and verify whether the user meets certain set conditions before granting permission to access the network.

The RADIUS messages are sent as User Datagram Protocol (UDP) messages, and the UDP payload of a RADIUS packet can include only one RADIUS message.

The following are different types of RADIUS message.

- **Access-request:** Sent by the RADIUS client to request authentication
- **Access-accept:** Sent by the RADIUS server in response to the access-request message
- **Access-reject:** Sent by access-server to the RADIUS client, informing them that the connection request is rejected
- **Access-challenge:** Sent by the RADIUS server to the RADIUS client in response to the access-request from the client
- **Accounting–request:** Sent by the RADIUS client to request information for a permitted connection
- **Accounting–response:** Sent by the RADIUS server in response to the accounting-request message from the RADIUS client

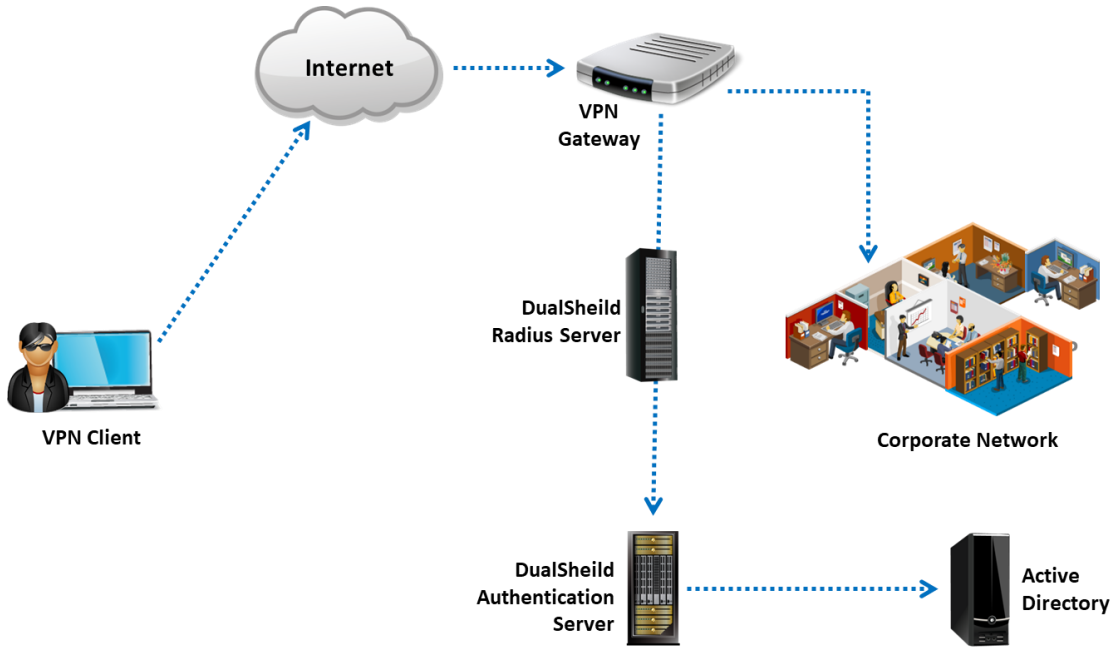


Figure 5.93: RADIUS server securing VPN

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

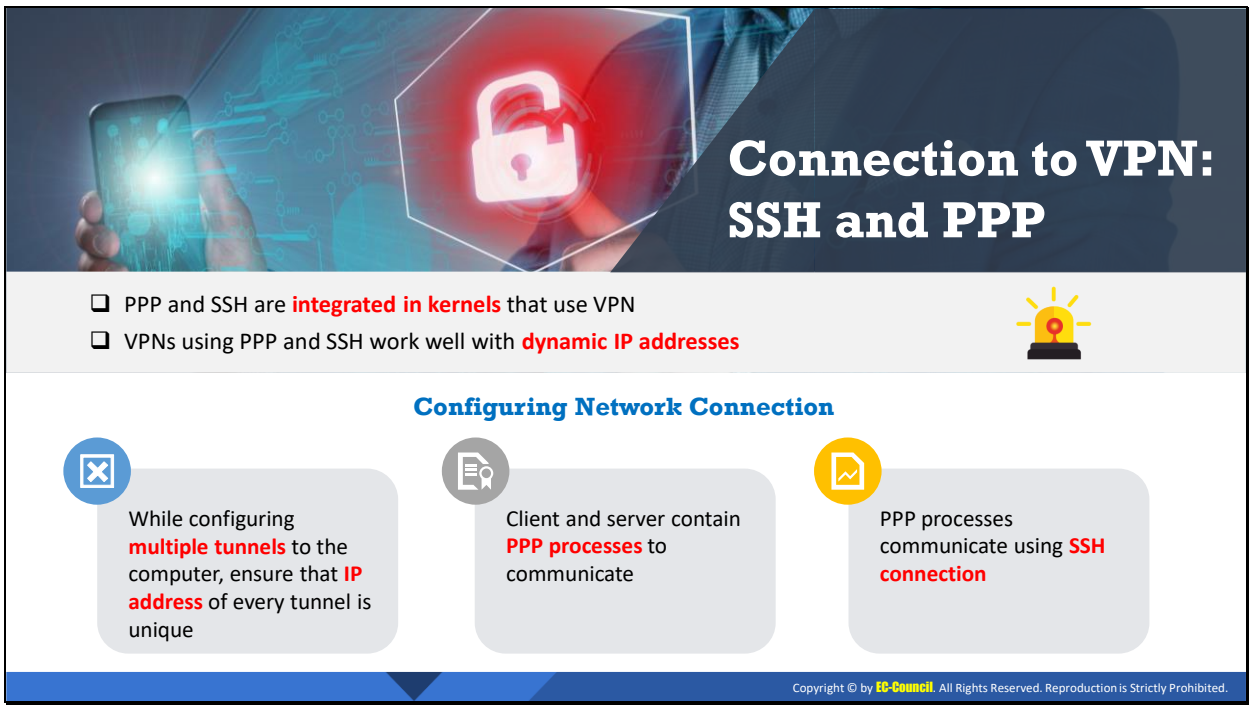
A RADIUS message consists of a RADIUS header and RADIUS attributes. The RADIUS attributes provide information regarding the number of connection attempts, username, password, service requested by the user, etc., each of which has a separate RADIUS attribute. RADIUS attributes are shared between RADIUS servers, RADIUS clients, and RADIUS proxies.

The following are the components of RADIUS:

- Access clients
- Access servers
- RADIUS proxies
- RADIUS servers
- User account databases

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

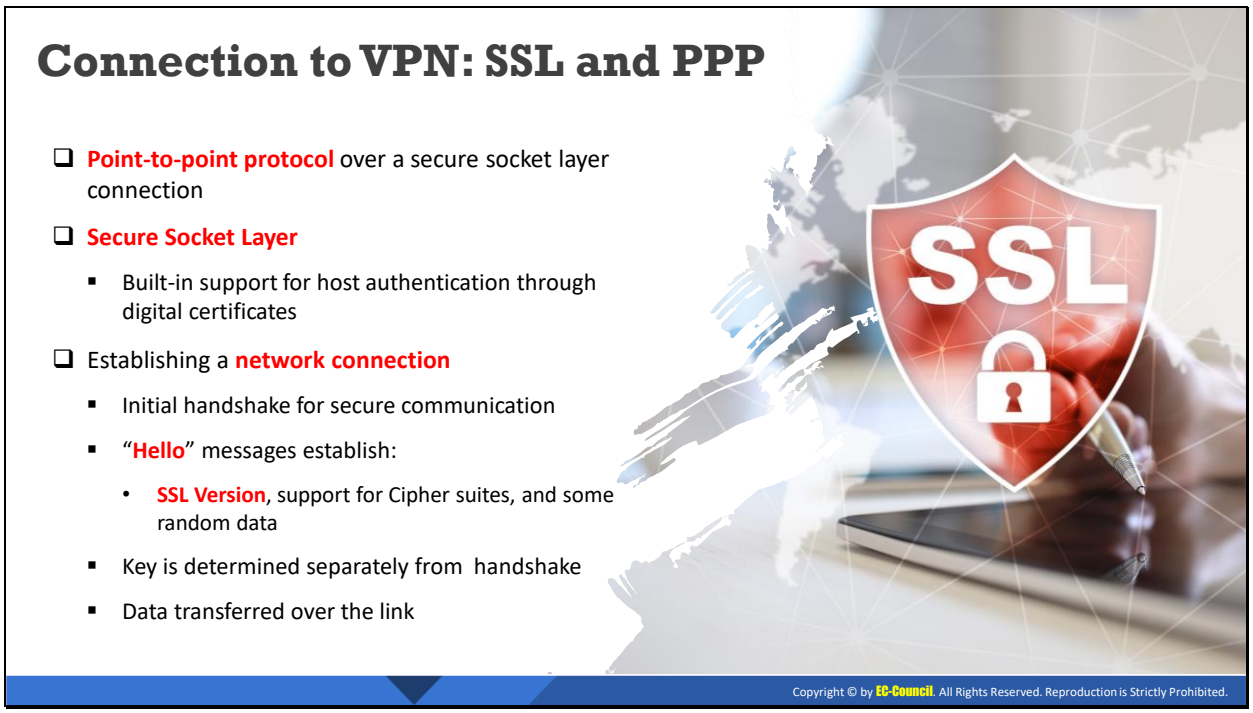


Connection to VPN: SSH and PPP

There are numerous benefits to setting up a PPP-SSH VPN. It is simpler than the other types of VPN. PPP and SSH are built-in with most distributions, and most kernels are pre-configured to utilize them well. If the SSH protocol presently crosses the organization's firewall, then PPP over SSH will cross the firewall as well. PPP-SSH VPNs do not have any problems with dynamic IP addresses.

Setting up a VPN over a dialup connection will not be a problem in the case of PPP-SSH VPNs, and multiple tunnels to a single computer can be set up. The user must ensure that the IP address for each tunnel's network interface is discrete. For establishing SSH connections, a VPN client and servers are required. Both the client and server have PPP daemons that communicate through the SSH connection.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



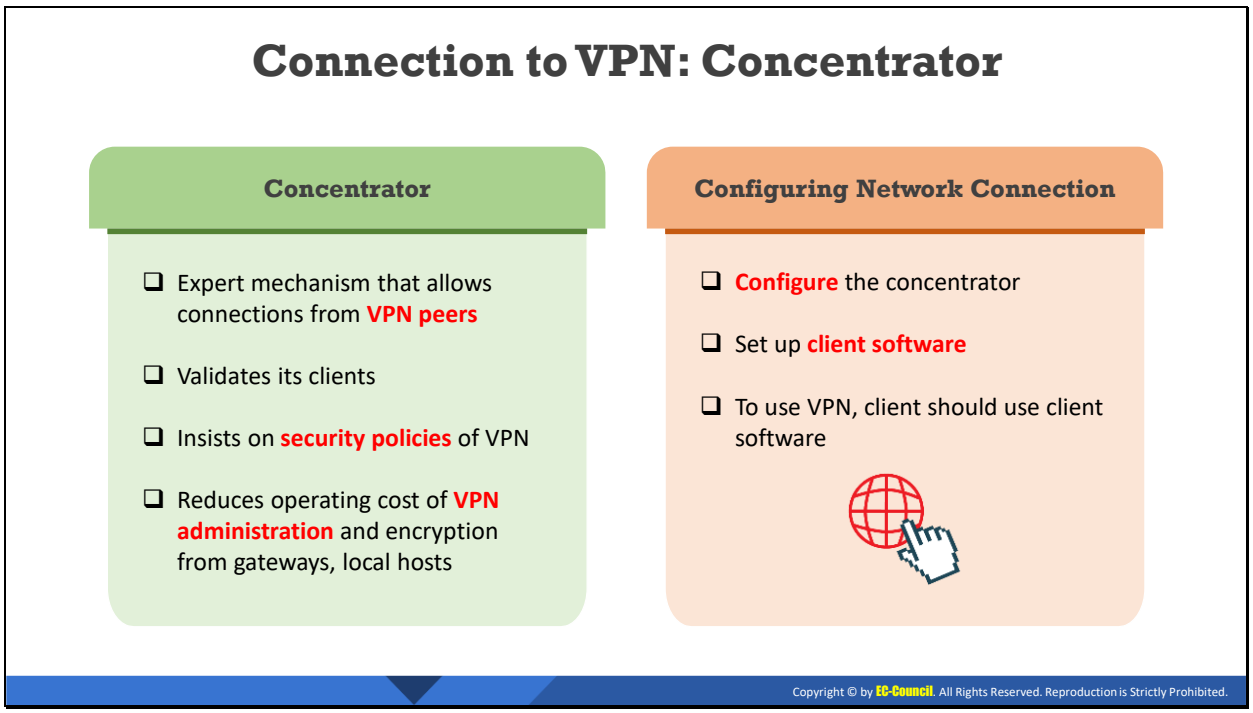
Connection to VPN: SSL and PPP

Point-to-Point Protocol (PPP) over a secure socket layer (SSL) connection provides built-in support for host authentication through digital certificates.

The following are the steps for establishing a network connection:

- An initial handshake is performed for secure communication.
- "Hello" messages establish the SSL version, support for cipher suites, and some random data.
- The key is determined separately from the handshake.
- Data are transferred over the link.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

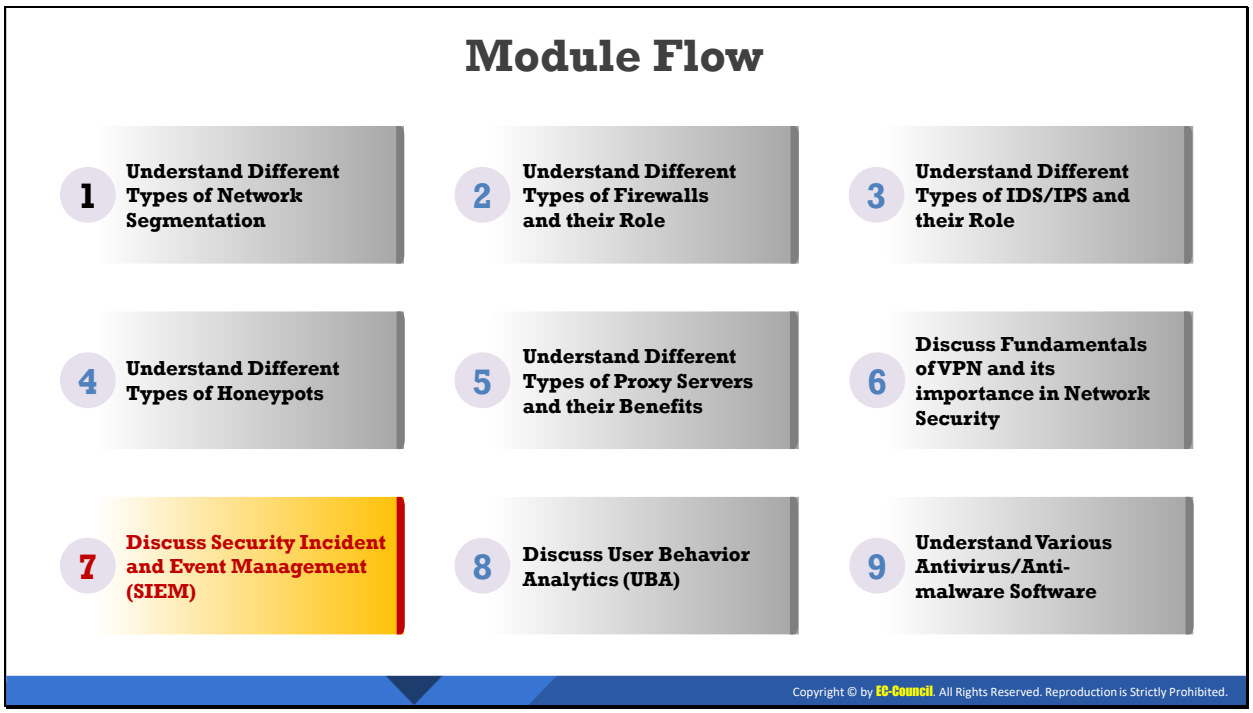


Connection to VPN: Concentrator

A VPN concentrator is used for remote-access VPNs and allows the use of an encrypted tunnel to securely access a corporate or any other kind of network via the Internet. Concentrator models differ depending on the number of users and amount of throughput. A VPN concentrator is also used to encrypt WLAN or wired traffic.

A concentrator must not be mistaken for a gateway or firewall. It is a specialized device that receives a connection from VPN peers by authenticating them. It enforces the security policies with regards to virtual private networking. It takes the overhead of VPN management and encryption off gateways and local hosts. Furthermore, it reduces the operating cost of VPN administration. To configure a network connection, the user must configure the concentrator and set up client software; to use the VPN, the user should use the client software.

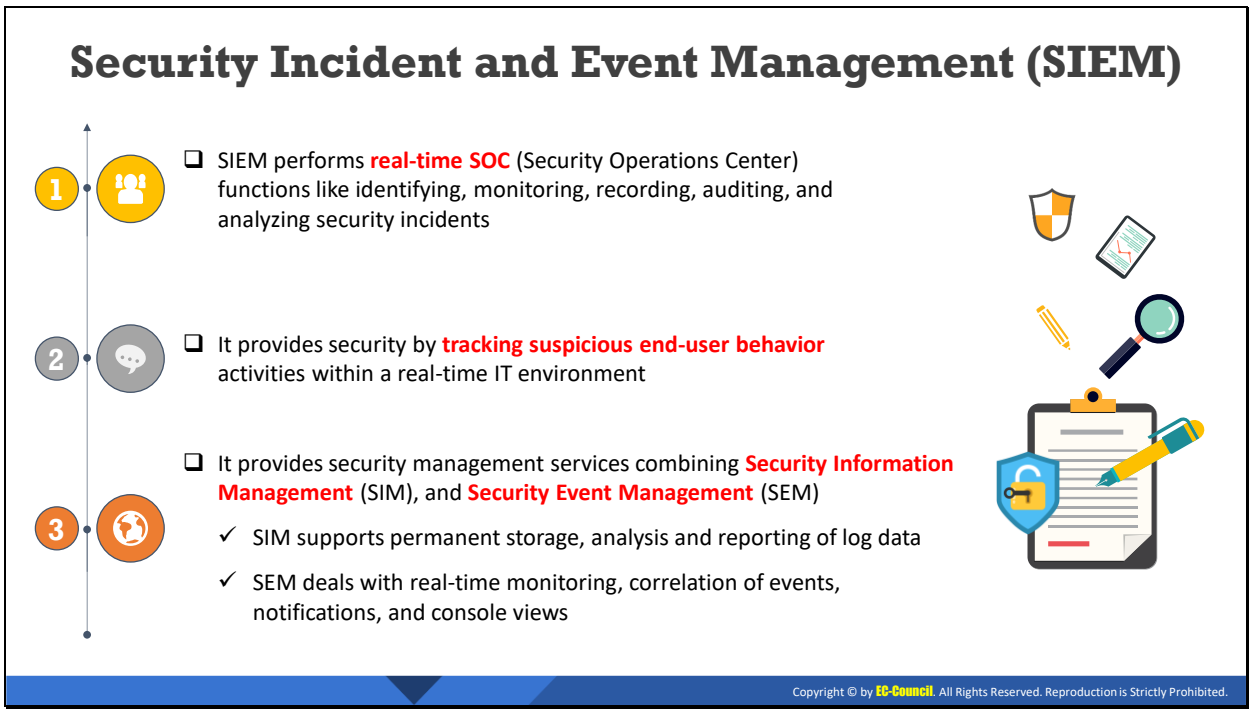
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Discuss Security Incident and Event Management (SIEM)

Today, organizations need to protect their IT assets from data breaches due to internal and external threats. To meet strict compliance requirements and for threat identification and mitigation, organizations must audit the information passing through their enterprise network. Security incident and event management (SIEM) systems are used to manage and store a huge collection of log data from different sources such as networks, applications, devices, security, and user activity in real time. SIEM performs the real-time monitoring and detection of security events, forensic and post-incident analysis, auditing, and IT security and regulatory compliance reporting. Thus, SIEM is highly important in network security.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

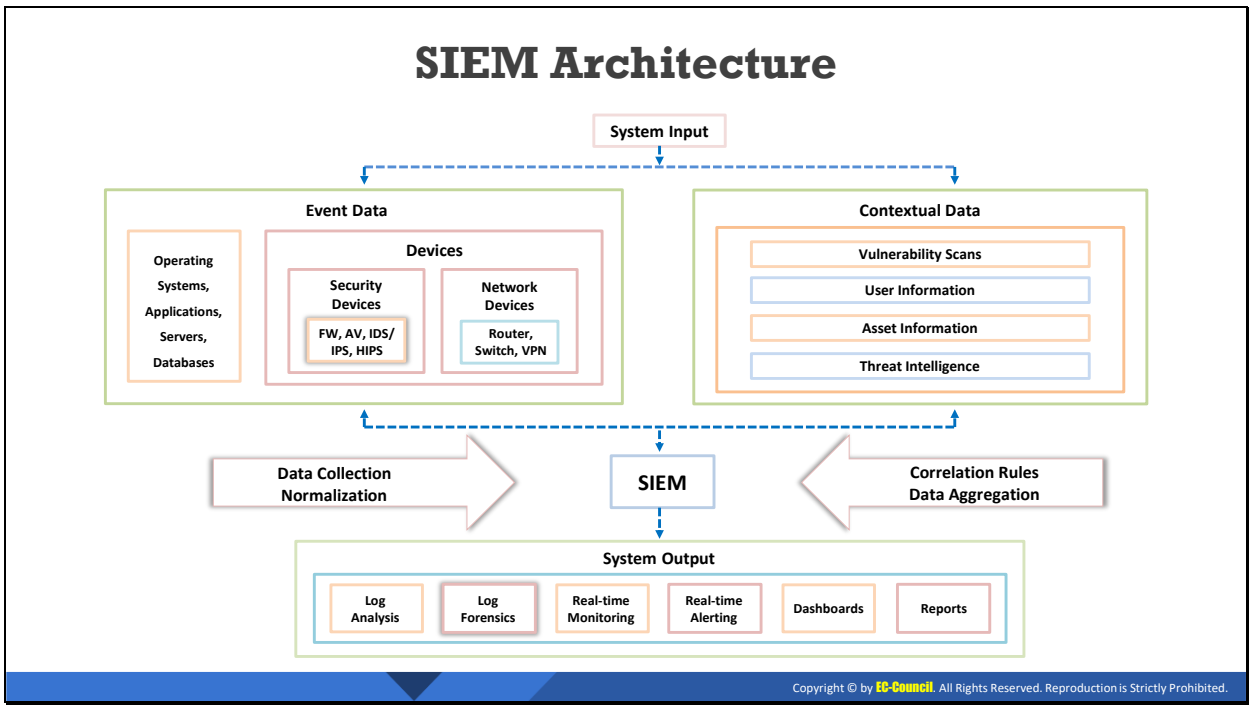


Security Incident and Event Management (SIEM)

Security incident and event management (SIEM), also known as security information and event management, performs real-time security operations center (SOC) functions such as identifying, monitoring, recording, auditing, and analyzing security incidents. It performs threat detection and security incident response activities. SIEM provides security by tracking suspicious end-user behavior activities within a real-time IT environment.

SIEM provides security management services combining security information management (SIM) and security event management (SEM). SIM supports the permanent storage, analysis, and reporting of log data. SEM deals with real-time monitoring, correlation of events, notifications, and console views. SIEM protects an organization's IT assets from data breaches due to internal and external threats.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



SIEM Architecture

SIEM technology provides SEM and SIM services. SEM supports threat management and security incident handling by collecting and analyzing event information from different data sources in real time. SIM supports log management and analysis, compliance monitoring, and the forensic investigation of logged data.

SIEM applies normalization and aggregation to event data and contextual data collected from different internal and external sources such as business applications, OSes, network devices, end points, access management, malware, vulnerabilities, and identity information. Correlation rules are applied to the normalized data to detect security incidents. SIEM monitors access to servers and databases, performs user activity monitoring across multiple systems and applications in real time, and provides protection from various internal and external threats.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

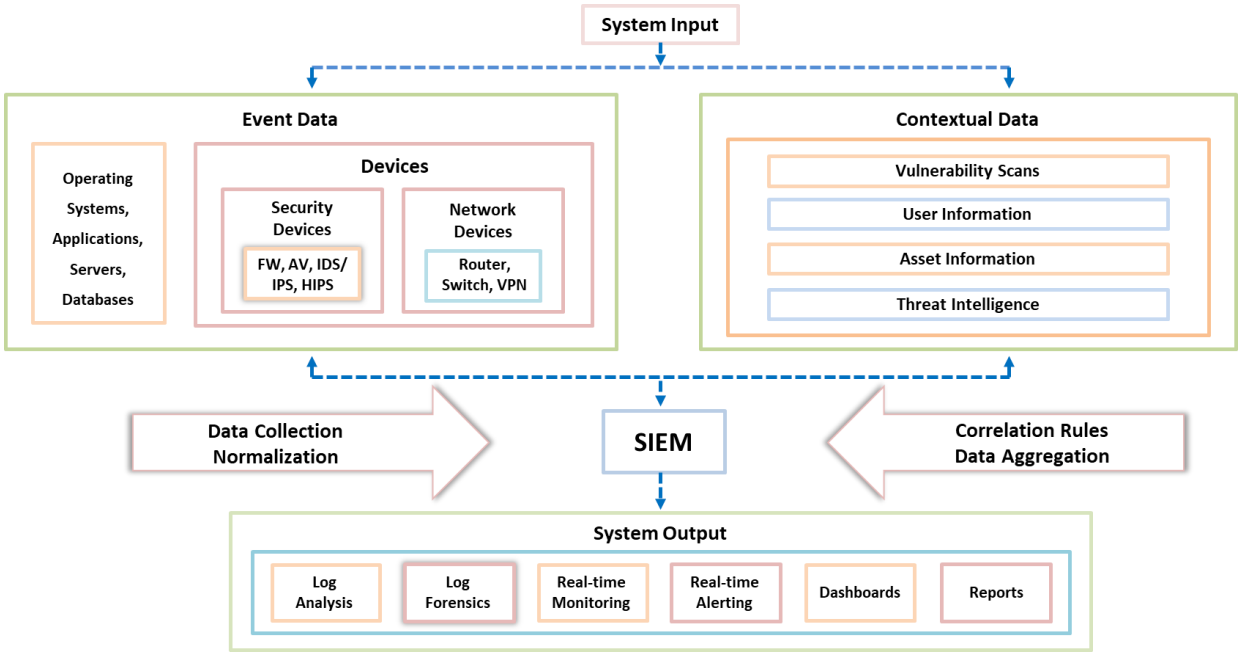
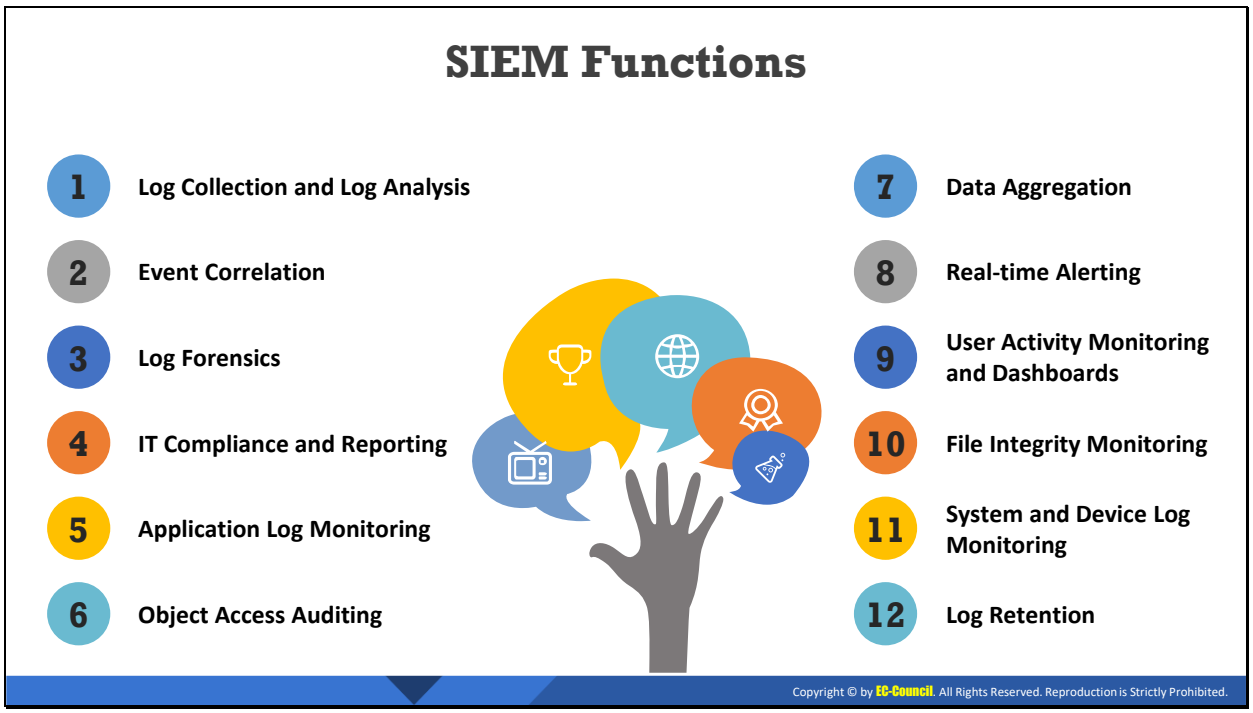


Figure 5.94: SIEM architecture

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



SIEM Functions

- **Log collection:** SIM collects and logs data from different sources such as networks, applications, devices, and user activity in real time in a central repository for analysis and reporting.
- **Log analysis:** SEM performs the real-time monitoring and analysis of security incidents. SIEM monitors all the security policies, mechanisms (confidentiality, authentication, authorization, etc.), and devices and applications (IDS/IPS, firewall, etc.) in real time. It detects malicious activities and issues alerts about security-related events.
- **Event correlation:** SIEM performs real-time event correlation and alerts analysts and administrators to secure the enterprise network from internal and external threats. SIEM uses rules to correlate events within a time period to understand interrelations between the events and issue alerts for intrusions and insider threats.
- **Log forensics:** SIEM collects, logs, and tracks information from different resources in the enterprise network. Further, it performs forensic analysis and generates various forensic reports such as user activity reports, compliance reports, and audit reports.
- **IT compliance and reporting:** SIEM ensures compliance in real time with various industry regulations such as FISMA, PCI/DSS, and HIPAA. It automatically collects the information necessary for compliance with organizational and government policies, and it generates compliance reports.
- **Application log monitoring:** SIEM monitors log files from various OSes, servers, and web applications and generates analysis reports when security events are detected.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **Object access auditing:** SIEM effectively collects and manages all the object access audit logs at the central repository. This helps in tracking successful and failed attempts to access organizational resources.
- **Data aggregation:** Using data aggregation, SIEM aggregates all similar events into one summary report. This report helps security analysts further investigate various security-related events effectively.
- **Real-time alerting:** SIEM issues real-time notifications through methods such as intuitive dashboards, emails, or text messages to alert analysts regarding security events.
- **User activity monitoring:** SIEM tracks suspicious user behavior and generates user-wise activity reports. It provides user activity monitoring, privileged user activity monitoring, and audit reports.
- **Dashboards:** SIEM utilizes dashboards to inform security analysts and administrators to take defensive actions quickly and make the right decisions during security events.
- **File integrity monitoring:** In SIEM, file integrity monitoring ensures the real-time monitoring and integrity of confidential data to meet compliance requirements. It helps security analysts and administrators record, access, and change system files and folders such as OS files, system configuration files, installed software, and running processes. It generates reports on all changes to the system files and folders, and it issues real-time alerts when an unauthorized user attempts to access any confidential files or folders.
- **System and device log monitoring:** SIEM provides both the static and dynamic monitoring of enterprise systems and networks. It analyzes log data to identify suspected activities related to system compromise. It dynamically collects, correlates, and evaluates data from heterogeneous systems and devices in the network to detect attacks as early as possible before any significant damage to enterprise resources.
- **Log retention:** SIEM stores logged data in a central repository for long periods to meet compliance and regulatory requirements and for conducting forensic analysis, investigation, and internal audits. The log data stored in the central repository are generally encrypted and time-stamped to protect the data from tampering.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

SIEM Solutions

- **Splunk Enterprise**

  Source: *https://www.splunk.com*

  Splunk Enterprise Security (ES) is an analytics-driven SEIM solution that provides the information needed to detect and respond to internal and external attacks quickly.

  - It automates the collection, indexing, and alerting of real-time machine data that are critical to an organization's operations.
  - It discovers actionable insights from all data, irrespective of whether they are structured or unstructured.
  - It leverages artificial intelligence powered by machine learning for actionable insights.

  Splunk ES provides organizations the ability to:

  - Improve security operations with faster response times
  - Improve the security posture by attaining end-to-end visibility across all machine data
  - Increase detection and investigation capabilities using advanced analytics
  - Make better-informed decisions by leveraging threat intelligence

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

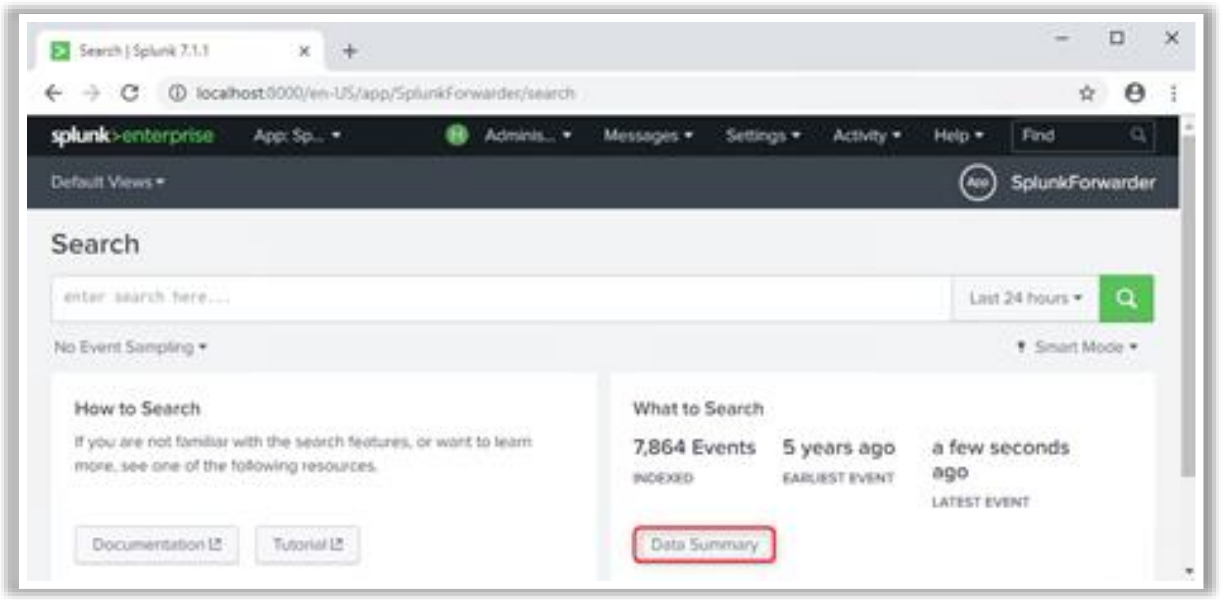
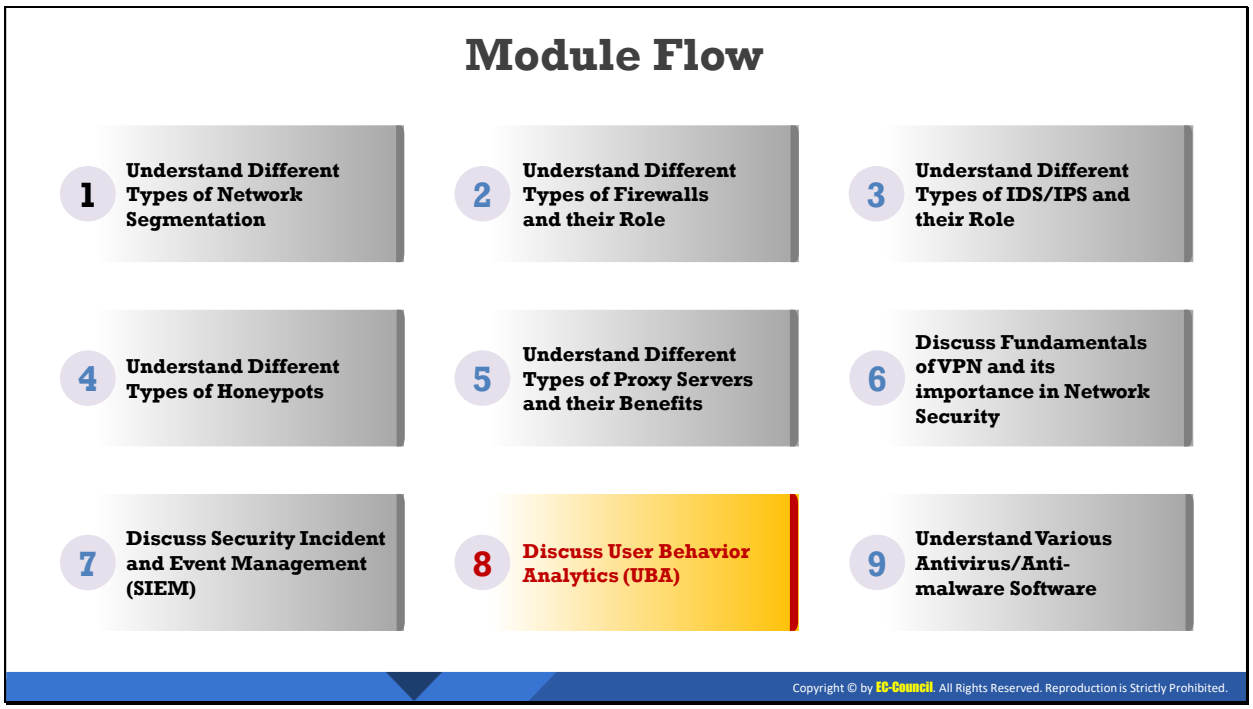


Figure 5.95: Screenshot of Splunk Enterprise

Some of the additional SIEM tools are listed below:

- ArcSight ESM (*https://www.microfocus.com*)
- IBM Qradar SIEM (*https://www.ibm.com*)
- AlienVault OSSIM (*https://cybersecurity.att.com*)
- FortiSIEM (*https://www.fortinet.com*)
- SolarWinds Security Event Manager (SEM) (*https://www.solarwinds.com*)

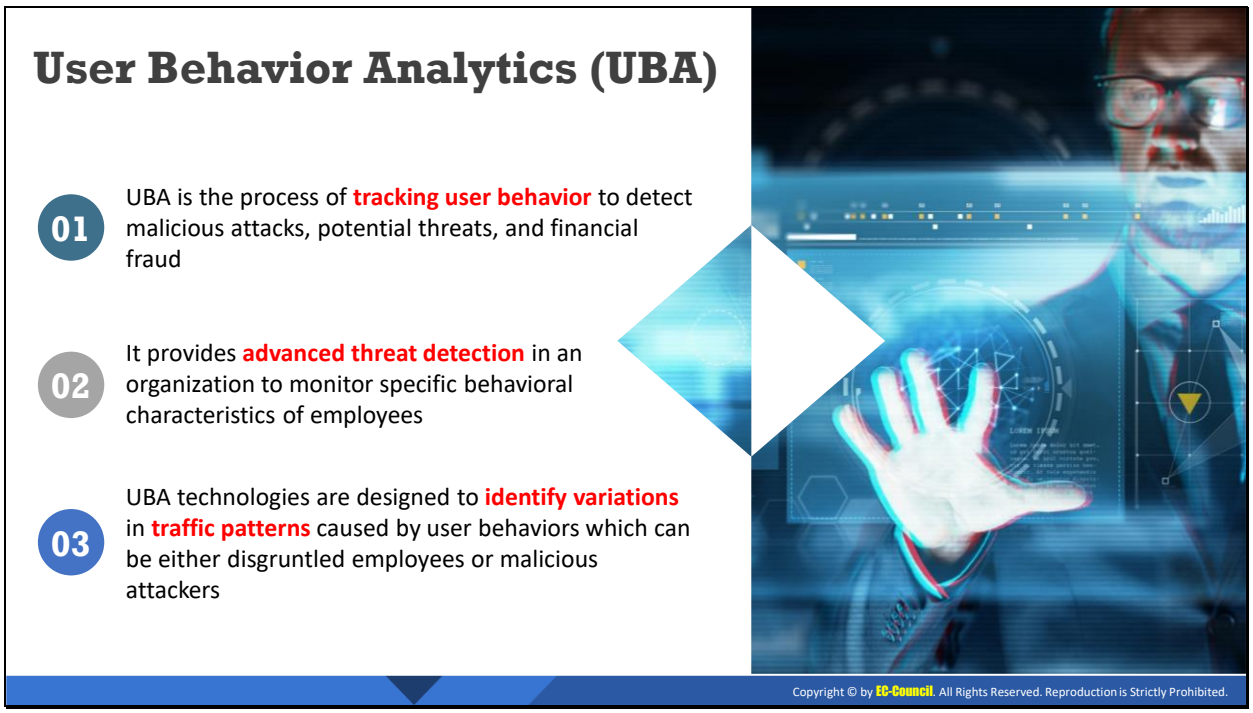
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Discuss User Behavior Analytics (UBA)

This section discusses the importance and role of user behavior analytics (UBA) solutions in network security.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

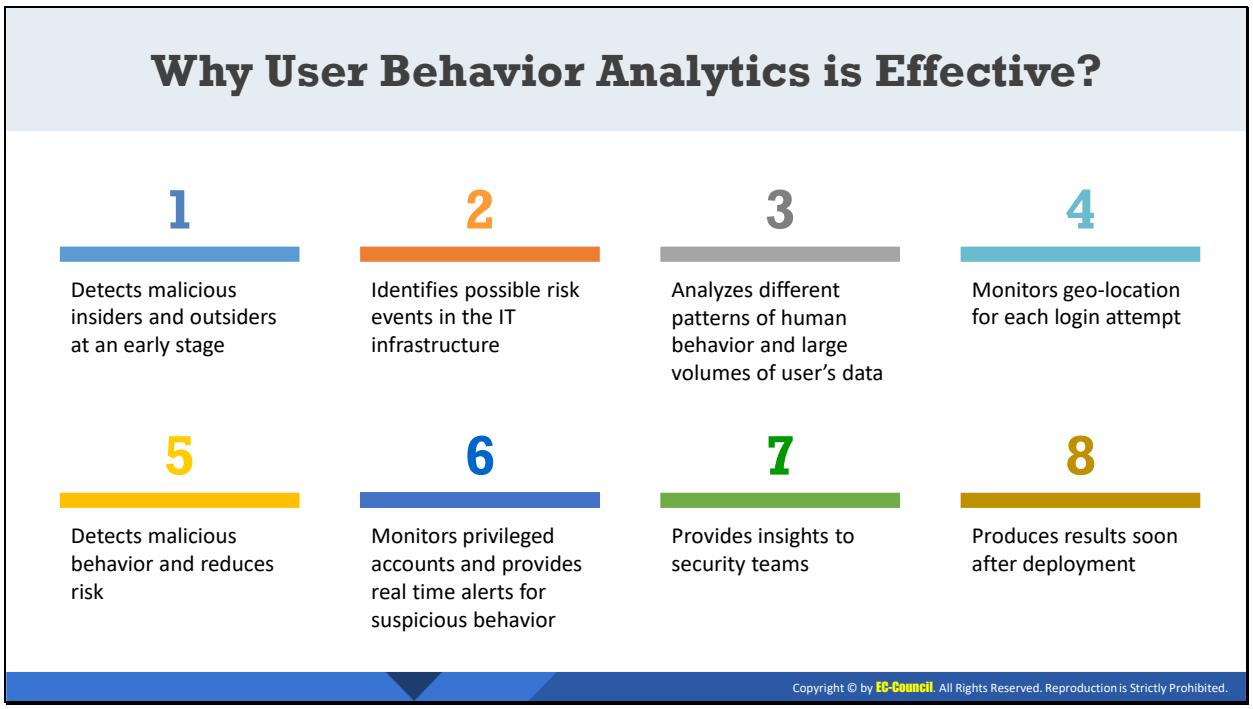


User Behavior Analytics (UBA)

UBA is the process of tracking user behavior to detect malicious attacks, potential threats, and financial frauds. It provides advanced threat detection in an organization to monitor specific behavioral characteristics of the employees. UBA technologies are designed to identify any unusual variations in traffic patterns caused by users, who can be either disgruntled employees or malicious attackers. UBA is used as a defense mechanism to address anomalous user behavior to overcome the most complicated issues faced by security professionals today.

The employees working in a company access different websites, tools, and applications. All their activities are logged and monitored. While these applications are running, there is a possibility of an intruder gaining access to the IT system and stealing credentials without the knowledge of the user. When an intruder (external attacker or an insider) stays on the company's network as a legitimate user, UBA distinguishes this unusual behavior of the account by comparing the behavior baselines of both the user and the attacker; it then issues an alert on its database and highlights the risk scores. When an alert is issued, a notification is sent to the user's personal device for confirmation. In case the user does not confirm this activity, it is considered a major security breach. Through UBA, the user's account can be disabled by the security teams depending on the severity of the incident and the risk level.

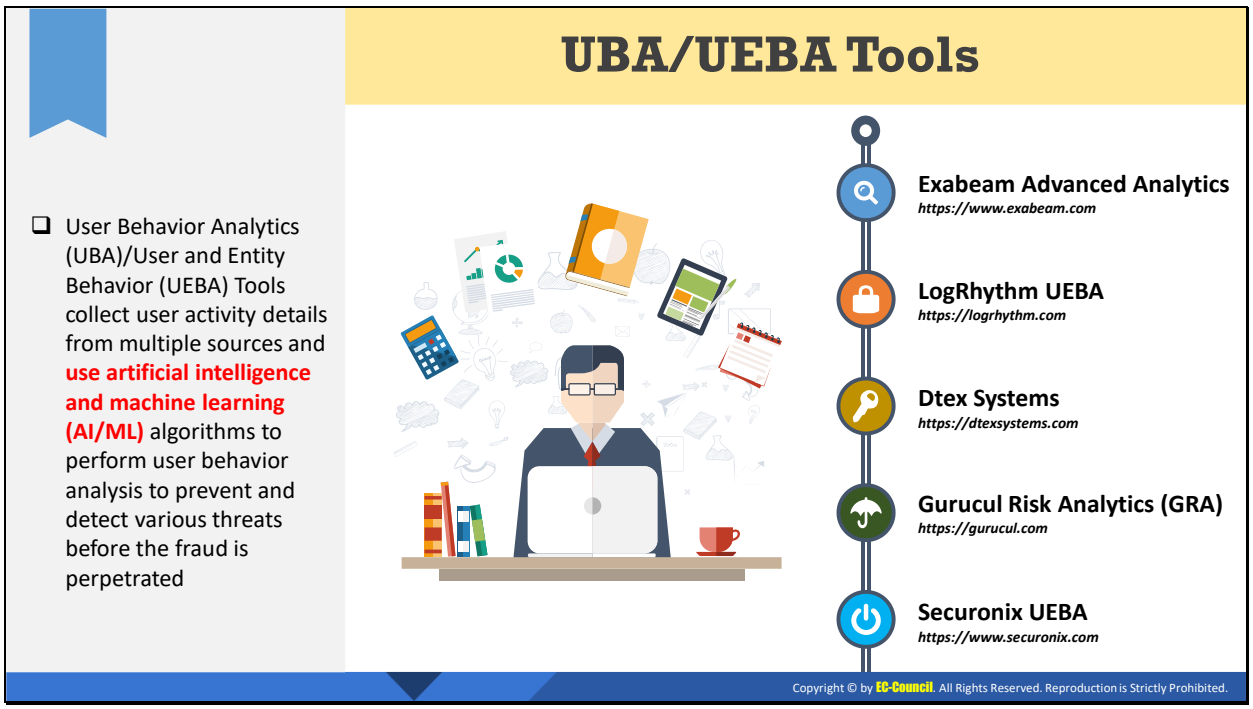
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Why User Behavior Analytics is Effective?

- Detects malicious insiders and outsiders at an early stage
- Identifies possible risk events in the IT infrastructure
- Analyzes different patterns of human behavior and large volumes of user data
- Monitors geo-location for each login attempt
- Detects malicious behavior and reduces risk
- Monitors privileged accounts and issues real-time alerts for suspicious behavior insights to security teams
- Provides insights to security teams
- Produces results soon after deployment

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



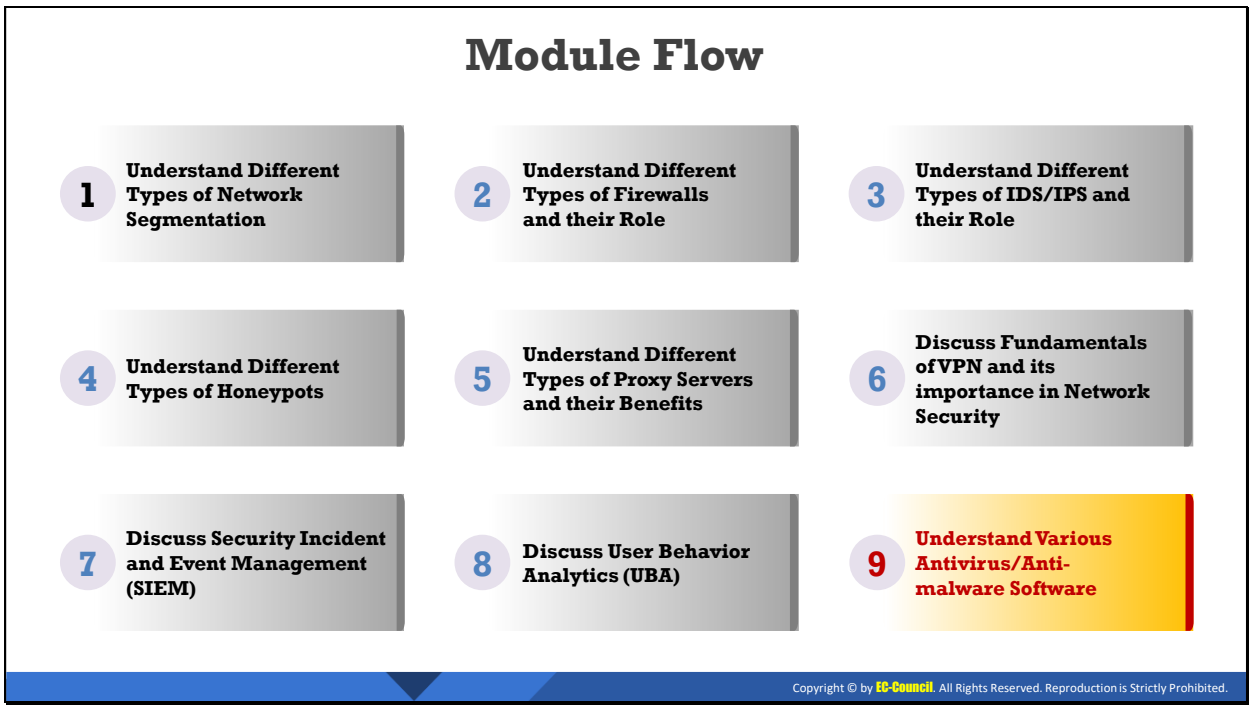
UBA/UEBA Tools

UBA or user and entity behavior analytics (UEBA) tools collect user activity details from multiple sources and use artificial intelligence and machine learning algorithms to perform UBA to prevent and detect various threats before a fraud is perpetrated.

Listed below are some of the important UBA/UEBA tools:

- Exabeam Advanced Analytics (*https://www.exabeam.com*)
- LogRhythm UEBA (*https://logrhythm.com*)
- Dtex Systems (*https://dtexsystems.com*)
- Gurucul Risk Analytics (GRA) (*https://gurucul.com*)
- Securonix UEBA (*https://www.securonix.com*)

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Understand Various Antivirus/Anti-malware Software

An attacker uses malware to commit online fraud or theft. Thus, the use of anti-malware software is recommended to help detect malware, remove it, and repair any damage it might cause. This section lists and describes various anti-malware (anti-Trojan and antivirus) software programs.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Anti-Trojan Software

Anti-Trojan software is a tool or program that is designed to identify and prevent malicious Trojans or malware from infecting computer systems or electronic devices. Anti-Trojan tools may employ scanning strategies as well as freeware or licensed tools to detect Trojans, rootkits, backdoors, and other types of potentially damaging software.

- **Kaspersky Internet Security**

  Source: *https://www.kaspersky.com*

  Kaspersky Internet Security protects devices from various types of intrusions due to Trojans, viruses, spyware, ransomware, phishing, and dangerous websites. It securely stores passwords for easy access on PC, Mac, and mobile. It makes backup copies of photos, music, and files and also encrypts data on PC. Furthermore, it automatically blocks inappropriate content and helps you manage the use of social networks. In addition, it provides extra security when you shop or bank online on PC or Mac.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

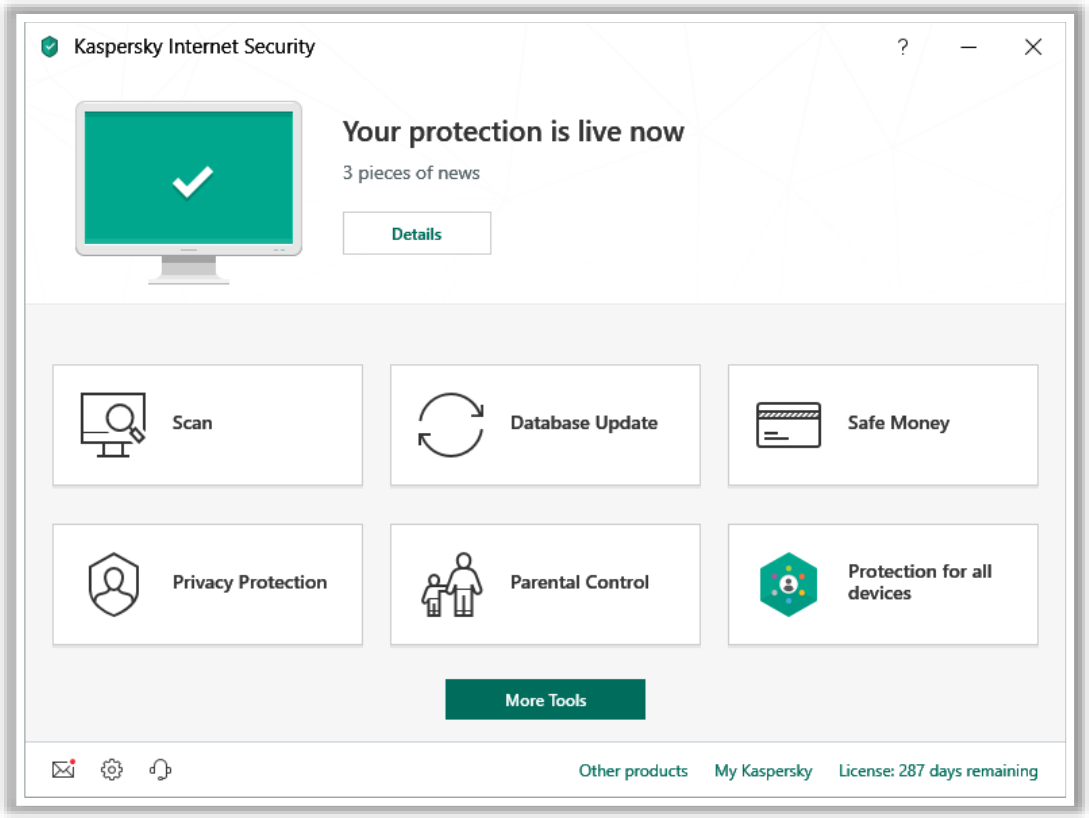


Figure 5.96: Screenshot of Kaspersky Internet Security

Some additional anti-Trojan software are as follows:

- McAfee® LiveSafe™ (*https://www.mcafee.com*)
- Bitdefender Total Security (*https://bitdefender.com*)
- HitmanPro (*https://www.hitmanpro.com*)
- Malwarebytes (*https://www.malwarebytes.org*)
- Zemana Antimalware (*https://www.zemana.com*)

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Antivirus Software

It is a good practice for organizations to install the most recent version of the antivirus software and regularly update it to keep up with the introduction of new viruses in the market. Updating of antivirus software by the respective vendors is a continuous process.

- **Bitdefender Antivirus Plus**

  Source: *https://www.bitdefender.com*

  Bitdefender Antivirus Plus works against all threats, from viruses, worms, and Trojans to ransomware, zero-day exploits, rootkits, and spyware. It uses a technique called behavioral detection to closely monitor active apps. As soon as it detects suspicious activity, it takes decisive action to prevent infection. It sniffs and blocks malicious websites that masquerade as trustworthy websites to steal financial data such as passwords or credit card numbers.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

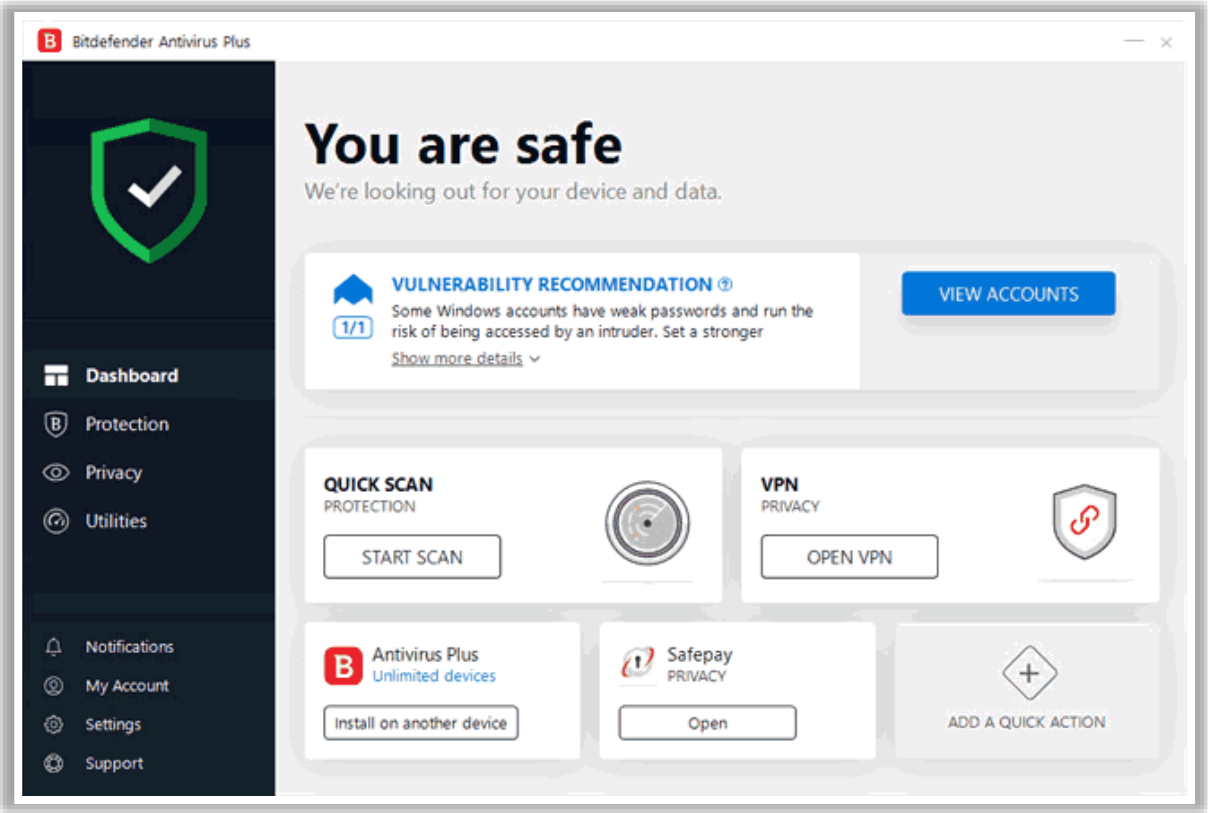
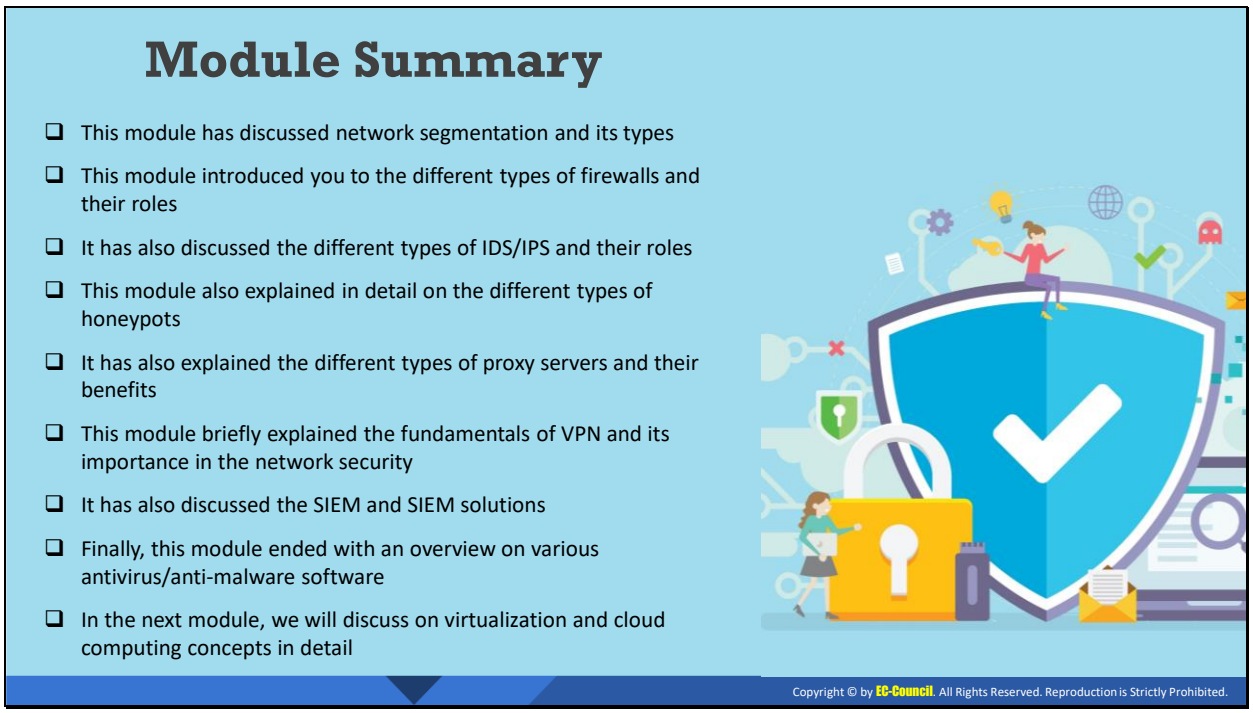


Figure 5.97: Screenshot of Bitdefender Antivirus Plus 2019

Some additional antivirus software are as follows:

- ClamWin (*http://www.clamwin.com*)
- Kaspersky Anti-Virus (*https://www.kaspersky.com*)
- McAfee Total Protection (*https://www.mcafee.com*)
- Avast Premier Antivirus (*https://www.avast.com*)
- ESET Internet Security (*https://www.eset.com*)

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Module Summary

This module discussed network segmentation and its types. It introduced the different types of firewalls and their roles. Furthermore, it discussed the different types of IDS/IPS and their roles. This module also explained in detail the different types of honeypots. Moreover, it explained the different types of proxy servers and their benefits. It also briefly explained the fundamentals of VPN and its importance in network security. Additionally, it discussed SIEM and SIEM solutions. Finally, this module presented an overview of various antivirus/anti-malware software.

In the next module, we will discuss virtualization and cloud computing concepts in detail.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

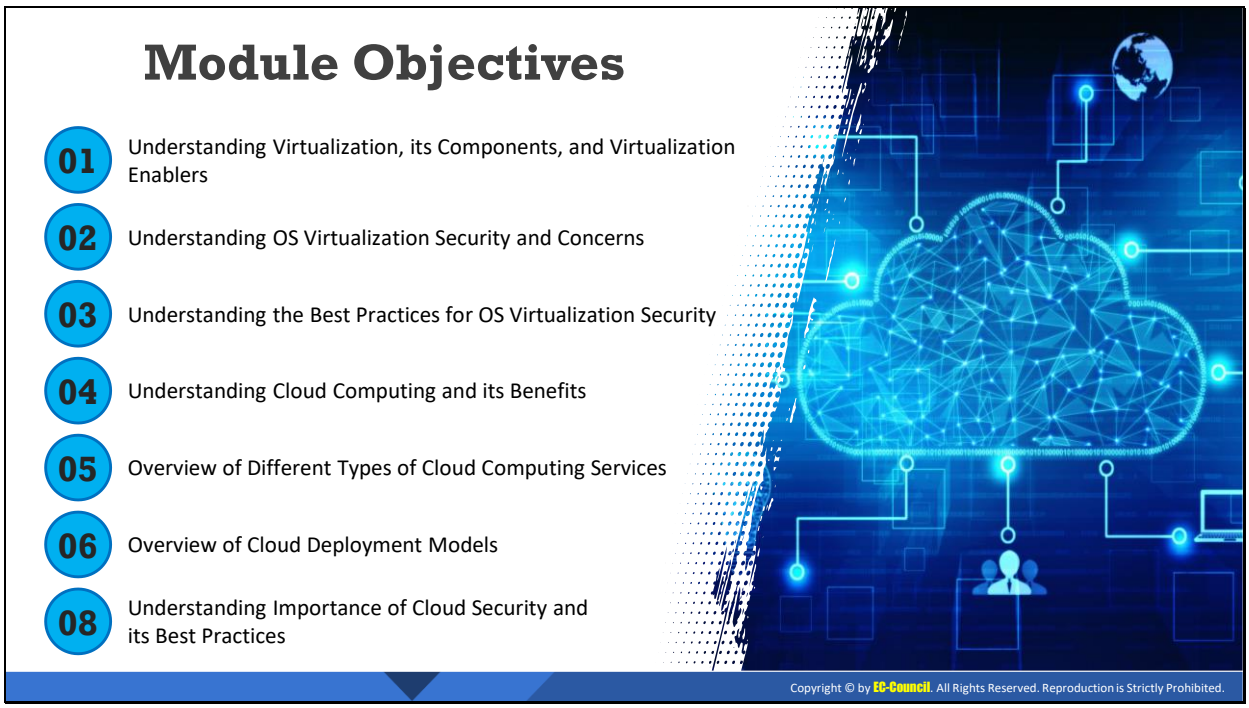
EC-Council

N|DE
Network Defense Essentials

Module 06

Virtualization and Cloud Computing

https://t.me/learningnets



Module Objectives

Modern IT environments use server virtualization, network virtualization, storage virtualization, and desktop virtualization for fast provisioning of network environments and to keep pace with modern technologies. Virtualization has been changing security concepts in modern IT environments, as the various security challenges associated with virtualization are unique and distinct from those of conventional environments.

Cloud computing is an emerging technology that delivers computing services such as online business applications, online data storage, and webmail over the Internet. Cloud implementation enables a distributed workforce, reduces organization expenses, provides data security, etc. Because of these benefits, many business organizations have recently been migrating their data and infrastructure to the cloud. However, the cloud environment also poses many threats and risks to organizations.

This module discusses virtualization concepts and technologies such as network virtualization, software-defined networks, and network function virtualization, as well as their security. This module also explains the various aspects of enterprise cloud security that are important for an organization to securely store or process data on the cloud. Furthermore, this module discusses various elements of cloud security, such as user identity and access management (IAM), encryption and key management, application-level security, data storage security, monitoring, logging, and compliance to secure sensitive data on the cloud.

At the end of this module, you will be able to do the following:

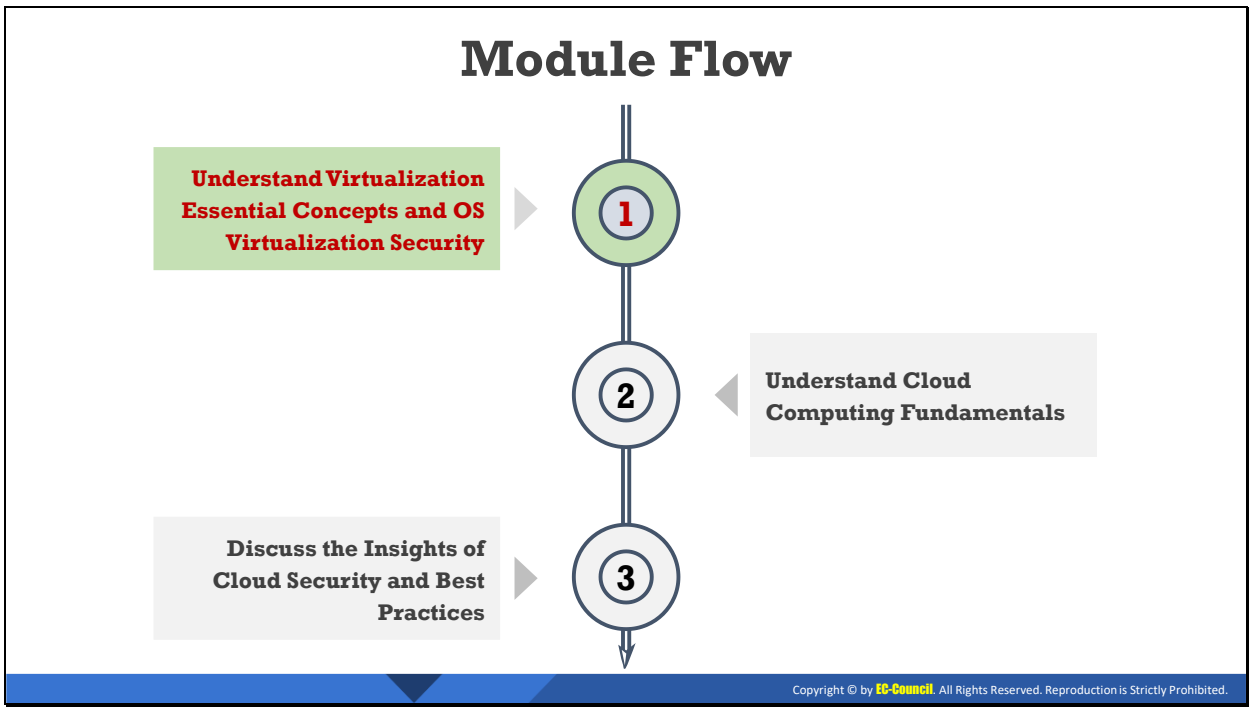
- Understand virtualization, its components, and virtualization enablers
- Understand OS virtualization security and concerns

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- Understand the best practices for OS virtualization security
- Explain cloud computing and its benefits
- Understand different types of cloud computing services
- Explain cloud deployment models
- Understand importance of cloud security and its best practices

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

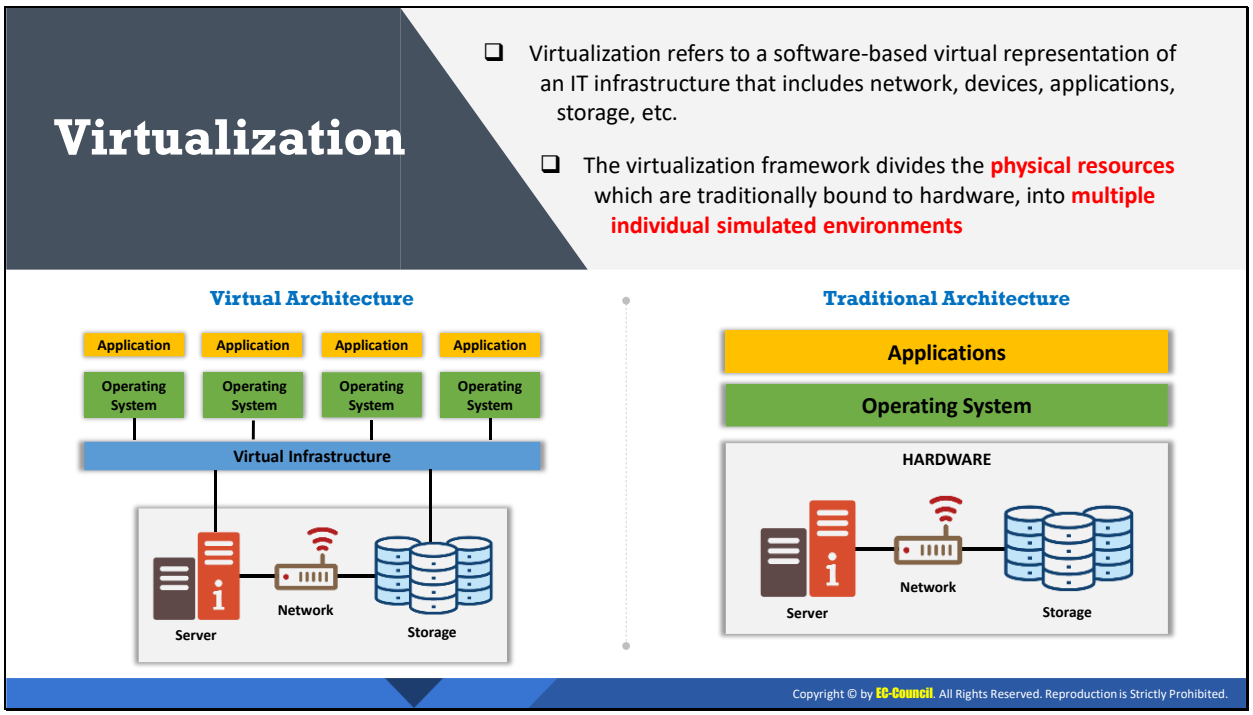
https://t.me/learningnets

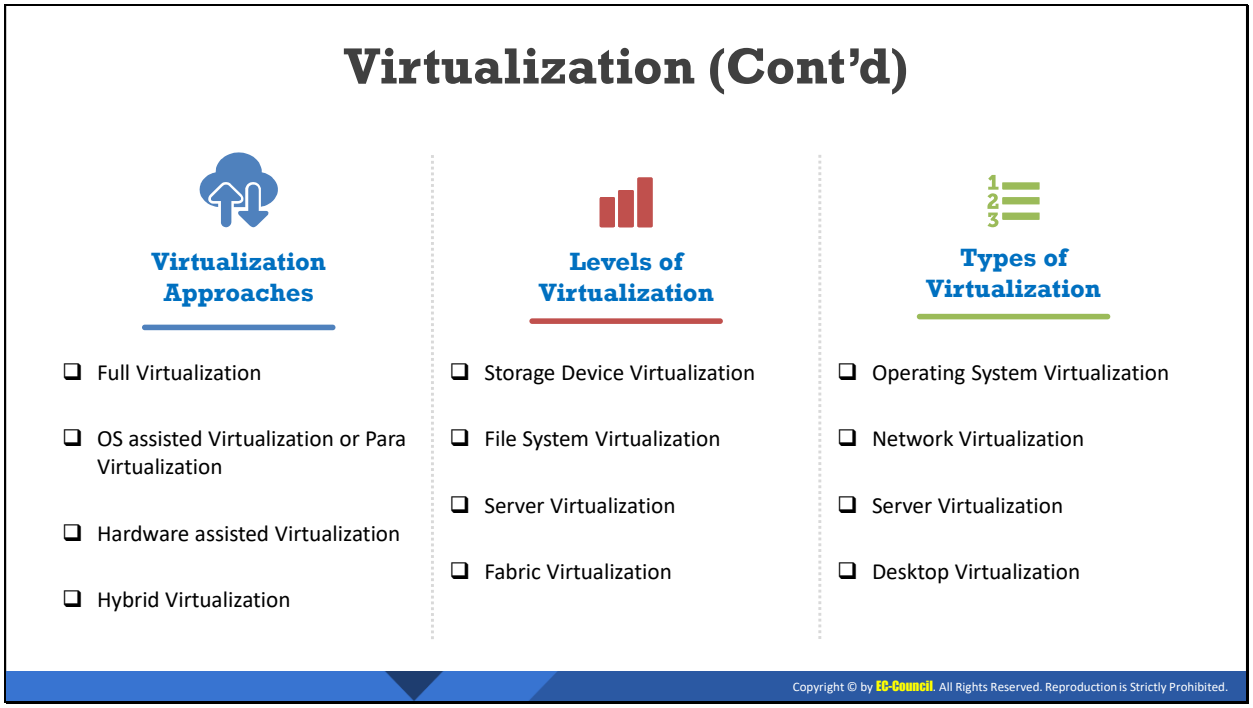


Understand Virtualization Essential Concepts and OS Virtualization Security

The objective of this section is to explain virtualization concepts, the types of virtualization, the various components of virtualization, the various enablers of virtualization technology, OS virtualization security and concerns, and best practices.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets





Virtualization

The virtualization architecture may be best illustrated by contrasting it with the traditional architecture. In the traditional architecture, the hardware infrastructure (host machine) runs a single operating system in which all applications are executed.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

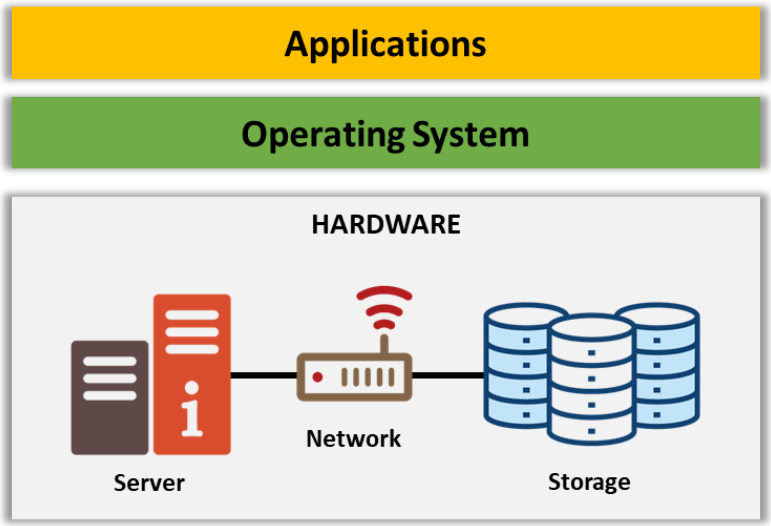


Figure 6.1: Traditional Architecture

The above figure illustrates the traditional architecture. In the figure, a single instance of an operating system, with a set of applications, completely utilizes the available 32-bit hardware infrastructure. The host OS directly interacts with the hardware to request system resources.

By contrast, in the virtualization architecture, the hardware platform (host machine) is used to run multiple sets of virtual operating systems (guest OSes) and their applications.

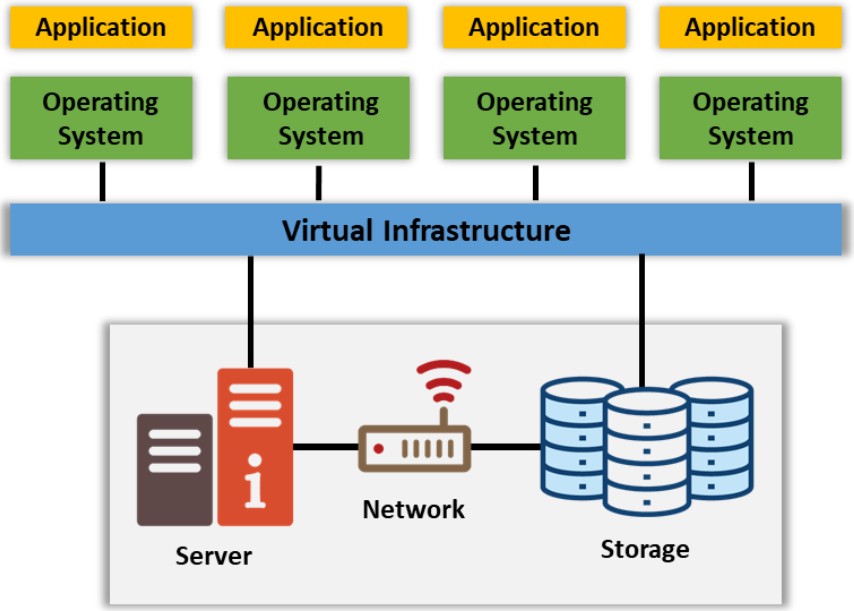


Figure 6.2: Virtualization Architecture

The above figure illustrates the virtualization architecture. As shown in the figure, the virtualization layer acts as middleware between the operating systems and the computer hardware. It logically partitions the hardware resources based on the requests received from the host and the guest operating systems. The host OS directly interacts with the computer hardware, but the guest OSes interact through the virtualization layer.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Virtualization Approaches

Various approaches can be adopted to achieve virtualization, as described below:

- **Full Virtualization:** In this type of virtualization, the guest OS is not aware that it is running in a virtualized environment. It sends commands to the virtual machine manager (VMM) to interact with the computer hardware. The VMM then translates the commands to binary instructions and forwards them to the host OS. The resources are allocated to the guest OS through the VMM.
- **OS assisted Virtualization or Para Virtualization:** In this type of virtualization, the guest OS is aware of the virtual environment in which it is running and communicates with the host machine to request for resources. The commands are translated into binary code by the guest OS for the computer hardware. The VMM is not involved in the request and response operations.
- **Hardware assisted Virtualization:** Modern microprocessor architectures have special instructions to aid the virtualization of hardware. These instructions enable the guest OS to execute privileged instructions directly on the processer. The operating system treats the system calls as user programs.
- **Hybrid Virtualization:** In this type of virtualization, the guest OS adopts the functionality of para virtualization and uses the VMM for binary translation to different types of hardware resources.

Further, the design of a virtual environment may incorporate several levels of virtualization.

The following are some levels of virtualization that a virtual environment may leverage.

- **Storage Device Virtualization:** This is the virtualization of storage devices using techniques such as data striping and data mirroring. RAID is an example of storage virtualization, in which multiple storage devices are combined into a single logical unit.
- **File System Virtualization:** This refers to the virtualization of data at the level of the file system. It facilitates convenience of sharing and protection of data within the software. Virtualized data pools manipulate files and data based on user demand.
- **Server Virtualization:** Server level virtualization enables the partition (or virtualization) of the server's operating system environment. This involves the logical partitioning of the server's hard drive.
- **Fabric Virtualization:** This level of virtualization makes the virtual devices independent of the physical computer hardware. It creates a massive pool of storage areas for different virtual machines running on the hardware. Storage area network (SAN) technology is used to achieve fabric level virtualization.

Types of Virtualization

- **Operating System Virtualization:** This type of virtualization enables the hardware to execute multiple operating systems simultaneously, thus enabling the user to run applications requiring different operating systems on a single system. This is done

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

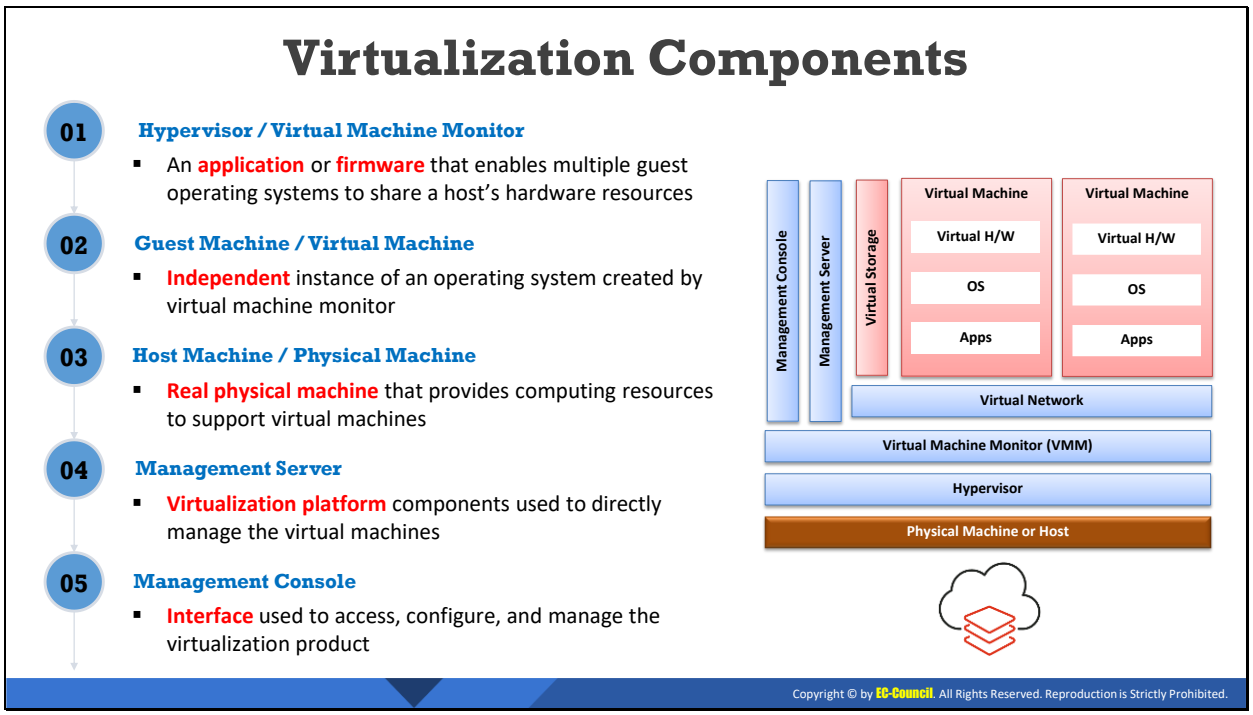
https://t.me/learningnets

directly in the kernel of the operating system, which not only reduces hardware costs, but also saves time spent on updating software on multiple machines.

- **Network Virtualization**: Virtualization has moved beyond just server and storage capacities and now encompasses the network as well. While actual hardware resources were visible and allocated to software in traditional networks, network virtualization creates an abstraction of these network resources. In network virtualization, multiple physical networks are combined into a single software-based virtual network, or a single physical network is divided and exists as multiple independent virtual networks.
- **Server Virtualization**: This is the virtualization of server resources such as physical servers, processors, and operating systems. This process enables the creation and abstraction of multiple virtual machines on a single server. Each virtual machine works independently and runs its own operating system.
- **Desktop Virtualization**: In this virtualization technology, the operating system instance, representing the user's desktop, is located within a central server on the cloud. This enables the user to control the desktop on the cloud and use any device to access it. The data and files are not stored on the system with which the user accesses the desktop but are instead stored in the cloud. Virtualized desktops can be accessed through a server and are hosted on a remote central server, which could be a cluster of computers, thus enabling the user to maintain a desktop on a single central server or cloud. Desktop virtualization reduces the cost of ownership and downtime, enables centralized management, and may enhance security.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Virtualization Components

The basic components of virtualization include,

- **Hypervisor/Virtual Machine Monitor:** An application or firmware that enables multiple guest operating systems to share a host's hardware resources.
- **Guest machine/virtual machine:** Independent instances of operating systems created by a virtual machine monitor (VMM). With the resources provided, the guest machine works as if it is an actual physical machine.
- **Host/physical machine:** Real physical machine which provides computing resources to support guest machines. It is the server component of the virtual machine that supports the guest machine.
- **Management Server:** Virtualization platform components used to directly manage the virtual machines and to simplify the administration of resources.
- **Management Console:** Component used to access, configure, and use the management interface of the virtualization product
- **Network Components:** Components for creating a virtual network to support virtual machines. Firewalls, load balancers, storage, switches, network interface cards, etc. are examples of the components of a virtual network.
- **Virtual Storage:** Components for abstracting physical storage in a single storage device. This enables the multiple systems present in the host machine to use the available storage among themselves.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

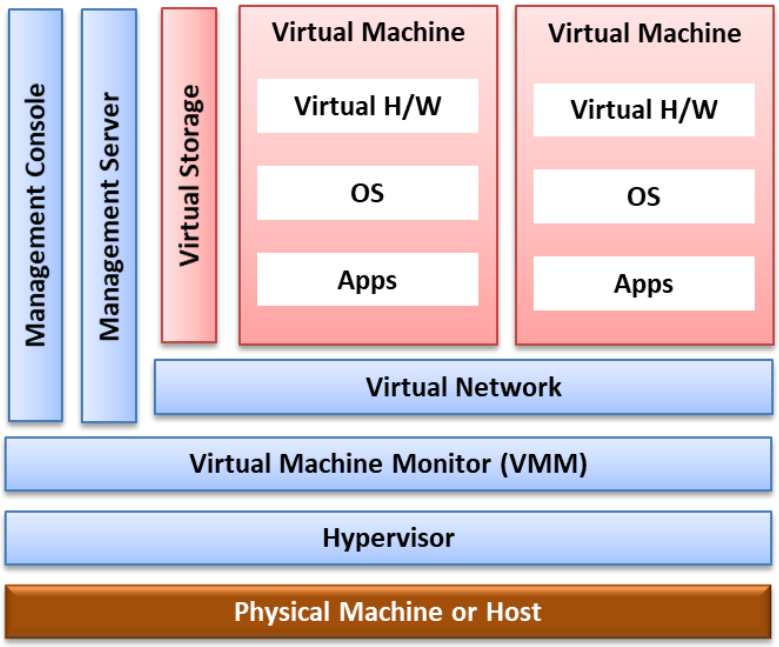
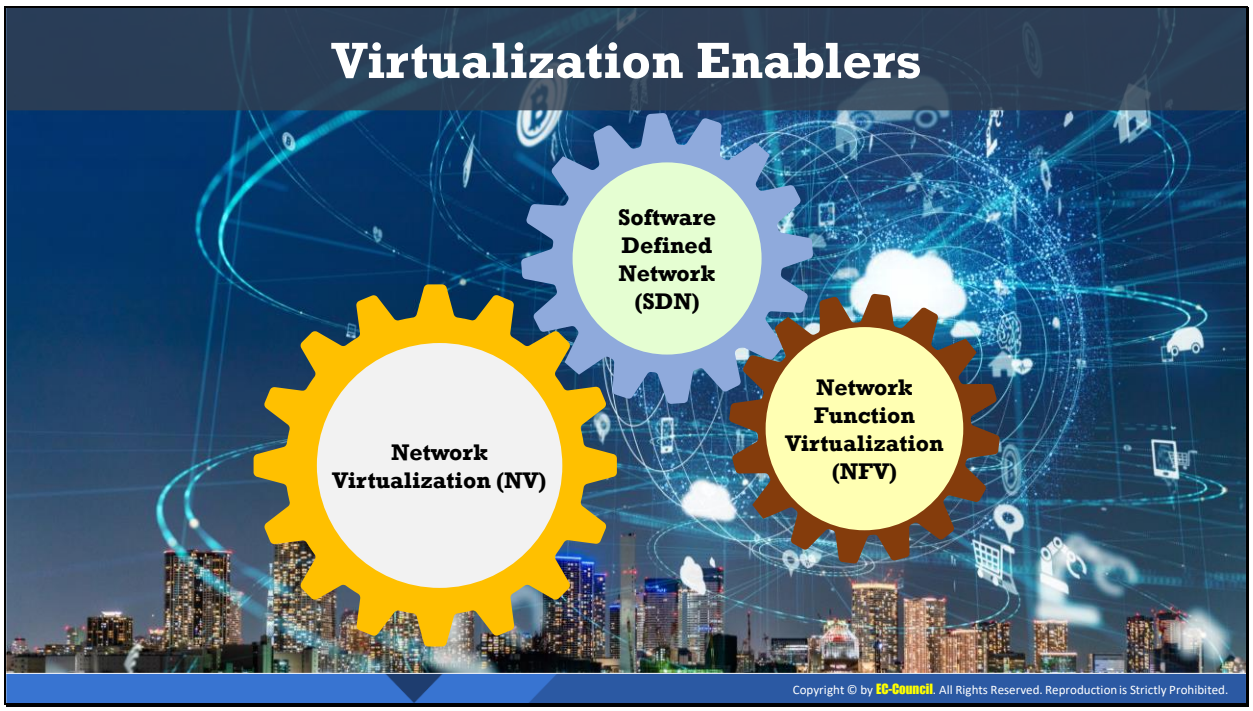


Figure 6.3: Components of virtualization

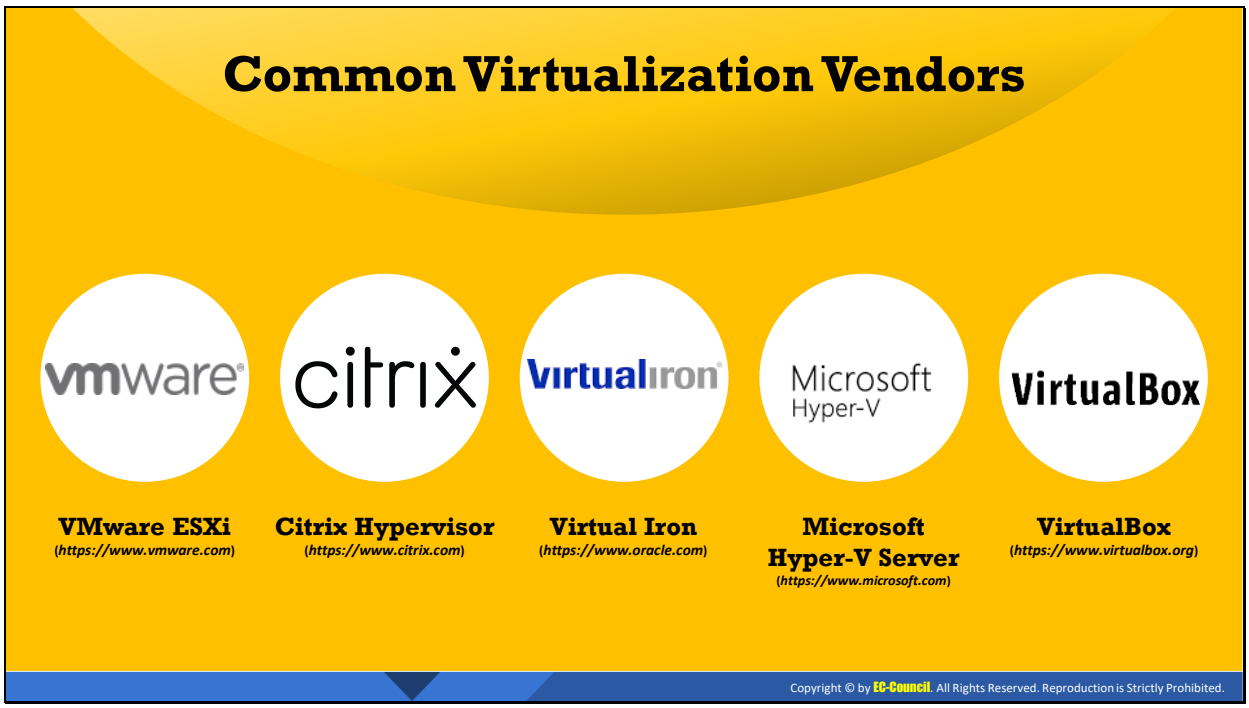
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Virtualization Enablers

Some examples of technologies by which virtualization can be realized are network virtualization (NV), software-defined network (SDN), and network function virtualization (NFV). These technologies are key enablers responsible for creating virtual environments. They help in creating logical and virtual networks that are decoupled from the underlying network hardware, and these virtual networks can be integrated with virtual environments. The virtual networks can run independently over a physical network in a hypervisor. Software-defined network (SDN) and network functions virtualization (NFV) are responsible for decoupling control and forwarding planes. These technologies combine hardware and software to create a completely software-defined network that enables simpler provisioning and management of network resources and play key role in virtualization.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Common Virtualization Vendors

A hypervisor is software that runs and manages virtual machines. Many popular hypervisors, provided by various vendors, exist. They include,

- **VMware ESXi**

  Source: *https://www.vmware.com*

  VMware ESXi effectively partitions hardware to consolidate applications and cut costs with direct access to and control of underlying resources. It installs directly onto a physical server. VMware ESXi enables,

  - Consolidation of hardware for higher capacity utilization.
  - Enhanced performance for a competitive edge.
  - Streamlining of IT administration through centralized management.
  - Reduced capital expenditure (CapEx) and operating expense (OpEx).
  - Minimization of hardware resources needed to run the hypervisor, resulting in greater efficiency.

- **Citrix Hypervisor**

  Source: *https://www.citrix.com*

  The Citrix Hypervisor virtualization management platform is optimized for application, desktop, and server virtualization infrastructures. It enables organizations of any vertical or size to transform their business IT computational infrastructures.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **Virtual Iron**

  Source: *https://www.oracle.com*

  Virtual Iron provides enterprise-class software for server virtualization and virtual infrastructure management. With advanced capabilities provided by Virtual Iron, users can:

  - Virtualize enterprise-class workloads running on unmodified Windows and Linux operating systems.
  - Improve the utilization of current systems and reduce power, space, and cooling issues through server consolidation.
  - Quickly set up development, test, and production environments.
  - Recover from failures quickly, reliably, and cost-efficiently.
  - Match resource capacity to workload demands automatically.
  - Reduce human labor and errors via policy-based automation.

- **Microsoft Hyper-V Server**

  Source: *https://www.microsoft.com*

  Hyper-V in Windows Server enables the creation of a virtualized computing environment to create and manage virtual machines. Multiple operating systems can be run on one physical computer and the operating systems can be isolated from each other.

- **VirtualBox**

  Source: *https://www.virtualbox.org*

  VirtualBox is a powerful x86 and AMD64/Intel64 virtualization product for enterprise as well as home use. VirtualBox is a feature-rich, high-performance product for enterprise customers, and is the only professional solution that is freely available as Open Source Software under the terms of the GNU General Public License (GPL) version 2.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

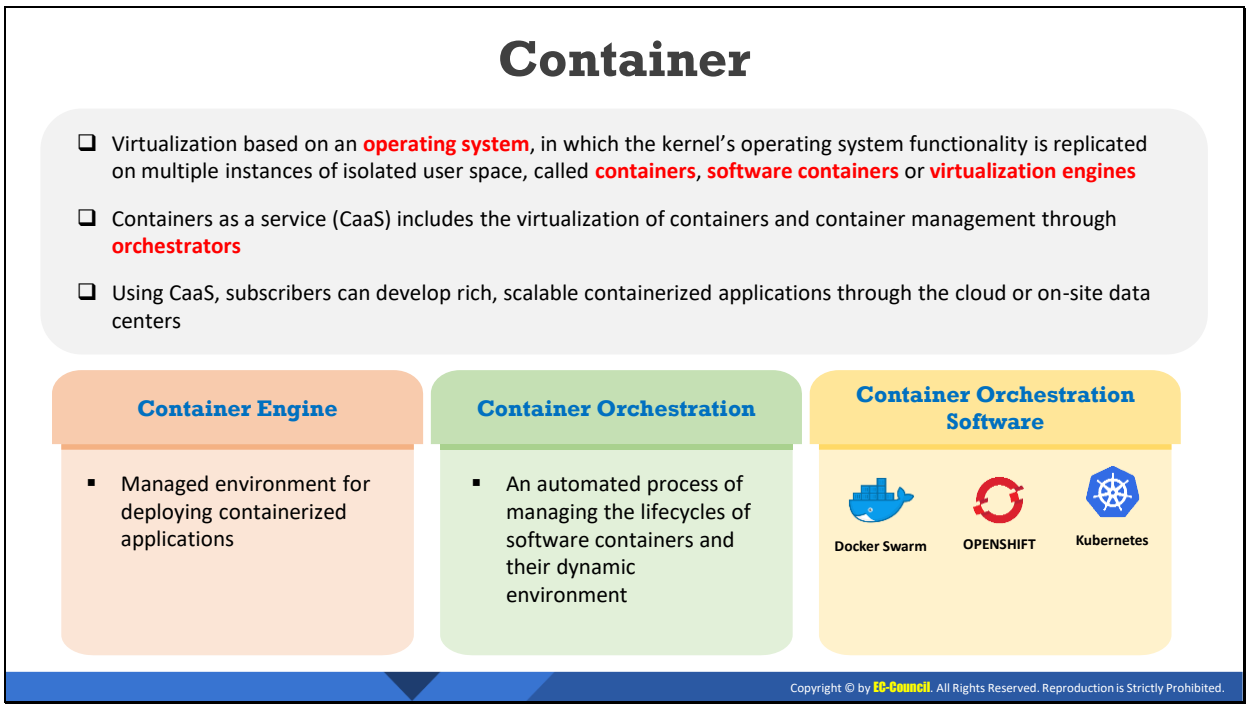
https://t.me/learningnets

OS Virtualization Security and Concerns

In OS virtualization, the host operating system's kernel is virtually replicated in multiple instances of isolated user space, called containers, software containers, or virtualization engines, thereby lending (virtualized) operating system functionality to each container.

A container is widely used for encapsulating an application and its dependencies in its own environment and runs in isolation from other containers and applications while utilizing the same resources and operating system. This section discusses vulnerabilities, attacks and security challenges associated with containers. The section also explains vulnerabilities, attacks and security challenges associated with Docker and Kubernetes, which are widely used for developing, packaging, running, and managing applications and all their dependencies in the form of containers.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Container

Containers (also called software containers or virtualization engines) refer to virtualization based on an operating system, in which the kernel's operating system functionality is replicated on multiple instances of isolated user space.

This can be used, for example, in a virtual hosting environment that requires segmentation of the physical resources among multiple users to enable each user to have their own virtual space. Containers help to manage the users and their respective resources, while keeping them isolated. The containers, are monitored and managed by the administrator having full admin rights to all the containers**.**

Many virtualization problems are effectively resolved with containerization. In containerization, although each user space instance runs in isolation, resources are not wasted since the actual operating system runs independently of the containers. A container encapsulates an application and its dependencies in its own environment while utilizing the same resources and operating system as other containers. Compared to VMs, each container image is more easily migrated and shared because of their smaller sizes. As only one operating system is involved, a container can be easily maintained. Containers also minimize hardware costs since multiple applications run on the same hardware, increasing the utilization of the hardware.

The following are some services and technologies that can be used to deploy and manage containers.

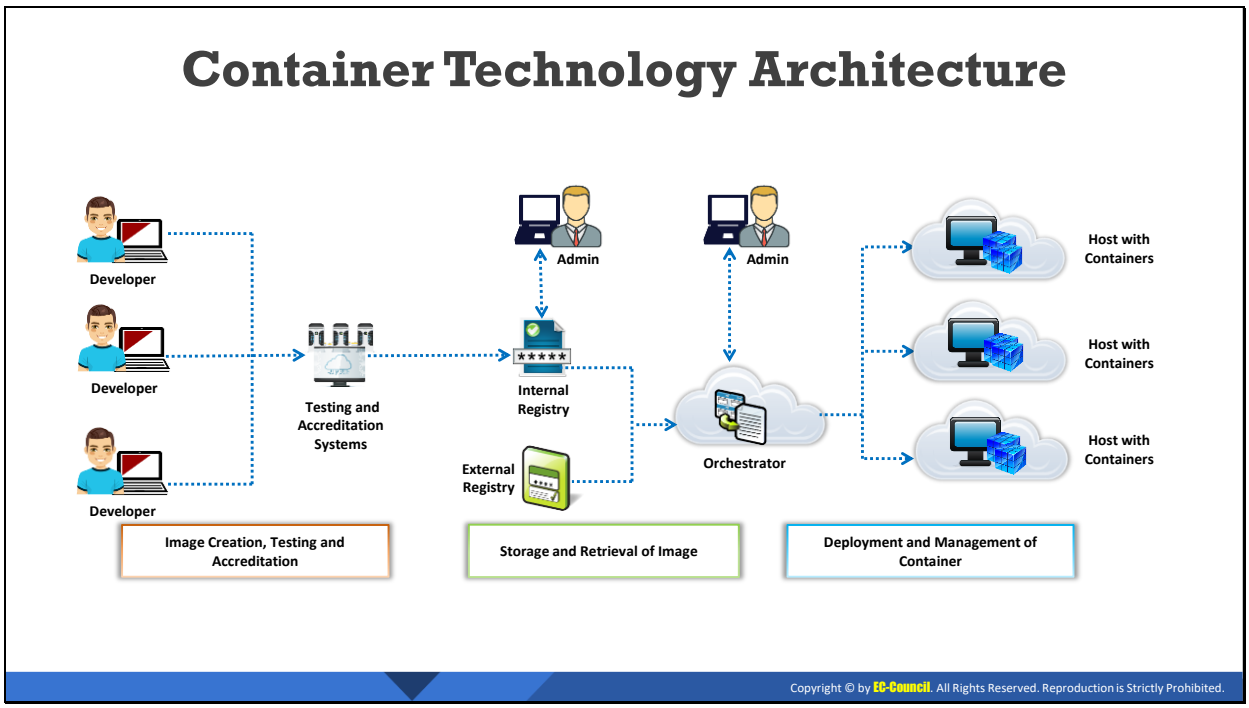
- **Containers as a service (CaaS):** This refers to services that enable the deployment of containers and container management through orchestrators. Using CaaS, subscribers can develop rich, scalable containerized applications through the cloud or on-site data centers.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **Container Engine:** A container engine can be used to create, add, and remove containers as per requirements. It manages the environment for deploying containerized applications.
- **Container Orchestration:** This refers to an automated process of managing the lifecycles of software containers and their dynamic environment. Currently available open-source container orchestrators are Kubernetes and Docker Swarm, and a commercial container orchestrator is OpenShift by Red Hat.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Container Technology Architecture

Container technology architecture comprises the following five tiers:

- The developer creates the images and sends them for testing and accreditation.
- The testing and accreditation systems validate, verify, and sign the images and send them to the registry.
- At registries, the images are stored and distributed upon request from an orchestrator.
- At orchestrators, the images are converted into containers and deployed to the hosts.
- The host runs and stops the containers on the direction of the orchestrator.

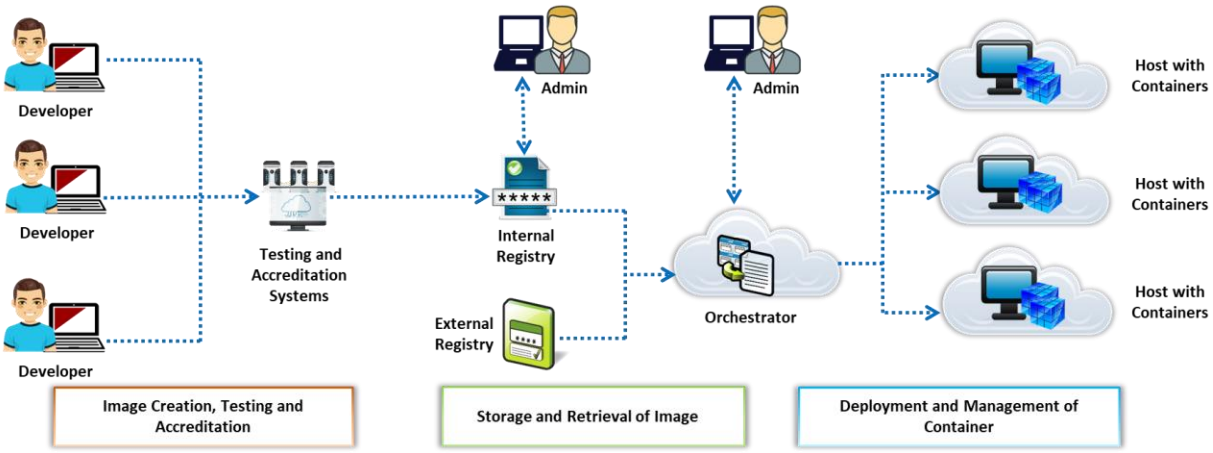
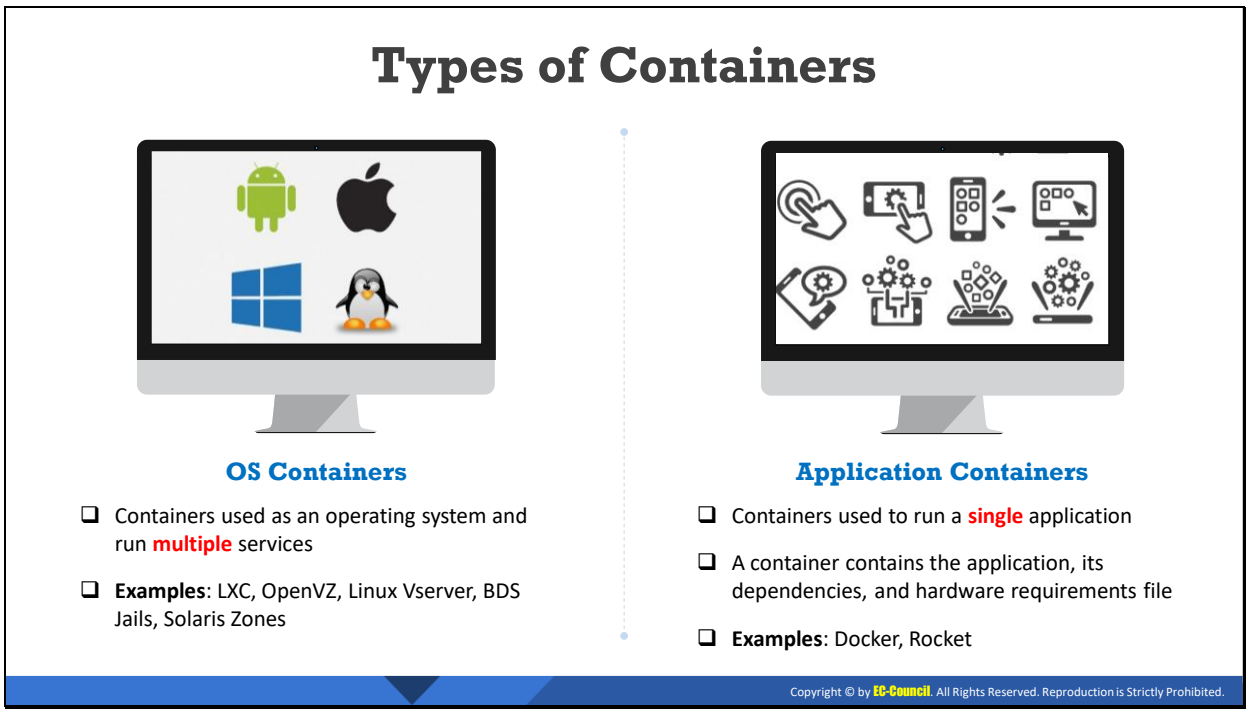


Figure 6.4: Container technology architecture

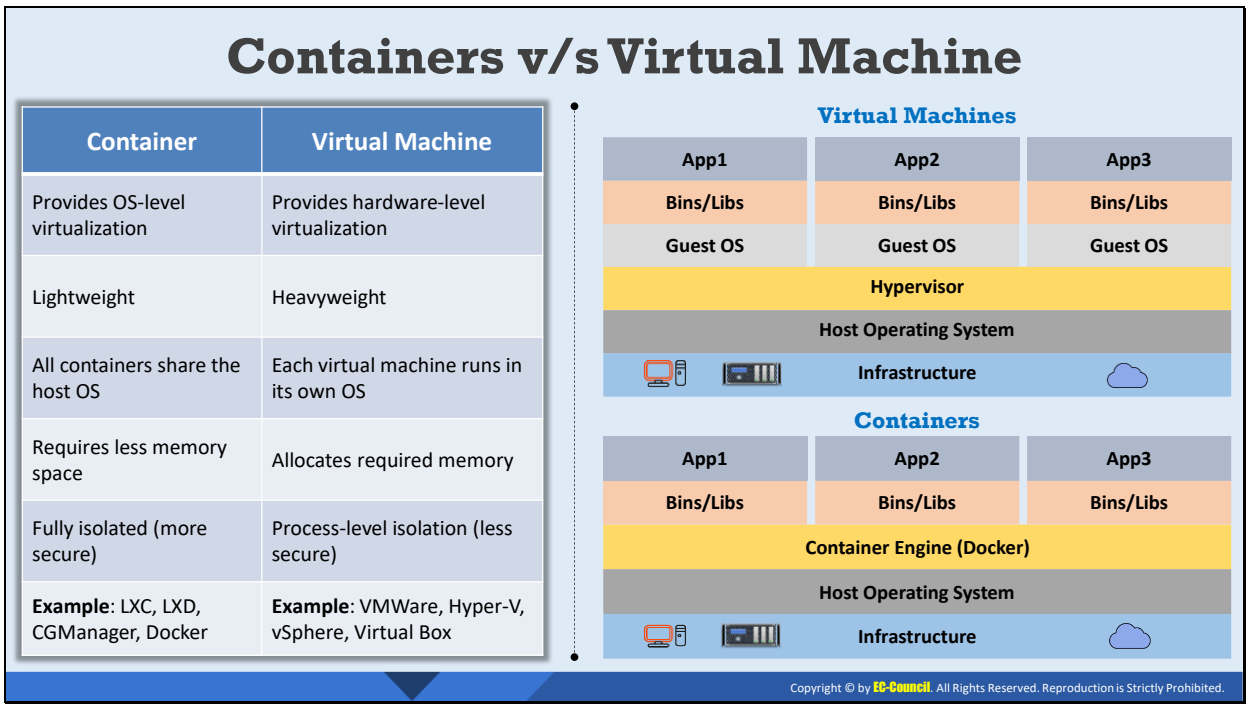
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Types of Containers

- **OS Containers**: OS containers are virtual environments sharing the kernel of the host environment that provides them isolated user space. The user can install, configure, and run different applications, libraries, etc. in OS containers. OS containers run multiple services and processes. OS containers are suitable for users that require an operating system to install various libraries, databases, etc. Examples of OS containers are LXC, OpenVZ, Linux Vserver, BSD Jails, and Solaris Zones.
- **Application Containers**: These are containers used to run a single service. They have layered file systems and are built on top of OS container technologies. Application containers are suitable for users that require to package an application and its components together for distribution. Examples of application containers are Docker and Rocket.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Containers v/s Virtual Machine

Containers and virtual machines decrease resource requirements and increase functionality. The differences between a container and a virtual machine are as follows.

	Container	Virtual Machine
Definition	Virtualization based on an operating system, in which the kernel's operating system functionality is replicated on multiple instances of isolated user space.	An operating system or application environment that runs on a physical machine.
Type	Lightweight.	Heavyweight.
Virtualization	Provides OS virtualization.	Provides hardware-level virtualization.
Memory Space	Requires less memory space.	Requires more memory space.
Security	Process-level isolation (less secure).	Fully isolated (more secure).
Start-up Time	Start-up time is in milliseconds.	Start-up time is in minutes.
Operating System	Host OS is shared.	Each VM has its own OS.
Providers	Examples: LXC, LXD, CGManager, Docker.	Examples: VMware, Hyper-V, vSphere, Virtual Box.

Table 6.1: Containers Vs Virtual Machines

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

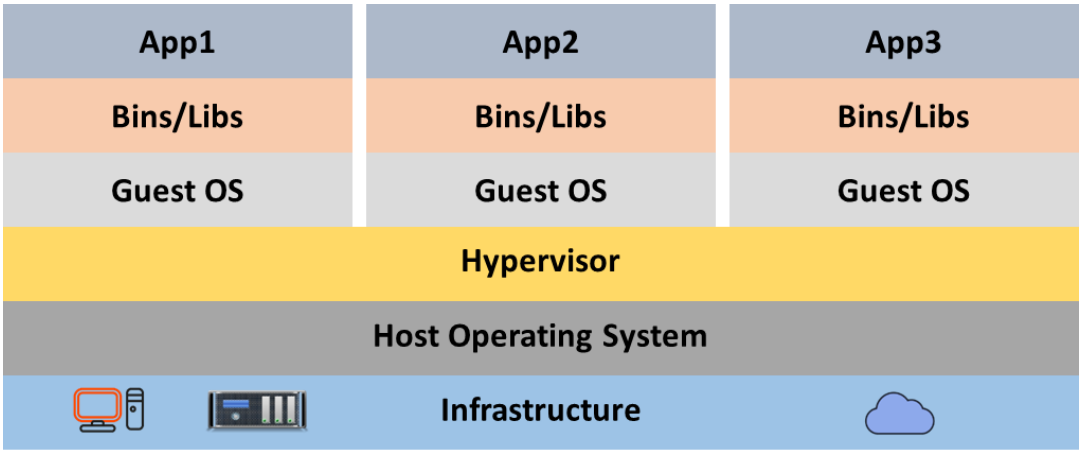


Figure 6.5: Virtual machine

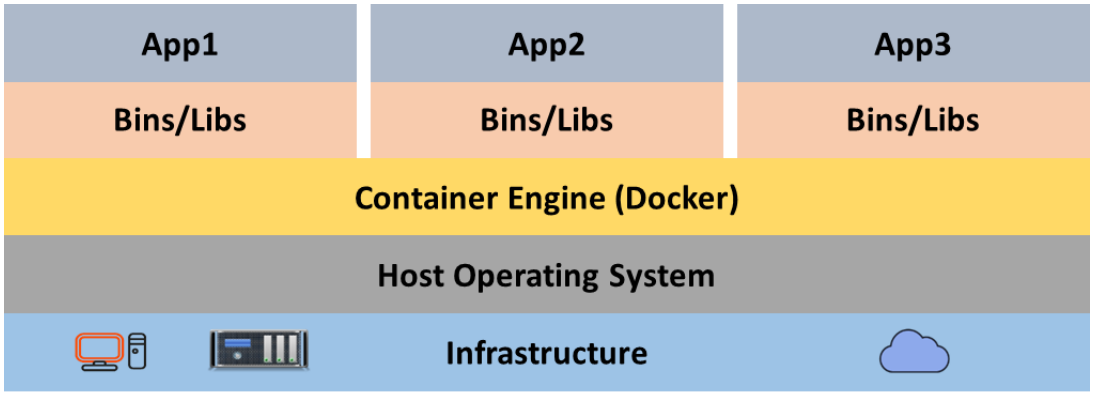
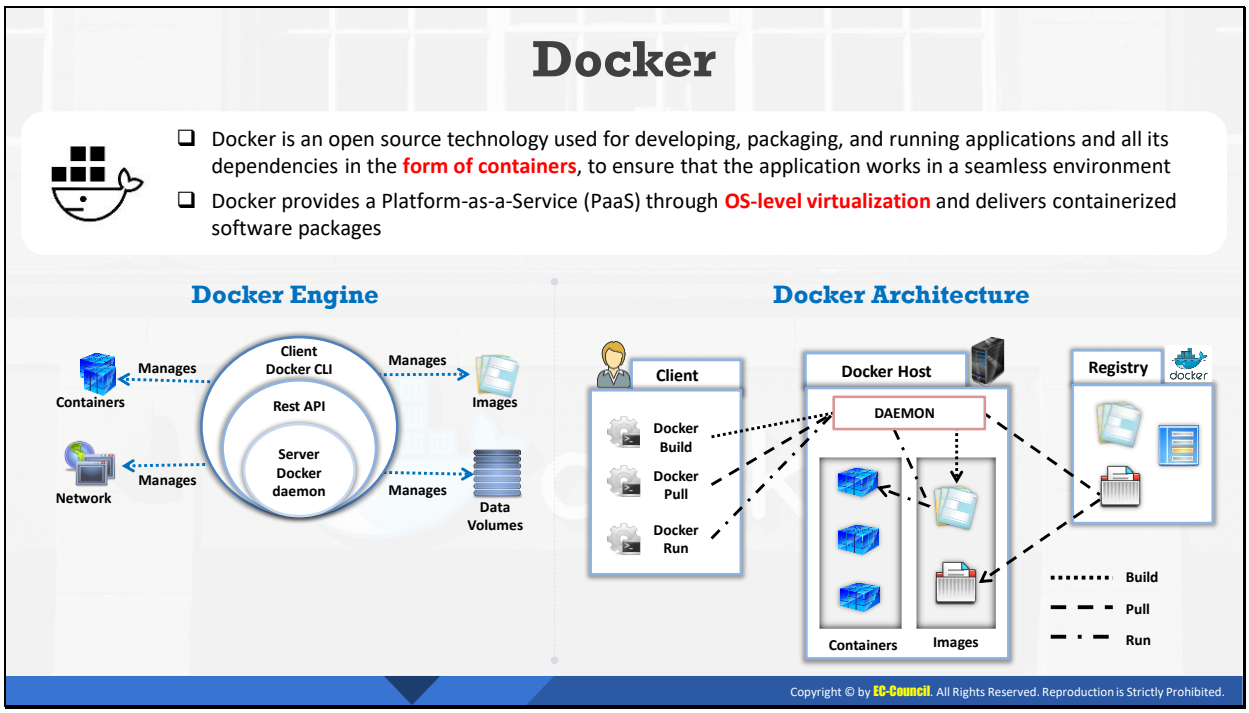


Figure 6.6: Container

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Docker

Docker is an open source technology used for developing, packaging, and running applications and all their dependencies in the form of containers, to ensure that each application works in a seamless environment. Docker provides platform-as-a-service (PaaS) through OS-level virtualization and delivers containerized software packages.

Docker Engine: This is an application installed on the host machine and uses the following components to develop, assemble, ship, and run applications.

- **Docker Daemon**: This manages the Docker images, containers, networks, and storage volume, and processes the requests of the Docker API. It is responsible for container-related actions and communicates with other daemons in order to manage its services.
- **Docker Engine REST API**: This API is used by an application to communicate with the Docker daemon.
- **Docker CLI**: This is a command line interface that is used to interact with the Docker daemon. Using CLI, users can execute commands (build, run, and stop applications) to a Docker daemon.

Docker Systems Working Mechanism: The Docker client interacts with the Docker daemon using a REST API through Unix sockets or a network interface. The Docker client and the Docker daemon can run on the same system, or the user can connect a Docker client to a remote Docker daemon.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Docker Architecture: The Docker architecture is based on a client-server model and has the following components:

- **Docker Client:** This enables the users to communicate with the Docker environment. The key function of the Docker client is to retrieve the images from the registry and run them on the Docker host. Some of the common commands of the Docker client are:

```
docker build
docker pull
docker run
```

- **Docker Host**: This provides the user an environment to run an application. The Docker host consists of Docker daemon, images, containers, networks, and storage. The following components are objects of the Docker host.
- **Images**: An image is a read-only binary template for building a container. Images are used to build a container or to configure the container with additional features. The container capabilities and requirements rely on the metadata of the images. Docker images are hosted by Docker registries.
- **Containers**: A container is an encapsulated environment to run an application. A container's access to resources is defined by the image. The user can also create a new image depending on the state of the container.
- **Networking**: Docker has networking drivers to support networking containers. It implements networking in an application-driven manner.
- **Docker Registries**: These are services that provide locations for storing and downloading images. While working with registries, frequently used commands are:

```
docker push
docker pull
docker run
```

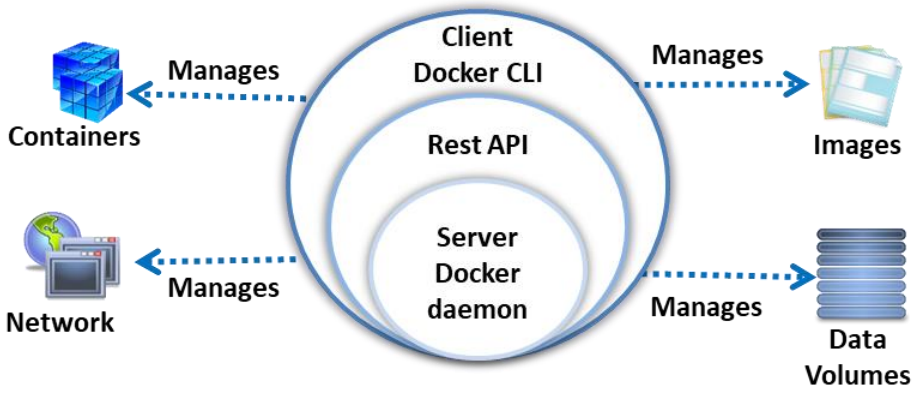


Figure 6.7: Docker engine

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

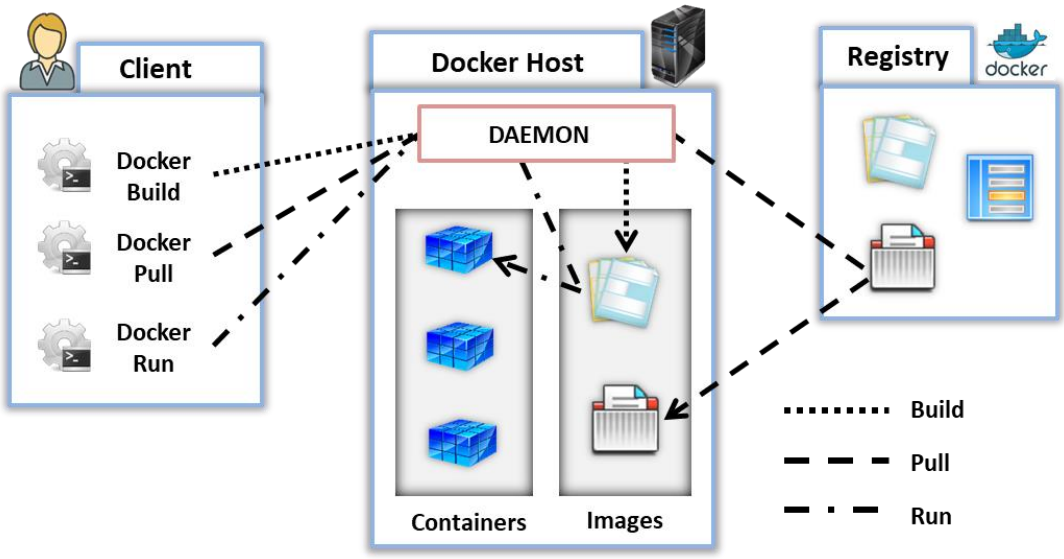
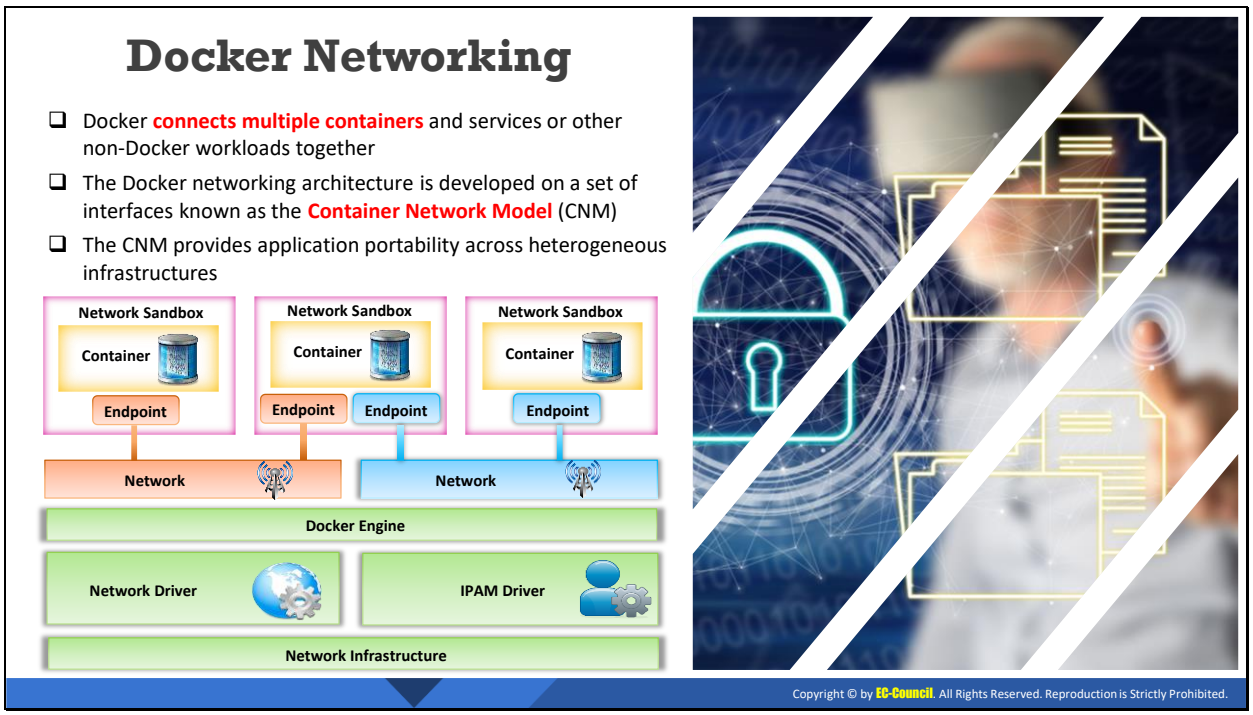


Figure 6.8: Docker architecture

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Docker Networking

Docker allows connecting multiple containers and services or other non-Docker workloads together. The Docker networking architecture is developed on a set of interfaces known as container network model (CNM). CNM provides application portability across heterogeneous infrastructures. CNM consists of the following five objects:

- **Sandbox**: This contains the configuration of a container's network stack such as routing table, management of container's interfaces, and DNS settings. It may have multiple endpoints from various networks. CNM sandbox can be implemented for Windows HNS, Linux network namespace, or a FreeBSD jail.
- **Endpoint**: This connects a sandbox to a network and abstracts the actual connection to the network from the application. An endpoint aids in maintaining portability, to enable the service to utilize various types of network drivers.
- **Network**: A network is a collection of endpoints that have connectivity between them. When a network is created or updated, the corresponding driver is notified. A CNM network can be used to implement a Linux bridge, VLAN, etc.
- **CNM Driver Interfaces**: CNM has two pluggable and open interfaces for the users, vendors, community, etc. to drive additional functionality, visibility, and control in the network. The following are the drivers in the CNM model:
  - **Network Drivers**: These are pluggable and provide the actual implementation for the functioning of the network. Multiple network drivers can be simultaneously used on a Docker engine or cluster, but each Docker network is represented by a single driver.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

There are two types of CNM network drivers.

- **Native Network Driver**: These drivers are provided by Docker.
- **Remote Network Driver**: These drivers are created by the community and vendors based on their requirements.

- **IPAM Drivers**: IP address management (IPAM) drivers in Docker provide default subnets or IP addressing to the network and the endpoints. A user can also assign an IP address manually through the network, container, and service create commands.

- **Docker Native Network Drivers:** These are native drivers in the Docker engine and can be used through Docker network commands. The following are the various Docker native network drivers.
  - **Host**: The host driver enables the container to use the host networking stack.
  - **Bridge**: With the bridge driver, a Linux bridge is created on the host, which is managed by the Docker.
  - **Overlay**: An overlay network is created with the overlay driver and enables container-to-container communication over the physical network infrastructure.
  - **MACVLAN**: With the MACVLAN driver, a network connection is created between container interfaces and its parent host interface (or sub-interfaces).
  - **None**: The none driver enables the container to implement its own networking stack and is isolated from the host networking stack.

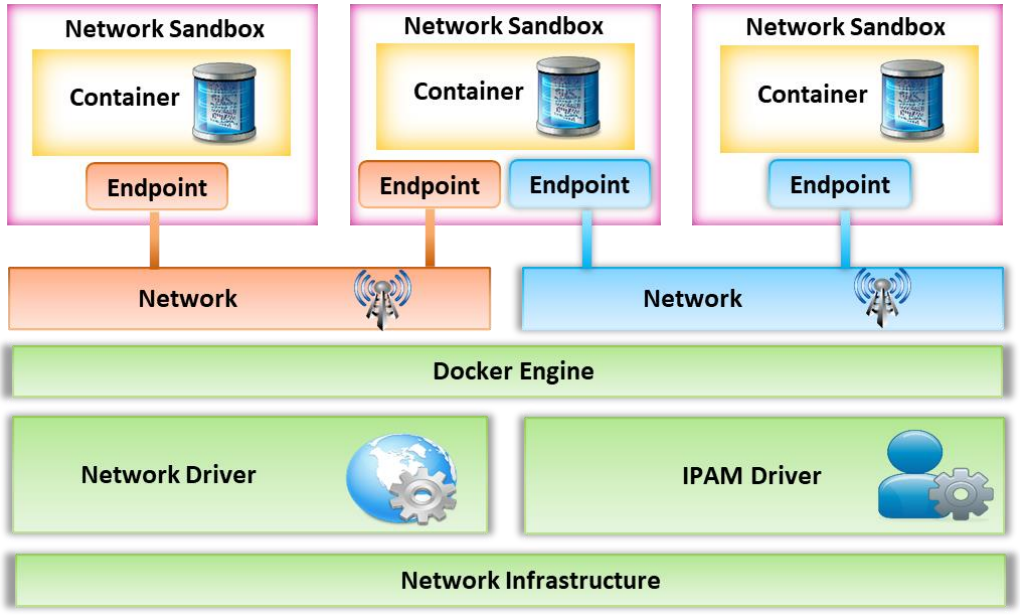
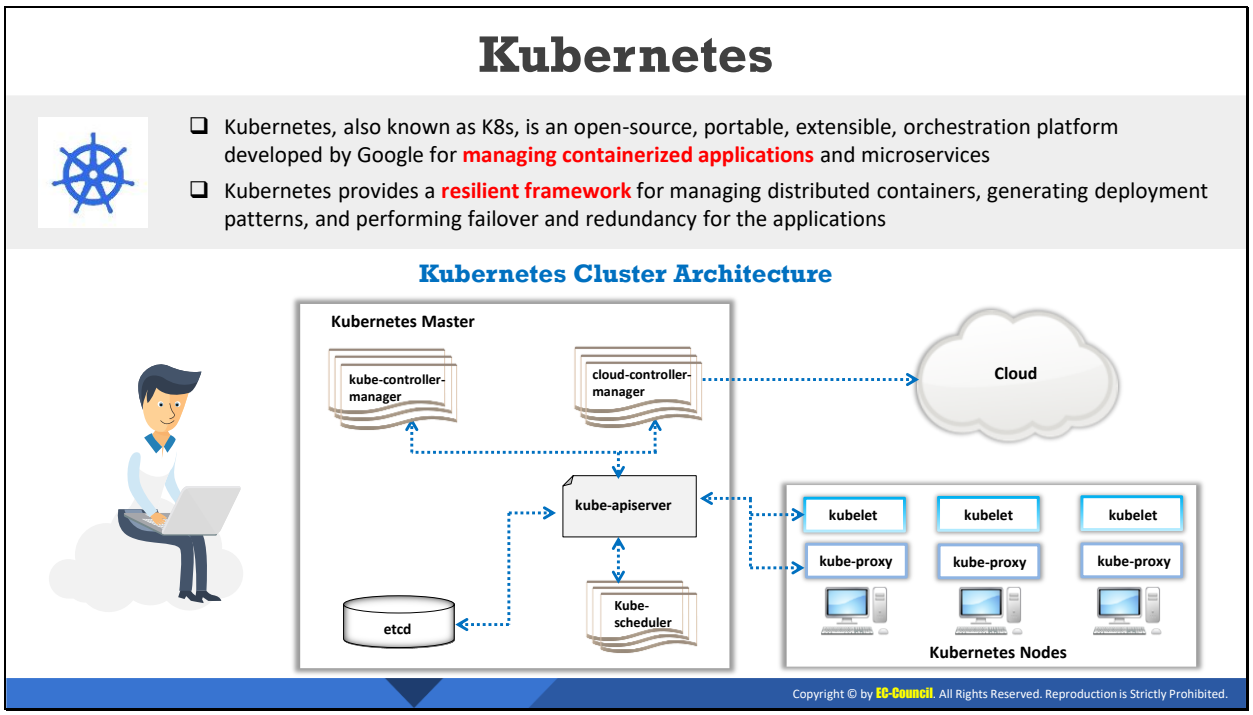


Figure 6.9: Docker Networking

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Kubernetes

Kubernetes, also known as K8s, is an open-source, portable, extensible, orchestration platform developed by Google for managing containerized applications and microservices. Kubernetes provides a resilient framework to manage distributed containers, generate deployment patterns, and perform failover and redundancy for the applications.

Kubernetes Cluster Architecture

In the Kubernetes cluster, the Kubernetes nodes are worker machines, which run the containerized applications. There should be at least one worker node in a cluster. The worker nodes host the pods, which refer to groups of containers that are deployed together on the same host. The components of a Kubernetes cluster are as follows:

- **Control Plane Components**

  The components of the control plane perform decisions for the Kubernetes cluster such as scheduling or staring a new pod. The following are the control plane components of the cluster:

  - **Kube-apiserver**: The Kubernetes control plane has an API server in its front end. Kube-apiserver is the implementation of the Kubernetes API server. The user can run multiple instances of kube-apiserver to facilitate the maintenance of the traffic between the instances.
  - **etcd**: This is a backing store for the data in the Kubernetes cluster. For example, if the user specifies that three instances of a specific pod should be executed, this information is stored in etcd. The data stored in etcd is used to determine the number of instances that are running. If an instance is not working, Kubernetes creates an additional instance of the same pod.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **Kube-scheduler**: The kube-scheduler monitors newly created pods that do not have any assigned nodes, and assigns each of them a node to run on.
- **kube-controller-manager:** Kube-controller-manager runs the controller processes. It consists of a node controller, replication controller, endpoints controller, service account, and token controllers. To minimize complexity, all these controllers are compiled and run as a single process.
- **cloud-controller-manager:** This runs the controller that communicates with the cloud providers. The cloud-provider-specific controller loops are run by cloud-controller-manager. When a kube-controller-manager is initialized, the user can disable the controller loops by setting the -cloud-provider flag to external. The controllers with cloud provider dependencies are node controller, route controller, service controller, and volume controller.

- **Kubernetes Node**

  A Kubernetes node is a worker machine that contains the services required to run the pods, and is managed by master components. The services on Kubernetes nodes are as follows:

  - **Kubelet:** This is a node agent that ensures that the containers are running in a pod. A pod contains a PodSpec, which is a YAML or JSON object. The kubelet ensures that the containers mentioned in the PodSpecs are running and healthy.
  - **Kube-proxy:** This is a network proxy that runs and maintains network rules on each node.
  - **Container Runtime:** This is a software that downloads the images and runs the containers. Kubernetes supports container runtimes such as Docker, CRI-O, and the Kubernetes container runtime interface (CRI).

- **Kubernetes Features**

  - **Service Discovery and Load Balancing**: Kubernetes represent a container using the DNS or its own IP address. In case the network traffic to the container is high, Kubernetes utilizes load balancing to distribute the traffic.
  - **Storage Orchestration**: Kubernetes enables the user to choose between storage systems such as local storage, public cloud providers (AWS or GCP), or a network storage system.
  - **Automated Rollouts and Rollbacks:** Kubernetes enables the user to change the actual state of the container to the desired state of the container at a controlled rate.
  - **Automatic bin packing:** To utilize resources effectively, Kubernetes fits the containers into nodes depending on the specifications provided by the user.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- **Self-healing:** Kubernetes self-heal the containers by restarting failed containers. If a node is dead, Kubernetes replaces and reschedules the containers. When a container fails to respond to user-defined health checks, Kubernetes kills the container. Kubernetes also advertises the containers that are in working condition.
- **Secret and Configuration Management:** Kubernetes enables users to store and manage confidential information such as passwords, OAuth tokens, and SSH keys.

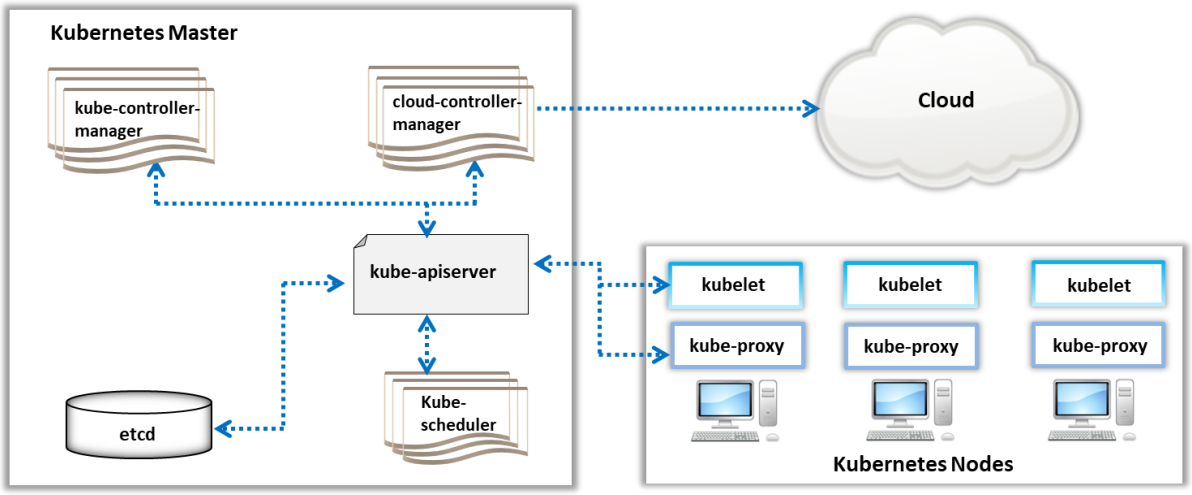
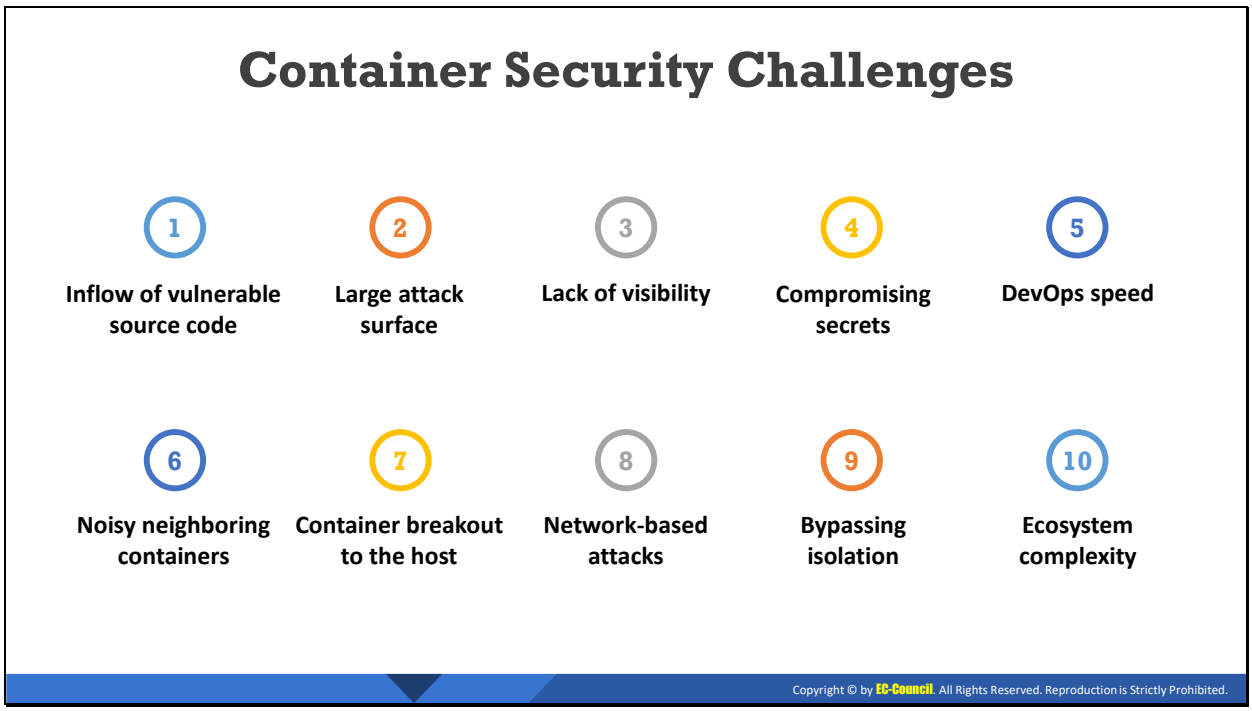


Figure 6.10: Kubernetes cluster architecture

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Container Security Challenges

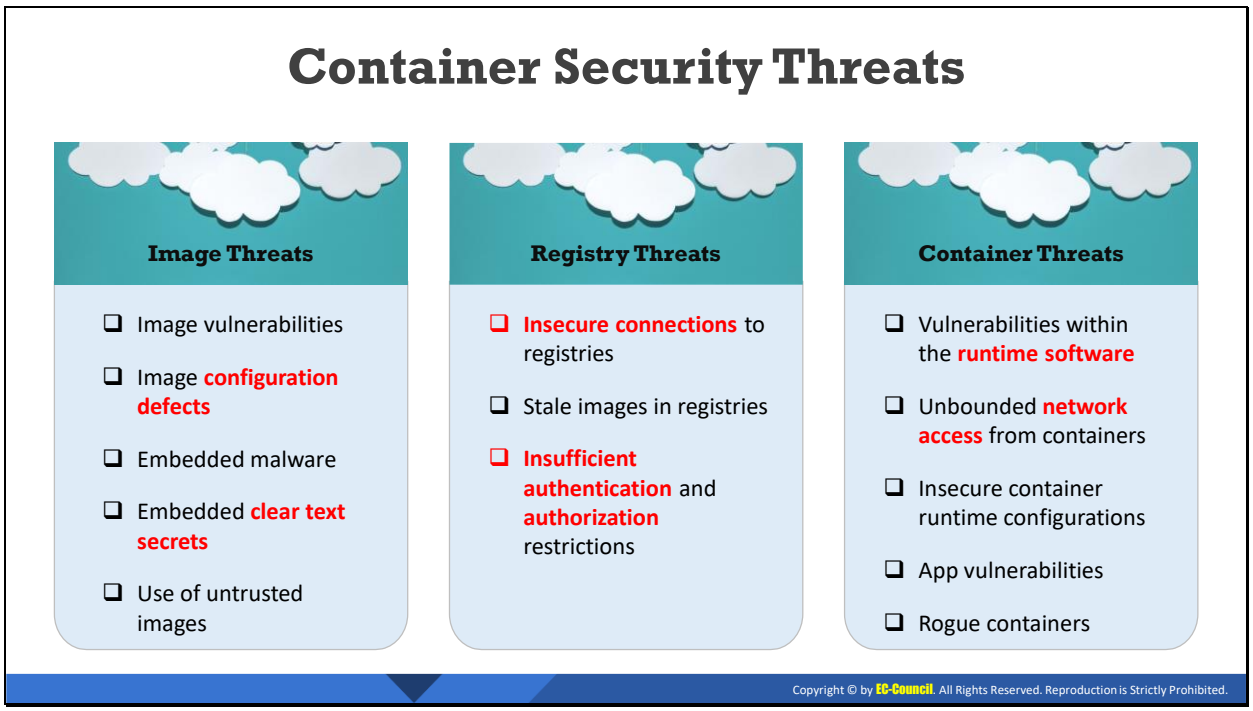
While containerization provides fast and continuous delivery of applications to developers and DevOps teams, there are certain security challenges associated with it. The primary security challenges for containers are as follows:

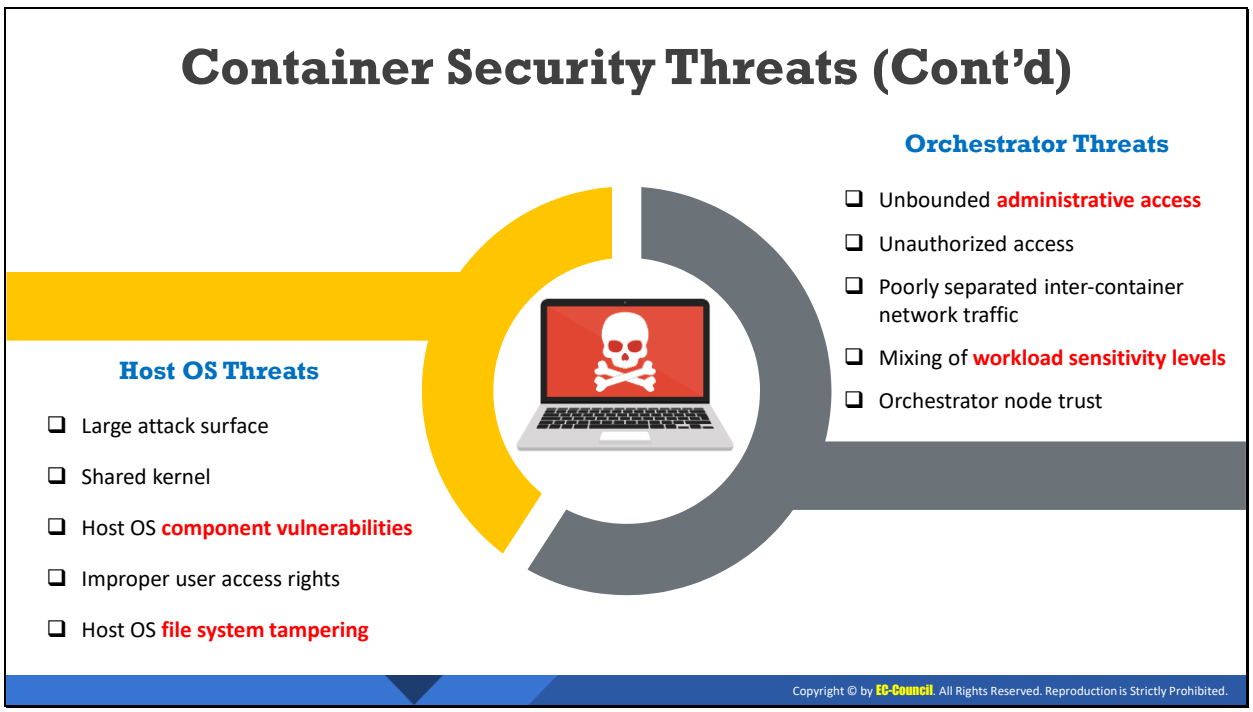
- **Inflow of Vulnerable Source Code**: Since containers are open source**,** the images that are created by the developers are frequently updated, stored, and used as needed. This causes an inflow of source code that may potentially harbor vulnerabilities and unexpected behaviors, into an organization.
- **Large Attack Surface:** In cloud or on-premises, there are many containers than run on multiple machines. This provides a large attack surface, and therefore causes challenges in the tracking and detection of anomalies.
- **Lack of Visibility:** The abstraction layer created by the container engine masks the activity of a particular container.
- **DevOps Speed:** On average, the lifespan of a container is four times less than virtual machines. Containers can be created instantly, run for a short duration of time, stopped, and removed. Due to this ephemerality, an attacker can execute an attack and disappear quickly.
- **Noisy Neighboring Containers:** The behavior of one container can potentially cause a DOS for another container. For example, opening sockets frequently can freeze up the host machine.
- **Container Breakout to the Host:** Containers that run as the root user can breakout and access the host's operating system.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **Network-based Attacks:** A jeopardized container is vulnerable to network-based attacks, especially in outbound networks with unrestricted raw sockets.
- **Bypassing isolation/Lack of isolation**: Any inadequacy in the isolation between containers can be a security challenge since an attacker who compromises one container can then easily access another container in the same host.
- **Ecosystem complexity**: The tools utilized to build, deploy, and manage containers are provided by different sources. Therefore, a user should keep the components secure and up-to-date.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets





Container Security Threats

Containers are among the most important technologies in DevOps, and many organizations are adopting this technology to develop, test, package, and deploy the applications. Nevertheless. the increased use of containers is exposing companies to new security threats. Therefore, there is a need to secure containers throughout the development pipelines from these security threats.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

The threats that are associated with container ecosystems are as follows:

- **Image Threats**
  - **Image Vulnerabilities**: Since images are static archive files consisting of components that run an application, lack of updates in the image components or the missing of critical security updates make the image vulnerable. If the version of the image that is utilized to make a container has vulnerabilities, it poses a risk to the containerized environment.
  - **Configuration Defects**: In addition to software defects, the image of a container is also subject to configuration defects. For example, an image may fail to configure with a specific user account, and instead run with greater privileges than required.
  - **Embedded Malware**: As an image is a collection of files that are packed together, there is a likelihood that malicious files are included in the image package intentionally or inadvertently. Such embedded malware has the same privileges as other components of the image and could be used to attack other containers or hosts.
  - **Embedded Clear Text Secrets**: Most applications require secrets to securely communicate with other components. For example, a web application requires a username and password to connect to the backend database. When an application is packed into an image, these secrets get embedded into the image. This embedded clear text secret poses a security risk as a user having access to the image can parse the image to extract these secrets.
  - **Use of Untrusted Image**: The use of untrusted images can introduce malware, leak data, or introduce components with vulnerabilities. It is recommended that running any image in a container from untrusted sources is avoided.
- **Registry Threats**
  - **Insecure Connections to Registries**: Images may contain sensitive components such as proprietary software and embedded secrets. An insecure connection to the registries can enable a man-in-the-middle attack.
  - **Stale Images in Registries**: A registry contains all images that an organization deploys. Over time, it is possible that the registry contains images that are vulnerable or out-of-date. These vulnerable images would not pose a threat during their storage in the registry but can increase the likelihood of accidental deployment of the vulnerable image.
  - **Insufficient Authentication and Authorization Restrictions**: Since registries contain images that may run sensitive or proprietary software, insufficient authentication and authorization expose the technical details of the application to the attacker.
- **Orchestrator Risks**
  - **Unbounded Administrative Access**: Most orchestrators are designed presuming that all the users that are interacting with them are administrators. In most cases, a

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

single orchestrator runs many applications, each managed by different teams. If access to a user or group is not scoped to their requirements, then a malicious user can affect the functionality of different containers managed by the orchestrator.

- **Unauthorized Access:** The orchestrators have their authentication directory service, which could be separated from other directories of an organization, leading to orphan accounts in orchestrator. These accounts are highly privileged, and their compromise can subsequently lead to system-wide compromise. The data storage volumes of a container are managed by the orchestration tool. Many organizations encrypt the stored data to prevent unauthorized access.
- **Poorly Separated Inter-Container Network Traffic:** The network traffic between each node is routed through a virtual overlay network, which is managed by the orchestrator and is obscure to network security and management tools.
- **Mixing of Workload Sensitivity Levels**: The orchestrators' primary focus is to enhance the density of workloads. By default, the orchestrator places the workloads of different sensitivities on the same host. For example, in a default state, the orchestrator may place a container running a public-facing web server and another processing financial data on the same host because the host has more available resources at the time of deployment. Due to the mixing of workload sensitivity levels, the container processing financial data can be easily compromised.
- **Orchestrator Node Trust:** Maintaining trust between the nodes in an environment is crucial. As the orchestrator is the foundational node, if the configuration of the orchestrator is weak, it can expose the orchestrator as well as other components of the container technology to increased risk.

- **Container Risks**
  - **Vulnerabilities within the Runtime Software:** The attacker can exploit vulnerabilities within the runtime software to compromise it. Subsequently, the attacker can utilize the compromised runtime software to perform other activities such as attack other containers and monitor container-to-container communication.
  - **Unbounded Network Access from Containers:** In the default state, most containers during runtime access other containers or the host OS through the network. In case a container is compromised, permitting it access to the network traffic significantly increases the risk to other containers in the environment.
  - **Insecure Container Runtime Configurations:** During container runtime, the administrator is exposed to many configurable options. The security of the system can be lowered if these options are improperly set.
  - **App Vulnerabilities:** Containers can be compromised because of flaws in an application that they run. This, however, is not a fault in the container, but rather that the vulnerabilities in the application within the container environment compromise the container.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

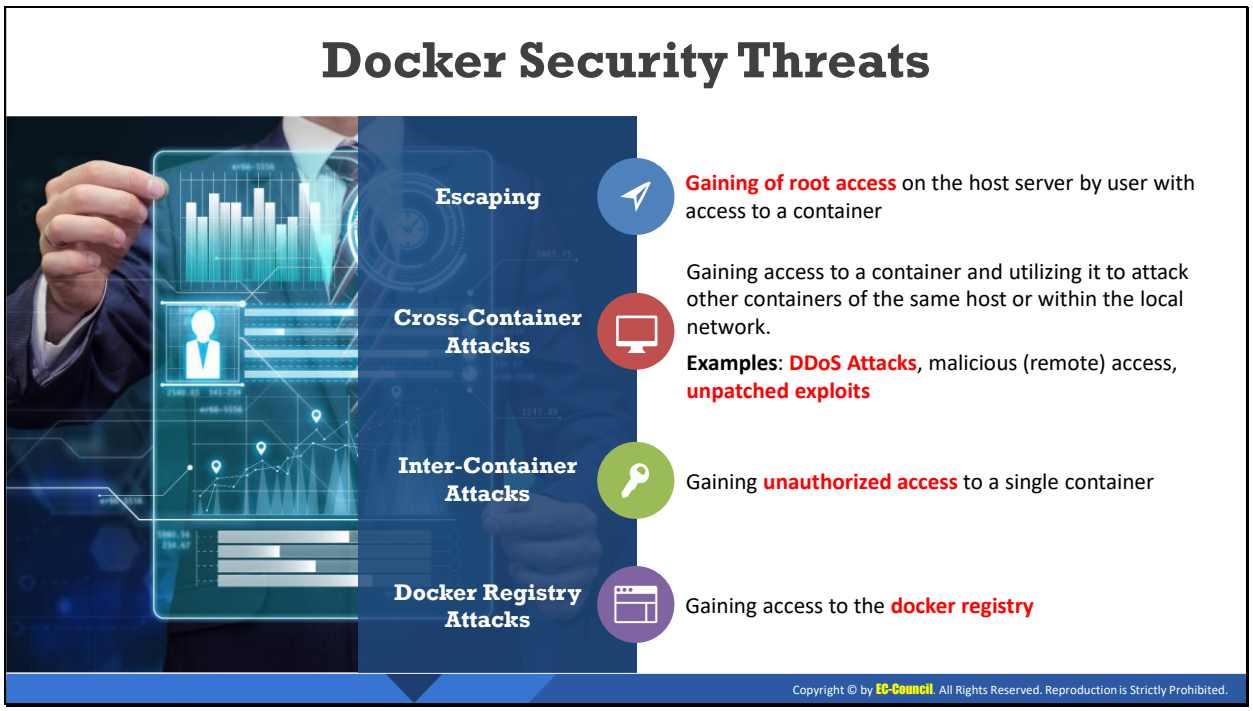
https://t.me/learningnets

- **Rogue Containers:** Rogue containers are unplanned or unsanctioned containers. They originate in the development environment when the application developer creates a container to test the code. If these containers are not properly configured or are not passed through the rigors of vulnerability scanning, they can be exploited.

- **Host OS Risks**
  - **Large Attack Surface:** The attack surface of the host OS is the collection of all possible points through which the adversary can attempt to gain access to and exploit the host OS vulnerabilities. A large attack surface increases the potential for an attacker to gain access to and compromise the host OS and the containers running on that host.
  - **Shared Kernel:** Compared to general-purpose OSes, container-specific OSes have a smaller attack surface area. However, a container has only software-level isolation of resources, and the usage of a shared kernel increases the inter-object attack surface.
  - **Host OS Component Vulnerabilities:** Vulnerabilities of the host OS components impact all the containers and applications running on the host.
  - **Improper User Access Rights:** An organization can be at risk when users sign in directly on the host to manage containers. Improper user access rights not only affect the host system but also all other containers present in it.
  - **Host OS File System Tampering**: If the configuration of a container is not secure, it exposes the host volumes to significant risk of file tampering. Host OS file system tampering affects the stability and security of the host and other containers running on it.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Docker Security Threats

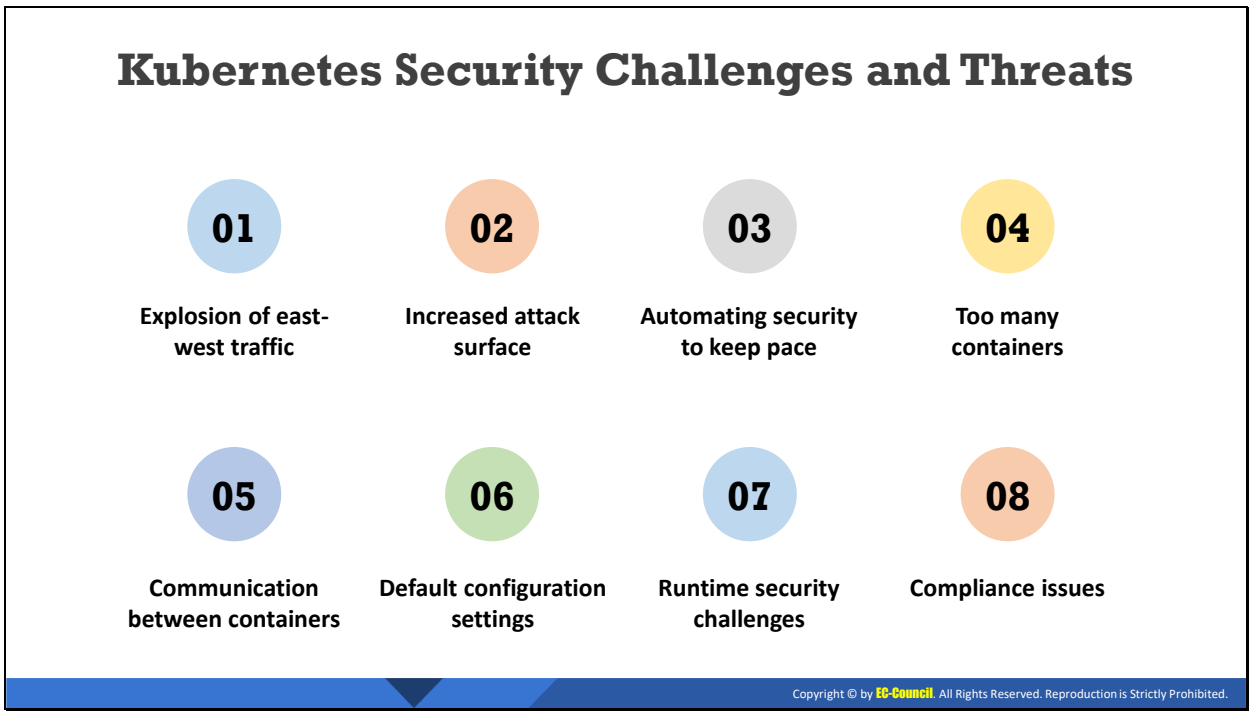
There are specific parts of the Docker infrastructure that are vulnerable to attacks. The following are common Docker security threats.

- **Escaping**: In this Docker-specific security threat, the adversary escapes the container and gains root access on the host server. The attacker then attempts to compromise other machines within the local network. The following factors may facilitate container breakouts:
  - Insecure defaults and weak configuration.
  - Information disclosure.
  - Weak network defaults.
  - Working with the root user (UID 0).
  - Mounting host directories inside containers.
- **Cross-Container Attacks:** In this type of attack, the adversary gains access to a container and utilizes it to attack other containers of the same host or within the local network. Cross-container attacks lead to DoS attacks (e.g. XML bombs), ARP spoofing and stealing of credentials, compromising of the sensitive container, etc. The following are common causes for cross-container attacks:
  - Weak network defaults.
  - Weak cgroup restrictions.
  - Working with the root user (UID0).

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **Inner-Container Attacks:** in this attack, the attacker gains unauthorized access to a single container. The potential causes for inner-container attacks are:
  - Overage software.
  - Exposure to insecure/untrusted networks.
  - Use of large base images.
  - Weak application security.
  - Working with the root user (UID 0)
- **Docker registry Attacks**
  - **Image forgery**: In an image forgery attack, the adversary gains access to the registry server and tampers the Docker image.
  - **Replay Attack**: In this type of attack, the adversary gains access to the registry server and provides outdated content.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Kubernetes Security Challenges and Threats

Kubernetes enables an organization to automate application deployment, which leads to tremendous growth in business. However, these deployments are vulnerable to attacks and exploitation from adversaries. Thus, security is a critical component for all deployments of Kubernetes. Containerization in clouds can be targeted through attacks such as ransomware attacks, cryptomining, data stealing, and service disruption. The hyperdynamic nature of containers is responsible for the following Kubernetes security challenges.

- **Explosion of East-West Traffic**: Since containers are dynamically deployed in multiple hosts or clouds, east-west traffic (traffic flow within a data center) and internal traffic should be monitored for attacks.
- **Increased Attack Surface**: Every container has an attack surface and vulnerabilities, which can be exploited by an adversary. Further, container orchestration tools like Docker and Kubernetes also increase the attack surface of the container.
- **Automating Security to Keep Pace:** Due to the dynamic nature and the constantly changing environment of the container, old models and security tools cannot provide complete protection. Therefore, there is a need to automate security for securing containers.
- **Too many containers:** Containers communicate with each other and with internal and external endpoints for proper functioning. However, if a container is exploited, all the other connected containers in the environment can also be breached.
- **Communication between containers:** Containers communicate with each other and with internal and external endpoints for proper functioning. However, if a container is exploited, all the other connected containers in the environment can also be breached.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

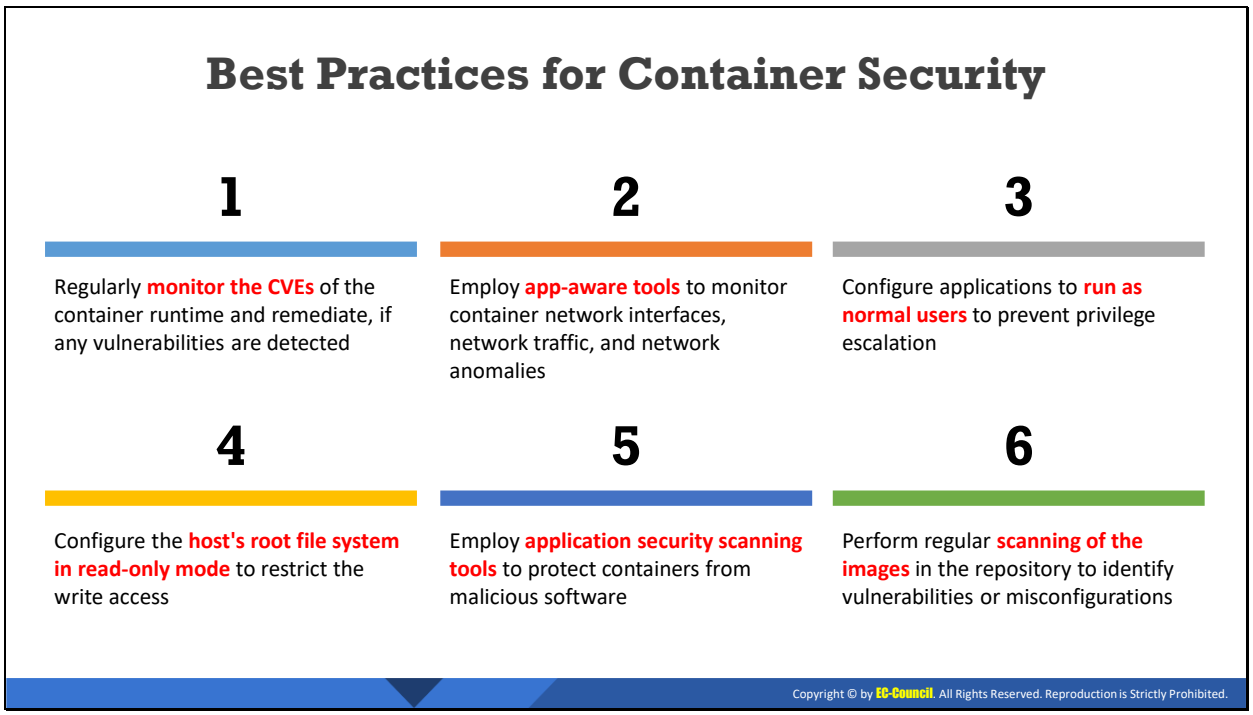
- **Default configuration settings:** Using the default settings in Kubernetes makes application development faster and helps in easy communication with all the components in the Kubernetes environment. However, using the default settings can also make Kubernetes more vulnerable and less secure.
- **Runtime security challenges:** The transient and fast nature of the container makes it difficult for an individual to monitor which container process is currently running. Hence, it also makes it more complex to detect any running malicious process.
- **Compliance issues:** Organizations should follow the techniques to ensure that the Kubernetes environment adheres to the security controls, industry standards, and internal organizational policies that were devised for conventional application architectures.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

OS Virtualization Security Best Practices

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

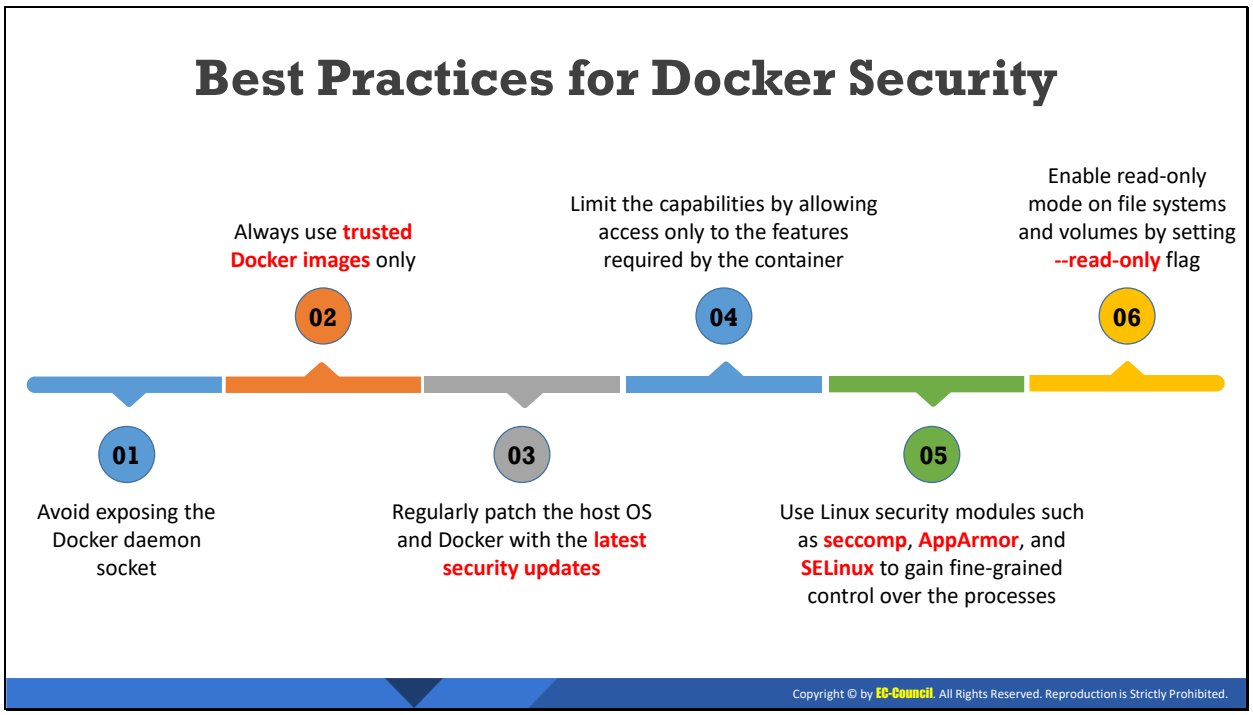


Best Practices for Container Security

Discussed below are various best practices for securing the container environment.

- Regularly monitor the CVEs of the container runtime and remediate, if vulnerabilities are detected.
- Employ app-aware tools to monitor container network interfaces, network traffic, and network anomalies.
- Configure applications to run as normal users to prevent privilege escalation.
- Configure the host's root file system in read-only mode to restrict the write access and prevent malware injection attacks.
- Avoid using third-party software and employ application security scanning tools to protect containers from malicious software.
- Perform regular scanning of the images in the repository to identify vulnerabilities or misconfigurations.
- Deploy application firewalls for enhancing container security and prevent threats entering the environment.
- Ensure the authenticated access to registries including sensitive images and data.
- Use a separate database for each application for greater visibility of individual applications and enhanced data management.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

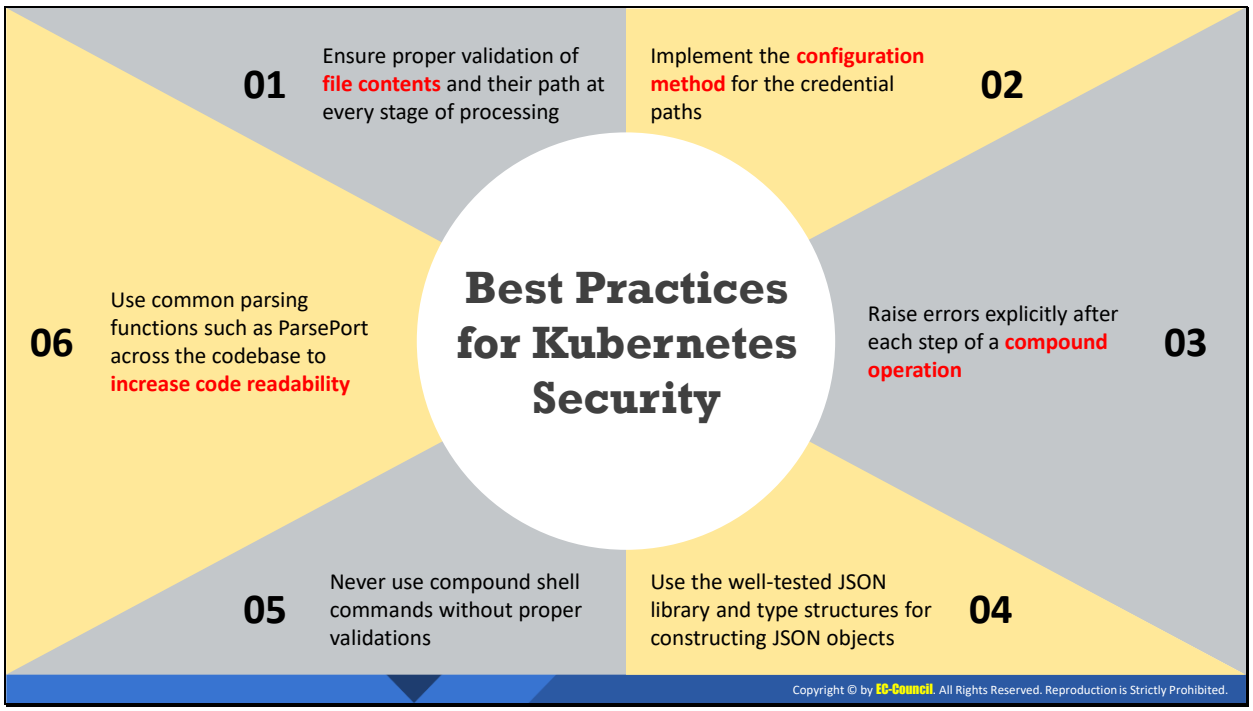


Best Practices for Docker Security

Discussed below are various best practices for securing Docker environment.

- Avoid exposing the Docker daemon socket because it is the basic entry point for the Docker API.
- Only use trusted Docker images because Docker images created by malicious users may be injected with backdoors.
- Regularly patch host OS and Docker with the latest security updates.
- Limit capabilities by allowing access only to the features required by the container.
- Use Linux security modules, such as seccomp, AppArmor, and SELinux, to gain fine-grained control over the processes.
- Limit resources such as memory, CPU, the maximum number of file descriptors, the maximum number of processes, and restarts to prevent DoS attacks.
- Enable read-only mode on filesystems and volumes by setting the `--read-only` flag.
- Set the Docker daemon log level to 'info' and avoid running Docker daemon using the 'debug' log level.
- The default user setting for the Docker image is root; configure the container application to run as unprivileged user to prevent privilege escalation attacks.
- Install only necessary packages to reduce the attack surface.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

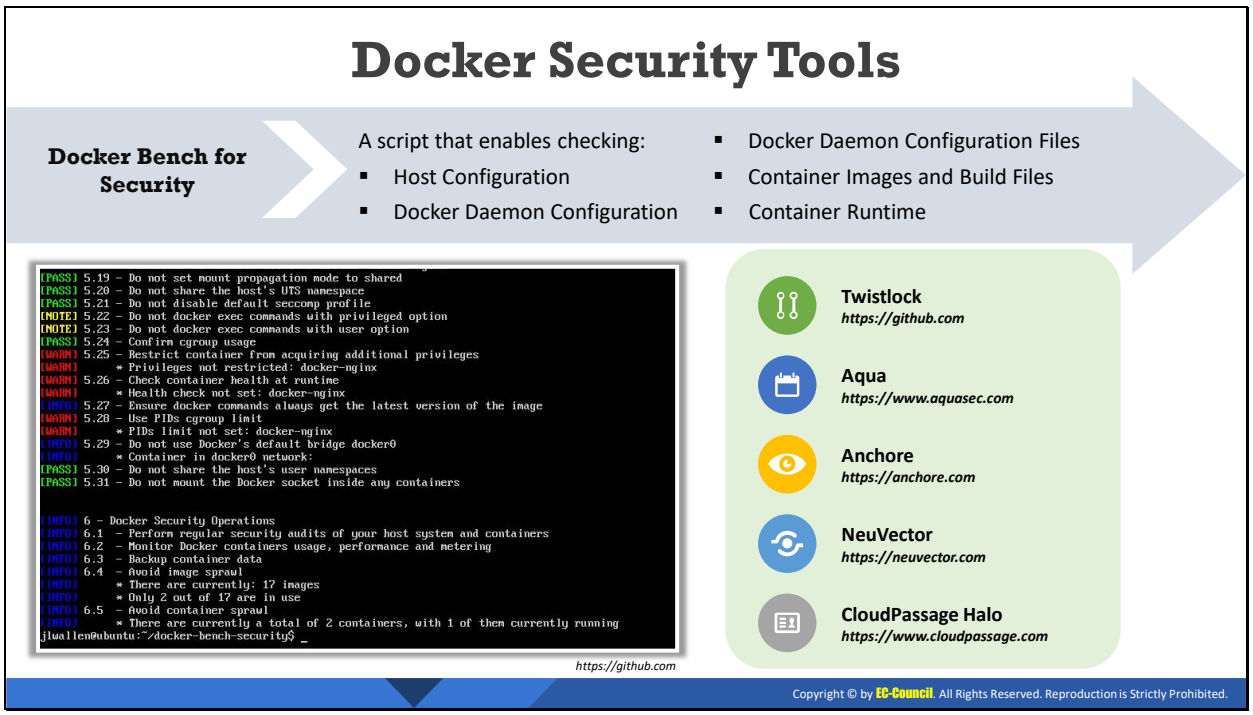


Best Practices for Kubernetes Security

Discussed below are various best practices for securing the Kubernetes environment.

- Ensure proper validation of file contents and their path at every stage of processing.
- Implement configuration method for the credential paths and do not depend on the hardcoded paths.
- Raise errors explicitly after each step of a compound operation.
- Use the well-tested JSON library and type structures for constructing JSON objects.
- Never use compound shell commands without proper validations because they affect the system state.
- Use centralized libraries to perform common tasks and use common parsing functions, such as ParsePort, across the codebase to increase code readability.
- Use persistent logs in place of log rotation, so that the logs can be written in linear order and new logs can be created when rotation is required.
- Use single encoding format for all configuration tasks because it supports centralized validation.
- Limit the size of manifest files to prevent out-of-memory errors in kubelet.
- Use kube-apiserver instances that maintain CRLs to check the presented certificates.
- Use key management services to enable secret data encryption and avoid using AES-Galois/Counter mode or cipher block chaining for encryption.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Docker Security Tools

- **Docker Bench for Security**

  Source: *https://github.com*

  The Docker Bench for Security is a script that checks for dozens of common best-practices around deploying Docker containers in production. It is a script that enables checking:

  - Host Configuration
  - Docker Daemon Configuration
  - Docker Daemon Configuration Files
  - Container Images and Build Files
  - Container Runtime

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

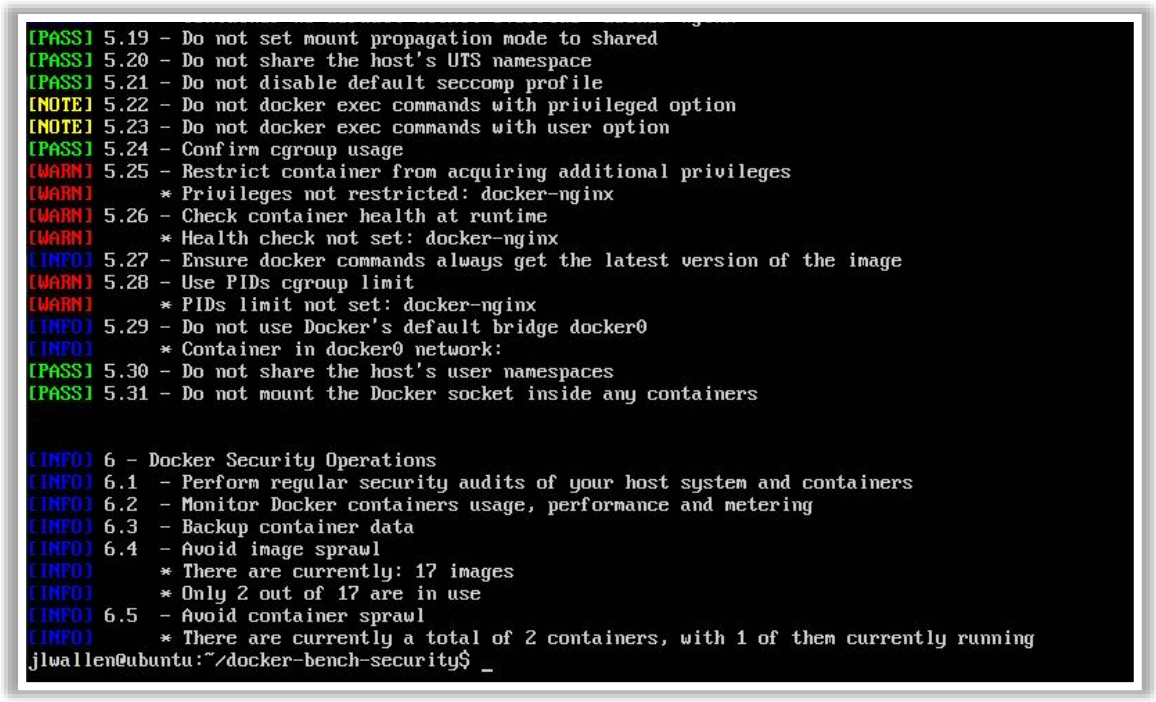


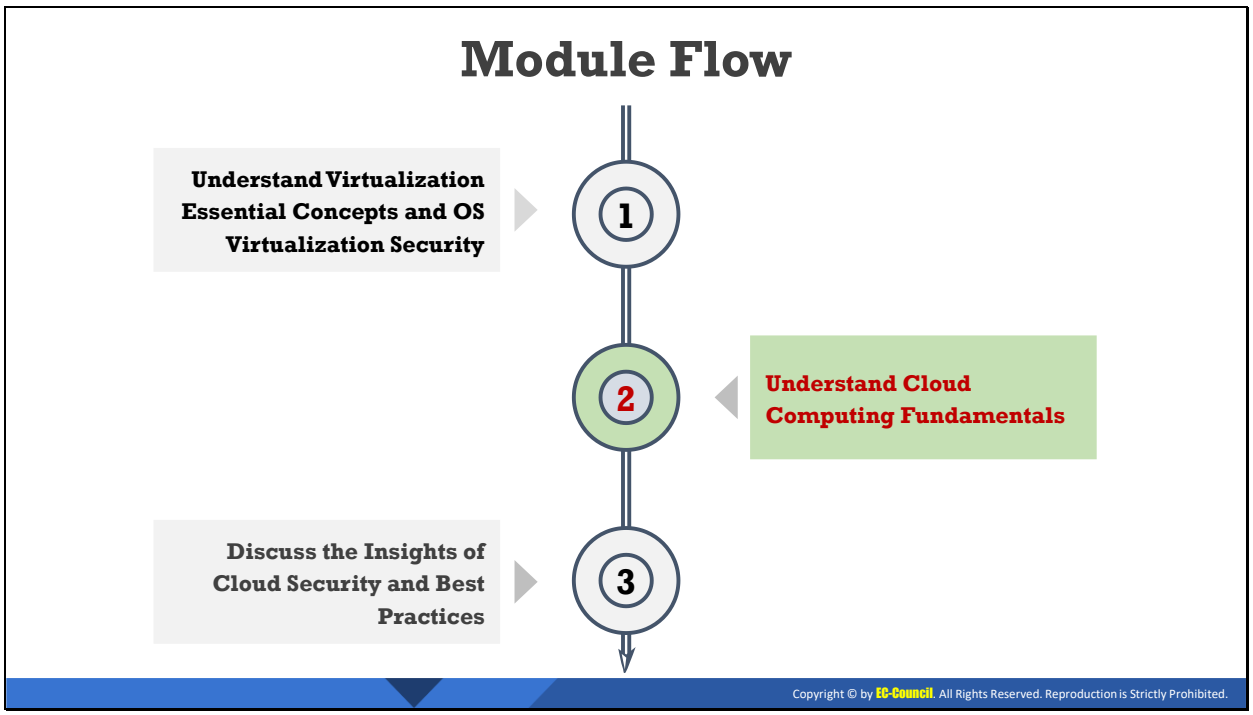
Figure 6.11: Screenshot of Docker Bench for Security

Some additional Docker security tools are listed below:

- Twistlock (*https://github.com*)
- Aqua (*https://www.aquasec.com*)
- Anchore (*https://anchore.com*)
- NeuVector (*https://neuvector.com*)
- CloudPassage Halo (*https://www.cloudpassage.com*)

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

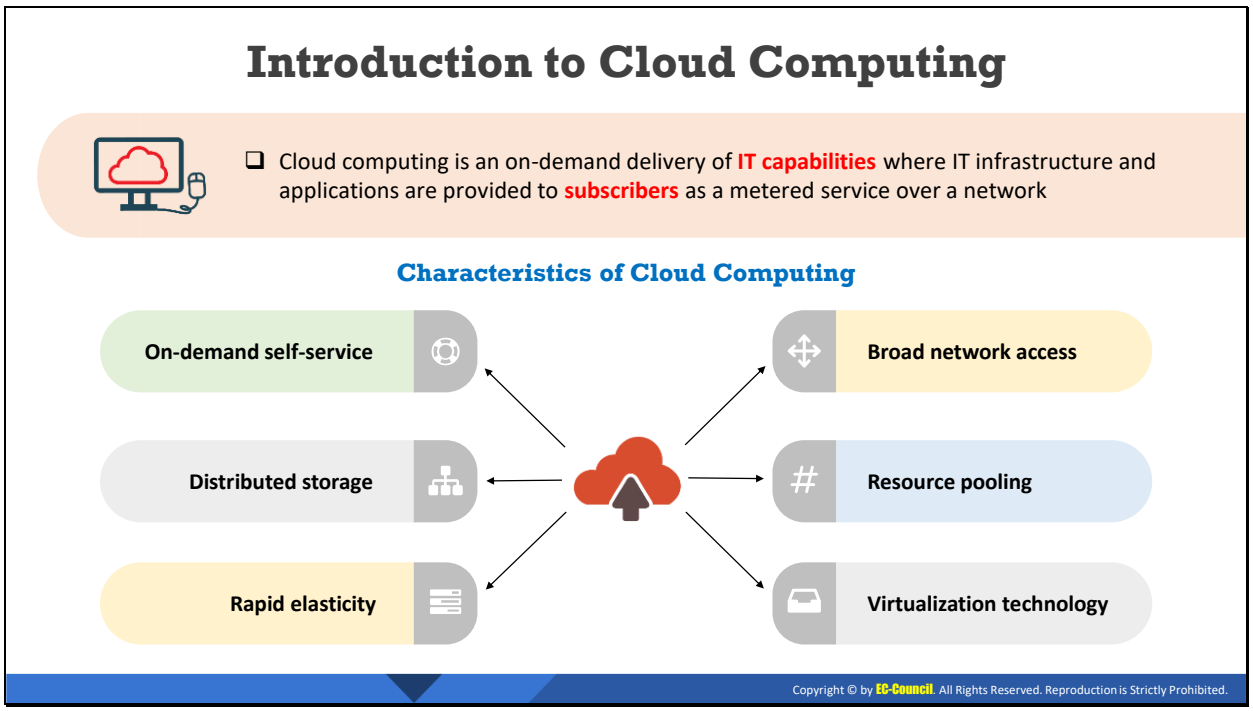


Understand Cloud Computing Fundamentals

Cloud computing delivers various types of services and applications over the Internet. These services enable users to utilize software and hardware managed by third parties at remote locations. Major cloud service providers include Google, Amazon, and Microsoft.

This section introduces cloud computing, the types of cloud computing services, the separation of responsibilities, the cloud deployment models, the NIST reference architecture and its benefits, the cloud storage architecture, and the cloud service providers.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Introduction to Cloud Computing

Cloud computing is an on-demand delivery of IT capabilities in which an IT infrastructure and applications are provided to subscribers as metered services over a network. Examples of cloud solutions include Gmail, Facebook, Dropbox, and Salesforce.

Characteristics of Cloud Computing

The characteristics of cloud computing that attract many businesses to adopt the cloud technology are discussed below.

- **On-demand self-service:** A type of service rendered by cloud service providers that provides on-demand cloud resources such as computing power, storage, and network, without the need for human interaction with service providers.
- **Distributed storage:** Distributed storage in cloud offers better scalability, availability, and reliability of data. However, it can potentially involve security and compliance concerns.
- **Rapid elasticity:** The cloud offers instant provisioning of capabilities to rapidly scale up or down according to demand. The resources available for provisioning to the consumers seem to be unlimited that can be purchased invariably in the desired quantity.
- **Automated management:** By minimizing user involvement, cloud automation speeds up the processes, reduces labor costs, and reduces the possibility of human error.
- **Broad network access:** Cloud resources are available over the network and can be accessed through standard procedures via a wide variety of platforms, including laptops, mobile phones, and PDAs.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

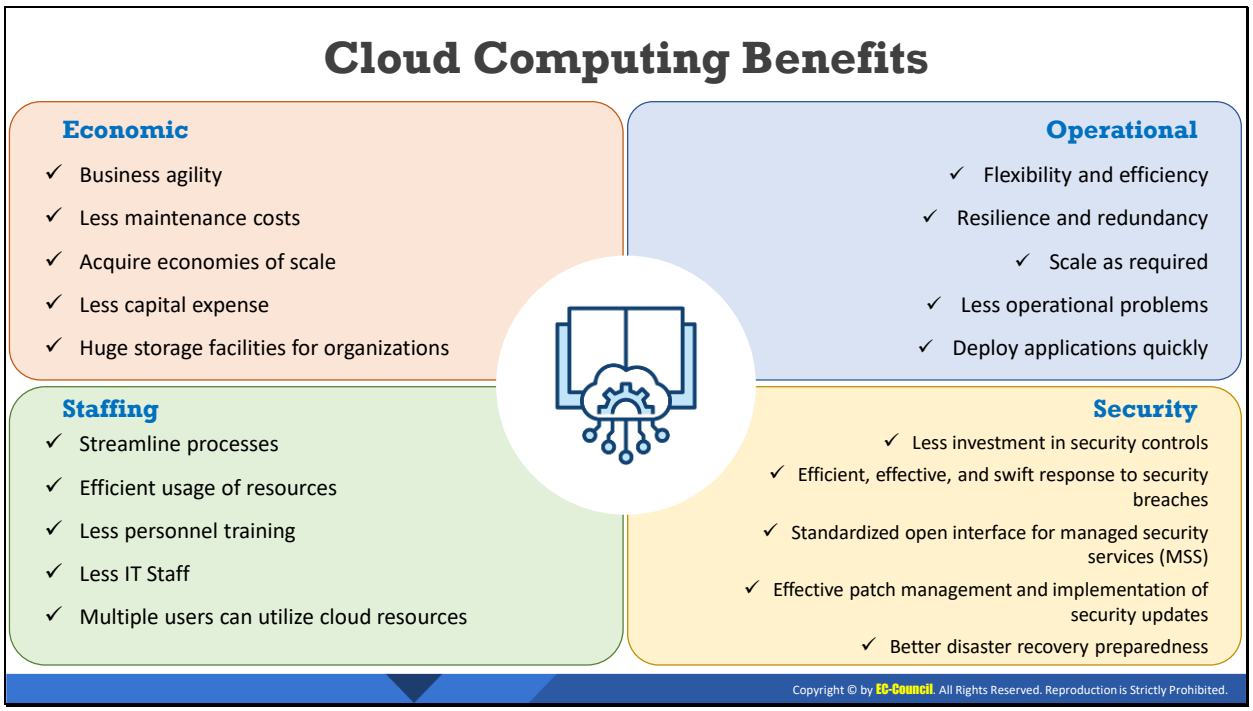
- **Resource pooling:** The cloud service provider pools all the resources together to serve multiple customers in a multi-tenant environment, wherein the physical and virtual resources are dynamically assigned and reassigned on demand by the consumers.
- **Measured service:** Cloud systems employ the "pay-per-use" metering method. Subscribers pay for the cloud services via monthly subscriptions or according to the usage of resources such as the storage levels, processing power, and bandwidth. Cloud service providers monitor, control, report, and charge the customers according to the resources consumed with complete transparency.
- **Virtualization technology:** It enables the rapid scaling of resources in such a way that could not be achieved by non-virtualized environments.

Limitations of Cloud Computing

- Organizations have limited control and flexibility
- Prone to outage and other technical issues
- Security, privacy, and compliance issues
- Contracts and lock-ins
- Dependence on network connections

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Cloud Computing Benefits

Cloud computing offers economic, operational, staffing, and security benefits.

- **Economic**
  - Business agility
  - Less maintenance costs
  - Acquire economies of scale
  - Less capital expenditure
  - Huge storage facilities for organizations
  - Environment friendly
  - Less total cost of ownership
  - Less power consumption
- **Operational**
  - Flexibility and efficiency
  - Resilience and redundancy
  - Scale as required
  - Less operational problems
  - Deploy applications quickly
  - Backup and disaster recovery

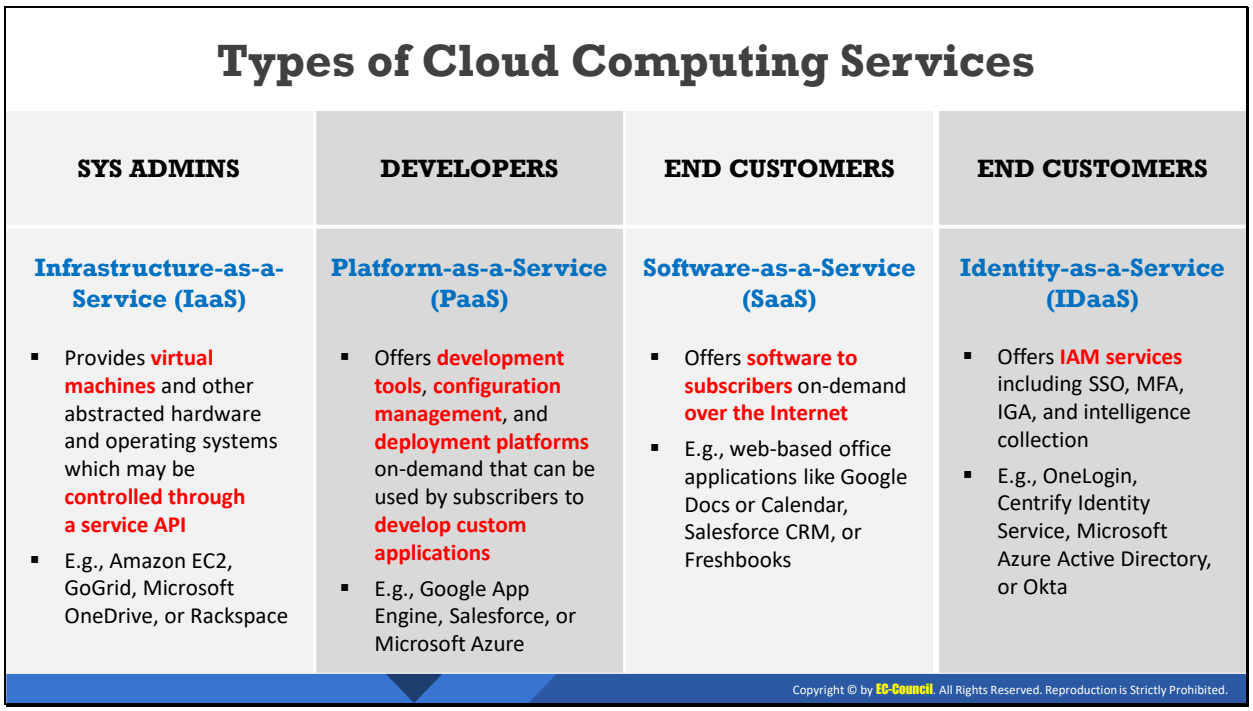
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

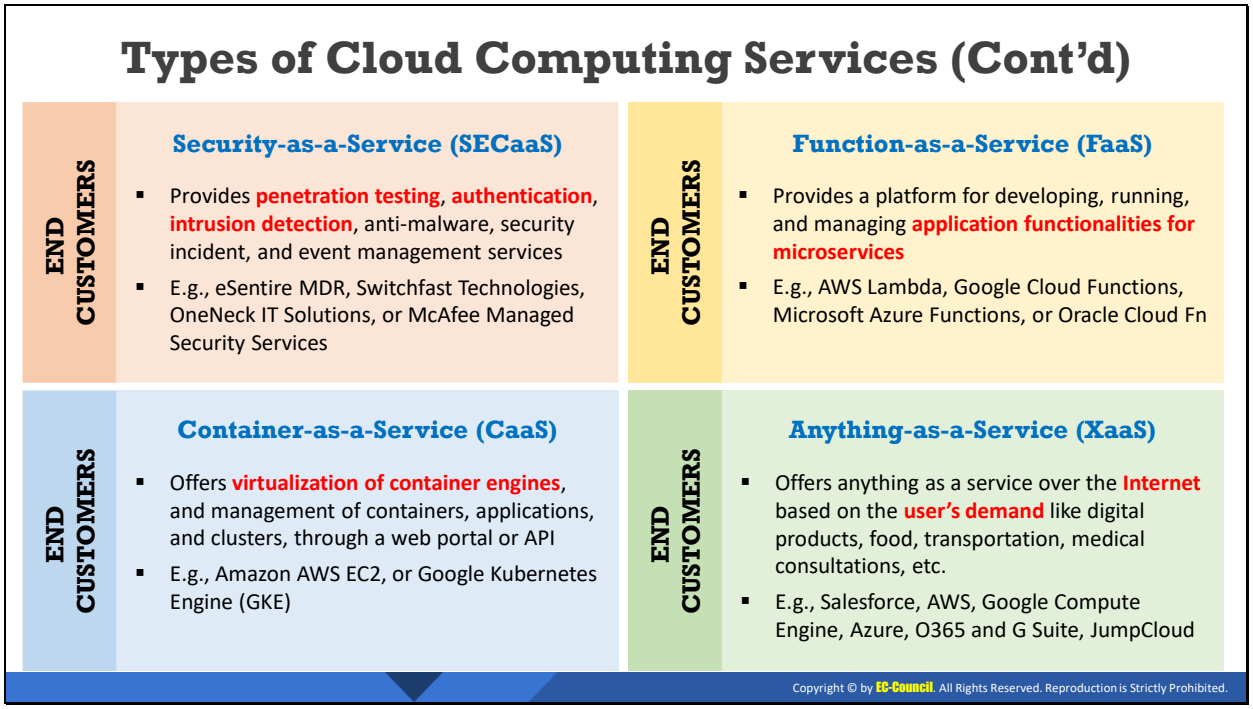
- Automatic updates

- **Staffing**
  - Streamline processes
  - Efficient usage of resources
  - Less personnel training
  - Less IT Staff
  - Multiple users can utilize cloud resources
  - Evolution of new business models
  - Simultaneous sharing of resources
- **Security**
  - Less investment in security controls
  - Efficient, effective, and swift response to security breaches
  - Standardized open interface for managed security services (MSS)
  - Effective patch management and implementation of security updates
  - Better disaster recovery preparedness
  - Ability to dynamically scale defensive resources on demand
  - Resource aggregation offers better management of security systems
  - Rigorous internal audits and risk assessment procedures

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets





Types of Cloud Computing Services

Cloud services are divided broadly into the following categories:

- **Infrastructure-as-a-Service (IaaS)**

  This cloud computing service enables subscribers to use on-demand fundamental IT resources, such as computing power, virtualization, data storage, and network. This service provides virtual machines and other abstracted hardware and operating systems

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

(OSs), which may be controlled through a service application programming interface (API). As cloud service providers are responsible for managing the underlying cloud computing infrastructure, subscribers can avoid costs of human capital, hardware, and others (e.g., Amazon EC2, Microsoft OneDrive, Rackspace).

Advantages:

- Dynamic infrastructure scaling
- Guaranteed uptime
- Automation of administrative tasks
- Elastic load balancing (ELB)
- Policy-based services
- Global accessibility

Disadvantages:

- Software security is at high risk (third-party providers are more prone to attacks)
- Performance issues and slow connection speeds

- **Platform-as-a-Service (PaaS)**

  This type of cloud computing service allows for the development of applications and services. Subscribers need not buy and manage the software and infrastructure underneath it but have authority over deployed applications and perhaps application hosting environment configurations. This offers development tools, configuration management, and deployment platforms on-demand, which can be used by subscribers to develop custom applications (e.g., Google App Engine, Salesforce, Microsoft Azure). Advantages of writing applications in the PaaS environment include dynamic scalability, automated backups, and other platform services, without the need to explicitly code for them.

  Advantages:

  - Simplified deployment
  - Prebuilt business functionality
  - Lower security risk compared to IaaS
  - Instant community
  - Pay-per-use model
  - Scalability

  Disadvantages:

  - Vendor lock-in
  - Data privacy

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- Integration with the rest of the system applications

- **Software-as-a-Service (SaaS)**

  This cloud computing service offers application software to subscribers on-demand over the Internet. The provider charges for the service on a pay-per-use basis, by subscription, by advertising, or by sharing among multiple users (e.g., web-based office applications like Google Docs or Calendar, Salesforce CRM, and Freshbooks).

  Advantages:

  - Low cost
  - Easy administration
  - Global accessibility
  - High compatibility (no specialized hardware or software is required)

  Disadvantages:

  - Security and latency issues
  - Total dependency on the Internet
  - Switching between SaaS vendors is difficult

- **Identity-as-a-Service (IDaaS)**

  This cloud computing service offers authentication services to the subscribed enterprises and is managed by a third-party vendor to provide identity and access management services. It provides services such as Single-Sign-On (SSO), Multi-Factor-Authentication (MFA), Identity Governance and Administration (IGA), access management, and intelligence collection. These services allow subscribers to access sensitive data more securely both on and off-premises (e.g., OneLogin, Centrify Identity Service, Microsoft Azure Active Directory, Okta).

  Advantages:

  - Low cost
  - Improved security
  - Simplify compliance
  - Reduced time
  - Central management of user accounts

  Disadvantages:

  - Single server failure may disrupt the service or create redundancy on other authentication servers
  - Vulnerable to account hijacking attacks

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- **Security-as-a-Service (SECaaS)**

  This cloud computing model integrates security services into corporate infrastructure in a cost-effective way. It is developed based on SaaS and does not require any physical hardware or equipment. Therefore, it drastically reduces the cost compared to that spent when organizations establish their own security capabilities. It provides services such as penetration testing, authentication, intrusion detection, anti-malware, security incident and event management (e.g., eSentire MDR, Switchfast Technologies, OneNeck IT Solutions, McAfee Managed Security Services).

  Advantages:

  - Low cost
  - Reduced complexity
  - Continuous protection
  - Improved security through best security expertise
  - Latest and updated security tools
  - Rapid user provisioning
  - Greater agility
  - Increased time on core competencies

  Disadvantages:

  - Increased attack surfaces and vulnerabilities
  - Unknown risk profile
  - Insecure APIs
  - No customization to business needs
  - Vulnerable to account hijacking attacks

- **Container-as-a-Service (CaaS)**

  This cloud computing model provides containers and clusters as a service to its subscribers. It provides services such as virtualization of container engines, management of containers, applications, and clusters through a web portal, or an API. Using these services, subscribers can develop rich scalable containerized applications through the cloud or on-site data centers. CaaS inherits features of both IaaS and PaaS (e.g., Amazon AWS EC2, Google Kubernetes Engine (GKE)).

  Advantages:

  - Streamlined development of containerized applications
  - Pay-per-resource
  - Increased quality

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- Portable and reliable application development
- Low cost
- Few resources
- Crash of application container does not affect other containers
- Improved security
- Improved patch management
- Improved response to bugs
- High scalability
- Streamlined development

Disadvantages:

- High operational overhead
- Platform deployment is the developer's responsibility

- **Function-as-a-Service (FaaS)**

  This cloud computing service provides a platform for developing, running, and managing application functionalities without the complexity of building and maintaining necessary infrastructure (serverless architecture). This model is mostly used while developing applications for microservices. It provides on-demand functionality to the subscribers that powers off the supporting infrastructure and incurs no charges when not in use. It provides data processing services, such as Internet of Things (IoT) services for connected devices, mobile and web applications, and batch-and-stream processing (e.g., AWS Lambda, Google Cloud Functions, Microsoft Azure Functions, Oracle Cloud Fn).

  Advantages:

  - Pay-per-use
  - Low cost
  - Efficient security updates
  - Easy deployment
  - High scalability

  Disadvantages:

  - High latency
  - Memory limitations
  - Monitoring and debugging limitations
  - Unstable tools and frameworks
  - Vendor lock-in

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- **Anything-as-a-Service (XaaS)**

  Anything as a service or everything as a service (XaaS) is a cloud-computing and remote-access service that offers anything as a service over the Internet based on the user's demand. The service may include digital products such as tools, applications, and technologies, as well as other types of services such as food, transportation, and medical consultations. The service is paid as per usage and cannot be purchased or licensed as regular products. Apart from common cloud services such as software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS), XaaS includes services such as network as a service (NaaS), storage as a service (STaaS), testing as a service (TaaS), malware as a service (MaaS), and disaster recovery as a service (DRaaS). XaaS offers secure services such as customer relationship management (CRM), cloud computing, and directory services (e.g., NetApp, AWS Elastic Beanstalk, Heroku, and Apache Stratos).

  Advantages:

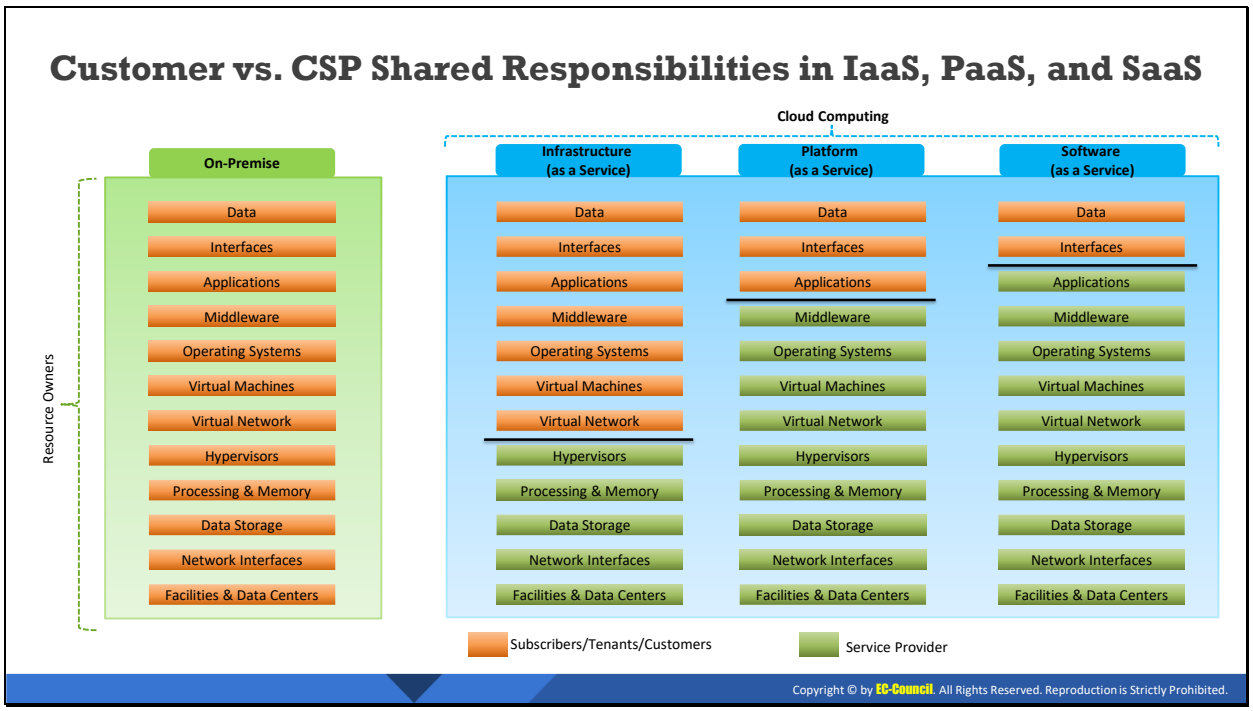
  - Highly scalable
  - Independent of location and devices
  - Fault tolerance and reduced redundancy
  - Reduced capital expenditure
  - Enhances business process by supporting rapid elasticity and resource sharing

  Disadvantages:

  - Chances of service outage as XaaS is dependent on the Internet
  - Performance issues due to high utilization of the same resources
  - Highly complex and difficult to troubleshoot at times

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Customer vs. CSP Shared Responsibilities in IaaS, PaaS, and SaaS

In cloud computing, it is important to ensure the separation of responsibilities of the subscribers and service providers. The separation of duties prevents conflicts of interest, illegal acts, fraud, abuse, and errors, and it helps in identifying security control failures, including information theft, security breaches, and invasion of security controls. It also helps in restricting the amount of influence held by an individual and ensures that there are no conflicting responsibilities. It is essential to know the limitations of each cloud service delivery model when accessing specific clouds and their models.

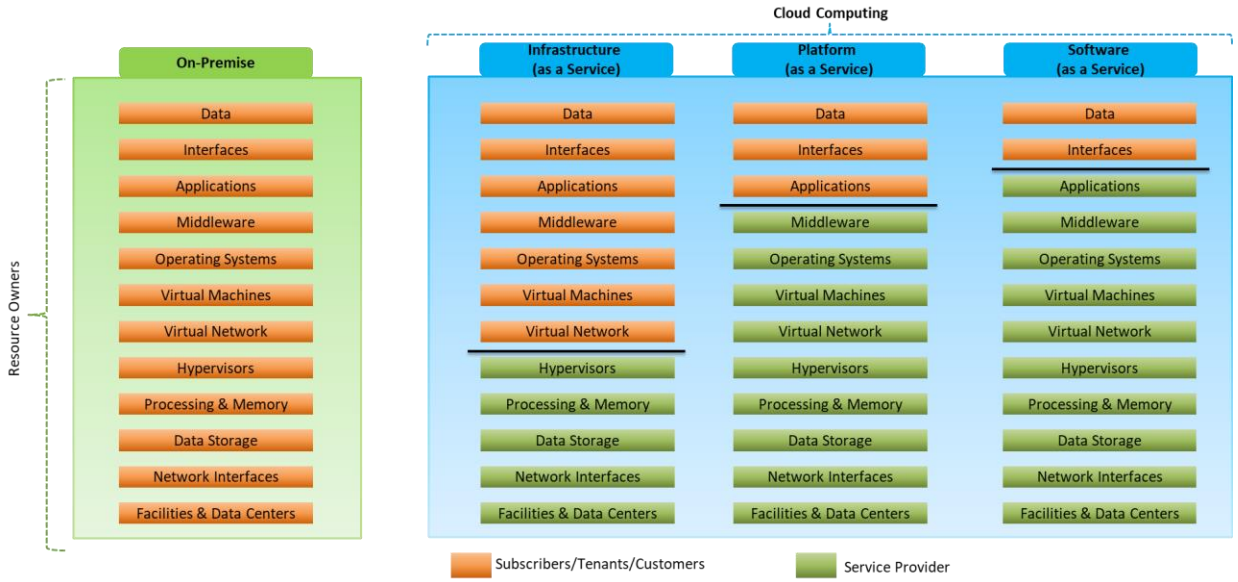


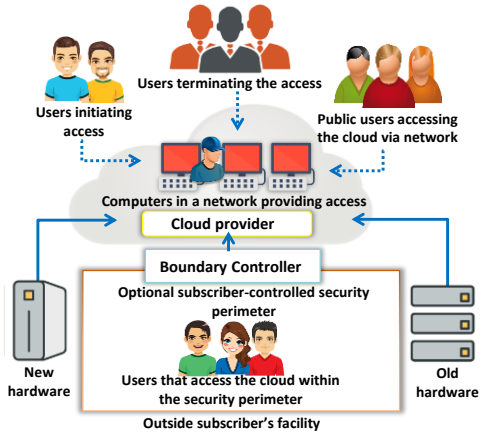
Figure 6.12: Customer vs. CSP Shared Responsibilities in IaaS, PaaS, and SaaS

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Cloud Deployment Models

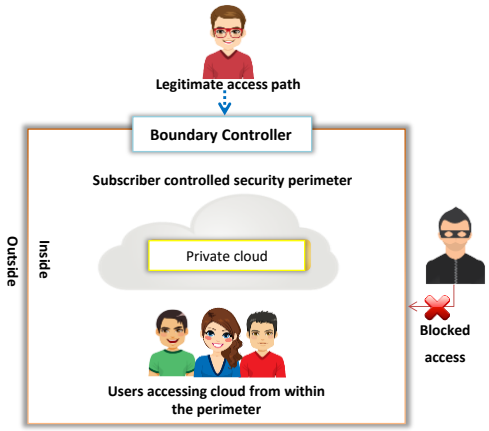
Public Cloud

Services are rendered over a network that is **open for public use**



Private Cloud

Cloud infrastructure is operated for a **single organization only**

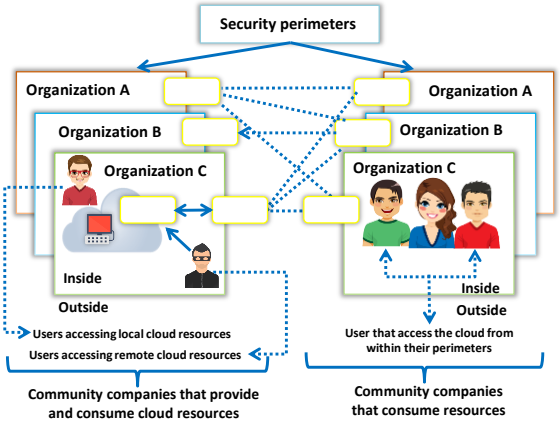


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Deployment Models (Cont'd)

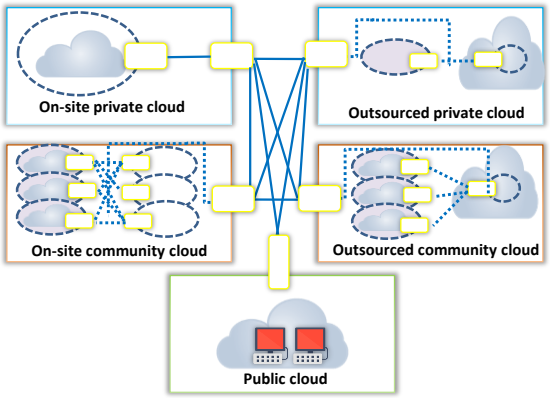
Community Cloud

Shared infrastructure between **several organizations from a specific community** with common concerns (security, compliance, jurisdiction, etc.)



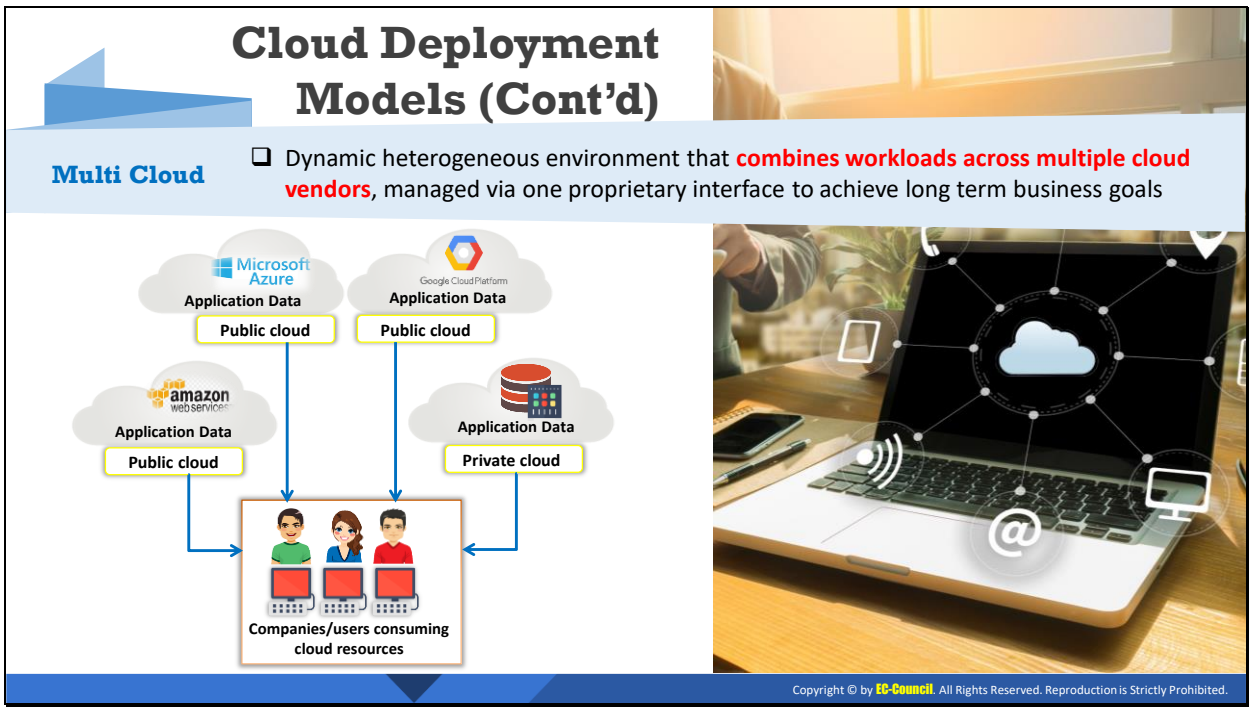
Hybrid Cloud

Combination of two or more clouds (private, community, or public) that remain unique entities but are bound together, thereby offering the benefits of multiple deployment models



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Cloud Deployment Models

Cloud deployment model selection is based on enterprise requirements. One can deploy cloud services in different ways, according to the factors given below:

- Host location of cloud computing services
- Security requirements
- Sharing of cloud services
- Ability to manage some or all of the cloud services
- Customization capabilities

The five standard cloud deployment models are

- **Public Cloud**

  In this model, the provider makes services such as applications, servers, and data storage available to the public over the Internet. Therefore, he is liable for the creation and constant maintenance of the public cloud and its IT resources. Public cloud services may be free or based on a pay-per-usage model (e.g., Amazon Elastic Compute Cloud (EC2), Google App Engine, Microsoft Azure, IBM Cloud).

  - **Advantages**:
    - Simplicity and efficiency
    - Low cost
    - Reduced time (when server crashes, needs to restart or reconfigure cloud)
    - No maintenance (public cloud service is hosted off-site)

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- No contracts (no long-term commitments)

○ **Disadvantages**:

- Security is not guaranteed
- Lack of control (third-party providers are in charge)
- Slow speed (relies on Internet connections; the data transfer rate is limited)

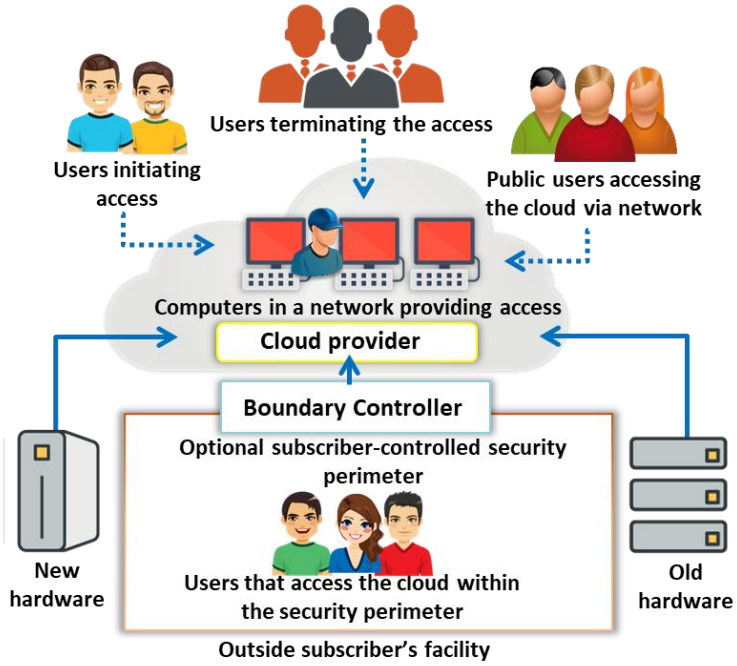


Figure 6.13: Public cloud deployment model

▪ **Private Cloud**

A private cloud, also known as the internal or corporate cloud, is a cloud infrastructure operated by a single organization and implemented within a corporate firewall. Organizations deploy private cloud infrastructures to retain full control over corporate data (e.g., BMC Software, VMware vRealize Suite, SAP Cloud Platform).

○ **Advantages**:

- Security enhancement (services are dedicated to a single organization)
- Increased control over resources (organization is in charge)
- High performance (cloud deployment within the firewall implies high data transfer rates)
- Customizable hardware, network, and storage performances (as the organization owns private cloud)
- Sarbanes Oxley, PCI DSS, and HIPAA compliance data are much easier to attain

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **Disadvantages**:
  - High cost
  - On-site maintenance

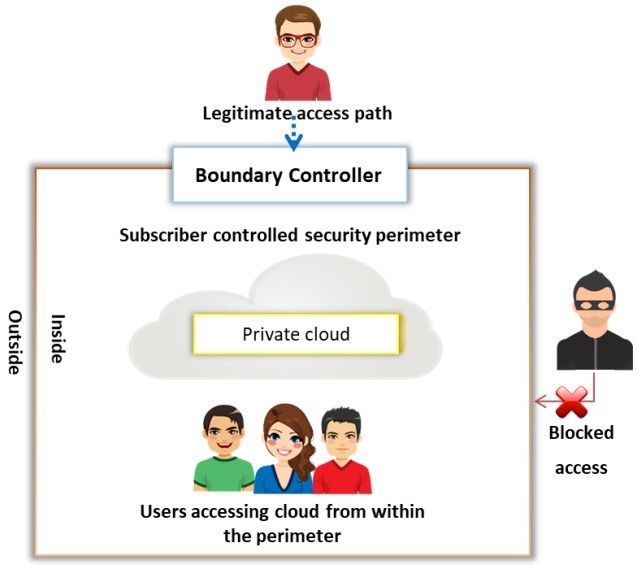


Figure 6.14: Private cloud deployment model

- **Community Cloud**

  It is a multi-tenant infrastructure shared among organizations from a specific community with common computing concerns, such as security, regulatory compliance, performance requirements, and jurisdiction. The community cloud can be either on- or off-premises and governed by the participated organizations or by a third-party managed service provider (e.g., Optum Health Cloud, Salesforce Health Cloud).

  - **Advantages**:
    - Less expensive compared to the private cloud
    - Flexibility to meet the community's needs
    - Compliance with legal regulations
    - High scalability
    - Organizations can share a pool of resources from anywhere via the Internet
  - **Disadvantages**:
    - Competition between consumers in resource usage
    - Inaccurate prediction of required resources
    - Lack of legal entity in case of liability
    - Moderate security (other tenants may be able to access data)
    - Trust and security concerns between tenants

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

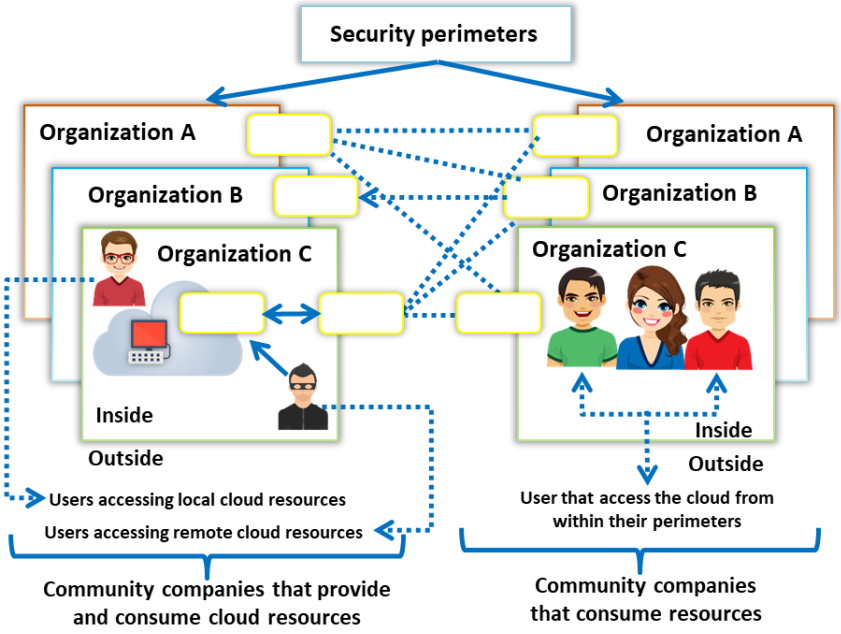


Figure 6.15: Community cloud deployment model

- **Hybrid Cloud**

  It is a cloud environment comprised of two or more clouds (private, public, or community) that remain unique entities but are bound together to offer the benefits of multiple deployment models. In this model, the organization makes available and manages some resources in-house and provides other resources externally (e.g., Microsoft Azure, Zymr, Parangat, Logicalis).

  Example: An organization performs its critical activities on the private cloud (e.g., operational customer data) and non-critical activities on the public cloud.

  - **Advantages**:
    - High scalability (contains both public and private clouds)
    - Offers both secure and scalable public resources
    - High level of security (comprises private cloud)
    - Allows to reduce and manage the cost according to requirements
  - **Disadvantages**:
    - Communication at the network level may be conflicted as it uses both public and private clouds
    - Difficult to achieve data compliance
    - Organization reliant on the internal IT infrastructure in case of outages (maintain redundancy across data centers to overcome)
    - Complex service level agreements (SLAs)

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

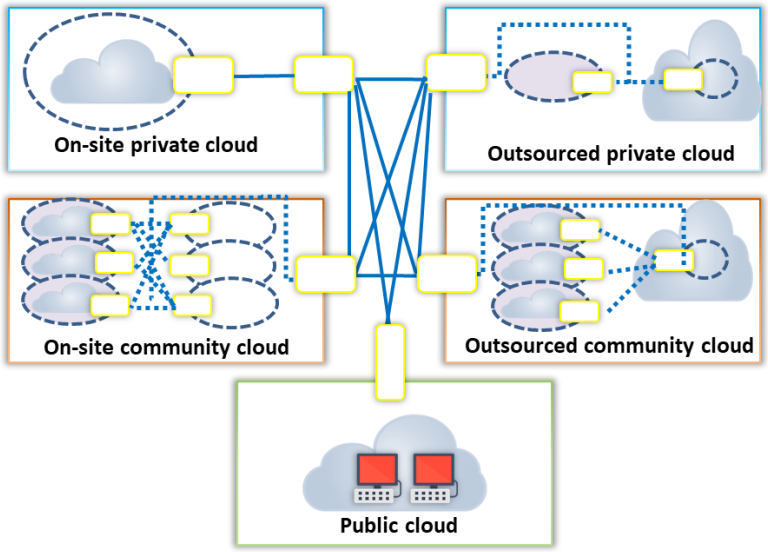


Figure 6.16: Hybrid cloud deployment model

- **Multi Cloud**

  It is a dynamic heterogeneous environment that combines workloads across multiple cloud vendors that are managed via one proprietary interface to achieve long-term business goals. The multi cloud uses multiple computing and storage services from different cloud vendors. It distributes cloud assets, software, applications, etc. across various cloud-hosting environments. Multi cloud environments are mostly all-private, all-public or a combination of both. Organizations use multi cloud environments for distributing computing resources, thereby increasing computing power and storage capabilities, and limiting the data loss and downtime risk to a great extent (e.g., Microsoft Azure Arc, AWS Kaavo IMOD, Google Cloud Anthos).

  - **Advantages**:
    - High reliability and low latency
    - Flexibility to meet business needs
    - Cost-performance optimization and risk mitigation
    - Low risk of distributed denial-of-service (DDoS) attacks
    - Increased storage availability and computing power
    - Low probability of vendor lock-in
  - **Disadvantages**:
    - Multi-cloud system failure affects business agility
    - Using more than one provider causes redundancy
    - Security risks due to complex and large attack surface
    - Operational overhead

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

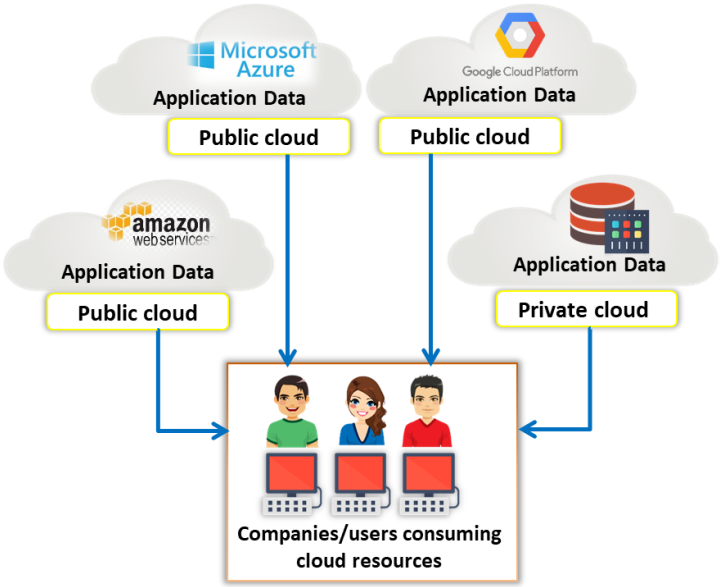
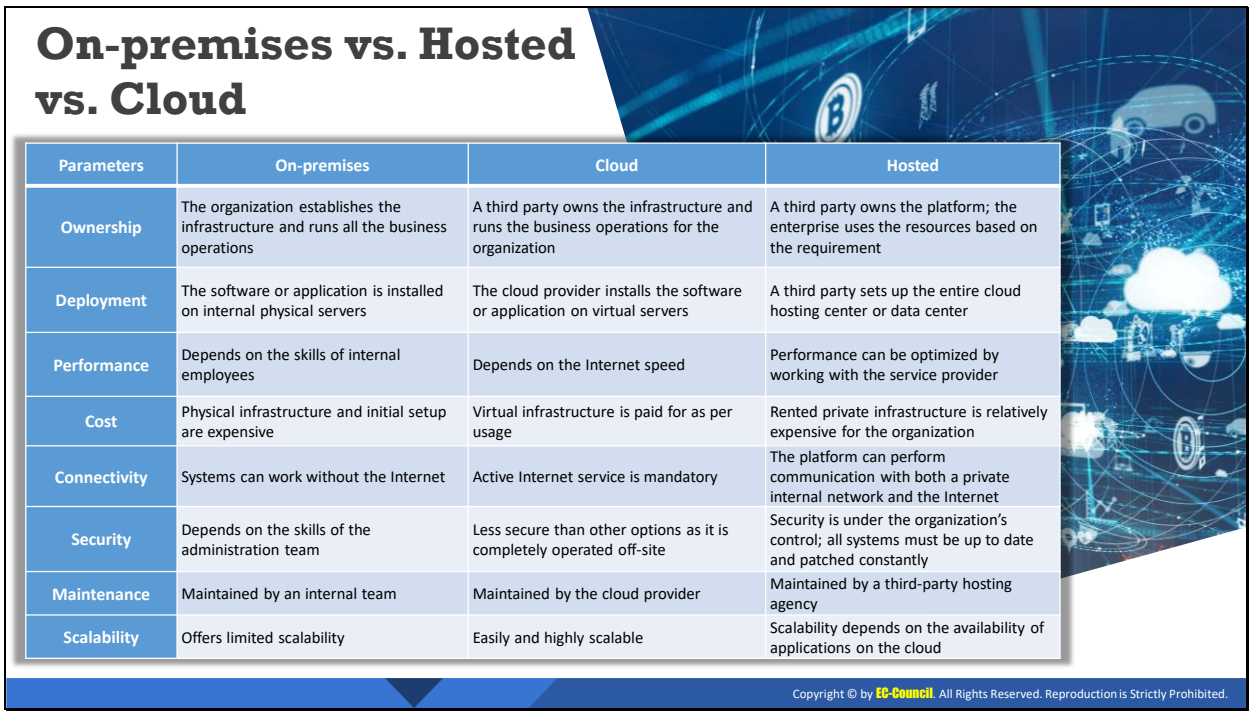


Figure 6.17: Multi cloud deployment model

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



On-premises vs. Hosted vs. Cloud

There are many technologies for organizations to choose and deploy applications or software to run their business effectively. An organization should consider various factors such as budget, business size, and maintenance challenges before choosing a deployment option. Choosing the appropriate deployment platform for their business is often a challenging task for organizations. Before choosing a deployment option, organizations should be aware of various technologies, their features, and how secure they are. The table below describes various IT deployment models and their services.

Parameters	On-premises	Cloud	Hosted
Ownership	The organization establishes the infrastructure and runs all the business operations.	A third party owns the infrastructure and runs the business operations for the organization.	A third party owns the platform; the enterprise uses the resources based on the requirement.
Deployment	The software or application is installed on internal physical servers.	The cloud provider installs the software or application on virtual servers.	A third party sets up the entire cloud hosting center or data center.
Performance	Depends on the skills of internal employees.	Depends on the Internet speed.	Performance can be optimized by working with the service provider.
Cost	Physical infrastructure and initial setup are expensive.	Virtual infrastructure is paid for as per usage.	Rented private infrastructure is relatively expensive for the organization.

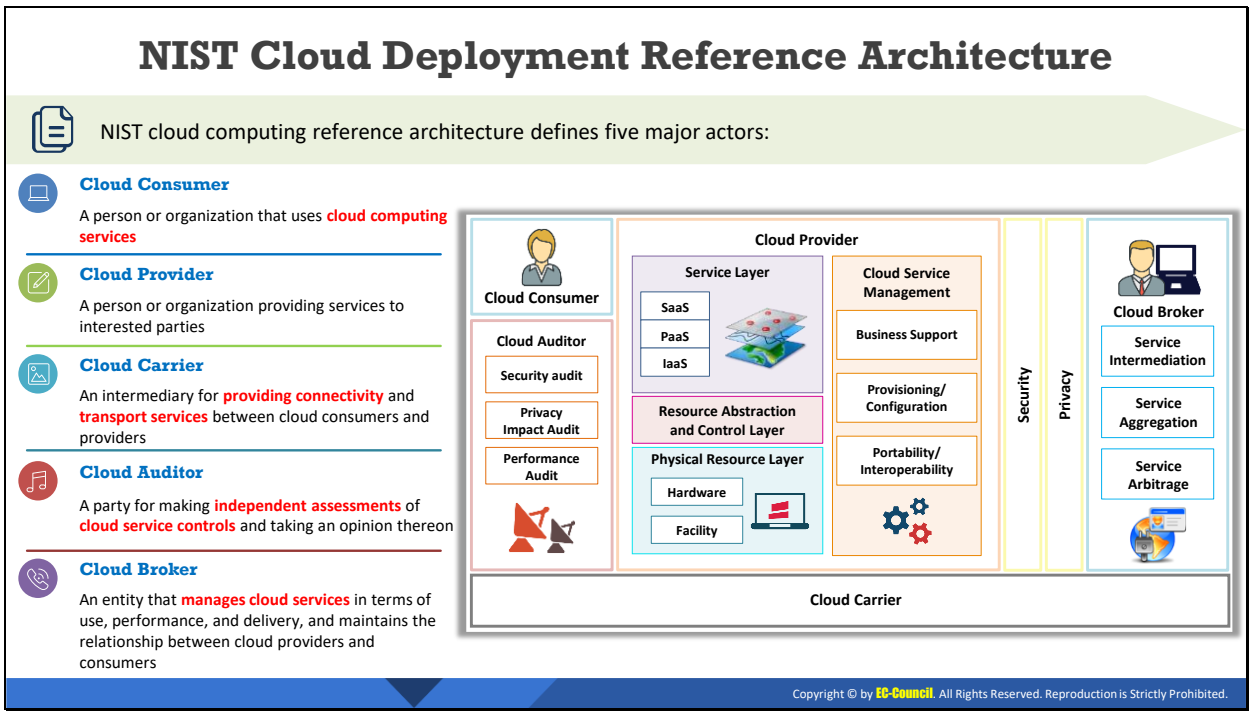
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Connectivity	Systems can work without the Internet.	Active Internet service is mandatory.	The platform can perform communication with both a private internal network and the Internet.
Security	Depends on the skills of the administration team.	Less secure than other options as it is completely operated off-site.	Security is under the organization's control; all systems must be up to date and patched constantly.
Maintenance	Maintained by an internal team.	Maintained by the cloud provider.	Maintained by a third-party hosting agency.
Scalability	Offers limited scalability.	Easily and highly scalable.	Scalability depends on the availability of applications on the cloud.

Table 6.2: Comparison among on-premises, hosted, and cloud IT deployment models

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



NIST Cloud Deployment Reference Architecture

The figure below gives an overview of the NIST cloud computing reference architecture; it displays the primary actors, activities, and functions in cloud computing. The diagram illustrates a generic high-level architecture, intended for better understanding the uses, requirements, characteristics, and standards of cloud computing.

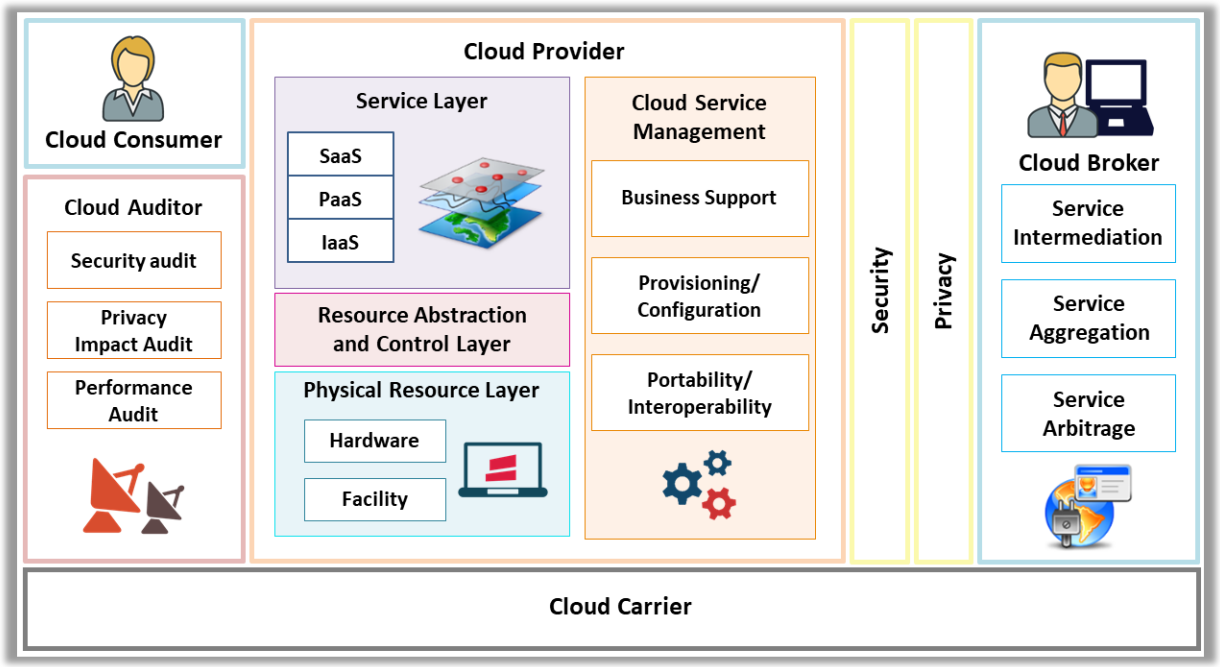


Figure 6.18: NIST cloud computing reference architecture

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

The five significant actors are as follows:

- **Cloud Consumer**

  A cloud consumer is a person or organization that maintains a business relationship with the cloud service providers (CSPs) and utilizes the cloud computing services. The cloud consumer browses the CSP's service catalog requests for the desired services, sets up service contracts with the CSP (either directly or via cloud broker), and uses the services. The CSP bills the consumer based on the services provided. The CSP should fulfill the service level agreement (SLA) in which the cloud consumer specifies the technical performance requirements, such as the quality of service, security, and remedies for performance failure. The CSP may also define limitations and obligations if any, that cloud consumers must accept.

  The services available to a cloud consumer in the **PaaS**, **IaaS, and SaaS** models are as follows:

  - **PaaS** – database (DB), business intelligence, application deployment, development and testing, and integration
  - **IaaS** – storage, services management, content delivery network (CDN), platform hosting, backup and recovery, and computing
  - **SaaS** – human resources, enterprise resource planning (ERP), sales, customer relationship management (CRM), collaboration, document management, email and office productivity, content management, financial services, and social networks.

- **Cloud Provider**

  A cloud provider is a person or organization who acquires and manages the computing infrastructure intended for providing services (directly or via a cloud broker) to interested parties via network access.

- **Cloud Carrier**

  A cloud carrier acts as an intermediary that provides connectivity and transport services between CSPs and cloud consumers. The cloud carrier provides access to consumers via a network, telecommunication, or other access devices.

- **Cloud Auditor**

  A cloud auditor is a party that performs an independent examination of cloud service controls to express an opinion thereon. Audits verify adherence to standards through a review of the objective evidence. A cloud auditor can evaluate the services provided by a CSP regarding security controls (management, operational, and technical safeguards intended to protect the confidentiality, integrity, and availability of the system and its information), privacy impact (compliance with applicable privacy laws and regulations governing an individual's privacy), performance, etc.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- **Cloud Broker**

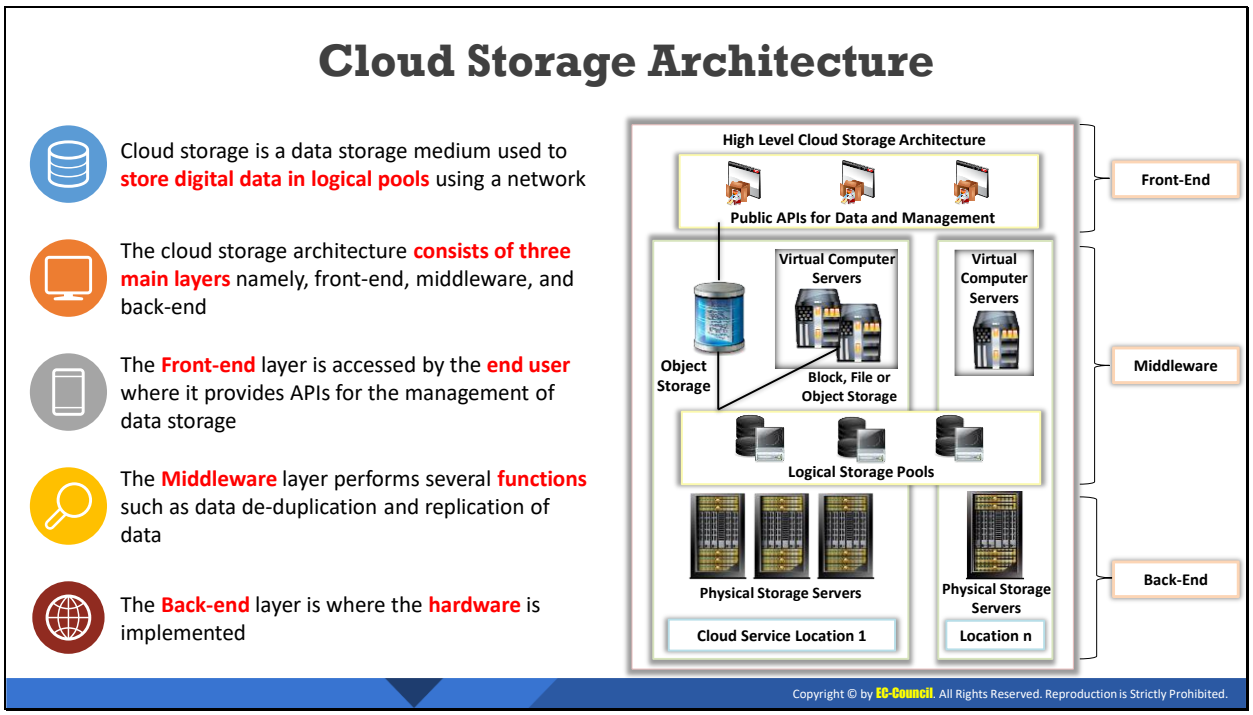
  The integration of cloud services is becoming too complicated for cloud consumers to manage. Thus, a cloud consumer may request cloud services from a cloud broker, rather than directly contacting a CSP. The cloud broker is an entity that manages cloud services regarding use, performance, and delivery and maintains the relationship between CSPs and cloud consumers.

  The services provided by cloud brokers fall in three categories:

  - **Service Intermediation:** Improves a given function by a specific capability and provides value-added services to cloud consumers.
  - **Service Aggregation:** Combines and integrates multiple services into one or more new services.
  - **Service Arbitrage:** Similar to service aggregation but without the fixing of the aggregated services (the cloud broker can choose services from multiple agencies).

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Cloud Storage Architecture

Cloud storage is a medium used to store digital data in logical pools using a network. The physical storage is distributed to multiple servers, which are owned by a hosting company. Organizations can buy storage capacity from the cloud storage providers for storing user, organization, or application data. Cloud storage providers are solely responsible for managing the data and keeping the data available and accessible. Cloud storage services can be accessed using a cloud computing service, a web service API, or any applications that use the API, such as cloud desktop storage, cloud storage gateway, or web-based content management systems. The cloud storage service is operated from an off-premises service, like Amazon S3.

The cloud storage architecture possesses the same characteristics as cloud computing in terms of scalability, accessible interfaces, and metered resources. It is built on highly virtualized infrastructure and relies on multiple layers to provide continuous storage services to users. The three main layers correspond to the front-end, middleware, and back-end. The front-end layer is accessed by the end-user and provides APIs for the management of data storage. The middleware layer performs functions such as data de-duplication and replication of data. The back-end layer is where the hardware is implemented.

Cloud storage is made of distributed resources. It is highly fault-tolerant through redundancy, consistent with data replication, and highly durable. Widely used object storage services include Amazon S3, Oracle Cloud Storage and Microsoft Azure Storage, Open Stack Swift, etc.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

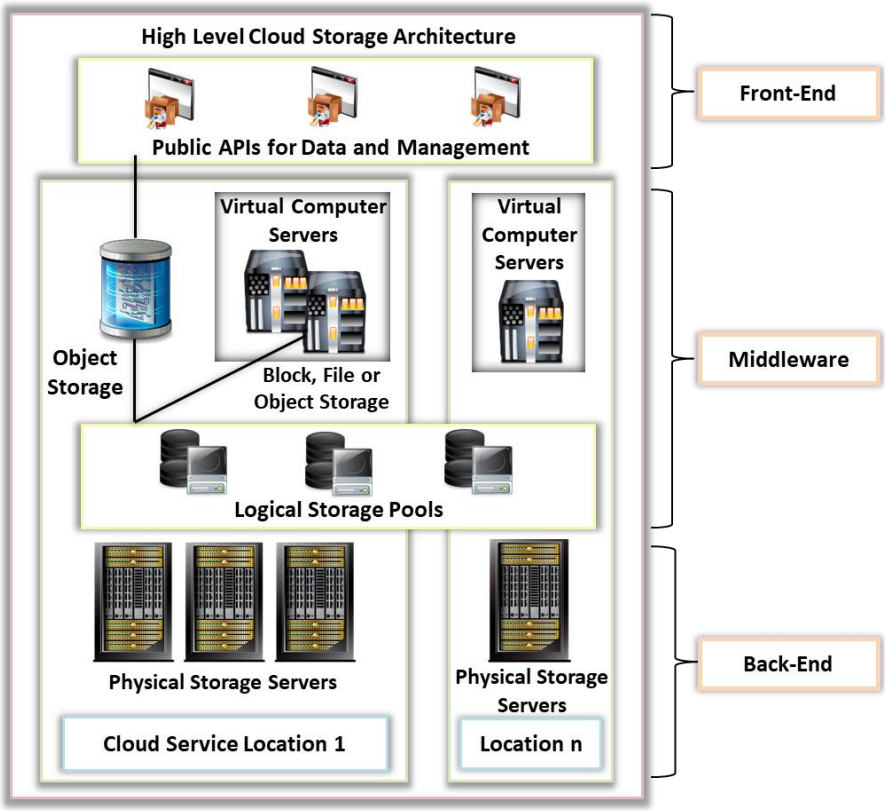
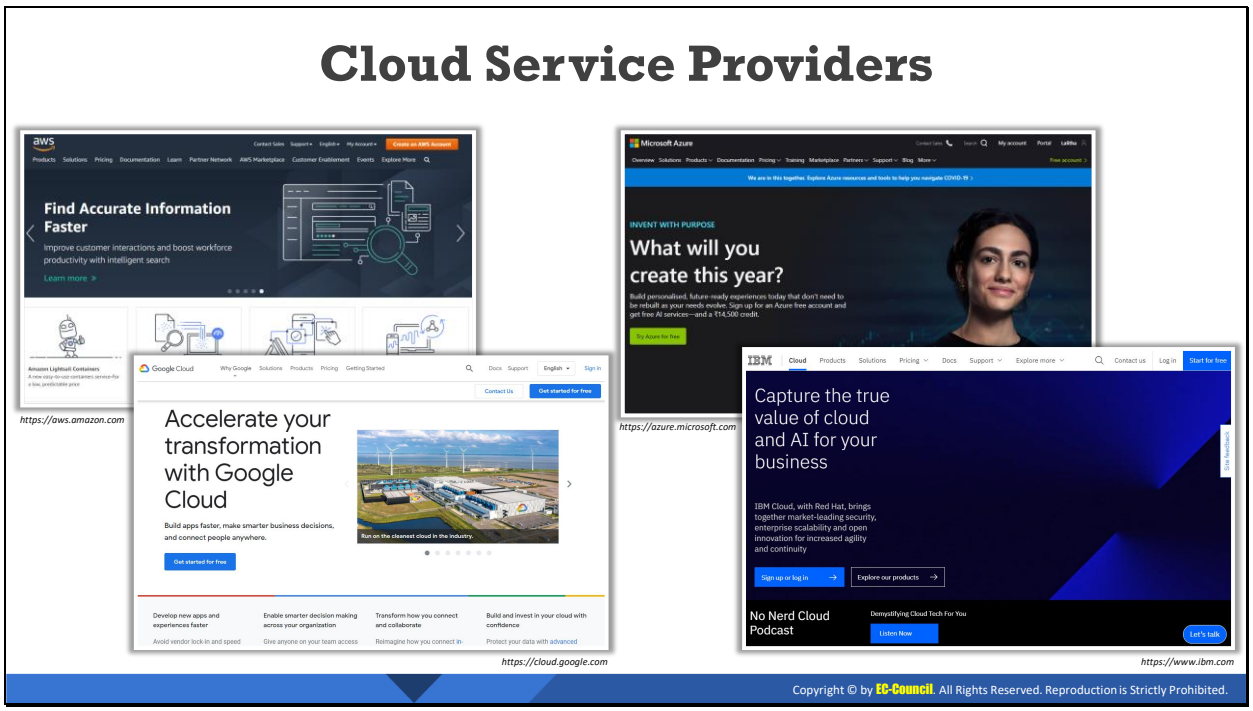


Figure 6.19: Cloud storage architecture

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Cloud Service Providers

Discussed below are some of the popular cloud service providers:

- **Amazon Web Service (AWS)**

  Source: *https://aws.amazon.com*

  AWS provides on-demand cloud computing services to individuals, organizations, the government, etc. on a pay-per-use basis. This service provides the necessary technical infrastructure through distributed computing and tools. The virtual environment provided by AWS includes CPU, GPU, RAM, HDD storage, operating systems, applications, and networking software such as web servers, databases, and CRM.

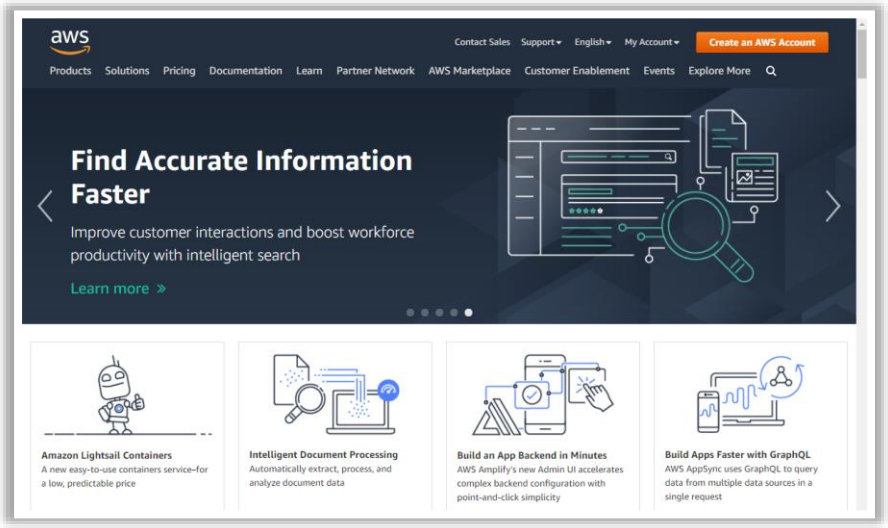


Figure 6.20: Screenshot of Amazon AWS

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- **Microsoft Azure**

  Source: *https://azure.microsoft.com*

  Microsoft Azure provides cloud computing services for building, testing, deploying, and managing applications and services through Azure data centers. It provides all types of cloud computing services, such as SaaS, PaaS, and IaaS. It offers various cloud services, such as computing, mobile storage, data management, messaging, media, machine learning, and IoT.

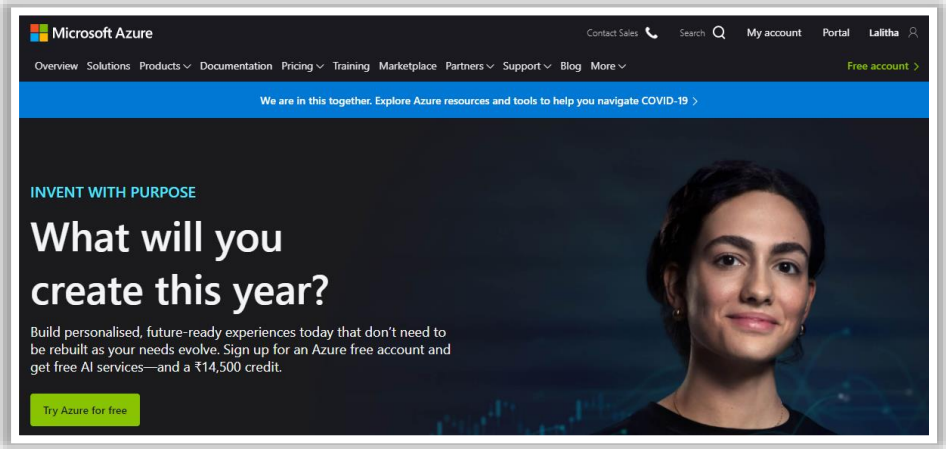


Figure 6.21: Screenshot of Microsoft Azure

- **Google Cloud Platform (GCP)**

  Source: *https://cloud.google.com*

  GCP provides IaaS, PaaS, and serverless computing services. These include computing, data storage and analytics, machine learning, networking, bigdata, cloud AI, management tools, identity and security, IoT, and API platforms.

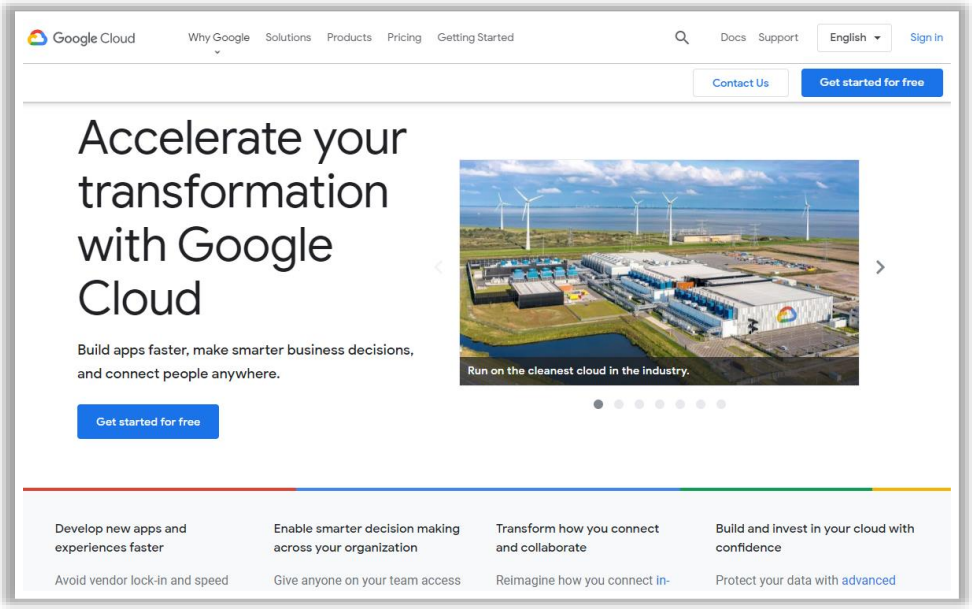


Figure 6.22: Screenshot of Google Cloud Platform

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **IBM Cloud**

  Source: *https://www.ibm.com*

  IBM Cloud™ is a robust suite of advanced data and AI tools and deep industry expertise. It provides various cloud services, such as IaaS, SaaS, and PaaS, through public, private, and hybrid cloud delivery models. These services include computing, networking, storage, management, security, databases, analytics, AI, IoT, mobile, Dev tools, and blockchain.

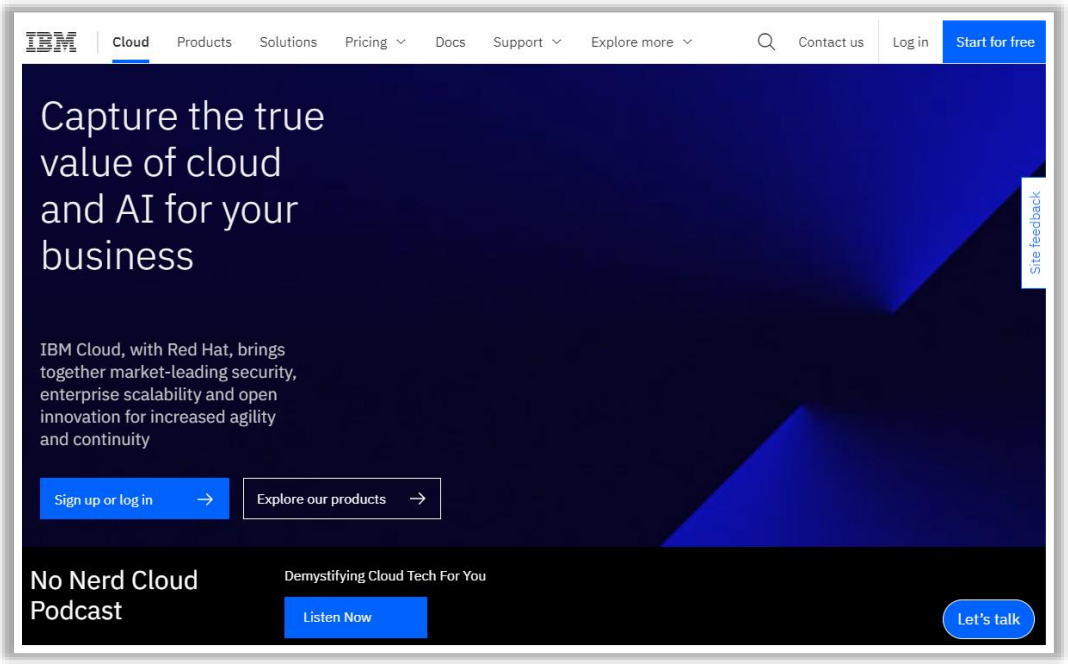
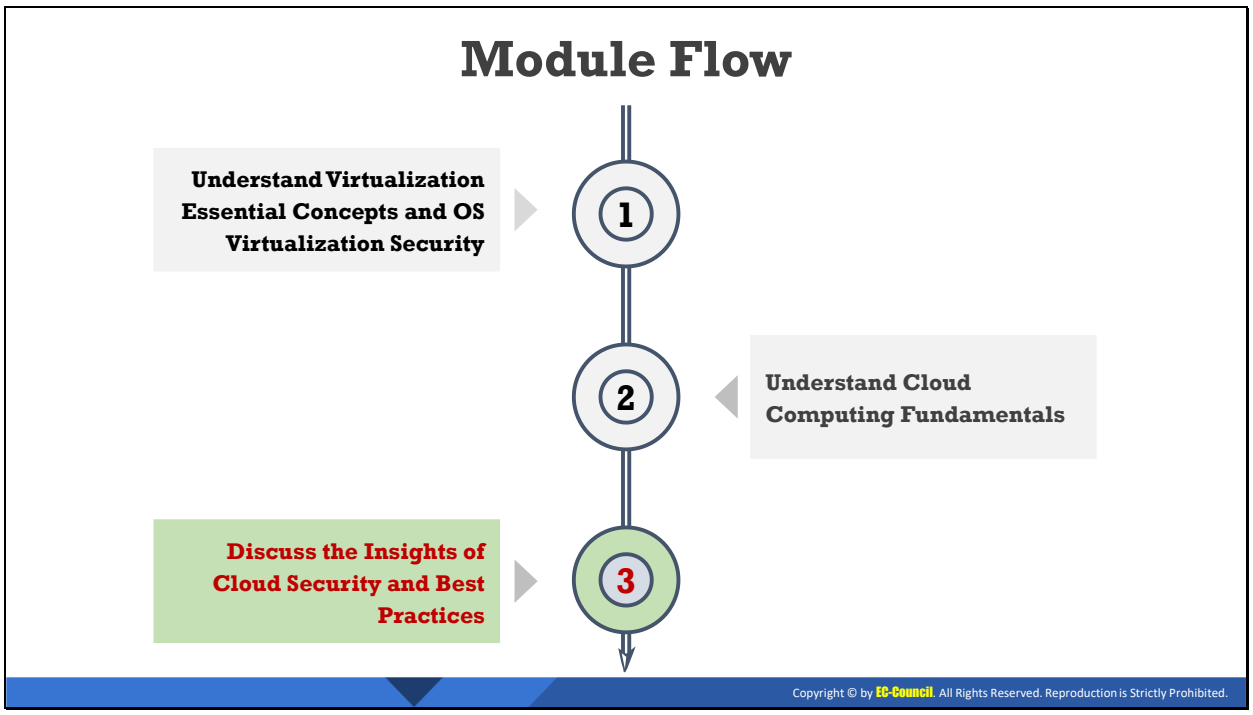


Figure 6.23: Screenshot of IBM Cloud

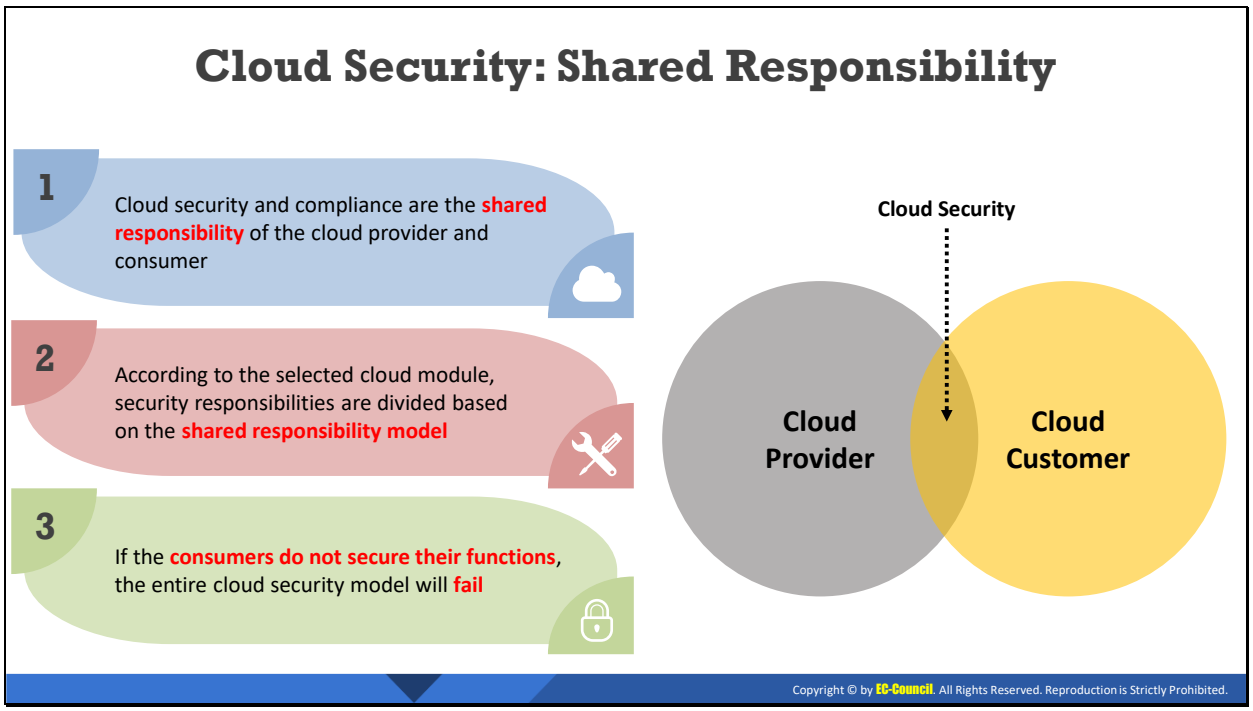
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

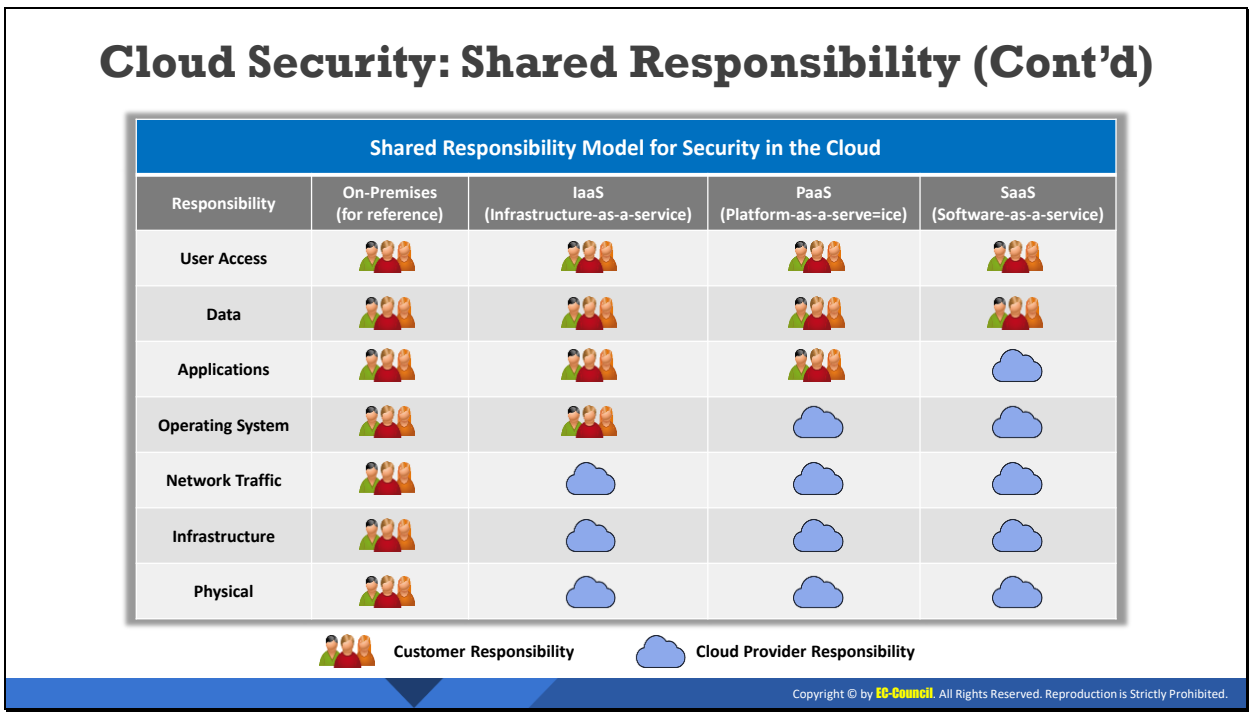


Discuss the Insights of Cloud Security and Best Practices

The objective of this section is to explain the shared responsibility of security in different cloud service models (IaaS, PaaS, and SaaS). This section explains the enterprise roles in securing the various elements of cloud such as user security and monitoring (e.g., IAM, encryption and key management, application-level security, data storage security, and monitoring), logging, and compliance. This section also explains various security best practices and tools used by enterprises for cloud security. This section explains the NIST recommendations for cloud security and various cloud security tools.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets





Cloud Security: Shared Responsibility

Security is a shared responsibility in cloud systems, wherein the cloud consumers and cloud service providers have varying levels of control over the available computing resources. According to the selected cloud module, security responsibilities are divided based on the shared responsibility model. If the consumers do not secure their functions, the entire cloud security model will fail.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

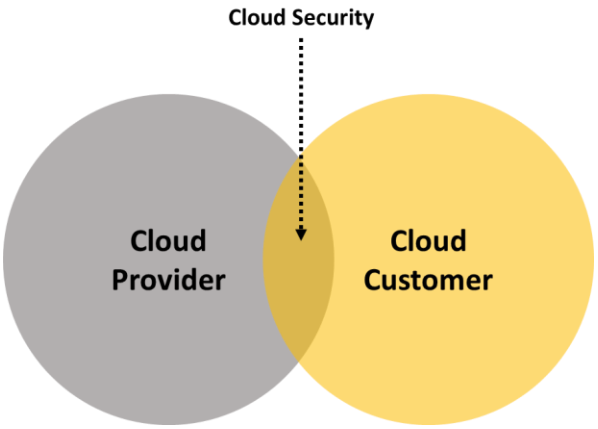


Figure 6.24: Cloud security: Shared responsibility

Compared to traditional IT systems, in which a single organization has authority over the complete stack of computing resources and the entire life cycle of systems, cloud service providers and consumers work together to design, build, deploy, and operate cloud-based systems. Therefore, both parties share responsibilities to maintain adequate security in these systems. Different cloud service models (IaaS, PaaS, and SaaS) imply varying levels of controls between the cloud service providers and cloud consumers.

Shared Responsibility Model for Security in the Cloud

Responsibility	On-Premises (for reference)	IaaS (Infrastructure-as-a-service)	PaaS (Platform-as-a-serve=ice)	SaaS (Software-as-a-service)
User Access	Customer	Customer	Customer	Customer
Data	Customer	Customer	Customer	Customer
Applications	Customer	Customer	Customer	Cloud Provider
Operating System	Customer	Customer	Cloud Provider	Cloud Provider
Network Traffic	Customer	Cloud Provider	Cloud Provider	Cloud Provider
Infrastructure	Customer	Cloud Provider	Cloud Provider	Cloud Provider
Physical	Customer	Cloud Provider	Cloud Provider	Cloud Provider

Customer Responsibility Cloud Provider Responsibility

Figure 6.25: Shared responsibility model for cloud security

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

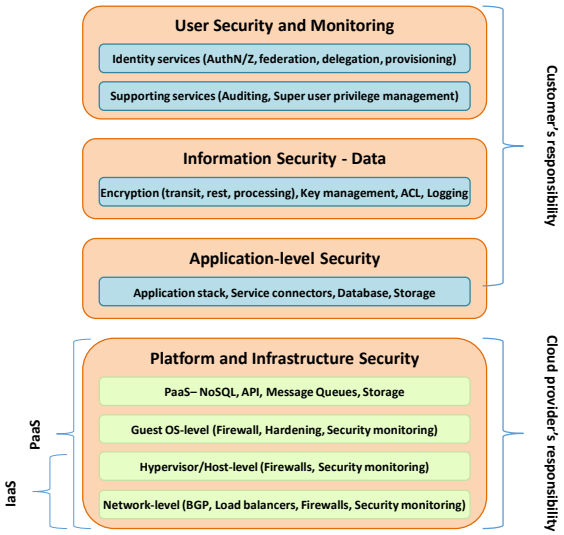
Elements of Cloud Security

Cloud Service Consumers

- Cloud service consumers are responsible for:
  - ✓ User security and monitoring (identity and access management (IAM)
  - ✓ Information security–data (encryption and key management)
  - ✓ Application-level security
  - ✓ Data storage security
  - ✓ Monitoring, logging, and compliance

Cloud Service Providers

- Cloud service providers are responsible for **securing the shared infrastructure**, including routers, switches, load balancers, firewalls, hypervisors, storage networks, management consoles, DNS, directory services, and cloud API

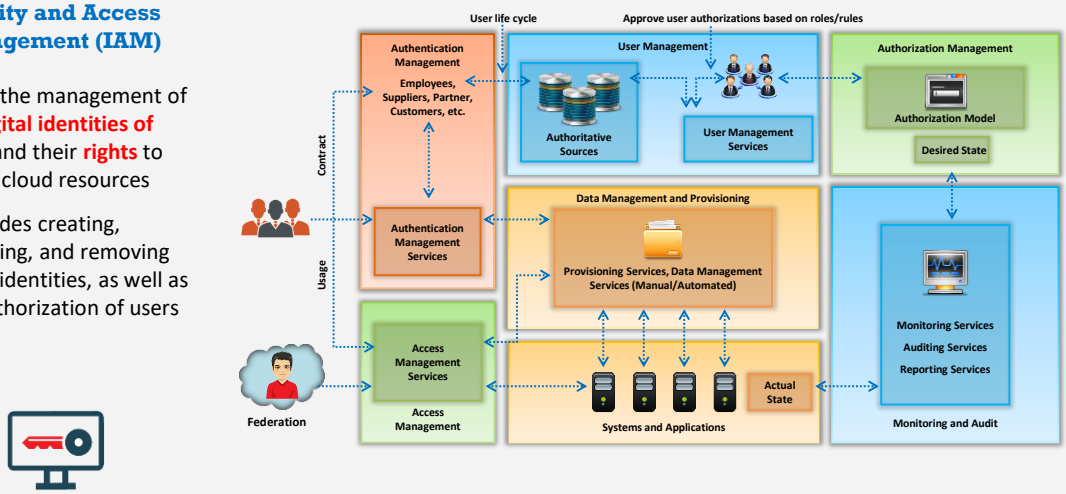


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Elements of Cloud Security (Cont'd)

Identity and Access Management (IAM)

- IAM is the management of the **digital identities of users** and their **rights** to access cloud resources
- It includes creating, managing, and removing digital identities, as well as the authorization of users



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Elements of Cloud Security (Cont'd)

Compliance

- A clear idea about the **regulation standards** that an organization wants to comply with along with its associated requirements allows organizations benefit from the business agility and growth
- **Compliance considerations** for the organizations to integrate their compliance programs with their cloud providers:
  - ✓ Know the requirements that impact an organization to know about the jurisdictions of an organization, industry, or activities employed by the organization to conduct business
  - ✓ Conduct regular compliance risk assessments to help the organizations to adopt the updated and revised risk assessment processes regularly
  - ✓ Monitoring and auditing the organization compliance program before a crisis hits helps organizations to determine the gaps and improving their compliance position

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Elements of Cloud Security (Cont'd)

Data Storage Security

- In a cloud, data are stored on internet-connected servers in **data centers** and it is the responsibility of data centers to secure the data
- The data storage security techniques includes local data encryption, key management, strong password management, periodic security assessment of data security controls, cloud data backup, etc.

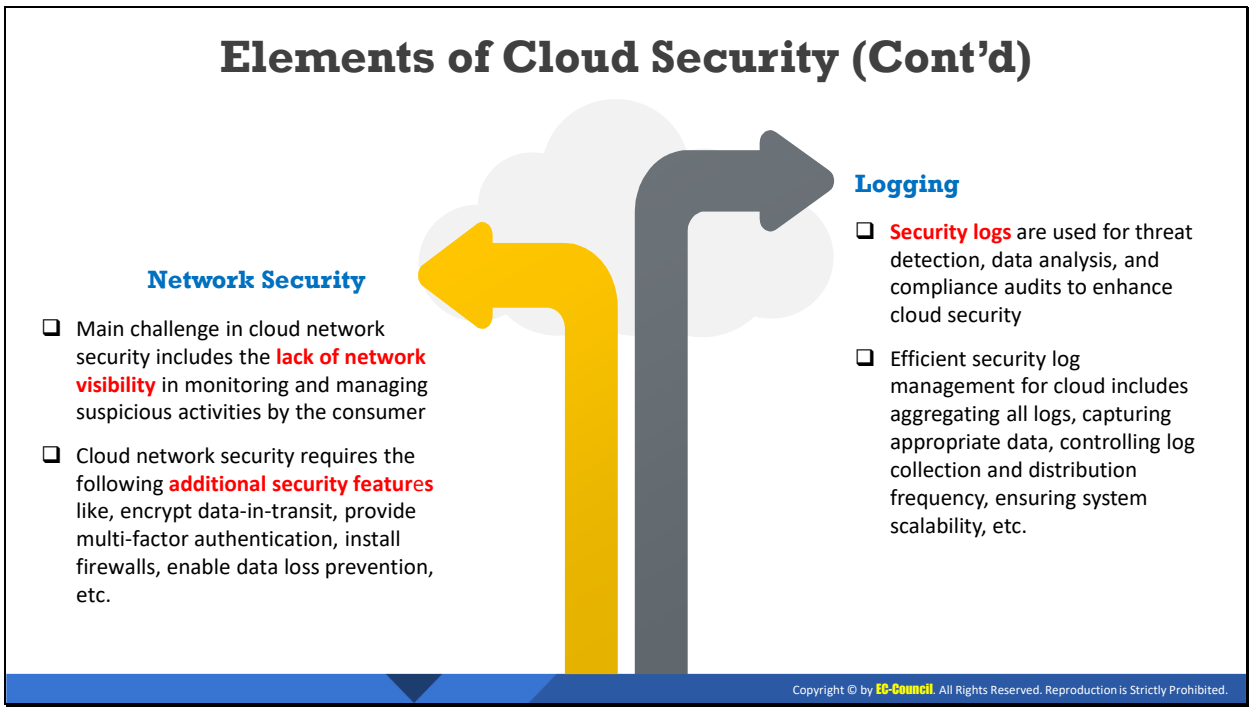
Monitoring

- Monitoring is required to manage **cloud-based services**, **applications**, and **infrastructure**
- Activity monitoring should observe the **activities** like data replication, data file name changes, data file classification changes, data ownership changes to monitor unauthorized data access, etc.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Elements of Cloud Security

Cloud Service Consumers

Cloud service consumers are responsible for:

- User security and monitoring (identity and access management (IAM)
- Information security–data (encryption and key management)
- Application-level security
- Data storage security
- Monitoring, logging, and compliance

Cloud Service Providers

Cloud service providers are responsible for securing the shared infrastructure, including routers, switches, load balancers, firewalls, hypervisors, storage networks, management consoles, DNS, directory services, and cloud API.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

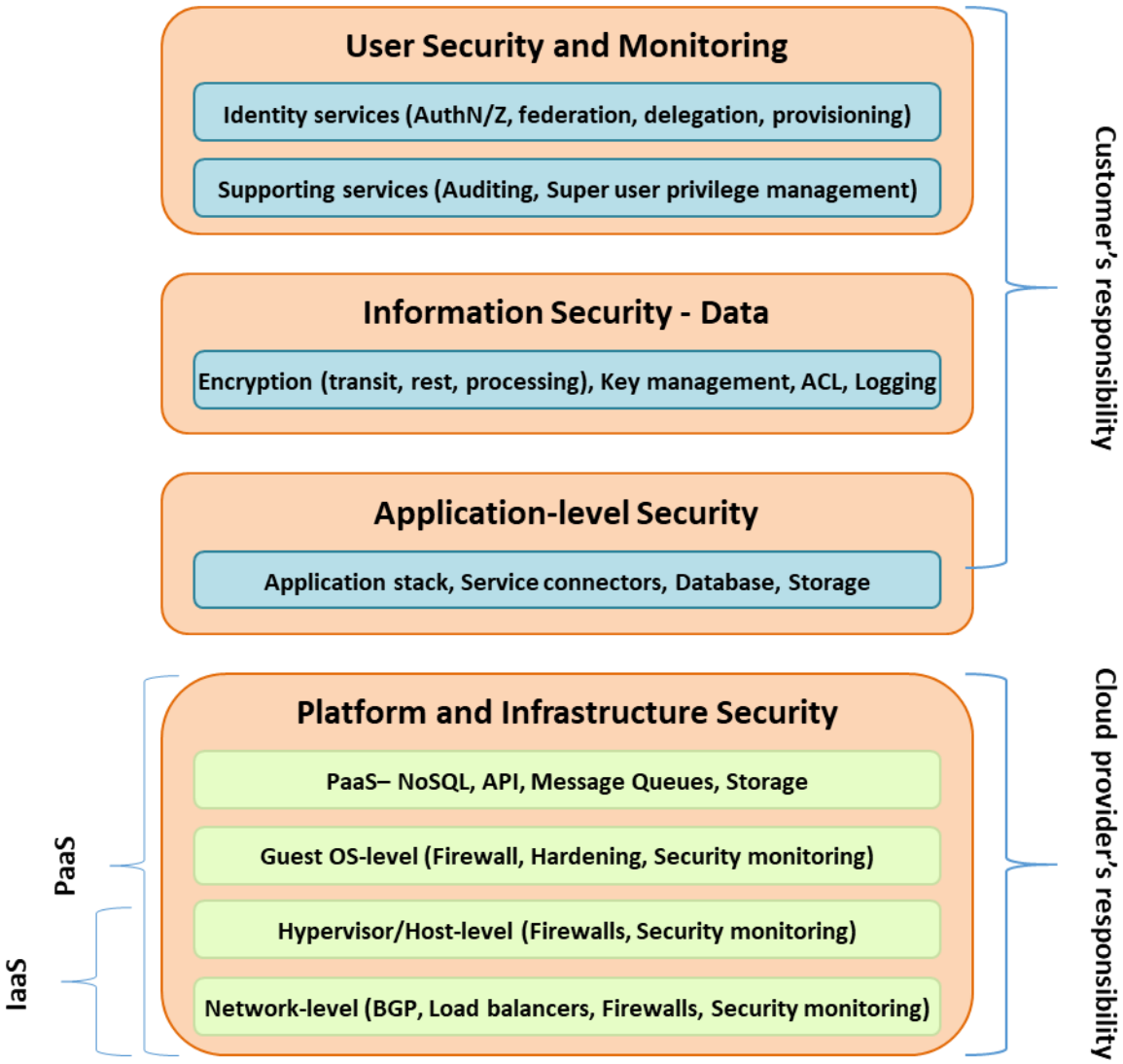


Figure 6.26: Elements of cloud security

Identity and Access Management (IAM)

Identity and Access Management (IAM) offers role-based access control to the customers or employees of an organization for accessing critical information within the enterprise. It comprises business processes, policies, and technologies that enable the surveillance of electronic or digital identities. IAM products provide tools and technologies to the system administrators for regulating user access (creating, managing, and removing access) to systems or networks based on the roles of individual users within the enterprise. Organizations generally prefer all-in-one authentication that can be extended to Identity Federation. Because Identity Federation includes IAM with single sign-on (SSO) and a centralized AD account for secure management. Additionally, IAM enables multi-factor authentication (MFA) for the root user and its associated user accounts. MFA is used to control the access to cloud service APIs. However, the best option is selecting either a virtual MFA or hardware device.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

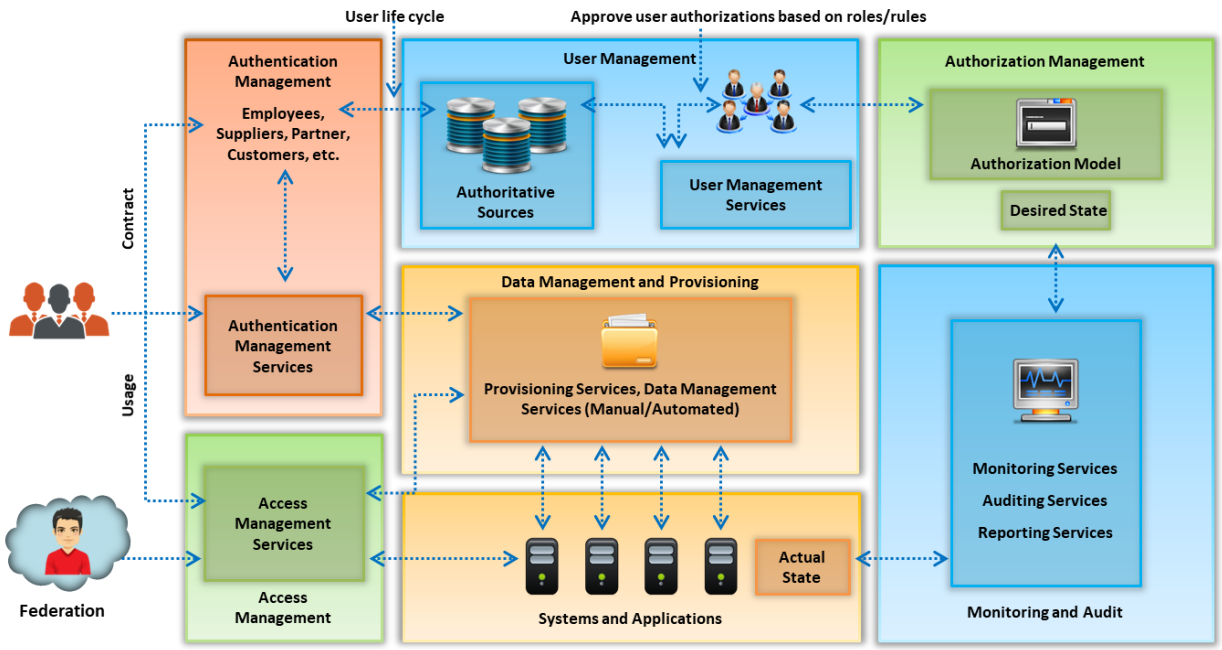


Figure 6.27: Identity and Access Management (IAM)

Compliance

A clear understanding of the requirements of an organization and how compliance is achieved can enable the organizations to benefit from business agility and growth. Compliance failure can lead to regulatory fines, lawsuits, cyber security incidents, and reputational damage.

Following are the compliance considerations for an organization to integrate its compliance programs with its cloud providers.

- **Knowing the requirements that impact an organization** is important. These requirements are based on the jurisdiction of an organization, industry, or the activities employed by an organization for its operation.
- **Conducting regular compliance risk assessments** helps organizations to establish the foundation of a strong compliance program. This process allows organizations to adopt the updated and revised risk assessment processes regularly.
- **Monitoring and auditing the compliance program of an organization proactively** or before a crisis hits can help organizations to find gaps and improve their compliance position.

Data Storage Security

In a cloud, data are stored on internet-connected servers in data centers, and it is the responsibility of data centers to secure the data. However, customers should protect their data to ensure comprehensive data security

Data Storage Security Techniques:

- **Local data encryption:** Ensuring confidentiality of sensitive data in the cloud.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **Key management:** Generating, using, protecting, storing, backing up, and deleting encryption keys. Key management in cloud ensures strict key security owing to the increased possibility of key exposure.
- **Strong password management:** Using strong passwords and changing them at regular intervals.
- **Periodic security assessment of data security controls:** Continuously monitoring and reviewing the implemented data security controls.
- **Cloud data backup:** Taking local backups of the cloud data prevents possible data loss in the organization.

Network Security

Main challenge in cloud network security includes the lack of network visibility in monitoring and managing suspicious activities by the consumer. Cloud network security requires the following additional security features in comparison to the traditional network security features.

- Encrypt data-in-transit
- Provide multi-factor authentication
- Install firewalls
- Enable data loss prevention

Methods to secure a cloud network

- Using DMZs
- Isolating resources with subnets, firewalls, and routing tables
- Securing DNS configurations
- Limiting inbound/outbound traffic
- Securing accidental exposures
- Intrusion detection and prevention systems
- Implementing layers of firewall

Monitoring

Cloud monitoring is required to manage cloud-based services, applications, and infrastructure. Effective cloud monitoring helps an organization to protect a cloud environment from potential threats, store, and transfer data in the cloud easily and safeguard the personal data of customers.

Activity monitoring should observe the following activities to monitor unauthorized data access:

- **Data replication**: It plays a key role in data management by migrating databases online and synchronizing the data in real time. Migration monitoring should be performed during data replication.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- **Data file name changes**: Data handling activities such as data file name changes should be monitored. The file change attributes should be utilized for monitoring changes in the file system.
- **File classification changes**: Activity monitoring through file classification changes helps in determining any changes in the cloud data files.
- **Data ownership changes**: Data activity monitoring via data ownership changes should be closely monitored to prevent unauthorized access and security breach.

Data monitoring should define thresholds and rules for normal activities, which can help in detecting unusual activities and send alerts to data owners if any breach is observed in the defined threshold.

Logging

Security logs provide a record of the activities in the IT environment of an organization. They are used for threat detection, data analysis, and compliance audits to enhance cloud security.

After the accelerated adoption of cloud platforms, instead of using a few servers, companies now maintain thousands of servers that play a smaller role within the application infrastructure stack. This complicates the aggregation of data silos.

To ensure efficient and secure log management in the cloud, organizations should follow the following practices.

- Aggregate All Logs
- Capture Appropriate Data
- Keep Applications Safe
- System Scalability

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

AWS Identity and Access Management

AWS identity and access management (IAM) is a web service that enables customer to securely control the access to AWS services and resources. It helps in establishing the access rules and permissions for specific users and applications. It controls who is authenticated (signed in) and authorized (has permissions) for resource access.

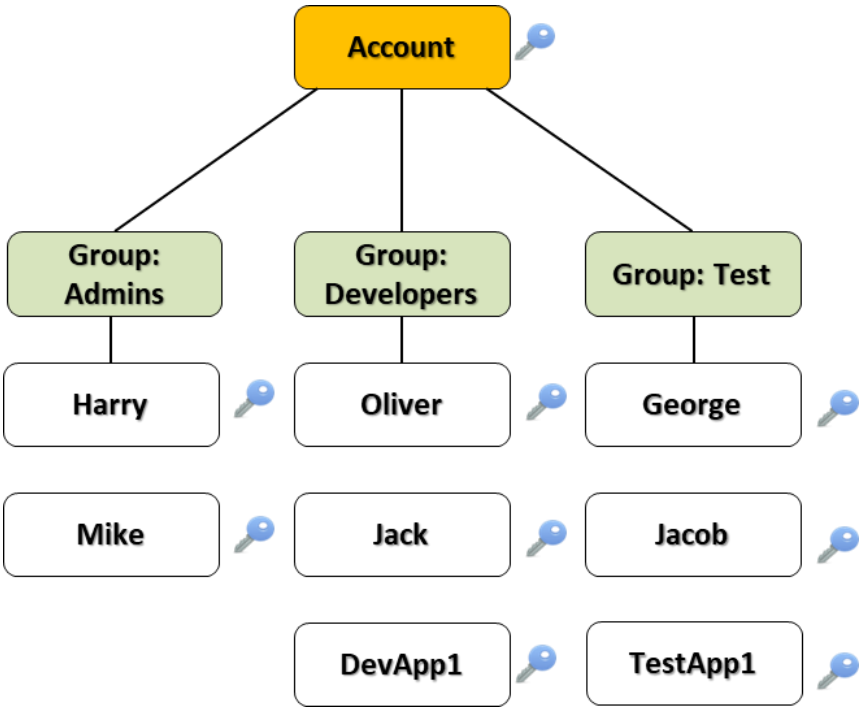


Figure 6.28: Accounts

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

IAM Features

Key features of IAM include

- **Shared access to AWS account/enhanced Security**

  Creating usernames and passwords for other users/groups to delegate access to specific AWS service APIs and resources without sharing your password or access key.

- **Granular permissions**

  Granting different permissions to different people for various resources to provide granularity to control user access to specific AWS services and resources.

- **Secure access to AWS resources for applications that run on Amazon EC2**

  Providing credentials for applications that run on EC2 instances to permit applications to access other AWS resources.

- **Multi-factor authentication**

  Adding two-factor authentication to the user accounts for additional security.

- **Identity federation**

  Allowing users who already have passwords elsewhere and allowing users to have just one password for on-premise and cloud environment work.

- **Identity information for assurance**

  Receiving log records if the users utilize AWS CloudTrail.

- **Payment Card Industry Data Security Standard**

  Supporting the Payment Card Industry Data Security Standard (PCI DSS) for organizations that handle branded credit cards from major card schemes.

- **Integrated with AWS Services**

  Enabling the provision of access controls from a specific location in the AWS management console, which will be implemented throughout the AWS environment.

- **Password Policy**

  Allowing to reset a password or rotate passwords remotely and setting rules for password usage.

- **Policies and Groups**

  Use IAM groups for easier permission management and following the best IAM practices. IAM enables the organization of IAM users into IAM groups and applies a policy to each group; individual users still possess their credentials.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

AWS IAM: Lock Your AWS Account Root User Access Keys

The access key (an access key ID and secret access key) enables programmatic requests to AWS. However, it is not recommended to use the AWS root user access key because it can provide complete access to all resources of the AWS services. It should be noted that users cannot reduce the permissions associated with their AWS root user access key.

Secure Root User Access Key

To protect the root user access key,

- **An AWS root user access key should not be created unless required**. Instead, the email address and password of the account should be used to sign in to the AWS management console and create an administrative IAM user.
- **The AWS root user access key should be regularly changed or deleted.**

  Steps to delete or change the root user access keys:

  - Go to the My Security Credentials page in the AWS management console.
  - Sign in with the email address and password of your account.
  - Manage access keys in the access keys section.
- **Never share the AWS root user password or access keys** to avoid having to embed them in an application.
- **Use strong passwords for logging in the AWS management console.**

  Steps to use strong passwords:

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- Select the desired account name or number; next, select **My Account** on the upper right corner of the AWS management console.
- Select **Edit** on the right side of the page next to the **Account Settings** section.
- Select **Edit** to change the password on the **Password** line.
- AWS requires the password to satisfy the following conditions:
  - The password should have a minimum of 8 and a maximum of 128 characters.
  - The password should include at least three of the following character types: uppercase, lowercase, numbers, and ! @ # $ % ^ & * () <> [] {} | _+-= symbols.
  - The password should not be identical to the AWS account name or email address.

- **Enable AWS MFA on the AWS root user account.**

  Steps for enabling MFA devices:

  - Acquire any of the following MFA device. Note that only one MFA device can be enabled per AWS root user account or IAM user.
    - Virtual MFA device
    - U2F device
    - Hardware-based MFA device
    - Mobile phone
  - Enable the MFA device.
    - IAM users with virtual or hardware MFA devices can enable their devices the AWS management console, AWS CLI, or IAM API.
    - For IAM users with U2F security keys or a mobile phone that can receive SMS texts, the MFA device can be enabled from the AWS management console.
    - For AWS root user accounts with any type of MFA device (except SMS MFA), the device can be enabled from the AWS management console.

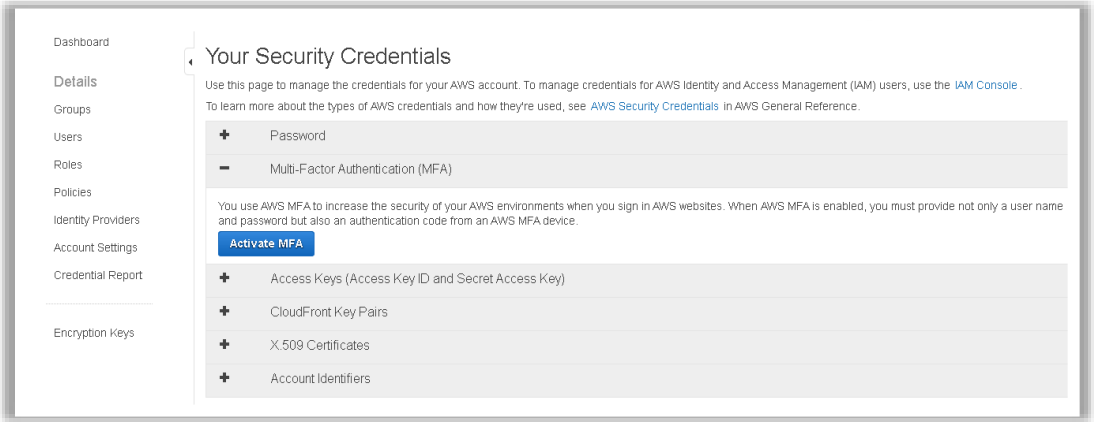


Figure 6.29: Enabling AWS MFA on AWS root user account

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

AWS IAM: Create Individual IAM Users

It is recommended to avoid using the AWS root user account to access AWS. Instead, individual user accounts should be created for accessing AWS. Accordingly, a user should create an IAM user for themselves and enable it with administrative permissions; this account should be used for all operations. Each IAM user should be provided with a unique set of security credentials and different permissions. The IAM user permissions should be changed or revoked if required.

Steps to create a new IAM user:

- Select **Users** from the **Identity and Access Management (IAM)** section and click **Add user** to create a new user.

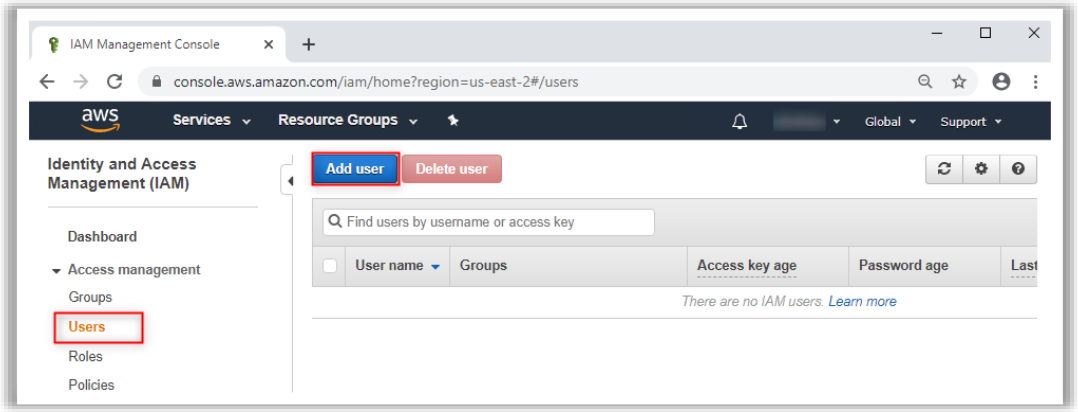


Figure 6.30: Add a User

- In the **User name** field, provide any name (here, **Alice**).

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- For **Access type**, provide **AWS Management Console access** to Alice under the **Select AWS access type** section. Select the **Custom password** radio button and enter a password in the **Password** field. The **Require password reset** tab is optional; however, enable this setting. Then, click on **Next Permission.**

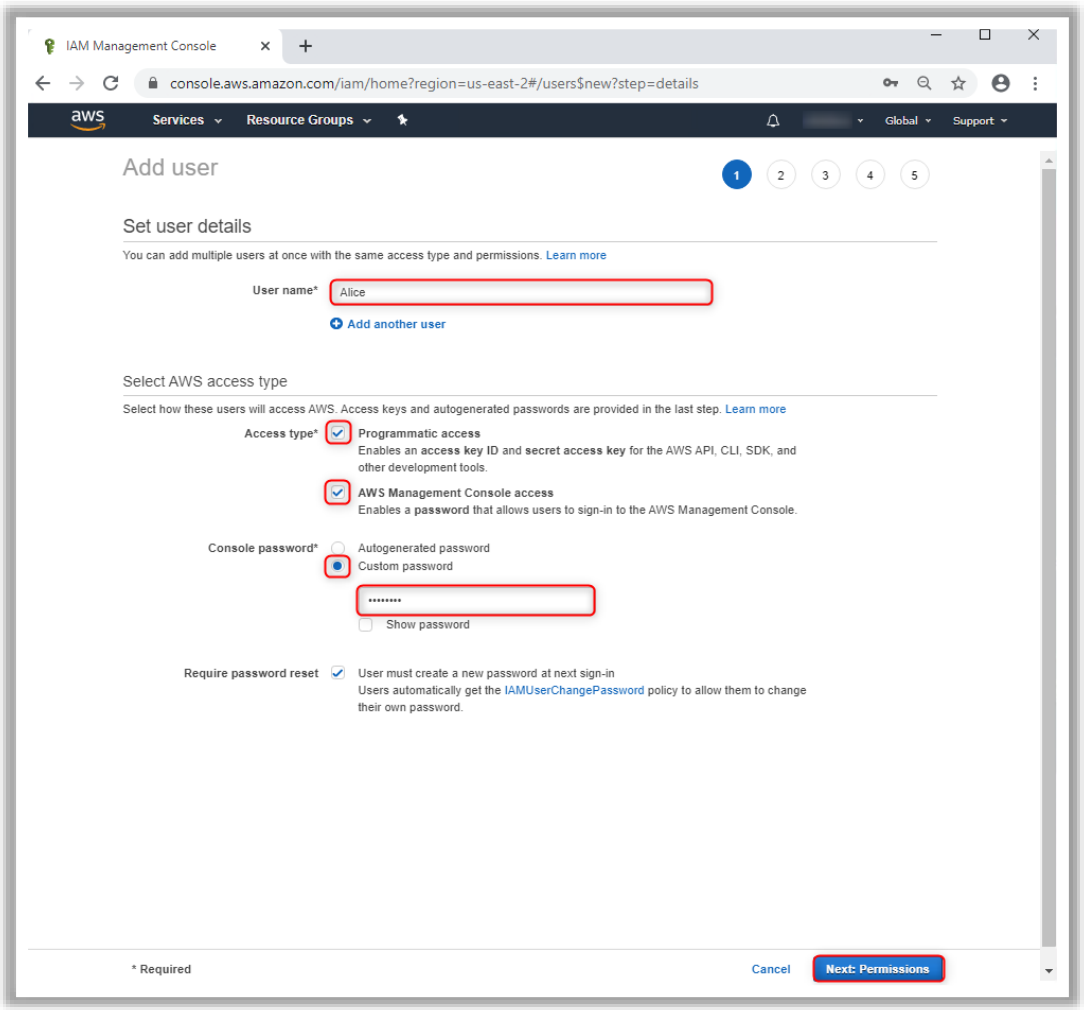


Figure 6.31: Set Console Password for User Alice

- Under the **Set permissions** section, the **Add user to group** option is selected by default. Check the newly created group (here, **Training_Group**); this will add the user to the group. Then, click on **Next: Tags**.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

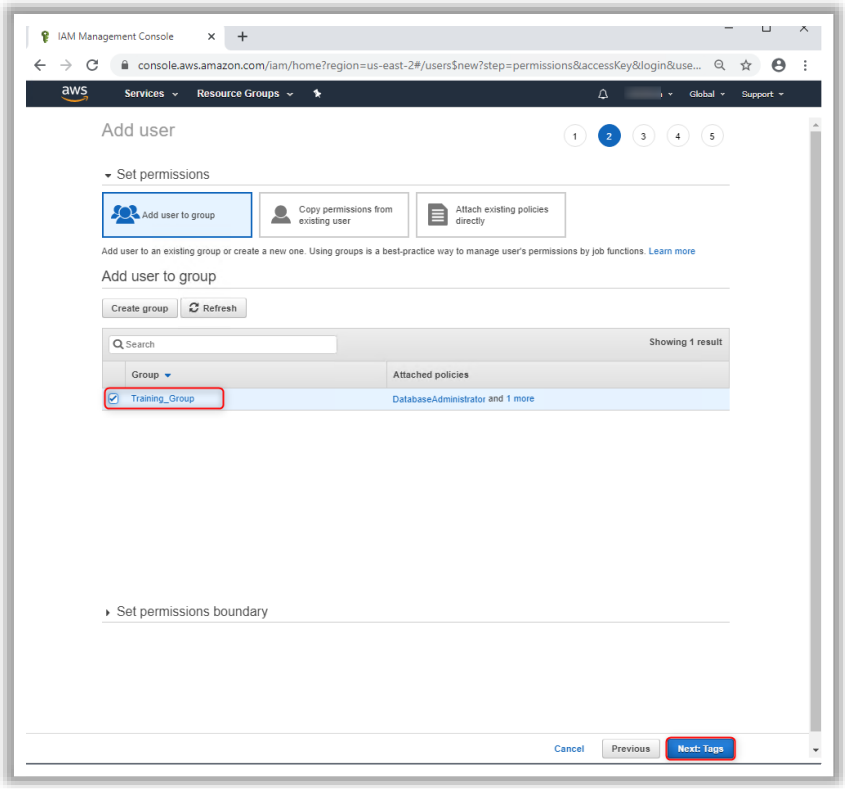


Figure 6.32: Add a User to Group

- Tags are optional; however, tagging helps in searching for Tag keys easily in the future. Specify **Department** as **Tag Key** and **Key-Value** as **Training**. Click **Next: Review** to review IAM User creation.

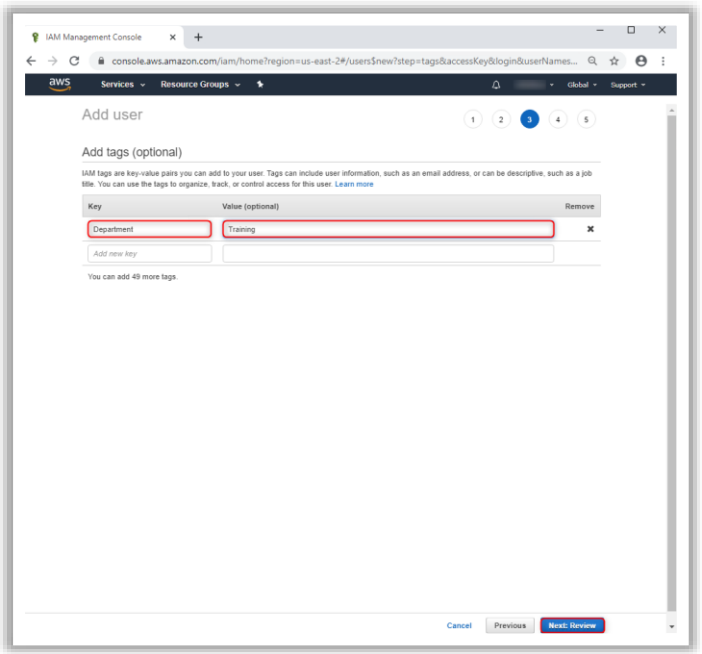


Figure 6.33: Specify Tags

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- After verifying the settings on the Review page, click on **Create user**.

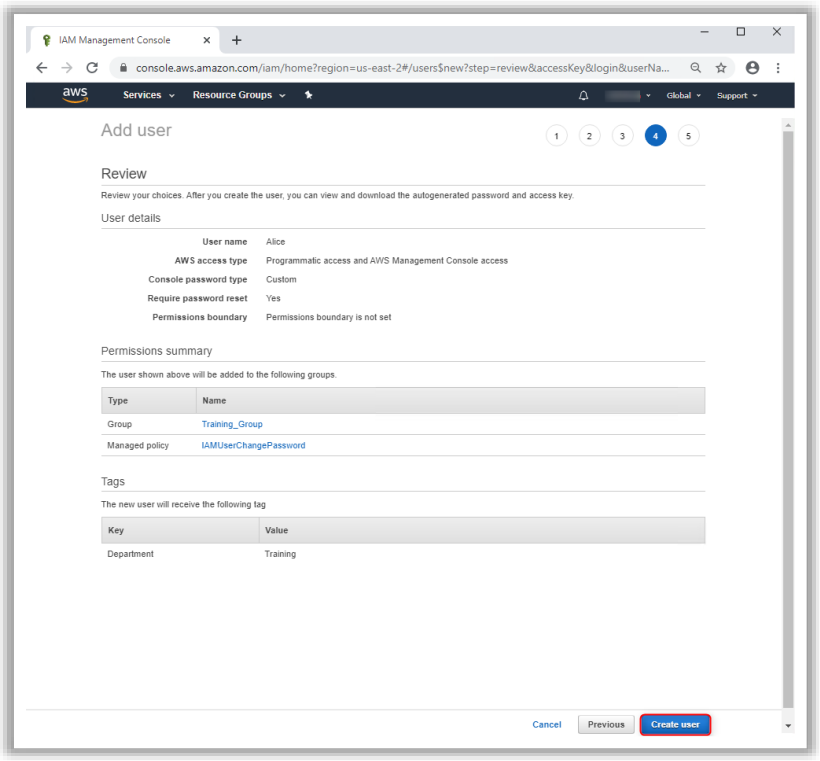


Figure 6.34: Create User

- After clicking on **Create user**, a success message is displayed.

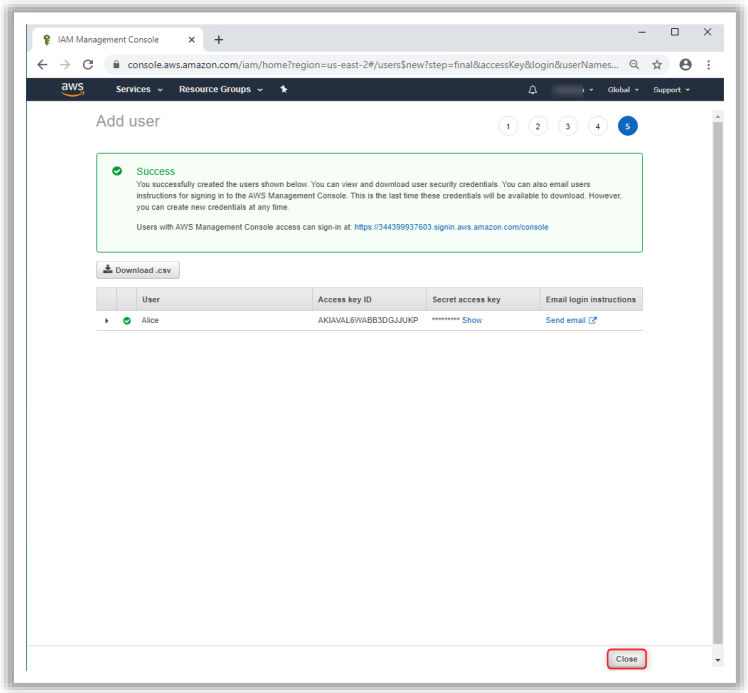
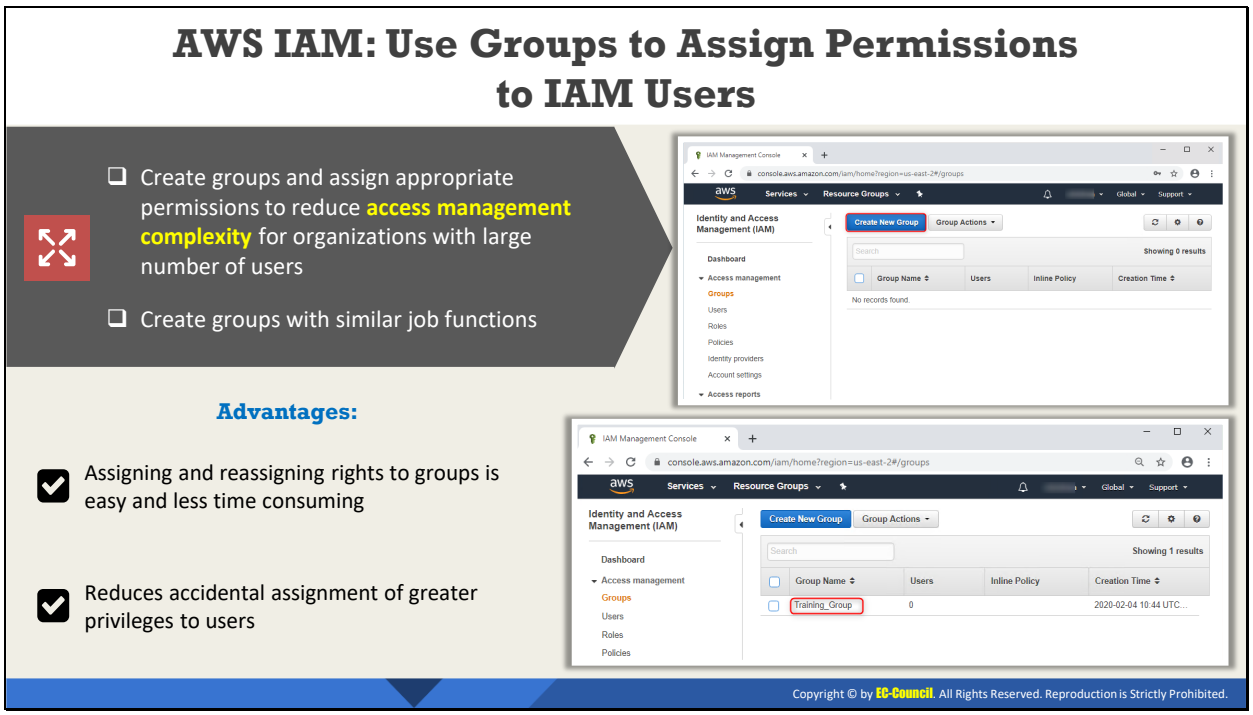


Figure 6.35: Confirmation Message

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



AWS IAM: Use Groups to Assign Permissions to IAM Users

Granting permissions to each IAM user can be a difficult task. Therefore, create groups and define specific rights and permissions for each group. Add IAM user accounts to these groups based on their job functions. This can help in modifying the IAM users of a specific group at one spot and reduce the access management complexity for organizations with numerous users and the accidental assignment of higher privilege to users. It is easy and less time-consuming to assign and reassign rights to groups. If the role of a user is changed, the IAM user account can be transferred to the new group.

- Click on **Groups** in the left pane under **Identity and Access Management (IAM).**

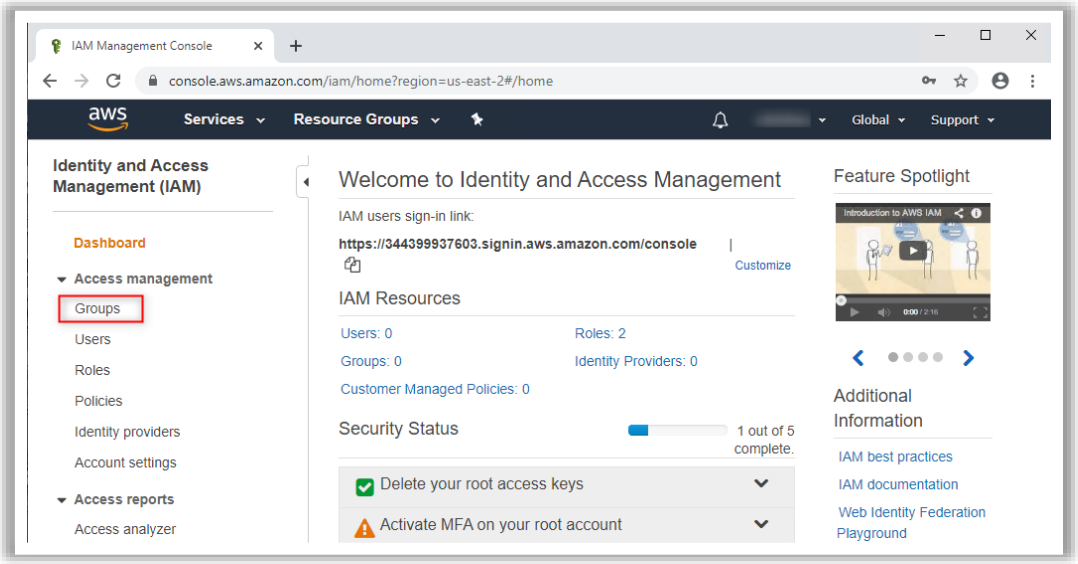


Figure 6.36: Click Groups in Dashboard

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- Click on **Create New Group**.

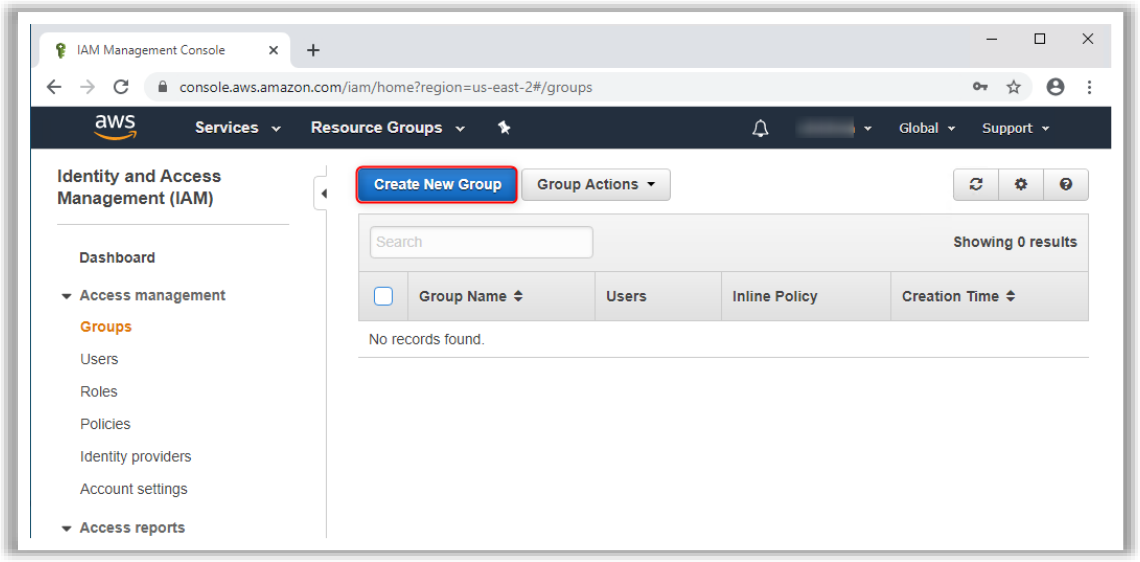


Figure 6.37: Click "Create New Group" Button

- Under the **Set Group Name** section, type the group name in the **Group Name** field (here, **Training_Group**) and click on **Next Step**.

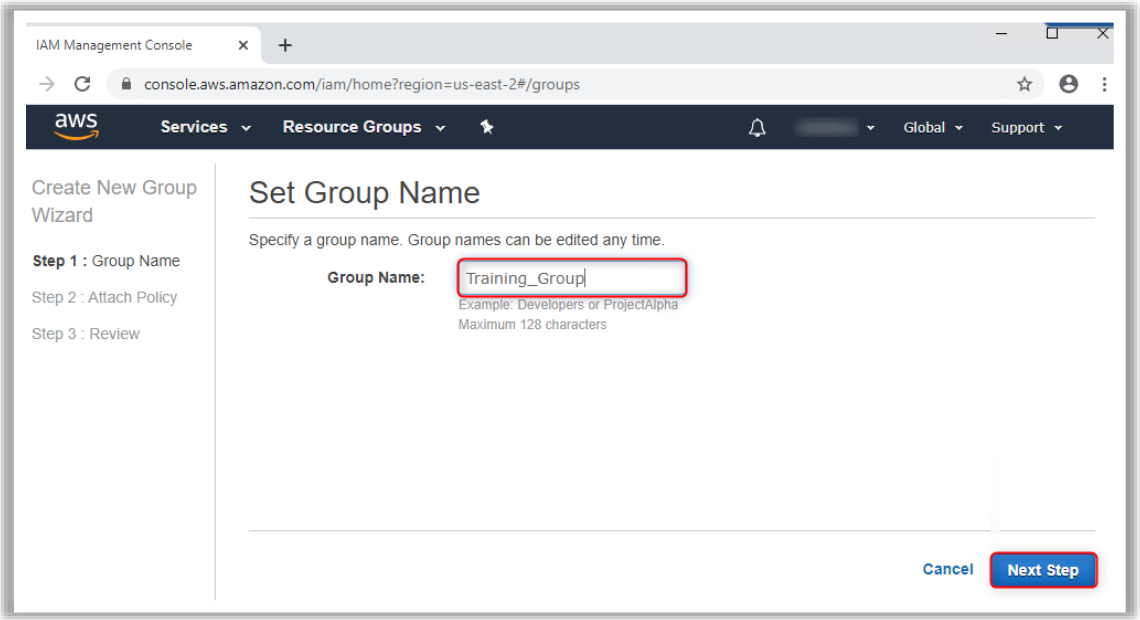


Figure 6.38: Set Group Name

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- In the **Attach Policy** section, search for **iamuserchangepassword**; the matching records get filtered, then check **IAMUserChangePassword**.

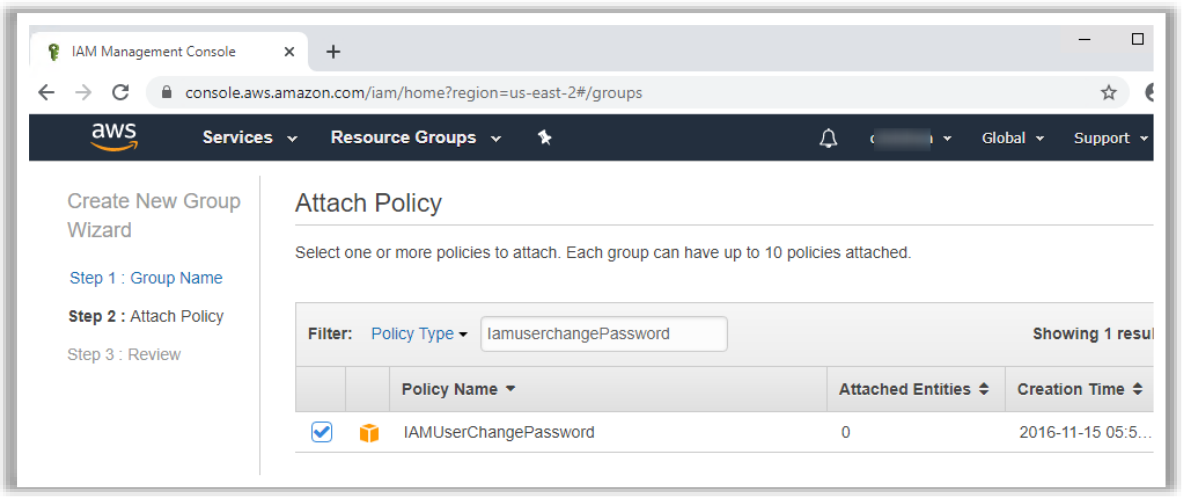


Figure 6.39: Check for "IamUserChangePassword" Policy Name

- Search for **databaseadministrator**; the matching records get filtered, then check **DatabaseAdministrator**, and click on **Next**.

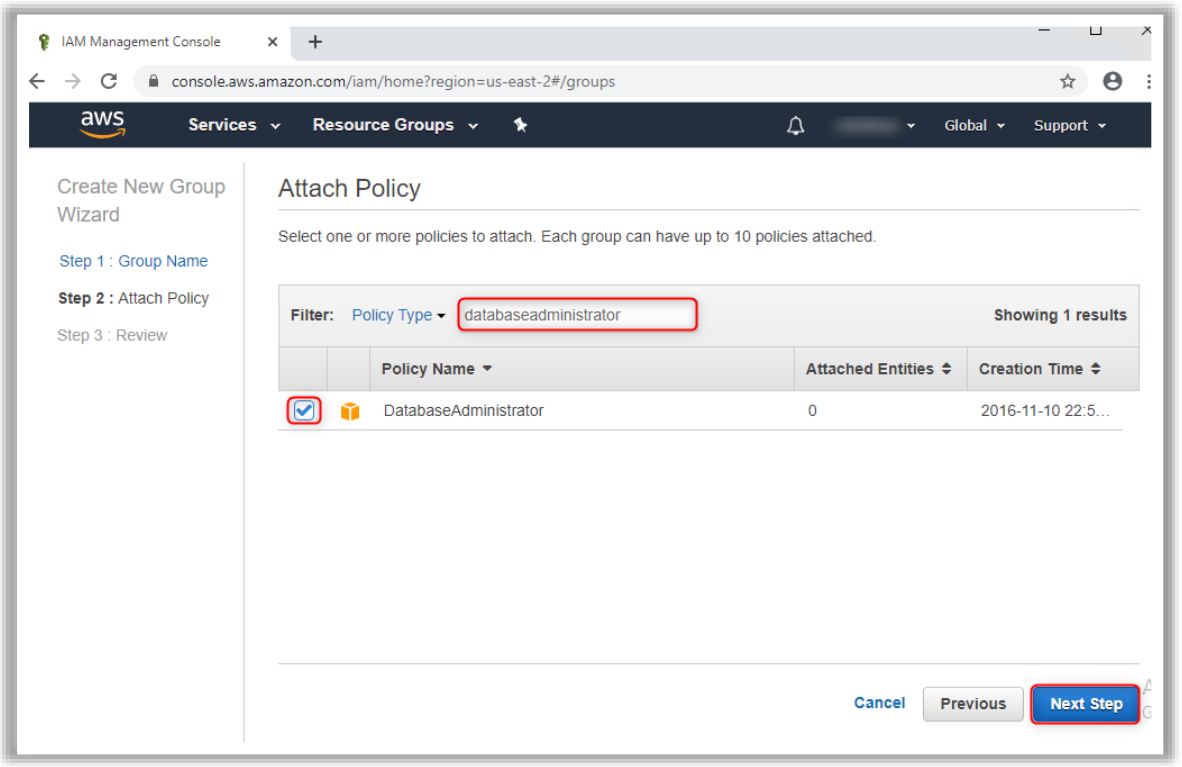


Figure 6.40: Check for "DatabaseAdministrator" Policy Name

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- In the **Review** section, two policies are added. Click on **Create Group**.

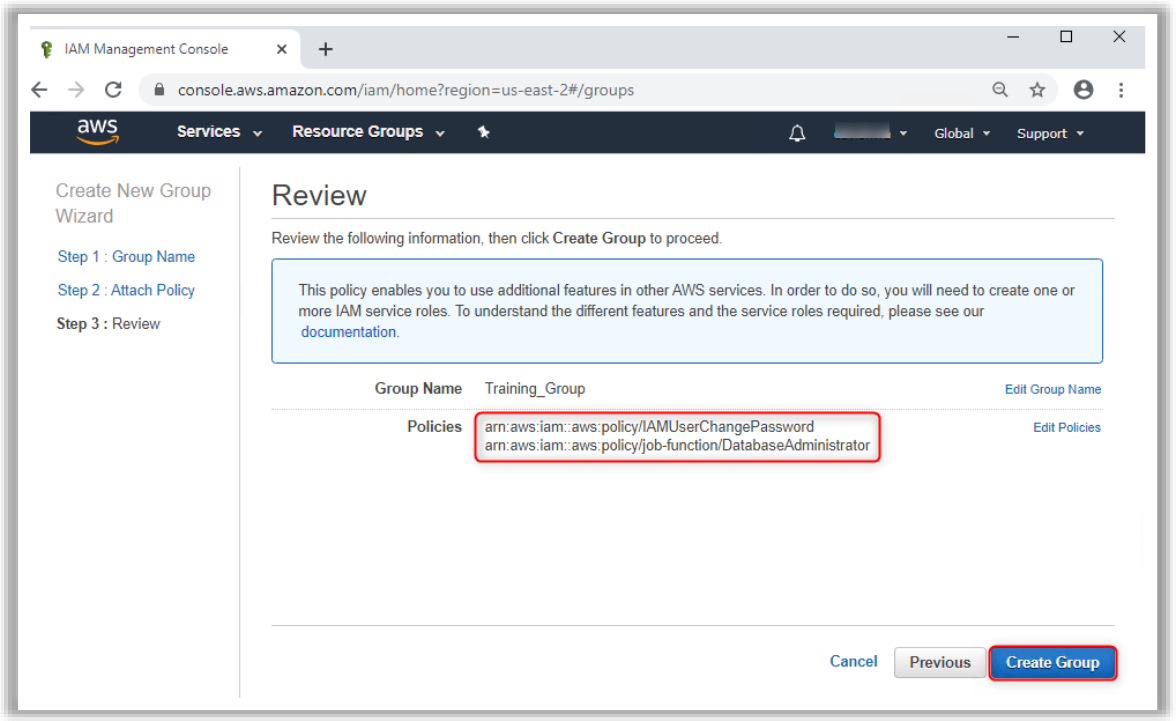


Figure 6.41: Create Group with the Selected Policies

- **Training_Group** is created under **Groups**.

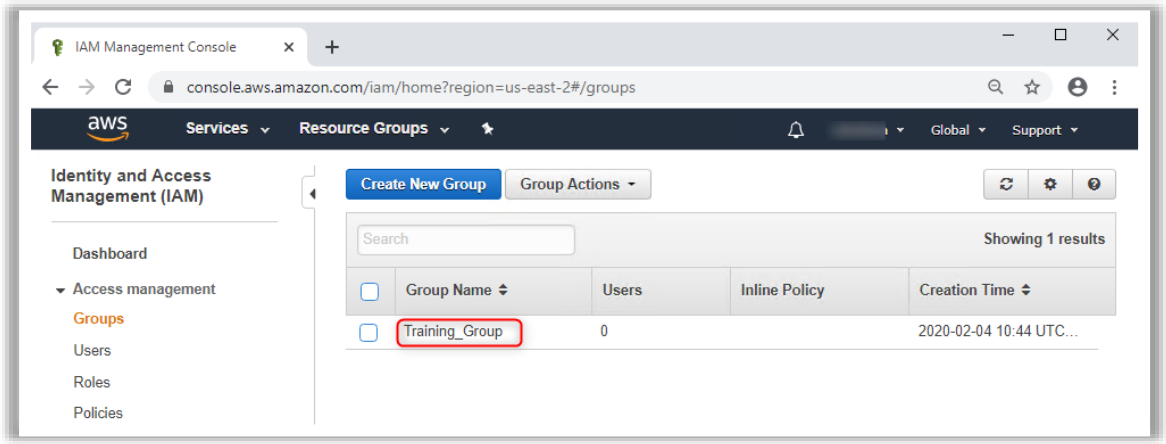
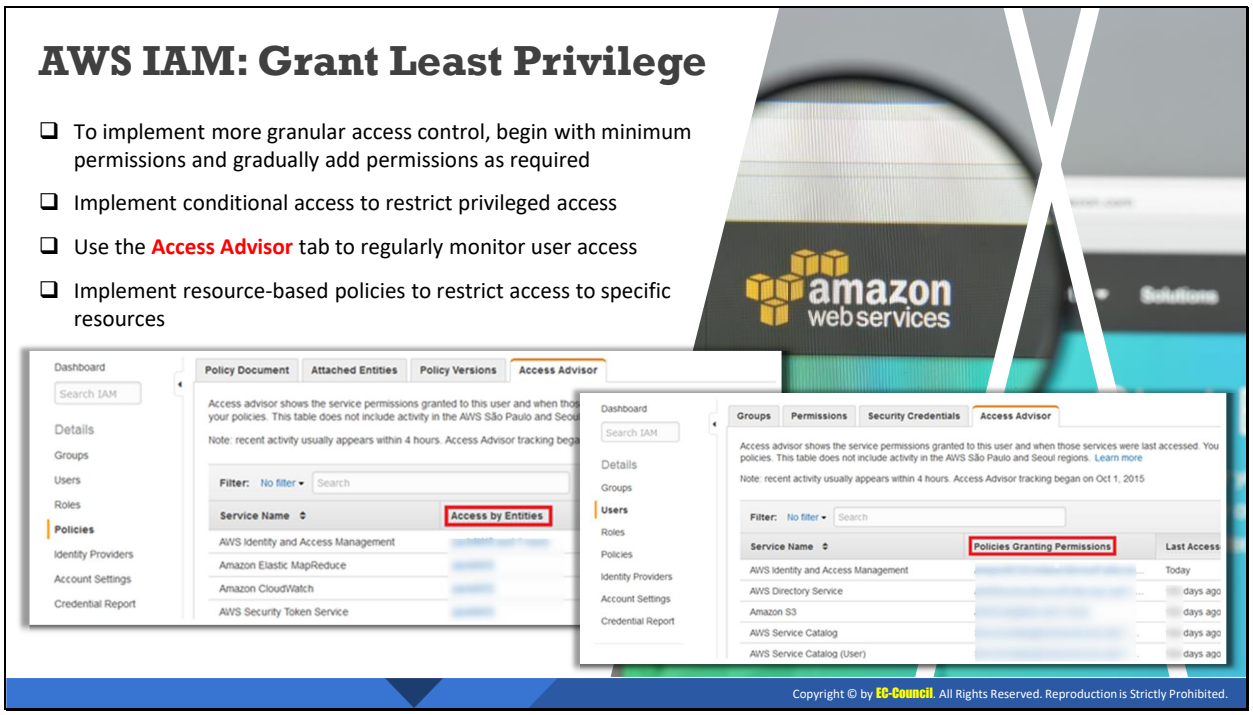


Figure 6.42: Create Group

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



AWS IAM: Grant Least Privilege

During the creation of IAM policies, permissions are required only to perform the required tasks. Thus, the policies should be formulated according to the roles of users. Initially, minimum permissions should be provided to ensure security; the permissions can be extended in the future. The action types include list, read, write, permission management, and tagging. For example, if actions are selected from the List and Read access levels, they are used to grant read-only access to the users. An example of the actions of policies and their descriptions are given below.

The “service last accessed” data feature can be used to view the data on the Access Advisor tab on the IAM console. The same data can be viewed on the AWS Organizations section of the IAM console if the user is logged in with the credentials of the master account. This information can be used to view the unnecessary permissions to refine them accordingly. The events of an account in AWS CloudTrail Event History can be used to implement further granular permissions.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

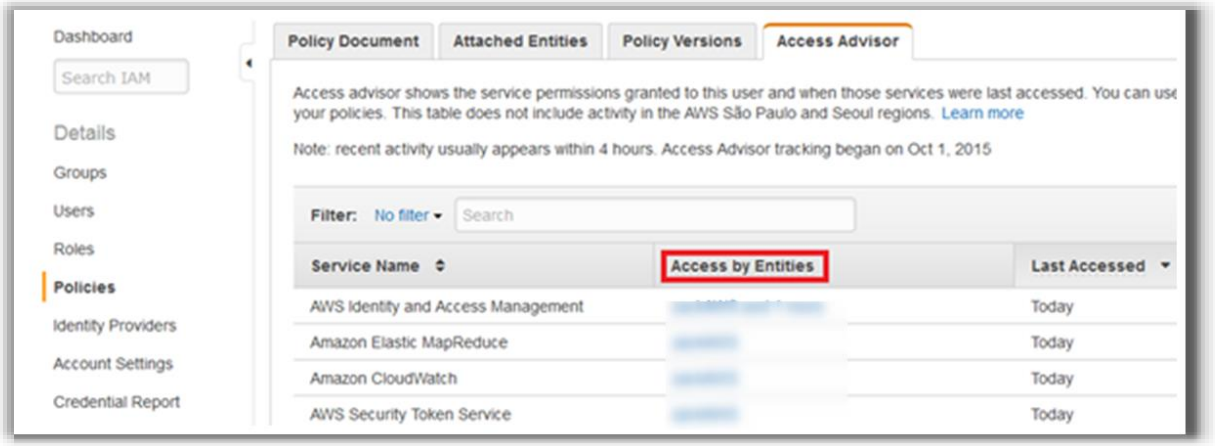


Figure 6.43: Service Permissions Granted to User and When a Service was Last Accessed

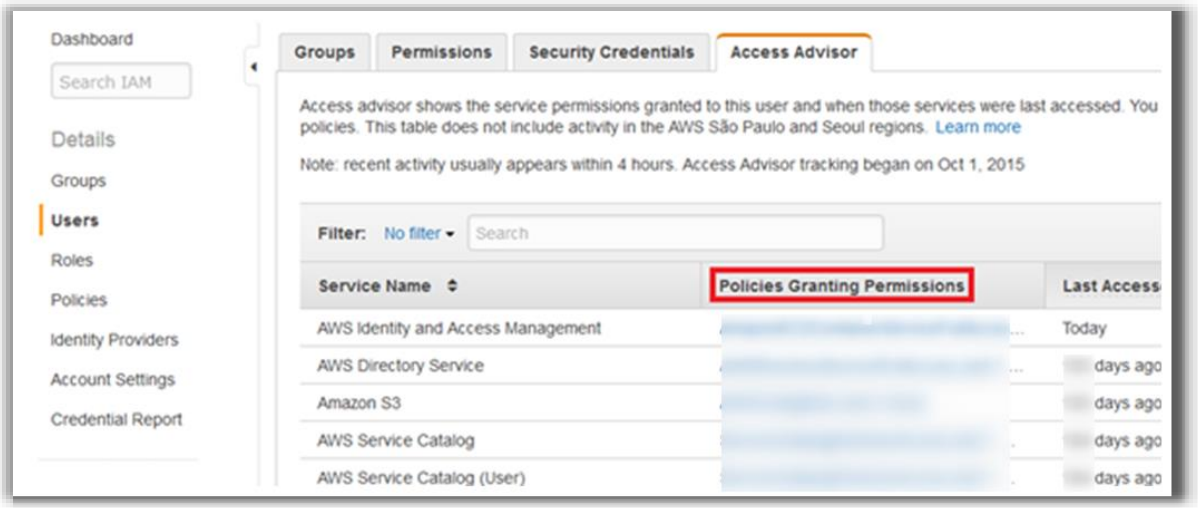
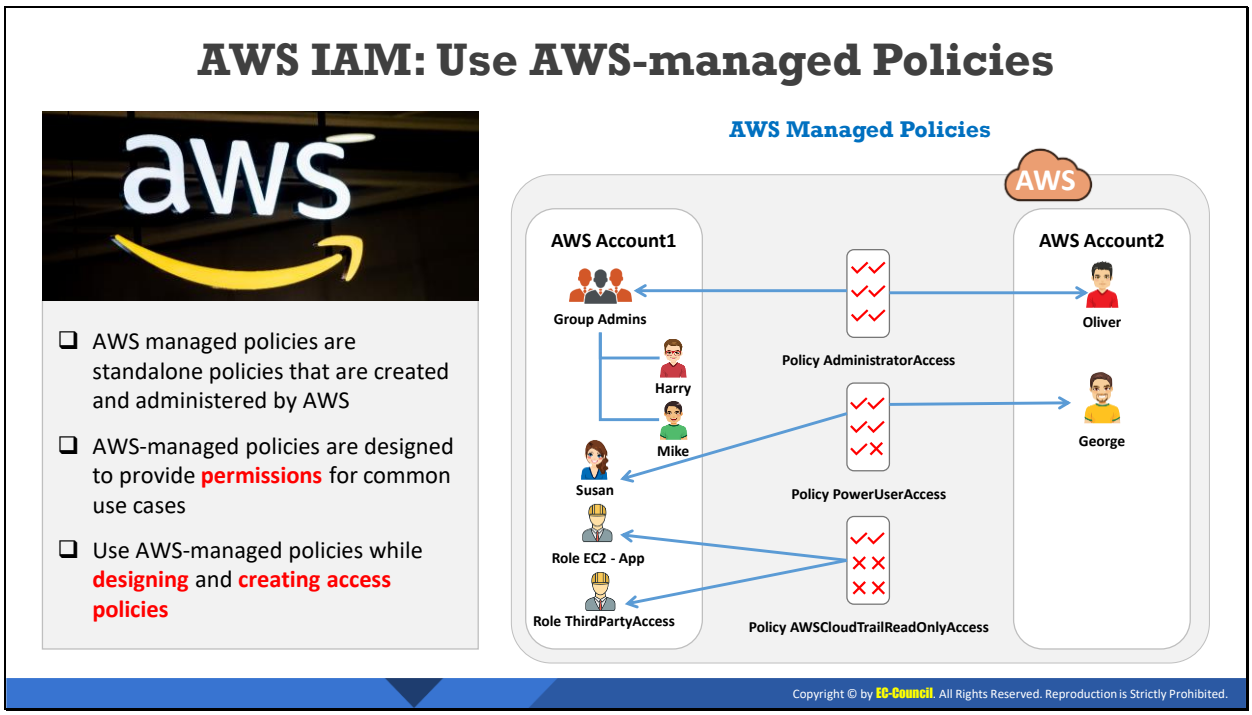


Figure 6.44: Viewing Policies Granting Permissions

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



AWS IAM: Use AWS-managed Policies

Admins need some time to understand the policies and provide them to the employees to perform the required tasks. They need to have a better understanding of the IAM policies, and they should test IAM before implementation. Users also need to be aware of the tasks that they should perform and understand the permissions granted to them.

For better understanding, AWS managed policies provide permissions to users and familiarize them with the tasks that they must perform with the granted permissions. AWS managed policies (standalone policies that are created and administered by AWS) helpful until designing and creating access policies.

The AWS managed policies provide permissions for many common use cases:

- **Full access AWS managed policies** define permissions for service administrators by granting full access to a service. For example, AmazonDynamoDBFullAccess and IAMFullAccess.
- **Power-user AWS managed policies** provide multiple levels of access to AWS services without allowing permission management. For example, AWSCodeCommitPowerUser and AWSKeyManagementServicePowerUser.
- **Partial-access AWS managed policies** provide specific levels of access to the AWS services. For example, AmazonMobileAnalyticsWriteOnlyAccess and AmazonEC2ReadOnlyAccess.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

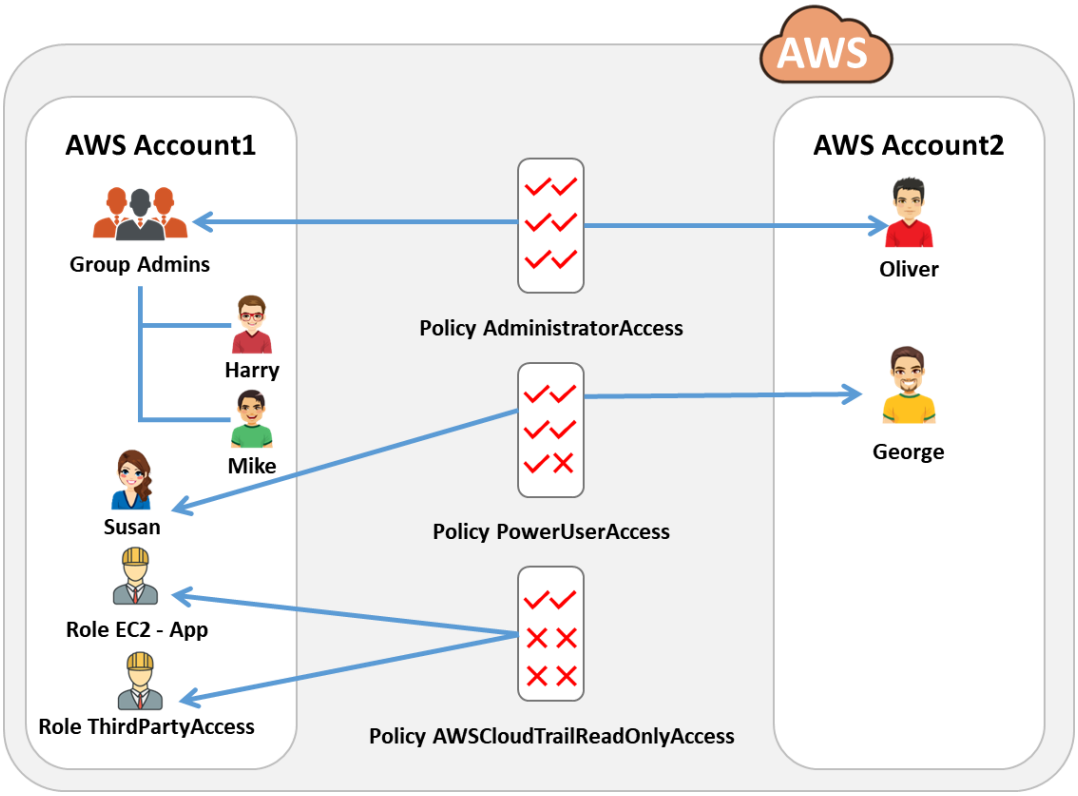
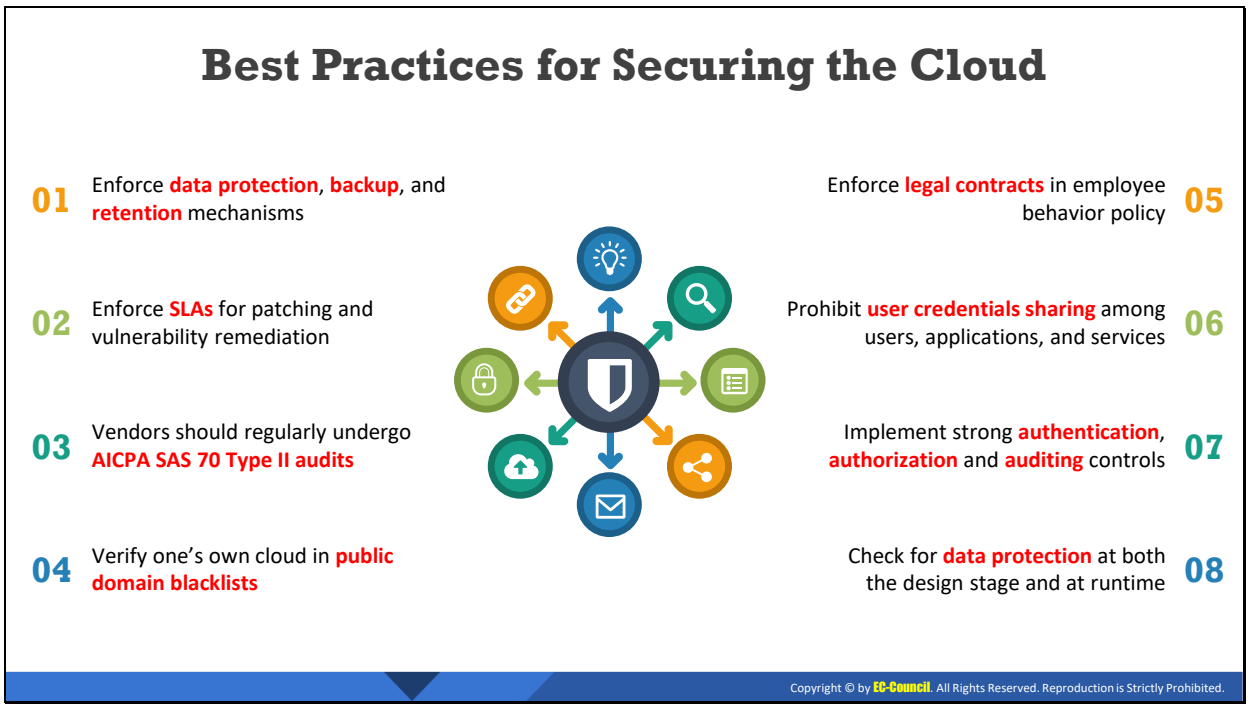


Figure 6.45: AWS Managed Policies

The above diagram illustrates three AWS managed policies: AdministratorAccess, PowerUserAccess, and AWSCloudTrailReadOnlyAccess. Here, a single AWS managed policy is attached to the principal entities in different AWS accounts and different principal entities in a single AWS account.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Best Practices for Securing the Cloud

Discussed below are various best practices for securing a cloud environment:

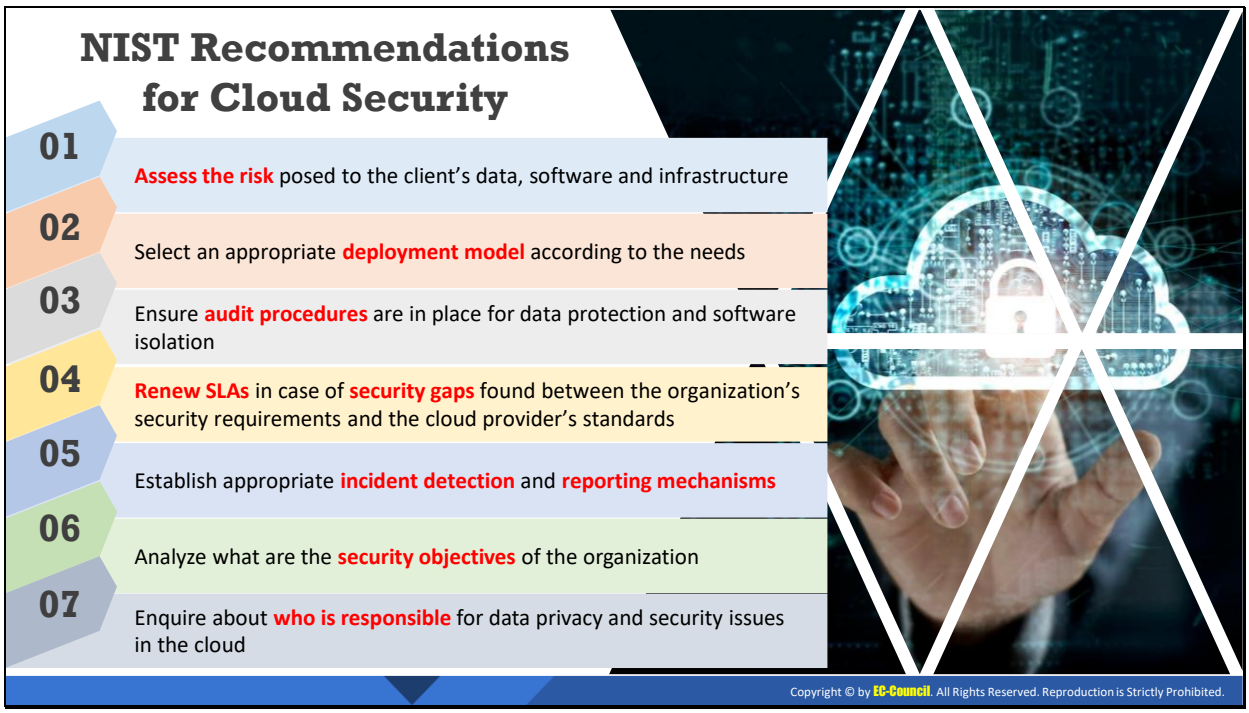
- Enforce data protection, backup, and retention mechanisms.
- Enforce SLAs for patching and vulnerability remediation.
- Vendors should regularly undergo AICPA SAS 70 Type II audits.
- Verify one's cloud in public domain blacklists.
- Enforce legal contracts in employee behavior policy.
- Prohibit user credentials sharing among users, applications, and services.
- Implement secure authentication, authorization, and auditing controls.
- Check for data protection at both design and runtime.
- Implement strong key generation, storage and management, and destruction practices.
- Monitor the client's traffic for malicious activities.
- Prevent unauthorized server access using security checkpoints.
- Disclose applicable logs and data to customers.
- Analyze cloud provider security policies and SLAs.
- Assess the security of cloud APIs and log customer network traffic.
- Ensure that the cloud undergoes regular security checks and updates.
- Ensure that physical security is a 24 x 7 x 365 affair.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- Enforce security standards in installation/configuration.
- Ensure that the memory, storage, and network access are isolated.
- Leverage strong two-factor authentication techniques, where possible.
- Apply a baseline security breach notification process.
- Analyze API dependency chain software modules.
- Enforce stringent registration and validation process.
- Perform vulnerability and configuration risk assessment.
- Disclose infrastructure information, security patching, and firewall details to customers.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

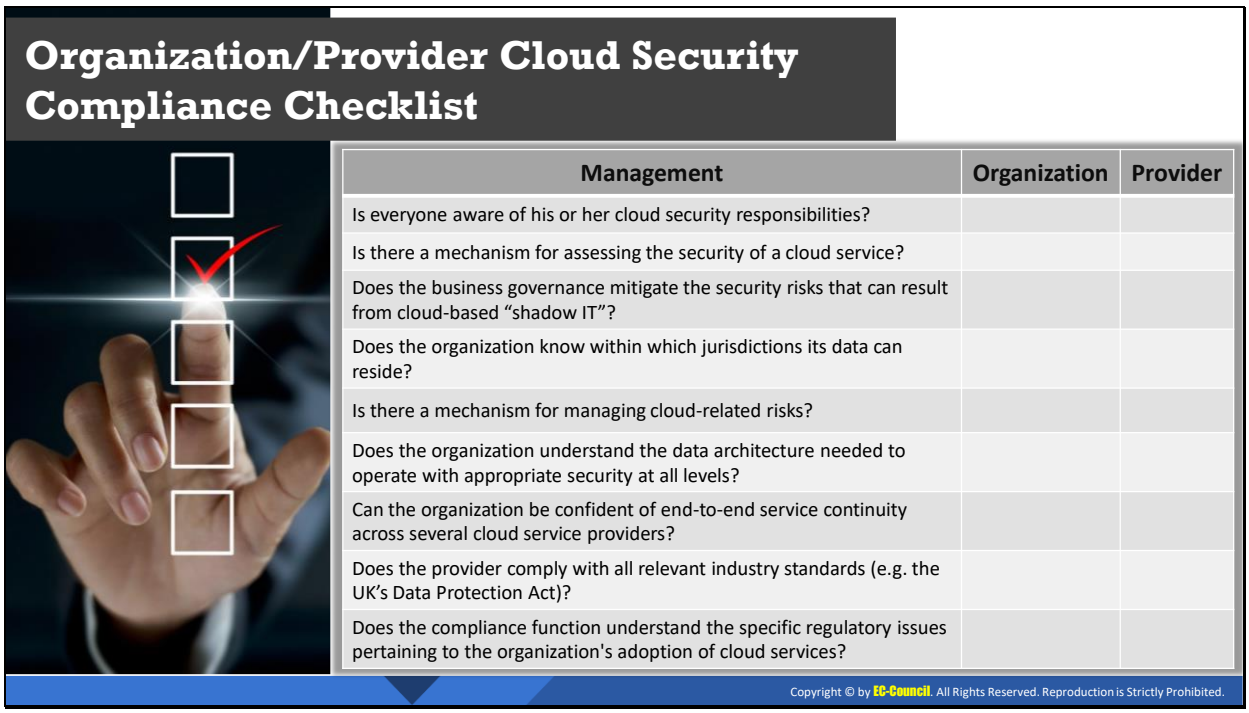
https://t.me/learningnets



NIST Recommendations for Cloud Security

- Assess the risk posed to the client's data, software, and infrastructure.
- Select an appropriate deployment model according to needs.
- Ensure audit procedures are in place for data protection and software isolation.
- Renew SLAs in case of security gaps between the organization's security requirements and cloud provider's standards.
- Establish appropriate incident detection and reporting mechanisms.
- Analyze the security objectives of the organization.
- Enquire about who is responsible for data privacy and security issues in the cloud.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Organization/Provider Cloud Security Compliance Checklist

The below tables provide checklists for determining whether the security team, the rest of the organization, and any proposed cloud provider can assure cloud security.

Checklists to determine if the CSP is fit and ready for cloud security:

	Security Team
Are the members of the security team formally trained in cloud technologies?	❑
Do the organization's security policies consider cloud infrastructure?	❑
Has the security team ever been involved in implementing cloud infrastructure?	❑
Has an organization defined security assessment procedures for cloud infrastructure?	❑
Has an organization ever been audited for cloud security threats?	❑
Will the organization's cloud adoption comply with the security standards that the organization follows?	❑
Has security governance been adapted to include cloud?	❑
Does the team have adequate resources to implement cloud infrastructure and security?	❑

Table 6.3: Checklist to determine if the security team is fit and ready for cloud security

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Operation	Organization	Provider
Are regulatory compliance reports, audit reports, and reporting information available from the provider?	❑	❑
Are the organization's incident handling and business continuity policies and procedures designed considering cloud security issues?	❑	❑
Are the cloud service provider's compliance and audit reports accessible to the organization?	❑	❑
Does the CSP's SLA address incident handling and business continuity concerns?	❑	❑
Does the CSP has clear policies and procedures to handle digital evidence in the cloud infrastructure?	❑	❑
Is the CSP itself compliant with the industry standards?	❑	❑
Does the CSP have skilled and sufficient staff for incident resolution and configuration management?	❑	❑
Has the CSP defined procedures to support the organization in case of incidents in a multi-tenant environment?	❑	❑
Does using a cloud provider give the organization an environmental advantage?	❑	❑
Does the organization know in which application or database each data entity is stored or mastered?	❑	❑
Is the cloud-based application maintained and disaster-tolerant (i.e., would it recover from an internal or external disaster)?	❑	❑
Are all personnel appropriately vetted, monitored, and supervised?	❑	❑
Does the CSP provide the flexibility of service relocation and switchovers?	❑	❑
Has the CSP implemented perimeter security controls (e.g., IDS, firewalls) and does it provide regular activity logs to the organization?	❑	❑
Does the CSP provide reasonable assurance of quality or availability of service?	❑	❑
Is it easy to securely integrate the cloud-based applications at runtime and contract termination?	❑	❑
Does the CSP provide 24/7 support for cloud operations and security-related issues?	❑	❑
Do the procurement processes contain cloud security requirements?	❑	❑
Does the CSP frequently perform vulnerability assessments to identify security gaps and apply necessary patches?	❑	❑

Table 6.4: Checklist to determine if the organization/provider is fit and ready for cloud security based on its operations

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

Technology	Organization	Provider
Are there appropriate access controls (e.g., federated single sign-on) that give users controlled access to cloud applications?	❑	❑
Is data separation maintained between the organization and customer information at runtime and during backup (including data disposal)?	❑	❑
Has the organization considered and addressed backup, recovery, archiving, and decommissioning of data stored in the cloud environment?	❑	❑
Are mechanisms in place for authentication, authorization, and key management in the cloud environment?	❑	❑
Are mechanisms in place to manage network congestion, misconnection, misconfiguration, lack of resource isolation, etc., which affect services and security?	❑	❑
Has the organization implemented sufficient security controls on the client devices used to access the cloud?	❑	❑
Are all cloud-based systems, infrastructure, and physical locations suitably protected?	❑	❑
Are the network designs suitably secure for the organization's cloud adoption strategy?	❑	❑

Table 6.5: Checklist to determine if the organization/provider is fit and ready for cloud security based on its technology

Management	Organization	Provider
Is everyone aware of their cloud security responsibilities?	❑	❑
Is there a mechanism for assessing the security of a cloud service?	❑	❑
Does the business governance mitigate the security risks that can result from cloud-based "shadow IT"?	❑	❑
Does the organization know within which jurisdictions its data can reside?	❑	❑
Is there a mechanism for managing cloud-related risks?	❑	❑
Does the organization understand the data architecture needed to operate with appropriate security at all levels?	❑	❑
Can the organization be confident of end-to-end service continuity across several cloud service providers?	❑	❑
Does the provider comply with all relevant industry standards (e.g., the UK's Data Protection Act)?	❑	❑
Does the compliance function understand the specific regulatory issues pertaining to the organization's adoption of cloud services?	❑	❑

Table 6.6: Checklist to determine if the organization/provider is fit and ready for cloud security based on its management

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

Cloud Security Tools

Some tools for securing cloud environment include the following:

- **Qualys Cloud Platform**

  Source: *https://www.qualys.com*

  Qualys Cloud Platform is an end-to-end IT security solution that provides a continuous, always-on assessment of the global security and compliance posture, with visibility across all IT assets irrespective of where they reside. It includes sensors that provide continuous visibility, and all cloud data can be analyzed in real-time. It responds to threats immediately, performs active vulnerability in internet control message protocol timestamp request, and visualizes results in one place with AssetView.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

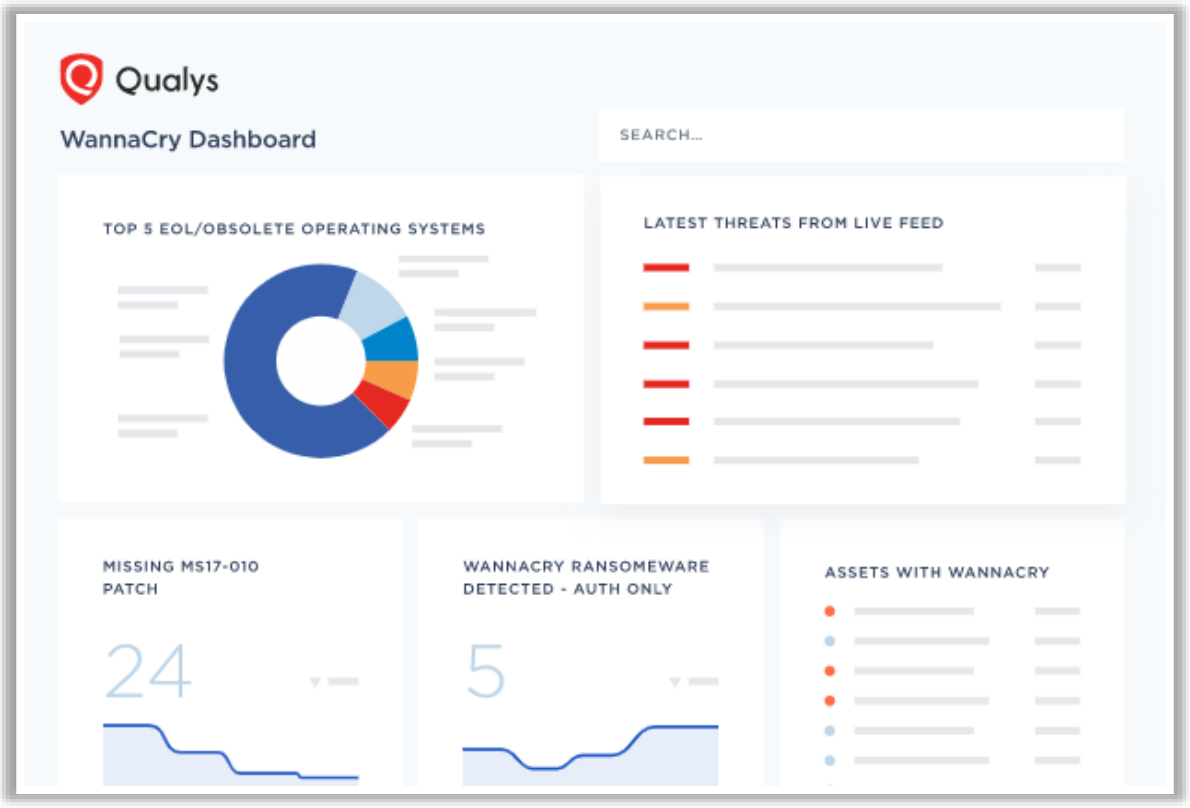


Figure 6.46: Screenshot of Qualys Cloud Platform

Additional cloud security tools include the following:

- CloudPassage Halo (*https://www.cloudpassage.com*)
- McAfee MVISION Cloud (*https://www.mcafee.com*)
- CipherCloud (*https://www.ciphercloud.com*)
- Netskope Security Cloud (*https://www.netskope.com*)
- Prisma Cloud (*https://www.paloaltonetworks.com*)

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Module Summary

This module discussed virtualization, its components, and virtualization enablers. It discussed OS virtualization security and concerns. It also discussed the best practices for OS virtualization security. Furthermore, this module discussed cloud computing and its benefits. It discussed different types of cloud computing services and cloud deployment models. Finally, this module presented a brief discussion on the importance of cloud security and its best practices.

In the next module, we will discuss wireless network security in detail.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

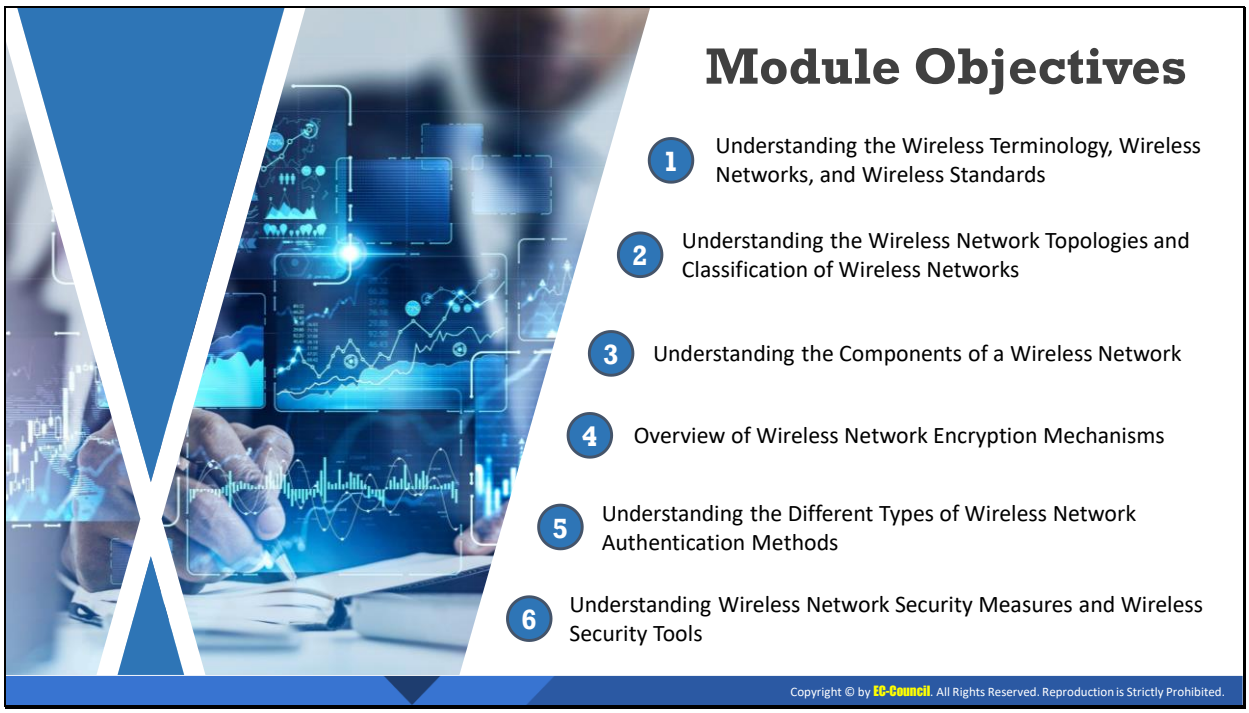
EC-Council

N|DE
Network Defense Essentials

Module 07

Wireless Network Security

https://t.me/learningnets



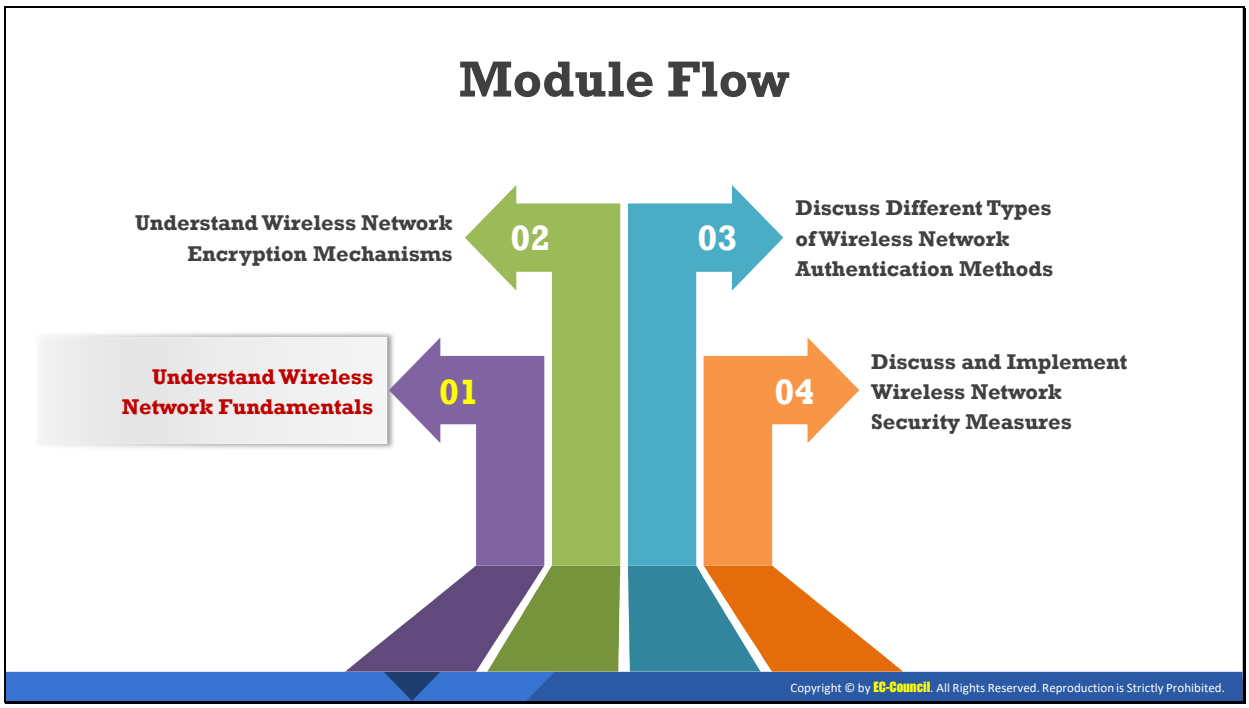
Module Objectives

This module deals with network security for wireless networks in enterprises. Wireless networks are widely used across organizations today and are prone to various attacks. Therefore, organizations need to focus on the planning for securing the wireless network across the organization.

At the end of this module, you will be able to do the following:

- Understand wireless terminology, wireless networks, and wireless standards
- Understand the wireless network topologies and classification of wireless networks
- Understand the components of a wireless network
- Explain the wireless network encryption mechanisms
- Understand the different types of wireless network authentication methods
- Explain wireless network security measures and wireless security tools

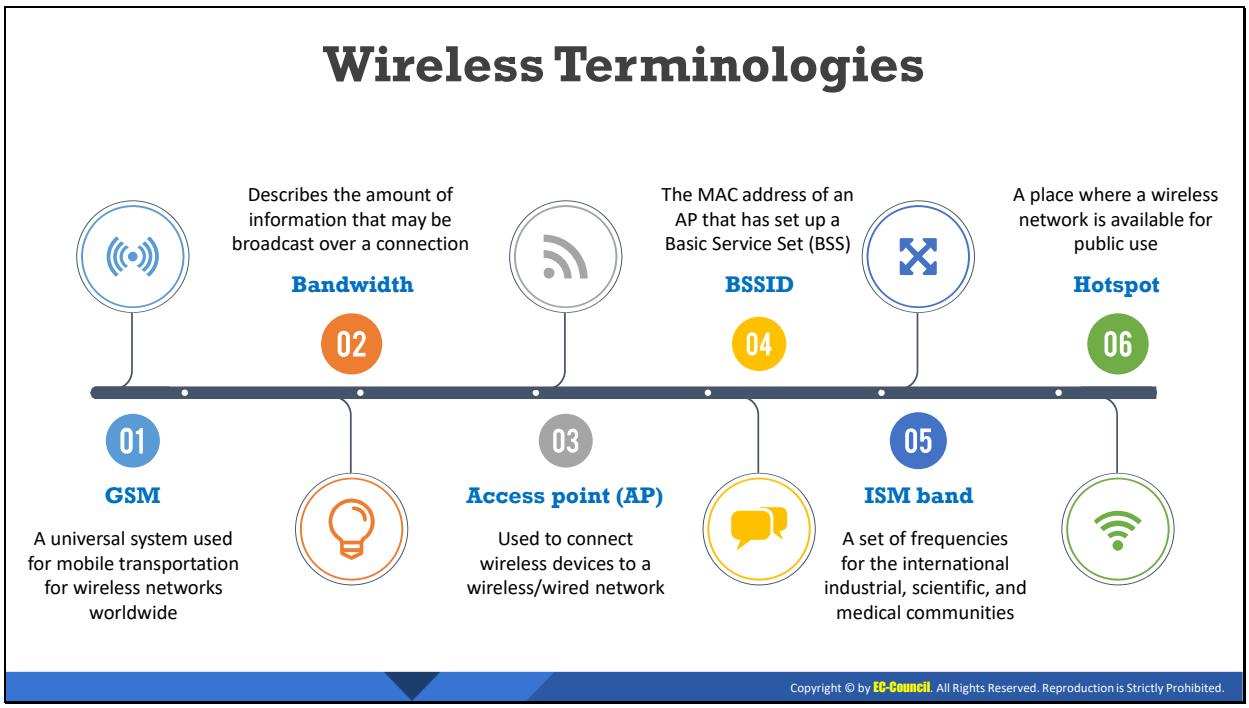
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

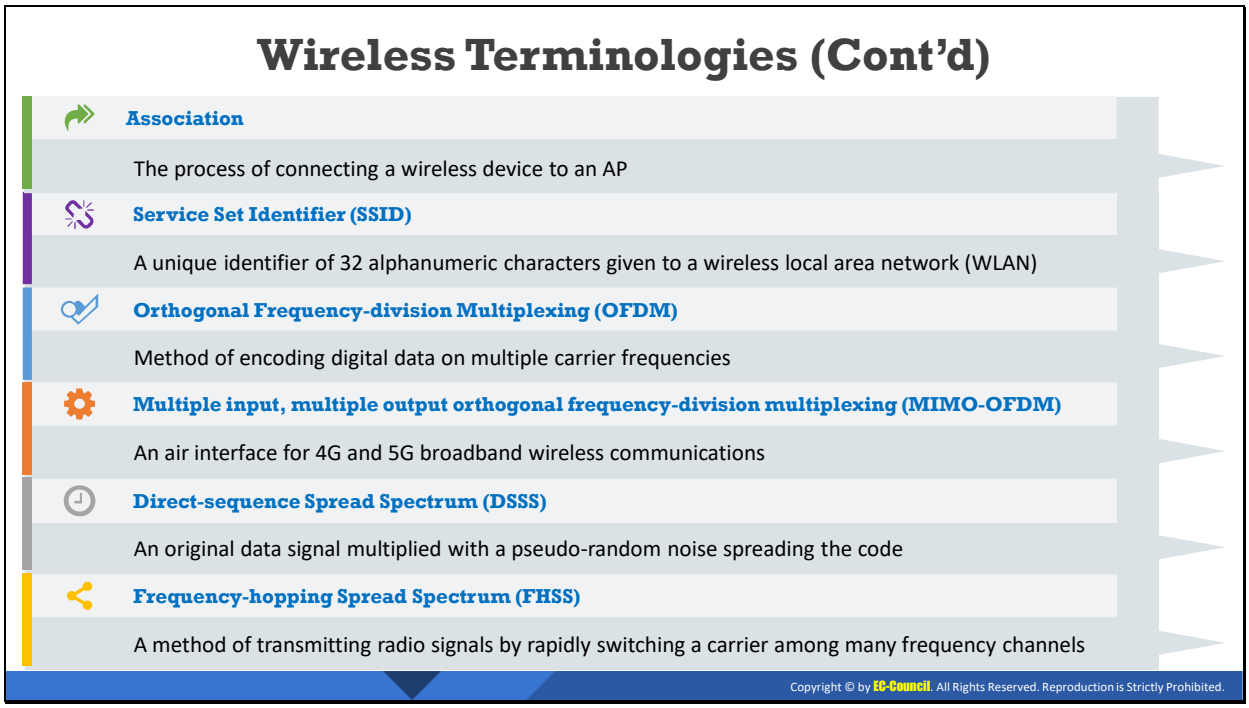


Understand Wireless Network Fundamentals

The objective of this section is to understand the fundamentals of wireless networks which includes the wireless network terminologies, components used in wireless networks, the uses of wireless networks, and their advantages and limitations. This section covers the different types of wireless technologies, wireless network standards, and topologies.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets





Wireless Terminologies

In a wireless network, data are transmitted through EM waves that carry signals over the communication path. Terms associated with wireless networks include the following:

- **Global System for Mobile Communications (GSM)**: It is a universal system used for mobile data transmission in wireless networks worldwide.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

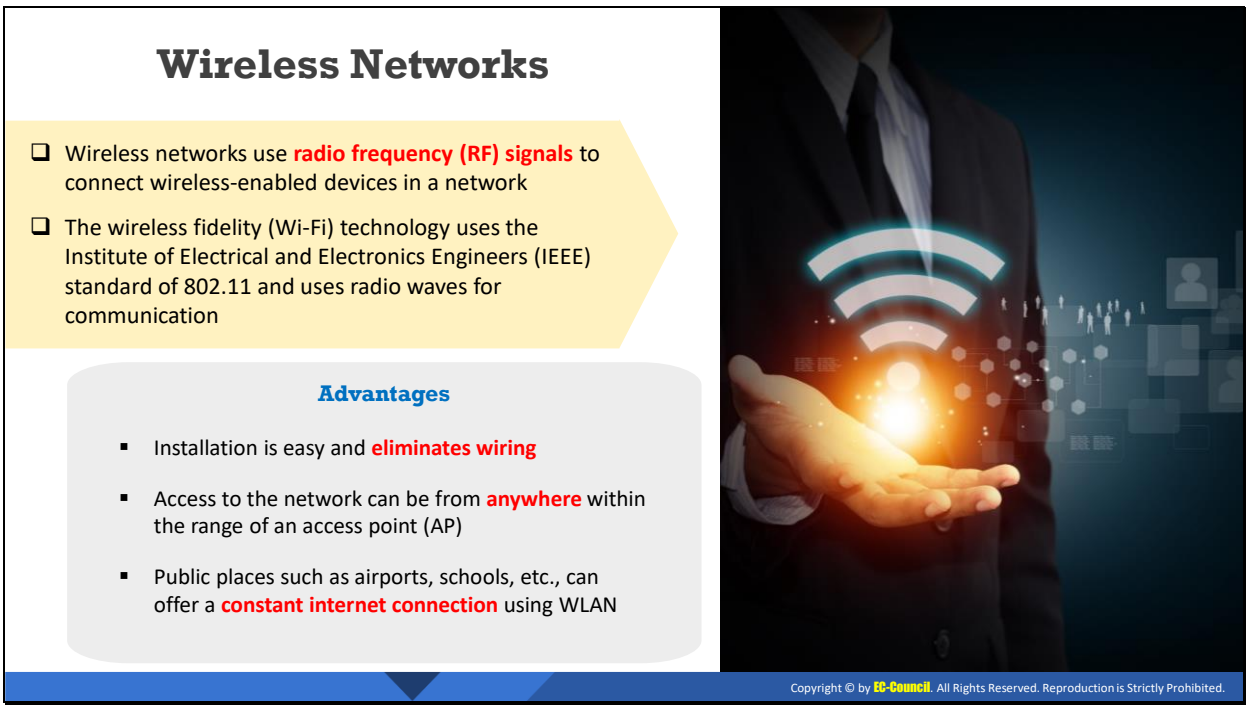
- **Bandwidth**: It describes the amount of information that may be broadcast over a connection. Usually, bandwidth refers to the data transfer rate and is measured in bits (amount of data) per second (bps).
- **Access point (AP)**: An AP is used to connect wireless devices to a wireless/wired network. It allows wireless communication devices to connect to a wireless network through wireless standards such as Bluetooth and Wi-Fi. It serves as a switch or hub between a wired LAN and wireless network.
- **Basic service set identifier (BSSID)**: It is the media access control (MAC) address of an access point (AP) or base station that has set up a basic service set (BSS). Generally, users are unaware of the BSS to which they belong. When a user moves a device, the BSS used by the device could change because of a variation in the range covered by the AP, but this change may not affect the connectivity of the wireless device.
- **Industrial, scientific, and medical (ISM) band**: This band is a set of frequencies used by the international industrial, scientific, and medical communities.
- **Hotspot**: These are places where wireless networks are available for public use. Hotspots refer to areas with Wi-Fi availability, where users can enable Wi-Fi on their devices and connect to the Internet.
- **Association**: It refers to the process of connecting a wireless device to an AP.
- **Service set identifier (SSID)**: An SSID is a 32-alphanumeric-character unique identifier given to a wireless local area network (WLAN) that acts as a wireless identifier of the network. The SSID permits connections to the desired network among available independent networks. Devices connecting to the same WLAN should use the same SSID to establish connections.
- **Orthogonal frequency-division multiplexing (OFDM)**: An OFDM is a method of digital modulation of data in which a signal, at a chosen frequency, is split into multiple carrier frequencies that are orthogonal (occurring at right angles) to each other. OFDM maps information on the changes in the carrier phase, frequency, amplitude, or a combination of these and shares bandwidth with other independent channels. It produces a transmission scheme that supports higher bit rates than parallel channel operation. It is also a method of encoding digital data on multiple carrier frequencies.
- **Multiple input, multiple output-orthogonal frequency-division multiplexing (MIMO-OFDM)**: MIMO-OFDM influences the spectral efficiency of 4G and 5G wireless communication services. Adopting the MIMO-OFDM technique reduces interference and increases the channel robustness.
- **Direct-sequence spread spectrum (DSSS)**: DSSS is a spread spectrum technique that multiplies the original data signal with a pseudo-random noise-spreading code. Also referred to as a data transmission scheme or modulation scheme, the technique protects signals against interference or jamming.
- **Frequency-hopping spread spectrum (FHSS)**: FHSS, also known as frequency-hopping code-division multiple access (FH-CDMA), is a method of transmitting radio signals by

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

rapidly switching a carrier among many frequency channels. It decreases the efficiency of unauthorized interception or jamming of telecommunications. In FHSS, a transmitter hops between available frequencies using a specified algorithm in a pseudorandom sequence known to both the sender and receiver.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Wireless Networks

The computer world is heading towards a new era of technological evolution by using wireless technologies. Wireless networking is revolutionizing the way people work and play. By removing the physical connection or cable, individuals are able to use networks in newer ways that make data portable, mobile, and accessible.

A wireless network environment opens up many new expansions and workflow possibilities. With the availability of a wireless network, there is no need to worry when a user wants to move their PC from one office to the next or when they want to work in a location that does not have an Ethernet port.

Wireless networking is very useful in public places including libraries, coffee shops, hotels, airports, and other establishments that offer WLAN connections.

The most important aspect in wireless networking is an access point through which a user can communicate with another mobile or fixed host. An access point is a device that contains a radio transceiver (that sends and receives signals) along with a registered jack 45 (RJ-45) wired network interface, which allows a user to connect to a standard wired network using a cable.

Advantages of a Wireless Network

- Installation is fast and easy without the need for wiring through walls and ceilings
- Easily provides connectivity in areas where it is difficult to lay cables
- The network can be accessed from anywhere within the range of an AP
- Public spaces such as airports, libraries, schools, and even coffee shops offer constant Internet connections through WLANs

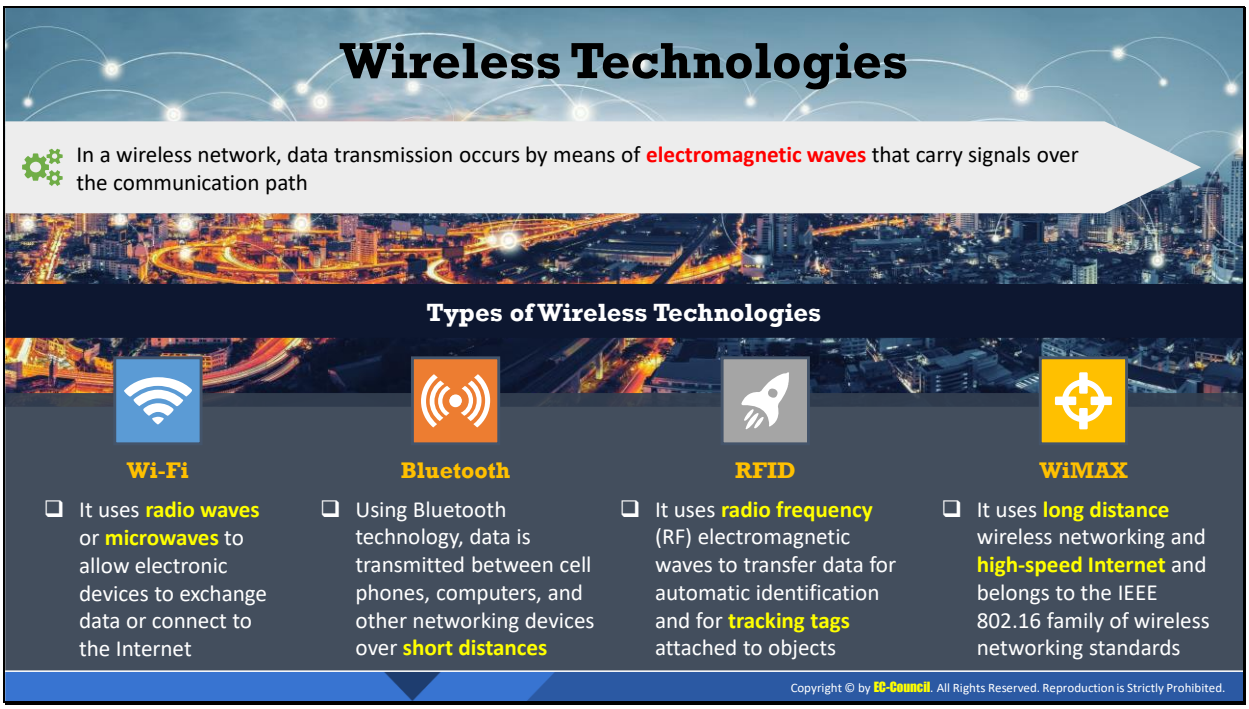
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Disadvantages of a Wireless Network

- Security may not meet expectations
- The bandwidth suffers as the number of devices in the network increases
- Wi-Fi upgrades may require new wireless cards and/or APs
- Some electronic equipment can interfere with Wi-Fi networks

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Wireless Technologies

In a wireless network, data transmission occurs by means of electromagnetic waves that carry signals over the communication path.

Types of Wireless Technologies

- **Wi-Fi**

  Wireless fidelity (Wi-Fi) is a part of the Institute of Electrical and Electronics Engineers (IEEE) 802.11 family of wireless networking standards. This technology uses radio waves or microwaves to allow electronic devices to exchange data or connect to the Internet. Many devices such as personal computers, laptops, digital cameras, smartphones, etc., support Wi-Fi technology. Wi-Fi operates in the frequency band between 2.4 GHz and 5 GHz. A Wi-Fi network uses radio waves to transmit the signals across the network. For this purpose, a computer should have a wireless adapter to translate the data into radio signals and pass them through an antenna and router. This is where the message is decoded, and the data is sent to the internet or through another network. Hotspots are areas that have Wi-Fi availability, where users can enable Wi-Fi on their devices and connect to the internet through a hotspot.

- **Bluetooth**

  In the Bluetooth technology, data is transmitted between cell phones, computers, and other networking devices over short distances. Signals transmitted via Bluetooth cover short distances of up to 10 m as compared to other modes of wireless communication. Bluetooth transfers the data at a speed of less than 1 Mbps and operates in the frequency range of 2.4 GHz. This technology comes under IEEE 802.15 and uses a radio technology called FHSS for transferring data to other Bluetooth-enabled devices.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **RFID**

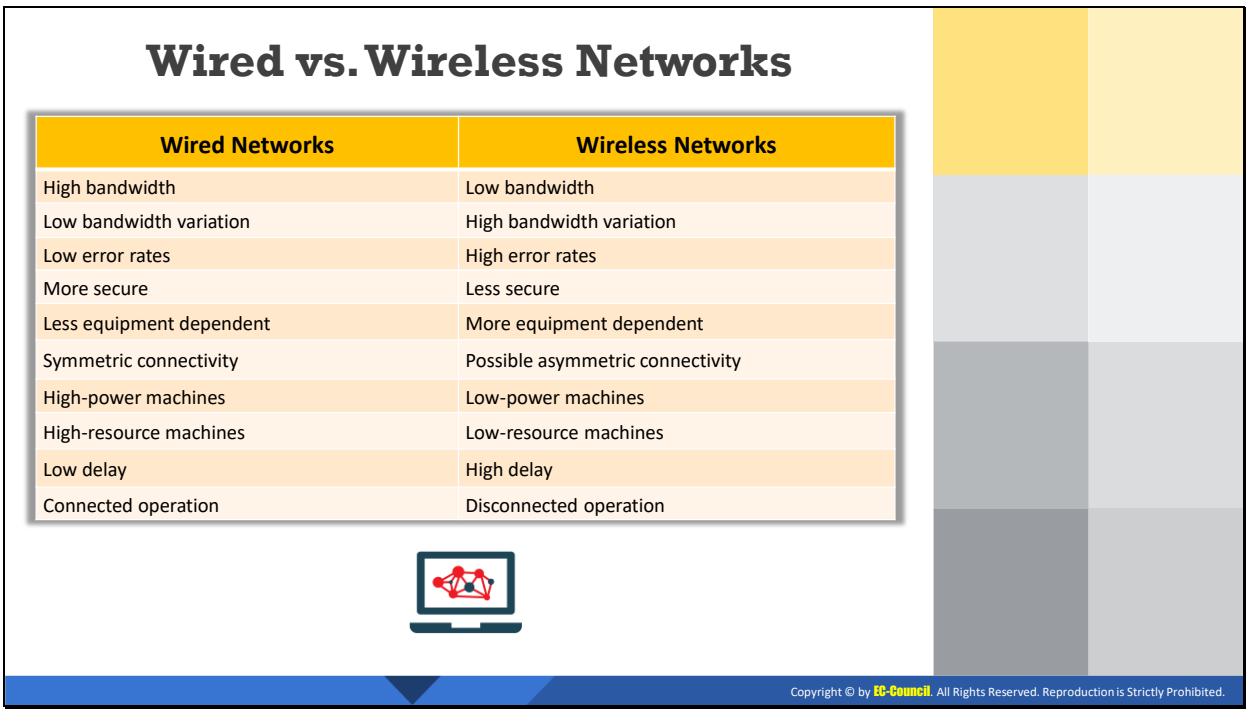
  The radio-frequency identification (RFID) technology uses radio frequency (RF) electromagnetic waves to transfer data for automatic identification and for tracking tags attached to objects. RFID devices work within a small range of up to 20 ft.

- **WiMAX**

  The worldwide interoperability for microwave access (WiMAX) technology uses long distance wireless networking and high-speed Internet. It belongs to the IEEE 802.16 family of wireless networking standards. WiMAX signals can function over a distance of several miles with data rates reaching up to 75 Mbps. It uses a fixed wireless application and mobile stations to provide high-speed data, voice, video calls, and internet connectivity to users. The WiMAX forum developed WiMAX and states that nearly 135 countries have deployed over 455 WiMAX networks.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Wired vs. Wireless Networks

The differences between a wired and a wireless network are as follows:

Wired Networks	Wireless Networks
High bandwidth	Low bandwidth
Low bandwidth variation	High bandwidth variation
Low error rates	High error rates
More secure	Less secure
Less equipment dependent	More equipment dependent
Symmetric connectivity	Possible asymmetric connectivity
High-power machines	Low-power machines
High-resource machines	Low-resource machines
Low delay	High delay
Connected operation	Disconnected operation

Table 7.1: Differences Between a Wired and a Wireless Network

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Wireless Standards

Protocol	Frequency (GHz)	Bandwidth (MHz)	Stream data rate (Mbits/s)	Modulation	Range (m)	
					Indoor	Outdoor
802.11 (Wi-Fi)	2.4	22	1, 2	DSSS, FHSS	20	100
802.11a	5	20	6, 9, 12, 18, 24, 36, 48, 54	OFDM	35	120
	3.7				—	5000
802.11b	2.4	22	1, 2, 5.5, 11	DSSS	35	140
802.11d	It is an enhanced version of 802.11a and 802.11b that enables global portability by allowing variation in frequencies, power levels, and bandwidth					
802.11e	It provides guidance for prioritization of data, voice, and video transmissions by enabling quality of service (QoS)					
802.11g	2.4	20	6, 9, 12, 18, 24, 36, 48, 54	OFDM		

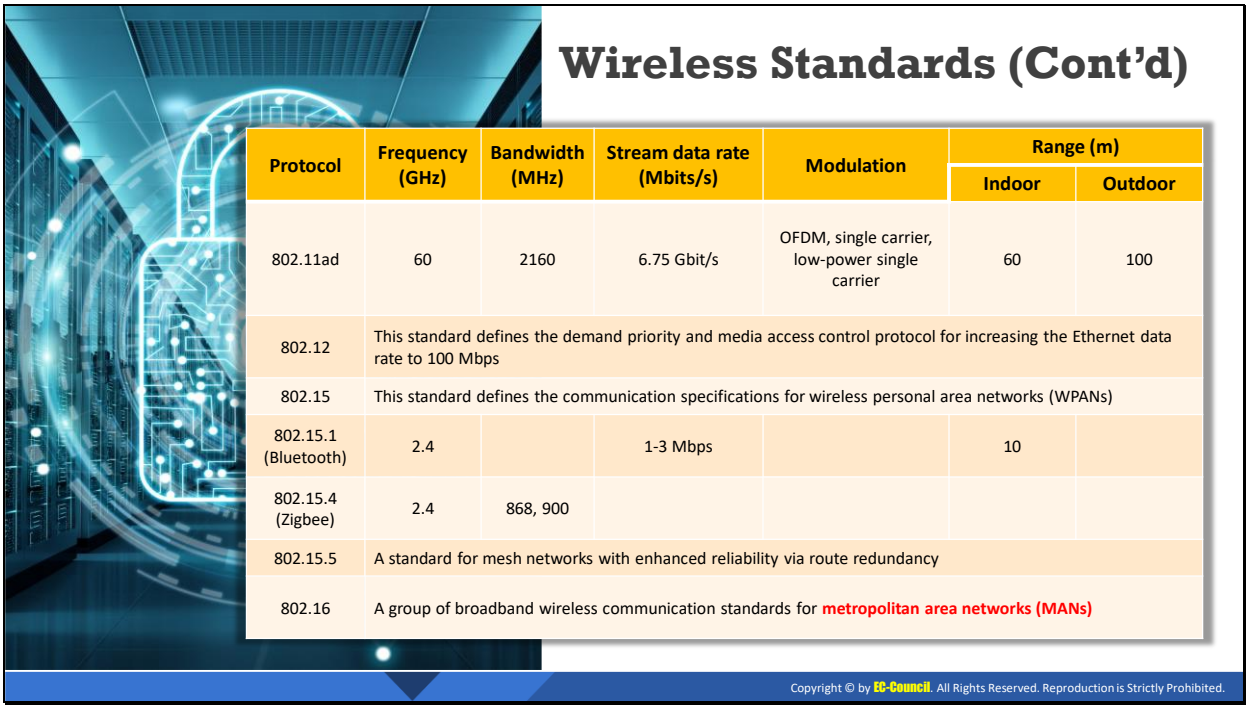
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Wireless Standards (Cont'd)

Protocol	Frequency (GHz)	Bandwidth (MHz)	Stream data rate (Mbits/s)	Modulation	Range (m)	
					Indoor	Outdoor
802.11i	This is a standard for WLANs that provides **improved encryption** for networks that use the 802.11a, 802.11b, and 802.11g standards					
802.11n	5	20	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2	MIMO-OFDM	70	150
	2.4	40	15, 30, 45, 60, 90, 120, 135, 150		70	150
802.11ac	5	20	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 86.7, 96.3	MIMO-OFDM	35	
		40	15, 30, 45, 60, 90, 120, 135, 150, 180, 200		35	
		80	32.5, 65, 97.5, 130, 195, 260, 292.5, 325, 390, 433.3		35	
		160	65, 130, 195, 260, 390, 520, 585, 650, 780, 866.7		35	
802.11ax	2.4/5/6	40	Up to 2294[F1]	MIMO-OFDM	30	120
		80	Up to 4803[F]			
		80+80	Up to 10530			

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Wireless Standards

The IEEE standards correspond to the various wireless networking transmission methods. They are as follows:

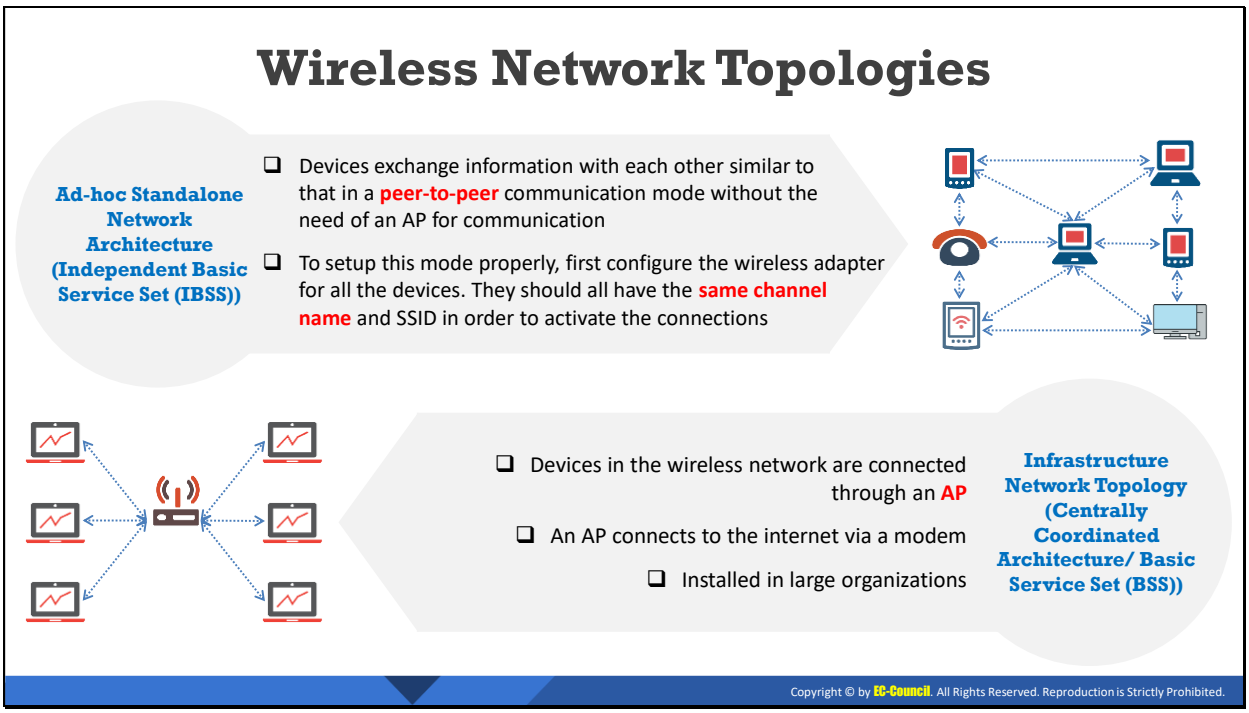
- **802.11 (Wi-Fi):** This standard corresponds to WLANs and uses FHSS or DSSS as the frequency hopping spectrum. It allows an electronic device to connect to the internet using a wireless connection that is established in any network.
- **802.11a:** This standard is the second extension to the original 802.11 standard. It operates in the 5 GHz frequency band and supports a bandwidth of up to 54 Mbps by using OFDM. It has a fast maximum speed but is more sensitive to walls and other obstacles.
- **802.11b:** IEEE expanded the 802.11 standard by creating the 802.11b specifications in 1999. This standard operates in the 2.4 GHz industrial, scientific, and medical (ISM) radio band and supports a bandwidth of up to 11 Mbps by using DSSS modulation.
- **802.11d:** This standard is an enhanced version of the 802.11a and 802.11b standards. It supports the regulatory domains. The particulars of this standard can be set at the media access control (MAC) layer.
- **802.11e:** This standard defines the quality of service (QoS) for wireless applications. The enhanced service is modified using the MAC layer. This standard maintains the quality of video and audio streaming, real-time online applications, voice over internet protocol (VoIP), etc.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **802.11g:** This standard is an extension of the 802.11 standard. It supports a maximum bandwidth of 54 Mbps using the OFDM technology and uses the same 2.4 GHz band as 802.11b. It is compatible with the 802.11b standard, which implies that 802.11b devices can work directly with an 802.11g access point.
- **802.11i:** This standard is used as a standard for WLANs and provides improved encryption for networks. 802.11i requires new protocols such as TKIP and advanced encryption standard (AES).
- **802.11n:** This standard was developed in 2009. It aims to improve the 802.11g standard in terms of the bandwidth. It operates on both the 2.4 and 5 GHz bands and supports a maximum data rate up to 300 Mbps. It uses multiple transmitters and receiver antennas (MIMO) to allow a maximum data rate along with security improvements.
- **802.11ac:** This standard provides a high throughput network at the frequency of 5 GHz. It is faster and more reliable than the 802.11n standard. It involves gigabit networking which provides an instantaneous data transfer experience.
- **802.11ax:** 802.11ax also known as Wi-Fi 6. It is the sixth generation of the Wi-Fi standard. It is designed to operate in all ISM bands between 1 and 6 GHz.
- **802.11ad:** 802.11ad involves the inclusion of a new physical layer for 802.11 networks. This standard works on the 60 GHz spectrum. The data propagation speed in this standard is significantly different from the bands operating at 2.4 GHz and 5 GHz. With a very high frequency spectrum, the transfer speed is much higher than that of 802.11n.
- **802.12:** This standard dominates media utilization by working on the demand priority protocol. Based on this standard, the ethernet speed increases to 100 Mbps. It is compatible with the 802.3 and 802.5 standards. Users currently on these standards can directly upgrade to the 802.12 standard.
- **802.15:** This defines the standards for a wireless personal area network (WPAN). It describes the specification for wireless connectivity with fixed or portable devices.
- **802.15.1 (Bluetooth):** Bluetooth is mainly used for exchanging data between fixed and mobile devices over short distances.
- **802.15.4 (Zigbee):** The 802.15.4 standard has a low data rate and complexity. Zigbee is the specification used in the 802.15.4 standard. It transmits long distance data through a mesh network. This specification handles applications operating at a low data rate, but longer battery life. Its data rate is 250 kbits/s.
- **802.15.5:** This standard deploys itself on a full mesh or a half mesh topology. It includes network initialization, addressing, and unicasting.
- **IEEE 802.16:** This standard is also known as WiMAX and is a specification for fixed broadband wireless metropolitan access networks (MANs) that use a point-to-multipoint architecture.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Wireless Network Topologies

In order to plan and install a wireless network, it is necessary to determine the type of architecture that would be suitable for the network environment.

There are two types of wireless topologies:

- **Ad-hoc Standalone Network Architecture (Independent Basic Service Set (IBSS))**

  The ad-hoc mode is also called as the independent basic service set (IBSS) mode. Devices connected over a wireless network communicate with each other directly, similar to that in the peer-to-peer communication mode. The ad-hoc mode does not implement a wireless access point (WAP)/access point (AP) for communication between devices. The wireless adaptors on each device are configured on the ad-hoc mode rather than on the infrastructure mode. Adaptors for all the devices must use the same channel name and SSID in order to establish the network connections successfully.

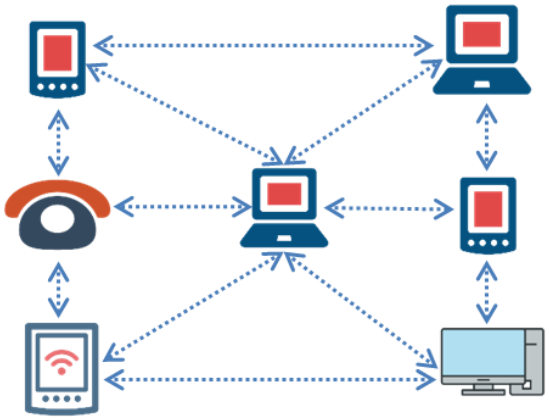


Figure 7.1: Standalone Architecture

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

The ad-hoc mode works effectively for a small group of devices and it is necessary to connect all the devices with each other in close proximity. The network performance degrades as the number of devices increases. It becomes cumbersome for a network administrator to manage the network in this mode, because devices connect and disconnect regularly. It is not possible to bridge this mode with a traditional wired network and it does not allow internet access until a special gateway is present.

The ad-hoc mode works better in a small area and does not require any access points (such as a router or a switch), thus minimizing the cost. This mode acts as a backup option and appears when there is a problem or a malfunction in the APs or a centrally coordinated network (infrastructure mode). This mode uses the functionality of each adaptor to enable security authentication and to use wireless services.

The key characteristics of an ad-hoc wireless network are as follows:

- The AP encrypts and decrypts text messages.
- Each AP operates independently and has its own respective configuration files.
- The network configuration remains constant with changes in the network conditions.

- **Infrastructure Network Topology (Centrally Coordinated Architecture/ Basic Service Set (BSS))**

A centrally coordinated architecture (infrastructure mode) or a basic service set (BSS) mode is an architecture where all wireless devices connect to each other through an AP. This AP (router or switch) receives Internet access by connecting to a broadband modem. This mode will work effectively when deployed in large organizations. It simplifies the network management and helps address the operational issues. It assures resiliency while allowing a number of systems to connect across the network.

This mode provides enhanced security options, scalability, stability, and easy management. The downside is that it is expensive since an AP (router or switch) is required to connect the devices to each other.

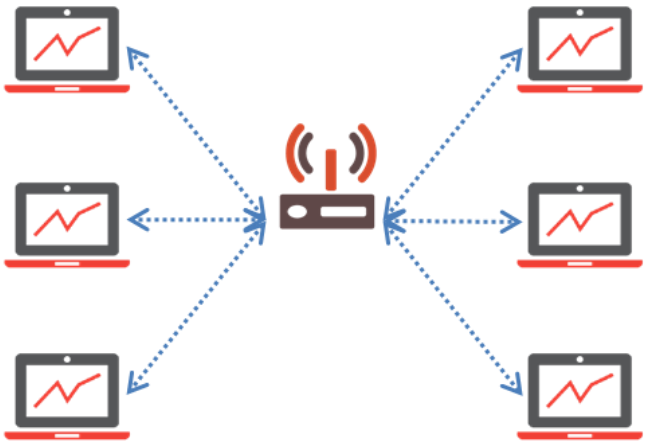


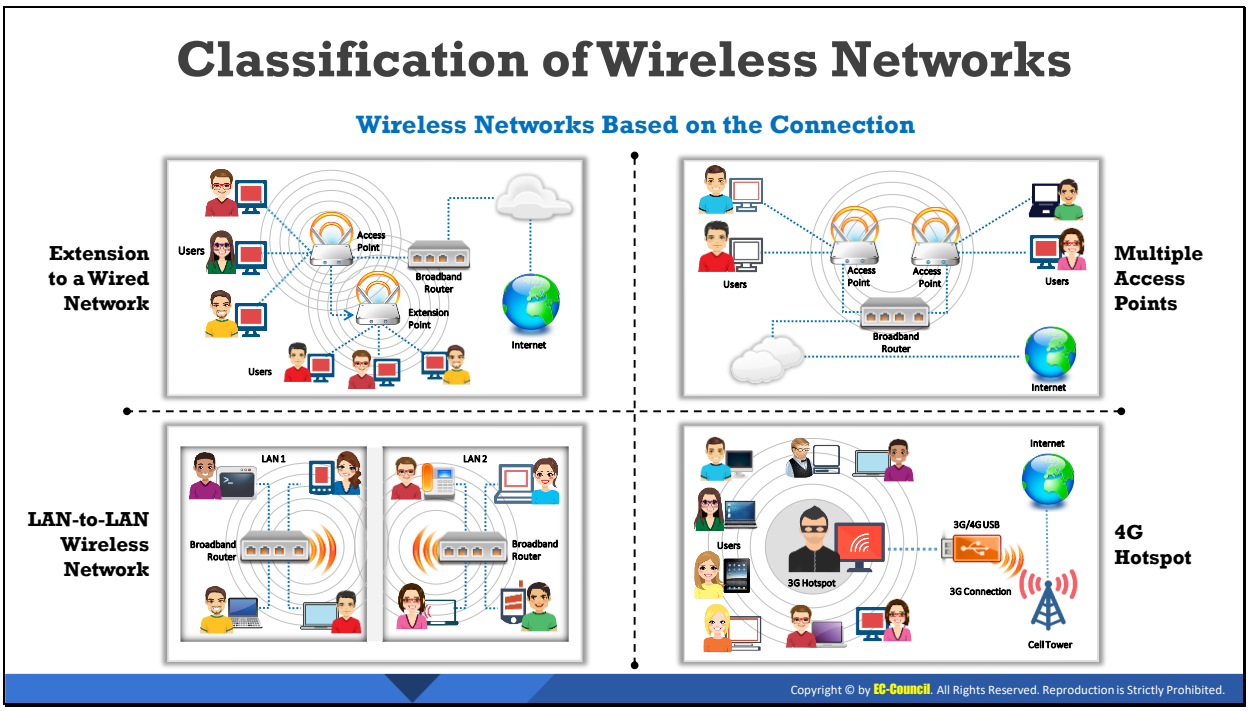
Figure 7.2: Centrally Coordinated Architecture

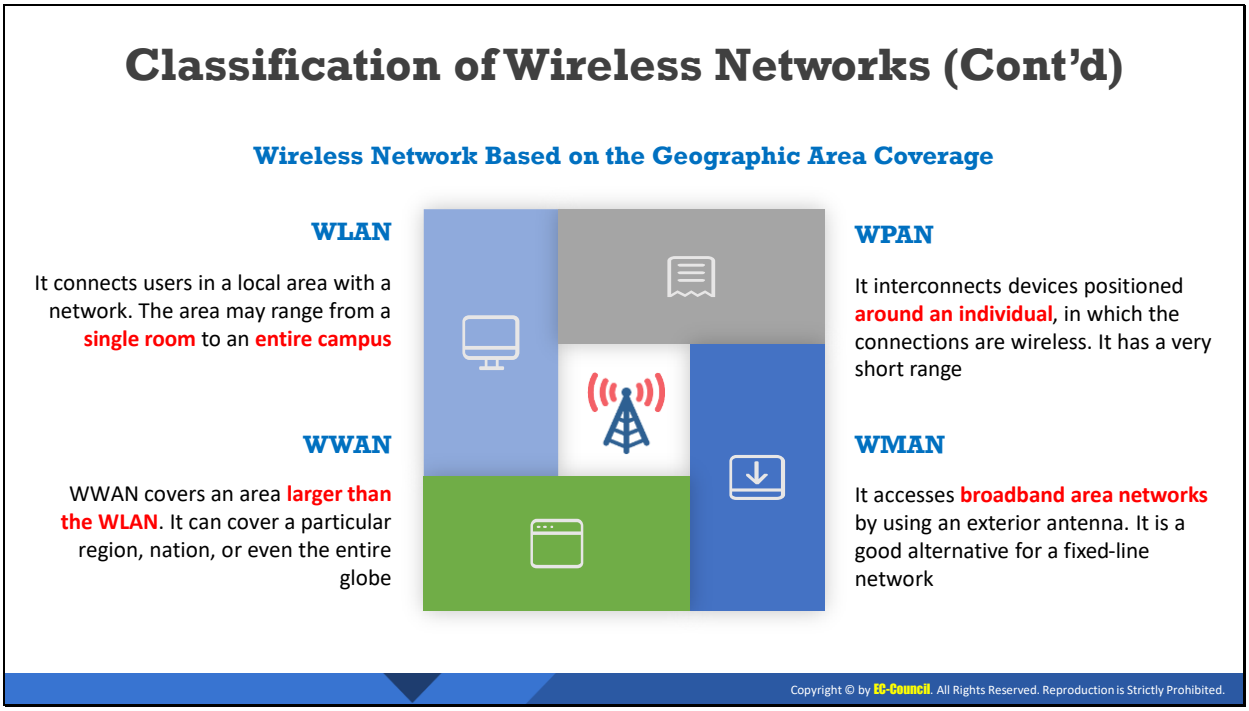
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

The following are the key characteristics of the infrastructure mode:

- It increases or decreases the range of the wireless network by adding and removing the APs.
- The controller reconfigures the network according to the changes in the RF footprint.
- The controller regularly monitors and controls the activities on the wireless network by reconfiguring the AP elements to maintain and protect the network.
- The wireless centralized controller manages all the AP tasks.
- The wireless network controller performs various crucial tasks such as user authentication, policy creation and enforcement, fault tolerances, network expansion, configuration control, etc.
- It maintains backups of other APs in a different location, and these are used when a particular AP malfunctions.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets





Classification of Wireless Networks

Wireless networks are classified on the basis of the connection used and the geographical area.

Wireless Networks Based on the Connection

- **Extension to a Wired Network**

  Extension to a wired network can be obtained by placing APs between a wired network and wireless devices.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

In this network, the AP acts as a hub that provides connectivity for wireless computers. It can also connect a wireless LAN to a wired LAN, which allows the wireless computers the access to LAN resources such as file servers or existing internet connectivity.

The two types of APs used in this type of wireless network are:

- **Software APs** that can be connected to a wired network and which run on a computer with a wireless network interface card.
- **Hardware APs (HAPs)** which provide a comprehensive support of most of the wireless features. With a suitable networking software support, users on the wireless LAN can share files and printers situated on the wired LAN and vice versa.

The network may be extended further in accordance with the size of the location and interference from other devices. This enables a wired/wireless connection across the location for multiple users.

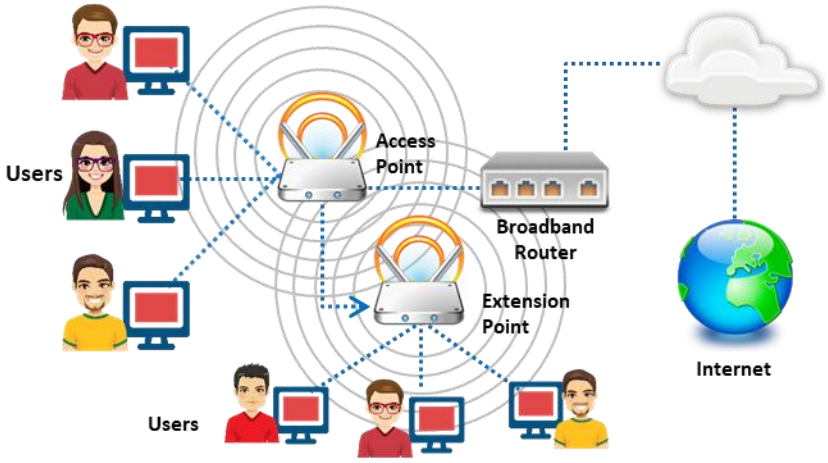


Figure 7.3: Extension to a wired network

- **Multiple Access Points (APs)**

Wireless computers connect using multiple APs. If a single large area is not covered by a single AP, multiple APs or extension points are used. Extension points are not defined in the wireless standard. When using multiple APs, each AP must cover its neighbors. This allows the users to move around seamlessly using a feature called roaming. Some manufacturers develop extension points which act as wireless relays, and thus extend the range of a single AP. Multiple extension points can be strung together to provide wireless access to distant locations from the central AP.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

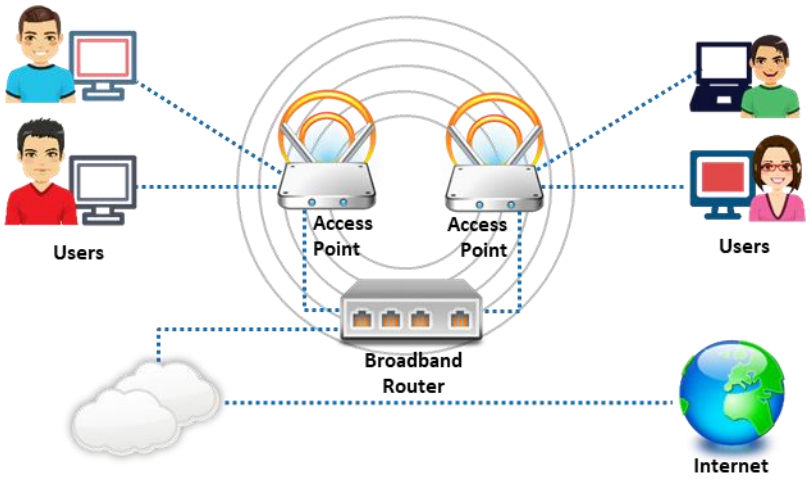


Figure 7.4: Multiple access points

- **LAN-to-LAN Wireless Network**

  APs provide wireless connectivity to local computers and computers on a different network. All HAPs have the capability of directly connecting to other HAPs. Building interconnecting LANs by using wireless connections is large and complex. Several LAN-enabled PCs can be connected to an AP for wireless communication.

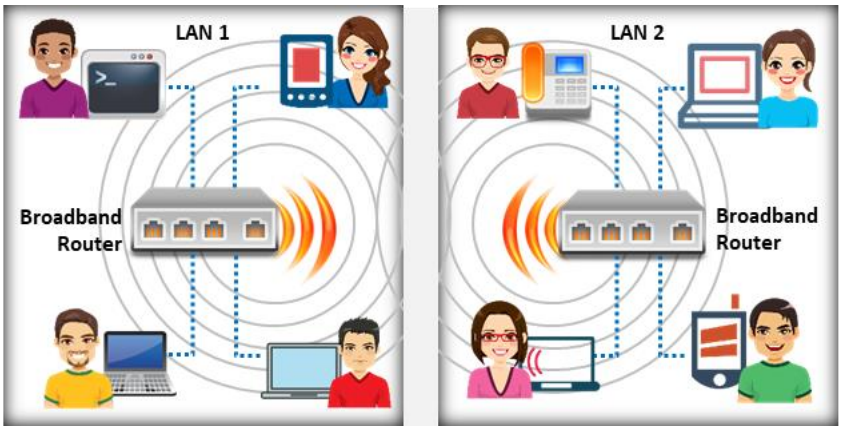


Figure 7.5: LAN-to-LAN wireless network

- **4G Hotspot**

  A hotspot provides internet access over a WLAN with the help of a router connected to the internet service provider (ISP). Multiple devices can be connected at the same time using a Wi-Fi network adapter. Hotspots use the service from cellular providers for 4G internet access. Computers generally scan for hotspots thereby identifying the SSID (network name) of the wireless network.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

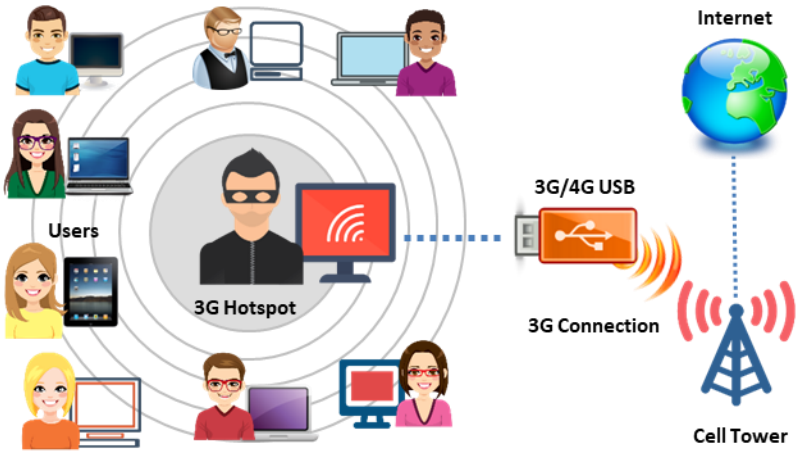


Figure 7.6: 4G hotspot

Wireless Network Based on the Geographic Area Coverage

Wireless networks are classified into WLAN, wireless wide-area network (WWAN), wireless personal area network (WPAN), and wireless metropolitan-area network (WMAN) based on the area they cover geographically.

- **WLAN**
  - A WLAN connects users in a local area with a network. The area may range from a single room to an entire campus.
  - It connects wireless users and the wired network.
  - It uses high-frequency radio waves.
  - WLAN is also known as a LAWN.
  - In 1990, IEEE created a group to develop a standard for wireless equipment.
  - In the peer-to-peer mode, wireless devices within each other's range communicate directly with each other without using a central AP.
  - In the infrastructure mode, the access point is wired to the internet with the wireless users. An access point functions as a mediator between the wired and wireless networks.

  Advantages:
  - WLAN is flexible to install.
  - Wireless networks are easy to set up and use.
  - Wireless networks are robust. If one base station is down, users can physically move their PCs in the range of another base station.
  - It has a better chance of surviving in case of a disaster.

  Disadvantage:
  - Data transfer speeds are normally slower than wired network.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **WWAN**
  - WWAN covers an area larger than the WLAN.
  - It handles cellular network technology such as code-division multiple access (CDMA), global system for mobile communications (GSM), general packet radio service (GPRS), and cellular digital packet data (CDPD) for data transmission.
  - This technology can cover a particular region, nation, or even the entire globe.
  - The system has a built-in cellular radio (GSM/CDMA) which helps users to send or receive data.
  - In WWAN, the wireless data consists of fixed microwave links, digital dispatch networks, wireless LANs, data over cellular networks, wireless WANs, satellite links, one-way and two-way paging networks, laser-based communications, diffuse infrared, keyless car entry, the global positioning system, and more.
- **WPAN**
  - WPAN interconnects devices positioned around an individual, in which the connections are wireless.
  - WPAN has a very short range. It can communicate within a range of 10 m. A WPAN interconnects the mobile network devices that people carry with them or have on their desk.
  - The main concept in WPAN technology is plugging in.
  - When any two WPAN devices come within a range of a few meters to the central server, they communicate with each other, similar to a wired network.
  - Another characteristic of a WPAN is the ability to lock out other devices and prevent interference.
  - Every device in a WPAN can connect to any other device in the same WPAN. However, to do so, they should be within the physical range of each another. Bluetooth is the best example of WPAN.
- **WMAN**

  WMAN covers a metropolitan area such as an entire city or a suburb.
  - It accesses broadband area networks by using an exterior antenna.
  - It is a good alternative for a fixed-line network. It is simple to build and is inexpensive.
  - In a WMAN, the subscriber stations communicate with the base station that is connected to a central network or hub.
  - A WMAN uses a wireless infrastructure or optical fiber connections to link the sites.

  A WMAN links between the WLANs. Distributed queue dual bus (DQDB), is the MAN standard for data communications, specified by the IEEE 802.6 standard. On the basis of DQDB, the network can be established over 30 mi with a speed of 34 to 154 Mbits/s.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

Components of a Wireless Network

Access Point (AP)

- It is a **hardware device** that allows wireless communication devices to connect to a wireless network via wireless standards such as Bluetooth, Wi-Fi, etc.

Wireless Cards (NIC)

- Systems connected to the wireless network require a network interface cards (NIC) to establish a standard **Ethernet connection**

Wireless Modem

- It is a device that receives and transmits **network signals** to other units without requiring physical cabling

Wireless Bridge

- It connects multiple LANs at the medium access control (MAC) layer and is separated either logically or physically. It is used for increasing the **coverage area of the wireless network**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Components of a Wireless Network (Cont'd)

Wireless Repeater

- **Retransmits** the existing signal captured from a wireless router or AP to create a new network

Wireless Router

- Performs the **functions of a router** as well as a wireless AP and provides Internet access to various devices

Wireless Gateways

- **Routes data packets** and functions as a wireless AP. An Internet connection can be shared between multiple stations

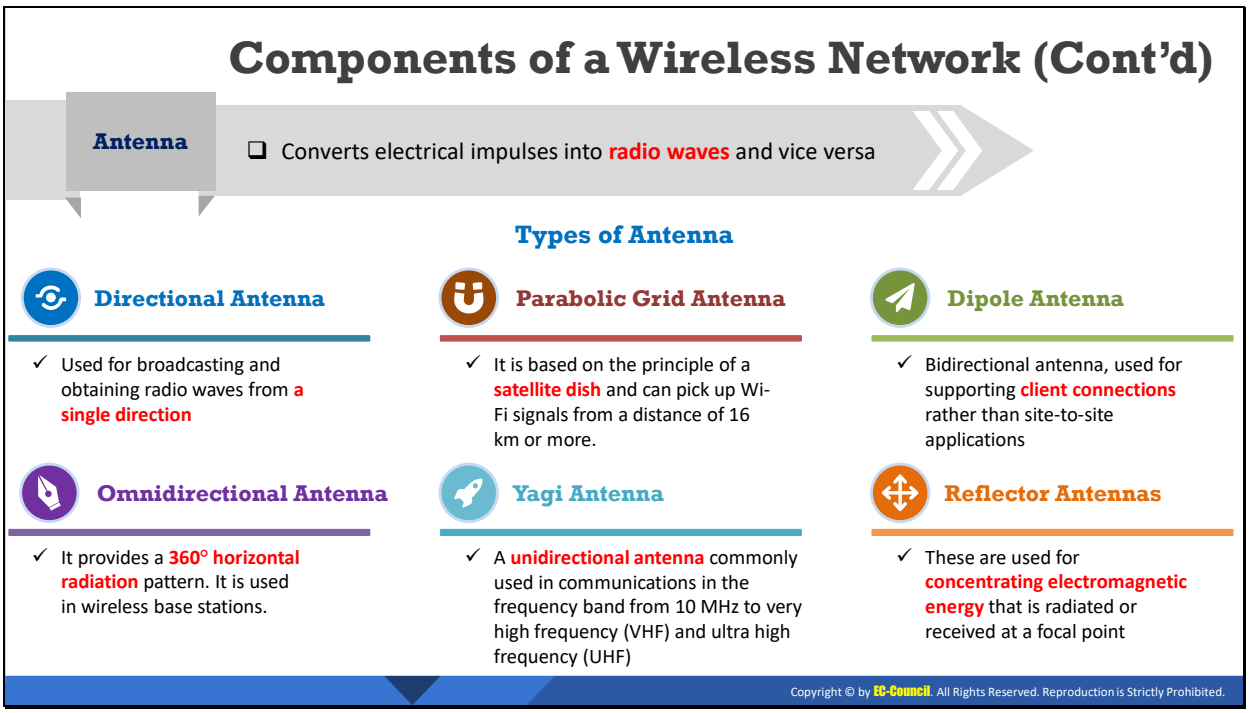
Wireless USB Adapter

- **Connects** different devices to a wireless network in order to access the Internet without a computer, router, or any other network device

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Components of a Wireless Network

The key components of a wireless network are as follows:

- **Access point:** An access point (AP) is a hardware device that uses the wireless infrastructure network mode to connect wireless components to a wired network for transmitting data. It serves as a switch or hub between a wired LAN and a wireless network. It has a built-in transmitter, receiver, and an antenna. The additional ports in the WAP help in expanding the network range and provide access to additional clients. The number of APs depends on the network size. However, multiple APs provide access to a larger number of wireless clients and, in turn, expand the range of the wireless network. The transmission range and distance that a client has to be from a wireless AP is a maximum default value; APs transmit usable signals well beyond the default range. The distance to which a wireless AP signal is transmitted depends on the wireless standards, obstructions, and environmental conditions between the clients and the APs.

  The transmission range and number of devices that a WAP can connect depends on the wireless standard used and the signal interference between the devices. In the wireless infrastructure network design, multiple APs can be used to cover an extensive area, or a single AP can be used for covering a small geographical area such as buildings, homes, etc.

- **Wireless network cards (NIC):** Wireless network cards or wireless network adapters (wireless network interface cards (NICs)) are cards that locate and communicate to an AP with a powerful signal, giving network access to the users. It is required on each device to connect to the wireless network. Laptops or desktop computers generally have built-in wireless NICs or have slots to attach them. These include two types of plug-in cards. One is called a personal computer memory card international association

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

(PCMCIA) card and the other is a peripheral component interconnect (PCI). Laptops have slots to insert the PCMCIA plug-in cards, whereas desktop computers have internal slots to add PCI cards. The functionality of a wired and a wireless network card is similar. The difference between the two cards is that a wired network card has a port to connect over a network, whereas a wireless network card has a built-in antenna to connect over a wireless network. Typically, computers having a PCI bus or USB ports can connect to the wireless NIC.

Data transmitted using an NIC provides the following features:

- Customization of the computer's internal data from parallel to series before transmission
- Division of data into small blocks which incorporates sending and receiving addresses
- It informs when to send the packets to the destination.
- It delivers the packet.

- **Wireless modem:** A wireless modem is a device that allows PCs to connect to a wireless network and access the Internet connection directly with the help of an ISP. They receive and transmit network signals to other units without a physical cable. Wi-Fi routers have the capacity to transmit an Internet service within a confined range, whereas wireless modems can be used in almost any location where a mobile phone is present. Portable devices such as laptops, mobile phones, PDAs, etc., use wireless modems to receive signals over the air, similar to a cellular network. There are various types of wireless modems. Users can choose a wireless modem based on their requirements. The common types of wireless modems include:
  - **Cards**: They are the oldest form of wireless connection. There are two types of cards, namely, data cards and connect cards, which are available from mobile providers and are used by laptops, PCs, and routers. They are small in size and easy to use.
    - **USB sticks**: They connect quickly to the internet using a wireless modem. They resemble a universal serial bus (USB) flash drive and fit easily into the USB port of a laptop. Computers require installation of special drivers and software to use them. They are portable.
    - Mobile hotspots
    - Wireless routers

  The following features are considered while deciding on a wireless modem:

  - Speed of the modem
  - Protocols it can support, such as ethernet, GPRS, integrated services digital network (ISDN), Evolution-data optimized (EVDO), Wi-Fi, CPCD
  - Frequency band 900 MHz, 2.4 GHz, 23 GHz, 5 Hz

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- Radio technique such as a DSSS or frequency hopping
- Total number of channels for transmitting and receiving data
- Maximum signal strength
- Full duplex or half duplex capability

- **Wireless bridge:** A wireless bridge connects multiple LANs at the medium access control (MAC) layer. These bridges separate networks either logically or physically. They cover longer distances than APs. Few wireless bridges support point-to-point connections to an AP, while some support point-to-multipoint connections to several other APs. Wireless bridging helps in connecting two LAN segments through a wireless link. Two segments reside on the same subnet and look like two ethernet switches connected with a cable to all computers within the subnet. Broadcasts reach all the machines on that subnet allowing dynamic host configuration protocol (DHCP) clients in one segment to obtain the respective addresses from a DHCP server from a different segment. A wireless bridge can be used for connecting computers in one room to computers in another room without a cable.
- **Wireless repeater (range expanders):** This device retransmits the existing signal captured from the wireless router or an AP to create a new network. It works as an AP and a station simultaneously. The clients who are too far away from the router or AP can integrate with the same WLAN via a repeater. It implies that this device extends the signal by taking it from a wireless AP and transmits it to the uncovered area. These repeaters require an omnidirectional antenna. They capture, boost, and retransmit the signals.
- **Wireless Router:** A wireless router is a device in a WLAN which interconnects two types of networks using radio waves to the wireless enabled devices such as computers, laptops, and tablets. It functions as a router in the LAN, but also provides mobility to users. It also functions as a wireless AP and provides Internet access to various devices. Wireless routers have the ability to filter the network traffic based on the sender's and receiver's IP address. A wireless router provides strong encryption, filters MAC addresses and controls SSID authentication.
- **Wireless gateways:** A wireless gateway is a key component of a wireless network. It is a device that allows Internet-enabled devices to access the network. It combines the functions of wireless APs and routers. Wireless gateways have the feature of network address translation (NAT), which translates the public IP into a private IP and DHCP. An Internet connection can be shared between multiple stations.
- **Wireless USB adapter:** A wireless USB adapter connects different devices to a wireless network in order to access the Internet without a computer, router, or any other network device. It also supports communication links and syncs between two or more devices. There are three main varieties of a wireless adapter:
  - Cellular
  - Bluetooth

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- Wi-Fi

- **Antenna:** An antenna is a device that is designed to transmit and receive electromagnetic waves at radio frequencies. It is a collection of metal rods and wires that captures radio waves and translates them into an electrical current. It converts electrical impulses into radio waves and vice versa. The size and shape of an antenna is designed depending on the frequency of the signal they are designed to receive.

  An antenna that receives high frequency signals is highly focused, whereas a low-gain antenna receives or transmits over a large angle. A transducer translates the RF fields into an alternating current (AC) and vice-versa.

  The following are the functions of antennas:

  - **Transmission line:** Antennas transmit or receive radio waves from one point to another. This power transmission takes place in free space through the natural media such as air, water, and earth. Antennas avoid power that is transmitted through other means.
  - **Radiator:** A radiator radiates energy powerfully. This radiated energy is transmitted through the medium. A radiator is always the size of half the wavelength.
  - **Resonator:** The use of a resonator is necessary in broadband applications. Resonances that occur must be attenuated.

  The characteristics of an antenna are as follows:

  - **Operating frequency band:** Antennas operate at a frequency band between 960 MHz and 1215 MHz.
  - **Transmission power:** Antennas transmit power at 1200 W peak and 140 W on an average.
  - **Typical gain:** Gain is the ratio of the power input to the antenna to the power output from the antenna. It is measured in decibels relative to an isotropic antenna (dBi). The gain is generally 3.0 dBi.
  - **Radiation pattern:** The radiation pattern of an antenna is obtained in the form of a 3-dimensional plot and is generally represented in terms of two parameters, namely, elevation and azimuth.
  - **Directivity:** The directivity gain of an antenna is the calculation of radiated power in a particular direction. It is generally the ratio of the radiation intensity in a given direction to the average radiation intensity.
  - **Polarization:** It is the orientation of electromagnetic waves from the source. There are a number of polarizations such as linear, vertical, horizontal, circular, left hand circular polarized (LHCP), and right hand circular polarized (RHCP).

  There are six types of wireless antennas:

  - **Directional antenna:** A directional antenna can broadcast and receive radio waves from a single direction. In order to improve the transmission and reception, a

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

directional antenna is designed to work effectively in a specified direction. This also helps in reducing interference.

- **Omnidirectional antenna:** Omnidirectional antennas radiate electromagnetic (EM) energy in all directions. It provides a 360° horizontal radiation pattern. They radiate strong waves uniformly in two dimensions, but the waves are usually not as strong in the third dimension. These antennas are efficient in areas where wireless stations use time-division multiple access technology. A good example for an omnidirectional antenna is the antenna used by radio stations. These antennas are effective for radio signal transmission because the receiver may not be stationary. Therefore, a radio can receive a signal regardless of its location.

  Advantage:

  - Omnidirectional antennas can deal with signals from any direction.

  Disadvantages:

  - The coverage area of an omnidirectional antenna may be limited owing to the interference of walls and other obstacles with the radiated signal.
  - It is difficult for an omnidirectional antenna to work in an internal environment.

- **Parabolic grid antenna:** A parabolic grid antenna uses the same principle as a satellite dish, but it does not have a solid dish. It consists of a semi-dish in the form of a grid consisting of aluminum wires. Parabolic grid antennas can achieve very-long-distance Wi-Fi transmissions through highly focused radio beams. This type of antenna is useful for transmitting weak radio signals over very long distances on the order of 10 miles. The design of this antenna saves weight and space, and it can receive Wi-Fi signals that are either horizontally or vertically polarized.

  Advantage:

  - This antenna is wind resistant.

  Disadvantages:

  - This antenna is expensive since it requires a feed system for reflecting the radio signals.
  - In addition to the feed system, the antenna requires a reflector. Assembling of these components makes the installation time consuming.

- **Yagi antenna:** Yagi antenna, also called as the Yagi-Uda antenna, is a unidirectional antenna commonly used in communications using the frequency band from 10 MHz to very high frequency (VHF) and ultra-high frequency (UHF). The main objectives of this antenna are to improve the gain of the antenna and to reduce the noise level of the radio signal. It has a unidirectional radiation emission and response pattern and concentrates the radiation and response. It consists of a reflector, dipole, and directors. This antenna generates an end-fire radiation pattern.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

Advantages:

- A Yagi antenna has a good range and ease of aiming the antenna.
- The Yagi antenna is directional, focusing the entire signal in a cardinal direction. This results in high throughput.
- The installation and assembly of this antenna is easy and less time consuming as compared to other antennas.

Disadvantage:

- The antenna is very large, especially when built for high gain levels.

- **Dipole antenna:** A dipole antenna is a straight electrical conductor measuring half a wavelength from end to end, and it is connected at the center of the radio frequency (RF) feed line. Also called a doublet, the antenna is bilaterally symmetrical; therefore, it is inherently a balanced antenna. This kind of antenna feeds on a balanced parallel-wire RF transmission line. It is used for supporting client connections rather than site-to-site applications.

  Advantages:

  - A dipole antenna offers balanced signals. With the two-pole design, the device receives signals from a variety of frequencies.

  Disadvantages:

  - Although an indoor dipole antenna might be small, an outdoor dipole antenna can be much larger, making it difficult to manage.
  - To achieve the perfect frequency, antennas are required to undergo multiple combinations. This can be a hassle especially in the case of outdoor antennas.

- **Reflector antennas:** Reflector antennas are used for concentrating electromagnetic energy that is radiated or received at a focal point. These reflectors are generally parabolic.

  Advantages:

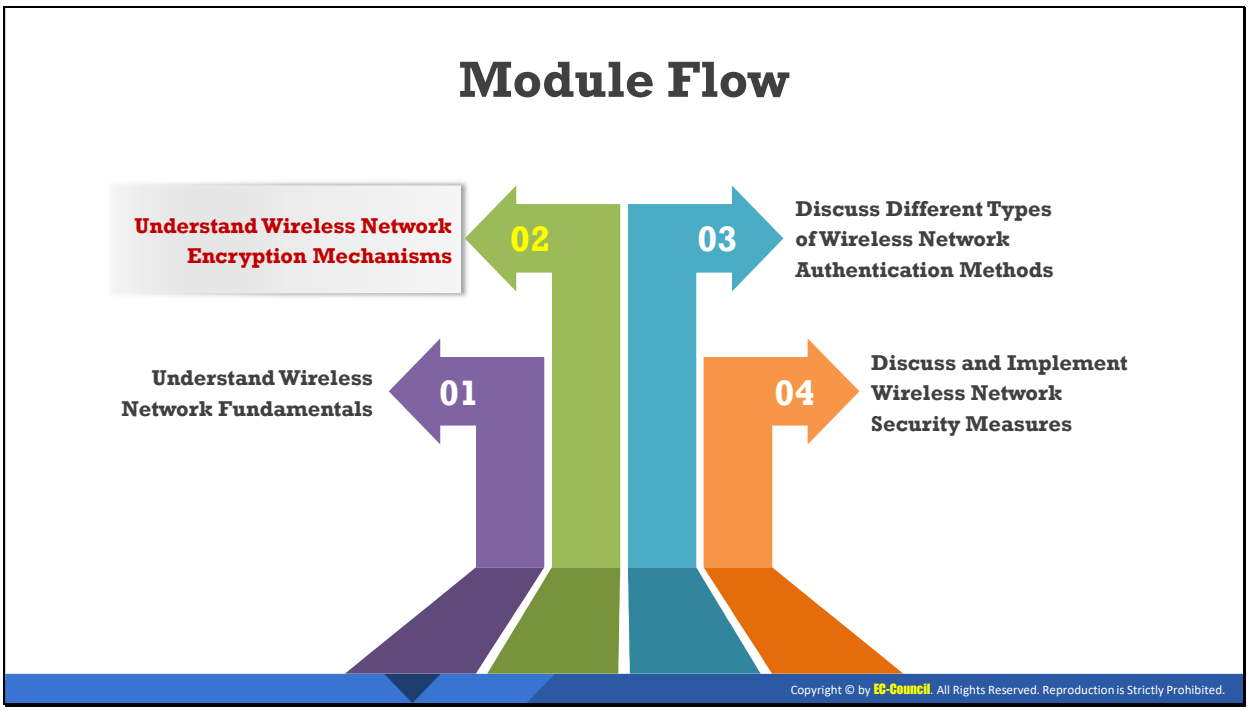
  - If the surface of the parabolic antenna is within the tolerance limit, it can be used as a primary mirror for all the frequencies. This can prevent interference while communicating with other satellites.
  - The larger the antenna reflector in terms of wavelengths, the higher is the gain.

  Disadvantage:

  - Reflector antennas reflect radio signals.
  - The manufacturing cost of the antenna is high.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

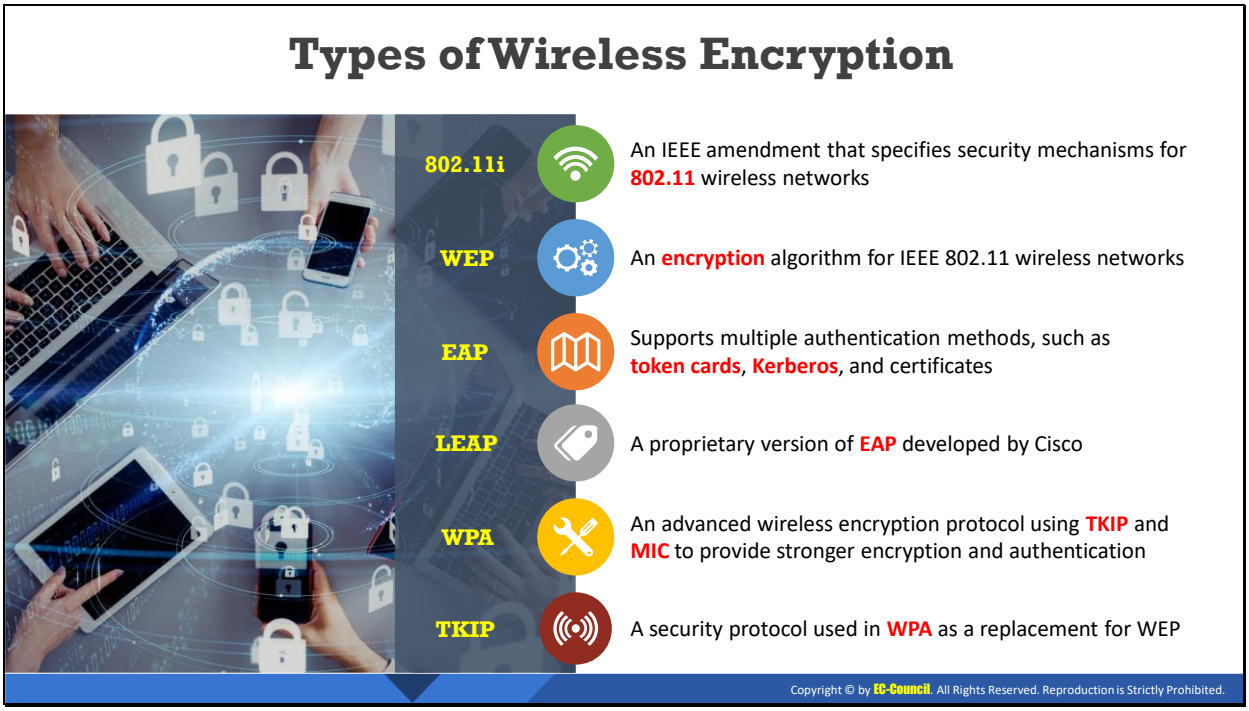
https://t.me/learningnets

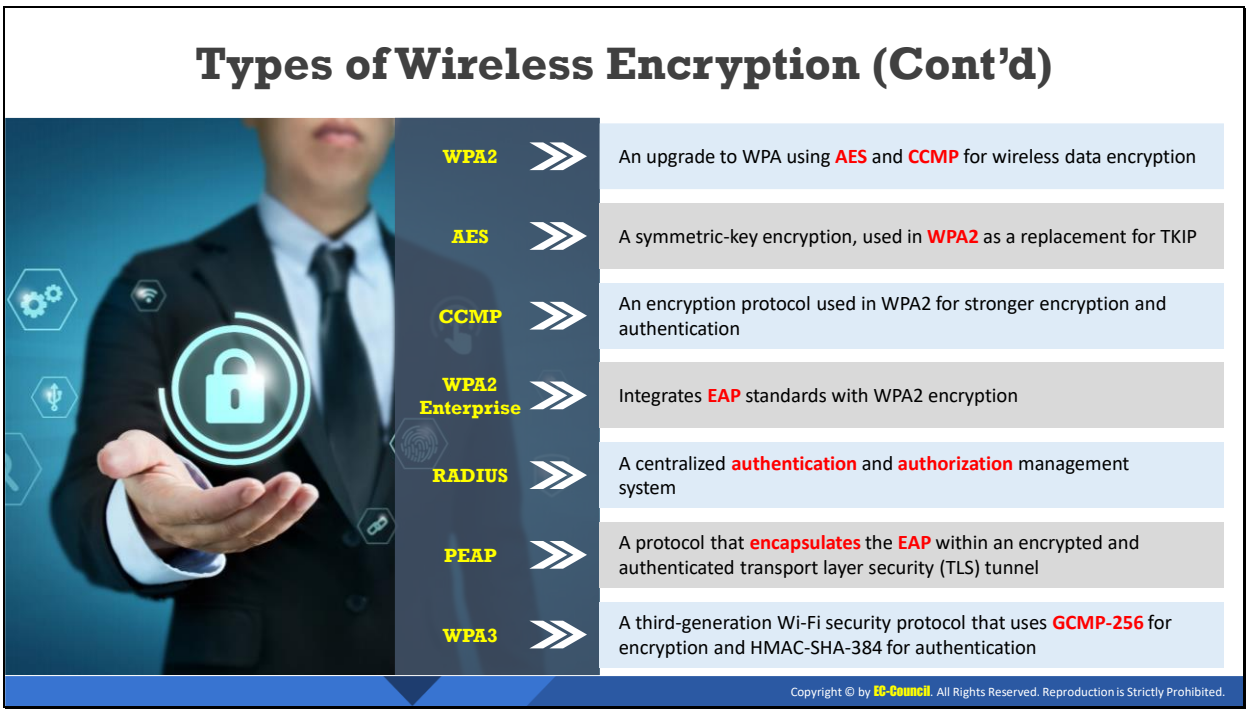


Understand Wireless Network Encryption Mechanisms

The objective of this section is to explain the various encryption mechanisms used in wireless networks, such as WEP encryption, wireless fidelity (Wi-Fi) protected access (WPA) Encryption, Wi-Fi protected access 2 (WPA2) encryption, Wi-Fi protected access 3 (WPA3) encryption. This section also describes the limitations of these encryption mechanisms.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets





Types of Wireless Encryption

There are several types of wireless encryption algorithms that can secure a wireless network. Each wireless encryption algorithm has advantages and disadvantages.

- **802.11i**: It is an IEEE amendment that specifies security mechanisms for 802.11 wireless networks.

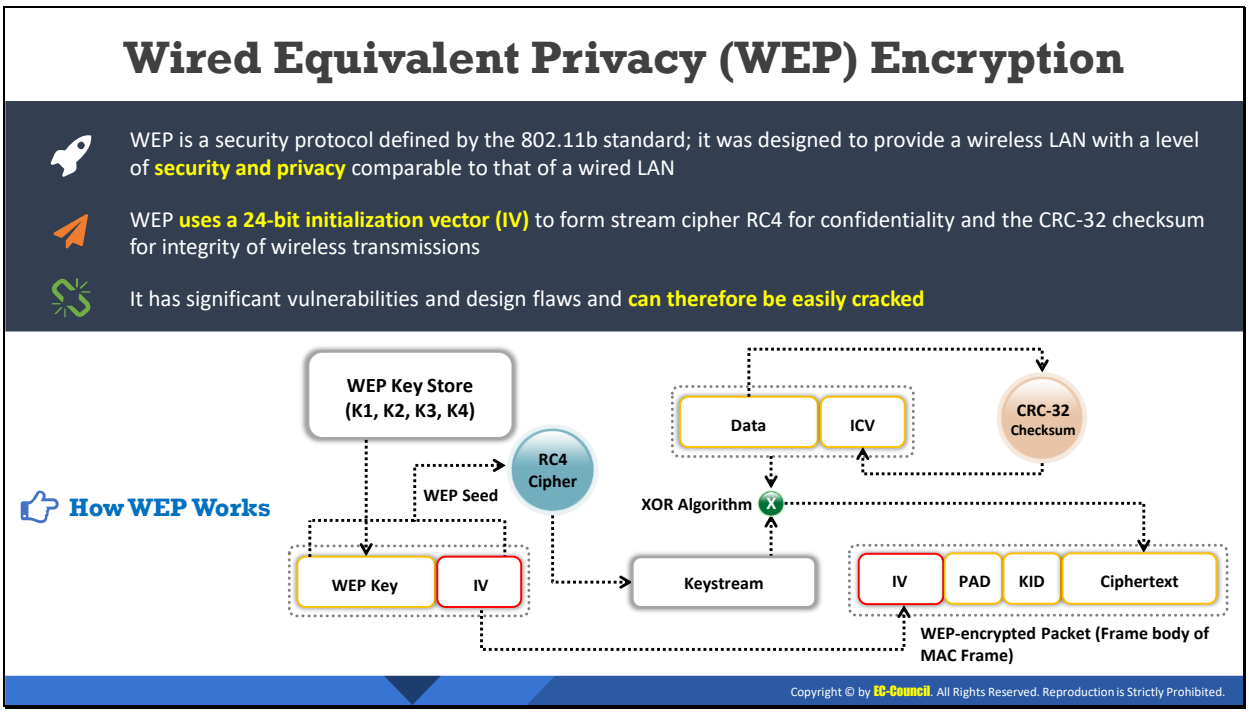
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- **WEP**: WEP is an encryption algorithm for IEEE 802.11 wireless networks. It is an old wireless security standard and can be cracked easily.
- **EAP**: The Extensible Authentication Protocol (EAP) supports multiple authentication methods, such as token cards, Kerberos, and certificates.
- **LEAP**: Lightweight EAP (LEAP) is a proprietary version of EAP developed by Cisco.
- **WPA**: It is an advanced wireless encryption protocol using TKIP and Message Integrity Check (MIC) to provide strong encryption and authentication. It uses a 48-bit initialization vector (IV), 32-bit cyclic redundancy check (CRC), and TKIP encryption for wireless security.
- **TKIP**: It is a security protocol used in WPA as a replacement for WEP.
- **WPA2**: It is an upgrade to WPA using AES and the Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP) for wireless data encryption.
- **AES**: It is a symmetric-key encryption used in WPA2 as a replacement for TKIP.
- **CCMP**: It is an encryption protocol used in WPA2 for strong encryption and authentication.
- **WPA2 Enterprise**: It integrates EAP standards with WPA2 encryption.
- **RADIUS**: It is a centralized authentication and authorization management system.
- **PEAP**: It is a protocol that encapsulates the EAP within an encrypted and authenticated Transport Layer Security (TLS) tunnel.
- **WPA3**: It is a third-generation Wi-Fi security protocol that provides new features for personal and enterprise usage. It uses Galois/Counter Mode-256 (GCMP-256) for encryption and the 384-bit hash message authentication code with the Secure Hash Algorithm (HMAC-SHA-384) for authentication.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Wired Equivalent Privacy (WEP) Encryption

WEP was an early attempt to protect wireless networks from security breaches, but as technology improved, it became evident that information encrypted with WEP is vulnerable to attack. We discuss WEP in detail here.

What is WEP Encryption?

WEP is a component of the IEEE 802.11 WLAN standards. Its primary purpose is to ensure data confidentiality on wireless networks at a level equivalent to that of wired LANs, which can use physical security to stop unauthorized access to a network.

In a WLAN, a user or an attacker can access the network without physically connecting to the LAN. Therefore, WEP utilizes an encryption mechanism at the data link layer for minimizing unauthorized access to the WLAN. This is accomplished by encrypting data with the symmetric Rivest Cipher 4 (RC4) encryption algorithm, which is a cryptographic mechanism used to defend against threats.

Role of WEP in Wireless Communication

- WEP protects against eavesdropping on wireless communications.
- It attempts to prevent unauthorized access to a wireless network.
- It depends on a secret key shared by a mobile station and an AP. This key encrypts packets before transmission. Performing an integrity check ensures that packets are not altered during transmission. 802.11 WEP encrypts only the data between network clients.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Main Advantages of WEP

- **Confidentiality**: It prevents link-layer eavesdropping.
- **Access Control**: It determines who may access data.
- **Data Integrity**: It protects the change of data by a third party.
- **Efficiency**

Key Points

WEP was developed without any academic or public review. In particular, it was not reviewed by cryptologists during development. Therefore, it has significant vulnerabilities and design flaws.

WEP is a stream cipher that uses RC4 to produce a stream of bytes that are XORed with plaintext. The length of the WEP and secret key are as follows:

- 64-bit WEP uses a 40-bit key
- 128-bit WEP uses a 104-bit key
- 256-bit WEP uses 232-bit key

Flaws of WEP

The following basic flaws undermine WEP's ability to protect against a serious attack.

- No defined method for encryption key distribution:
  - Pre-shared keys (PSKs) are set once at installation and are rarely (if ever) changed.
  - It is easy to recover the number of plaintext messages encrypted with the same key.
- RC4 was designed to be used in a more randomized environment than that utilized by WEP:
  - As the PSK is rarely changed, the same key is used repeatedly.
  - An attacker monitors the traffic and finds different ways to work with the plaintext message.
  - With knowledge of the ciphertext and plaintext, an attacker can compute the key.
- Attackers analyze the traffic from passive data captures and crack WEP keys with the help of tools such as AirSnort and WEPCrack.
- Key scheduling algorithms are also vulnerable to attack.

How WEP Works

- CRC-32 checksum is used to calculate a 32-bit integrity check value (ICV) for the data, which, in turn, is added to the data frame.
- A 24-bit arbitrary number known as the initialization vector (IV) is added to the WEP key; the WEP key and IV are together called the WEP seed.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- The WEP seed is used as the input to the RC4 algorithm to generate a keystream, which is bit-wise XORed with a combination of the data and ICV to produce the encrypted data.
- The IV field (IV + PAD + KID) is added to the ciphertext to generate a MAC frame.

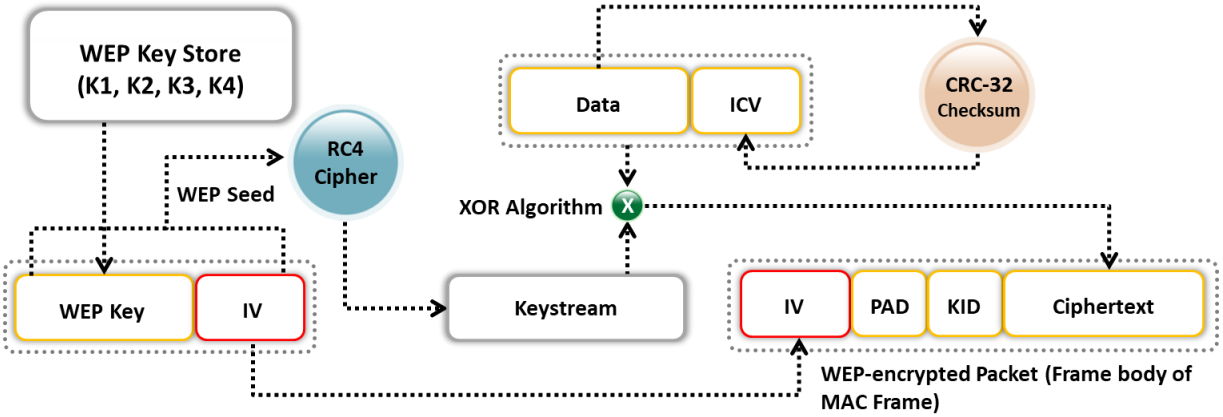
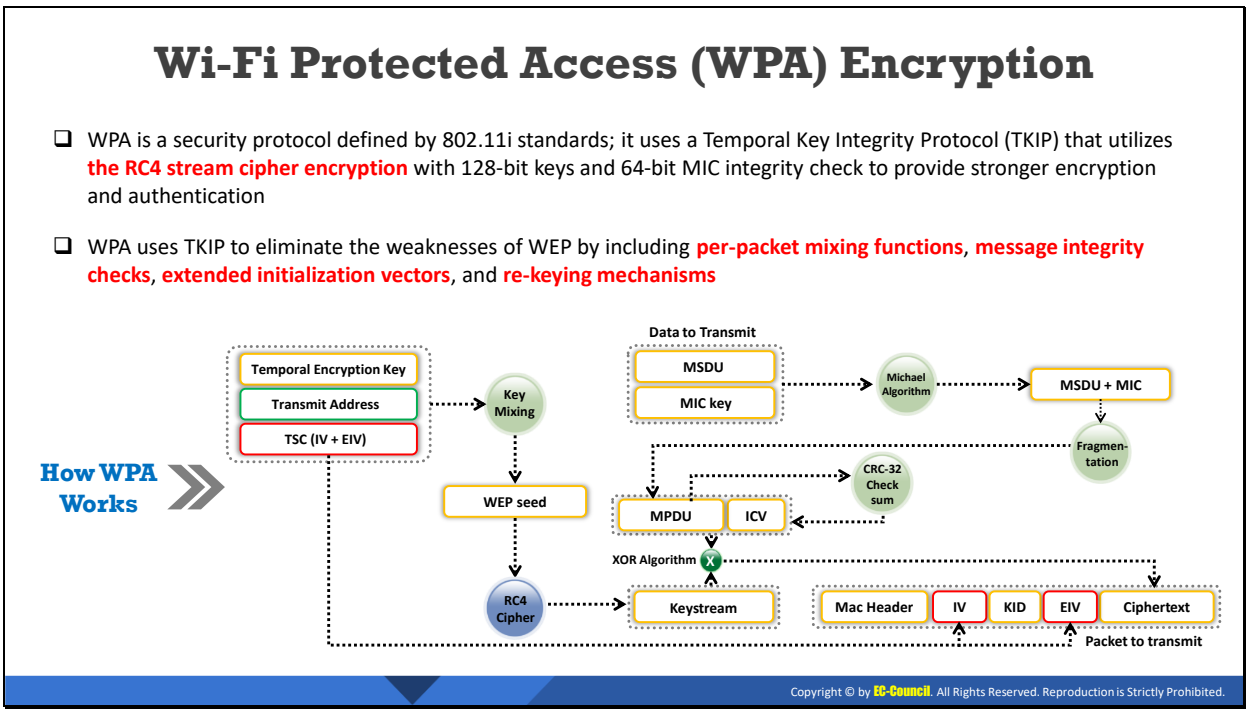


Figure 7.7: Operational flow of WEP

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Wi-Fi Protected Access (WPA) Encryption

Wi-Fi Protected Access (WPA) is a security protocol defined by the 802.11i standard. In the past, the primary security mechanism used between wireless APs and wireless clients was WEP encryption, which has a major drawback in that it uses a static encryption key. An attacker can exploit this weakness using tools that are freely available on the Internet. IEEE defines WPA as "an expansion to the 802.11 protocols that can allow for increased security." Nearly every Wi-Fi manufacturer provides WPA.

WPA has better data encryption security than WEP because messages pass through a Message Integrity Check (MIC) using the Temporal Key Integrity Protocol (TKIP), which utilizes the RC4 stream cipher encryption with 128-bit keys and 64-bit MIC to provide strong encryption and authentication. WPA is an example of how 802.11i provides stronger encryption and enables pre-shared key (PSK) or EAP authentication. WPA uses TKIP for data encryption, which eliminates the weaknesses of WEP by including per-packet mixing functions, MICs, extended IVs and re-keying mechanisms.

How WPA Works

- A TK, transmit address, and TKIP sequence counter (TSC) are used as input to the RC4 algorithm to generate a keystream.
  - The IV or TK sequence, transmit address or MAC destination address, and TK are combined with a hash function or mixing function to generate a 128-bit and 104-bit key.
  - This key is then combined with RC4 to produce the keystream, which should be of the same length as the original message.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- The MAC service data unit (MSDU) and message integrity check (MIC) are combined using the Michael algorithm.
- The combination of MSDU and MIC is fragmented to generate the MAC protocol data unit (MPDU).
- A 32-bit ICV is calculated for the MPDU.
- The combination of MPDU and ICV is bitwise XORed with the keystream to produce the encrypted data.
- The IV is added to the encrypted data to generate the MAC frame.

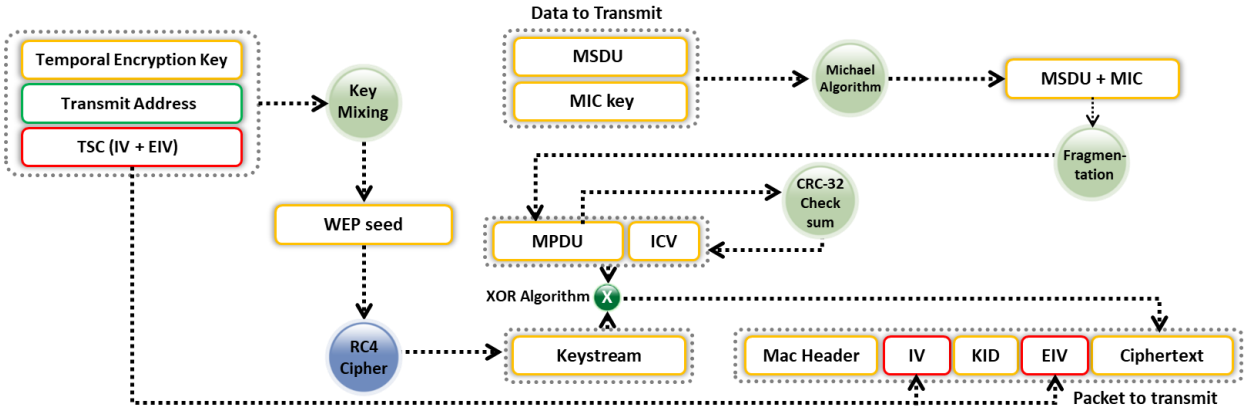
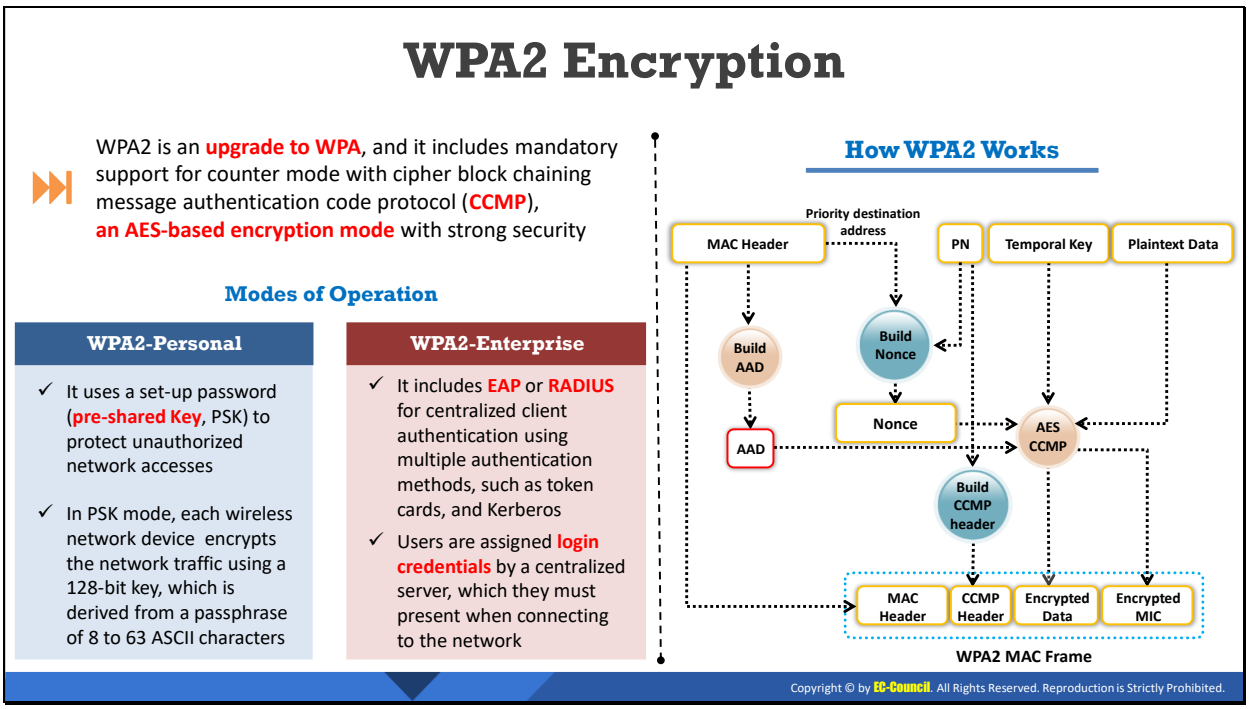


Figure 7.8: Operational flow of WPA

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



WPA2 Encryption

Wi-Fi Protected Access 2 (WPA2) is a security protocol used to safeguard wireless networks. WPA2 replaced WPA in 2006. It is compatible with the 802.11i standard and supports many security features that WPA does not. WPA2 introduces the use of the National Institute of Standards and Technology (NIST) FIPS 140-2-compliant AES encryption algorithm, which is a strong wireless encryption algorithm, and the Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP). It provides stronger data protection and network access control than WPA. Furthermore, it gives a high level of security to Wi-Fi connections so that only authorized users can access the network.

Modes of Operation

WPA2 offers two modes of operation:

- **WPA2-Personal**: WPA2-Personal uses a password set in advance, called the pre-shared key (PSK), to protect unauthorized network access. Each wireless device uses the same 256-bit key generated from a password to authenticate with the AP. In the PSK mode, each wireless network device encrypts the network traffic using a 128-bit key derived from a passphrase of 8–63 ASCII characters. The router uses the combination of a passphrase, network SSID, and TKIP to generate a unique encryption key for each wireless client. These encryption keys change continually.
- **WPA2-Enterprise**: WPA2-Enterprise uses EAP or RADIUS for centralized client authentication using multiple authentication methods, such as token cards, Kerberos, and certificates. WPA-Enterprise assigns a unique ciphered key to every system and hides it from the user in order to provide additional security and to prevent the sharing of keys. Users are allocated login credentials by a centralized server, which they must present when connecting to the network.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

How WPA2 Works

During CCMP implementation, additional authentication data (AAD) are generated using a MAC header and included in the encryption process that uses both AES and CCMP encryptions. Consequently, the non-encrypted portion of the frame is protected from any alteration or distortion. The protocol uses a sequenced packet number (PN) and a portion of the MAC header to generate a Nonce that it uses in the encryption process. The protocol gives plaintext data, and temporal keys, AAD, and Nonce are used as input for the data encryption process that uses both AES and CCMP algorithms.

A PN is included in the CCMP header for protection against replay attacks. The resultant data from the AES and CCMP algorithms produce encrypted text and an encrypted MIC value. Finally, the assembled MAC header, CCMP header, encrypted data, and encrypted MIC form the WPA2 MAC frame. The below figure shows the operational flow of WPA2.

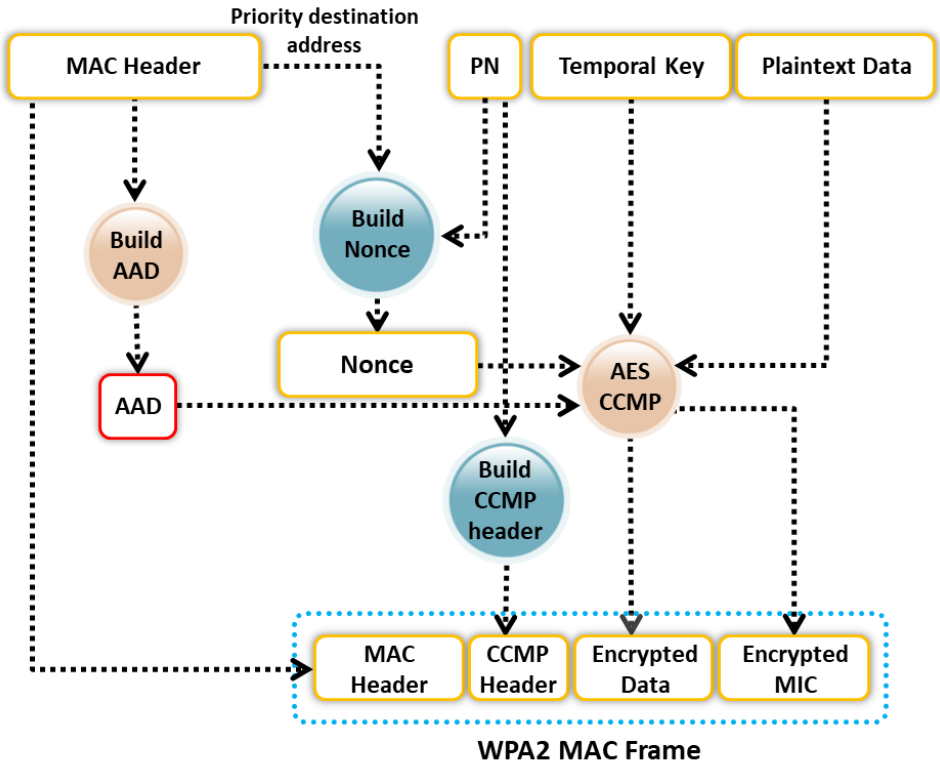
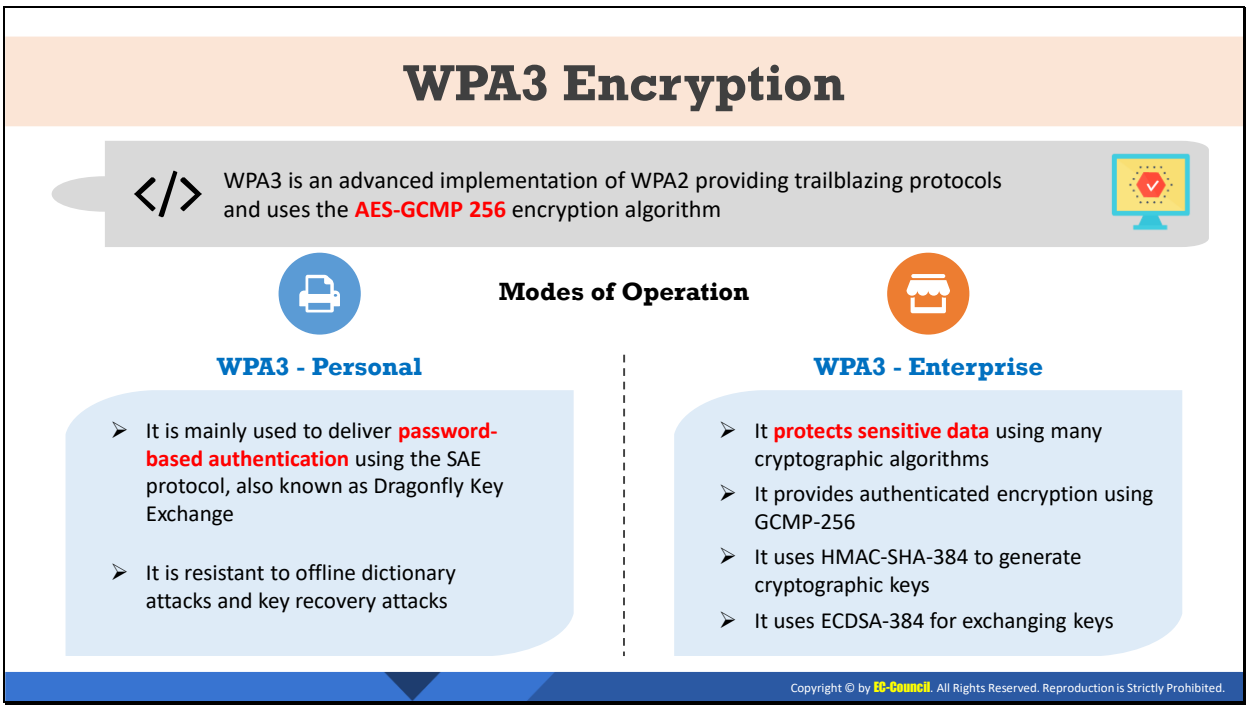


Figure 7.9: Operational flow of WPA2

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



WPA3 Encryption

Wi-Fi Protected Access 3 (WPA3) was announced by the Wi-Fi Alliance on January 2018 as an advanced implementation of WPA2 that provides trailblazing protocols. Like WPA2, the WPA3 protocol has two variants: WPA3-Personal and WPA3-Enterprise.

WPA3 provides cutting-edge features to simplify Wi-Fi security and provides the capabilities necessary to support different network deployments ranging from corporate networks to home networks. It also ensures cryptographic consistency using encryption algorithms such as AES and TKIP to defend against network attacks. Furthermore, it provides network resilience through Protected Management Frames (PMF) that deliver a high level of protection against eavesdropping and forging attacks. WPA3 also disallows outdated legacy protocols.

Modes of Operation

WPA3 offers two modes of operation:

- **WPA3-Personal**: This mode is mainly used to deliver password-based authentication. WPA3 is more rigid to attacks than WPA2 because it uses a modern key establishment protocol called the Simultaneous Authentication of Equals (SAE), also known as Dragonfly Key Exchange, which replaces the PSK concept used in WPA2-Personal. Some of the features of WPA3-Personal are described below.
  - **Resistance to offline dictionary attacks**: It prevents passive password attacks such as brute-forcing.
  - **Resistance to key recovery**: Even when a password is determined, it is impossible to capture and determine session keys while maintaining the forward secrecy of network traffic.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **Natural password choice**: It allows users to choose weak or popular phrases as passwords, which are easy to remember.
- **Easy accessibility**: It can provide greater protection than WPA2 without changing the previous methods used by users for connecting to a network.

- **WPA3-Enterprise**: This mode is based on WPA2. It offers better security than WPA2 across the network and protects sensitive data using many cryptographic concepts and tools. Some of the security protocols used by WPA3-Enterprise are described below.
  - **Authenticated encryption**: It helps in maintaining the authenticity and confidentiality of data. For this purpose, WPA3 uses the 256-bit Galois/Counter Mode Protocol (GCMP-256).
  - **Key derivation and validation**: It helps in generating a cryptographic key from a password or master key. It uses the 384-bit hashed message authentication mode (HMAC) with the Secure Hash Algorithm, termed HMAC-SHA-384.
  - **Key establishment and verification**: It helps in exchanging cryptographic keys among two parties. For this purpose, WPA3 uses Elliptic Curve Diffie–Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA) using a 384-bit elliptic curve.
  - **Frame protection and robust administration**: WPA3 uses 256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256) for this purpose.

Enhancements in WPA3 with Respect to WPA2

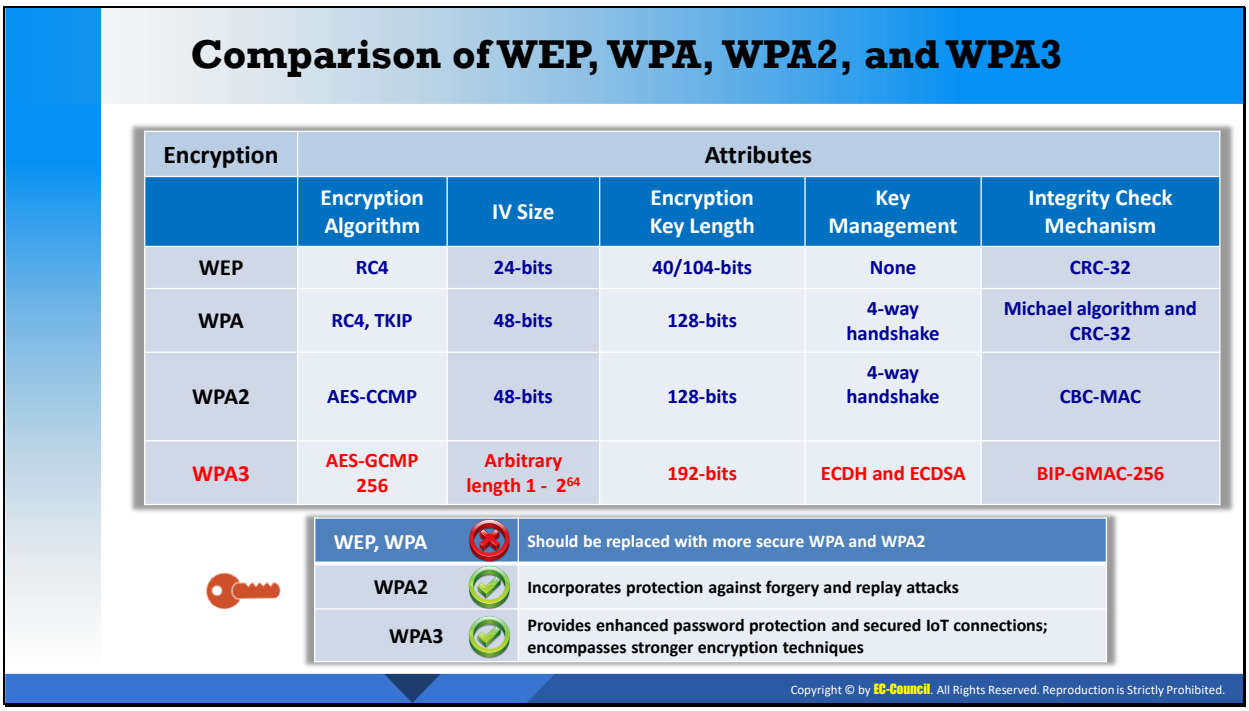
WPA3 can be used to implement a layered security strategy that can protect all aspects of a Wi-Fi network. WPA3 has a certification program that specifies the prevailing standards the product must support. The Dragonfly handshake/SAE protocol is mandatory for WPA3 certification.

The important features of WPA3 are as follows.

1. **Secured handshake**: The Simultaneous Authentication of Equals (SAE) protocol, also known as the Dragonfly handshake, can be used to make a password resistant to dictionary and brute-force attacks, preventing the offline decryption of data.
2. **Wi-Fi Easy Connect**: This feature simplifies the security configuration process by managing different interface connections in a network with one interface using the Wi-Fi Device Provisioning Protocol (DPP). This can securely allow a plethora of smart devices in a network to connect to one device using a quick response (QR) code or password. It also helps set up a connection between different IoT devices.
3. **Unauthenticated encryption**: It uses a new feature called Opportunistic Wireless Encryption (OWE) that replaces the 802.11 “open” authentication by providing better protection when using public hotspots and public networks.
4. **Bigger session keys**: The cryptographic security process of WPA3-Enterprise supports key sizes of 192 bits or higher, which are difficult to crack, ensuring rigid protection.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



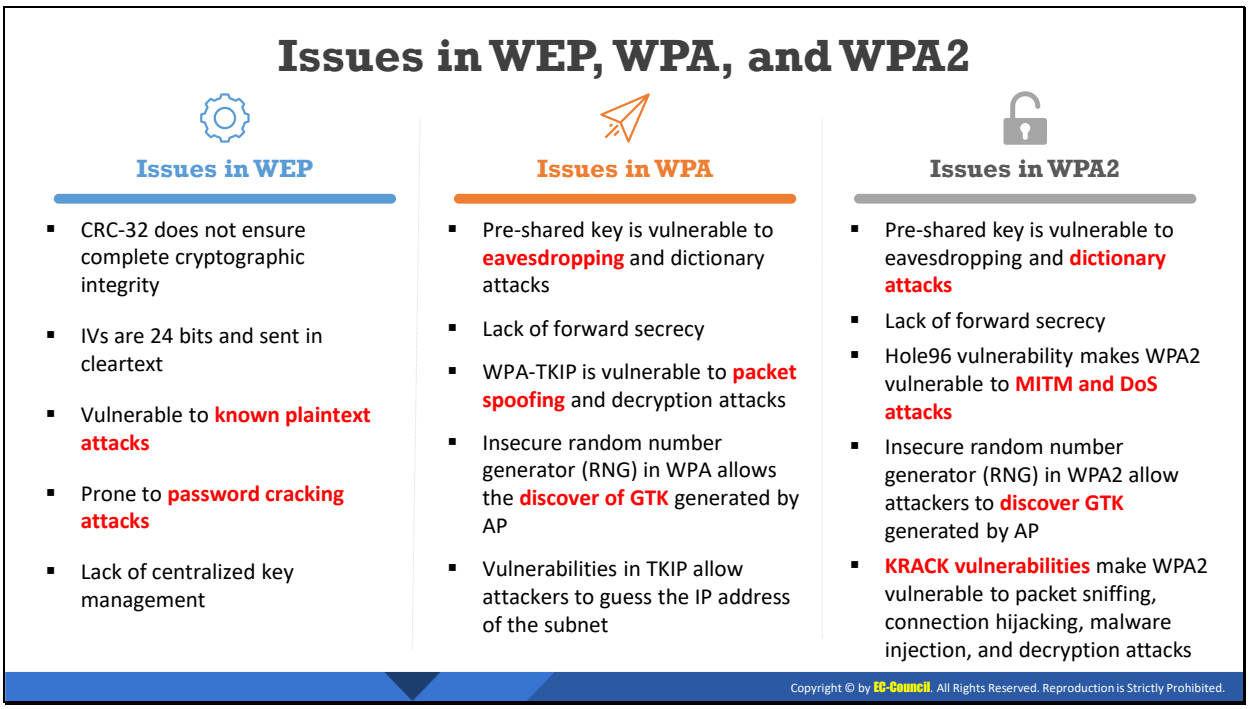
Comparison of WEP, WPA, WPA2, and WPA3

WEP provides data confidentiality on wireless networks, but it is weak and fails to meet any of its security goals. While WPA fixes most of WEP's problems, WPA2 makes wireless networks almost as secure as wired networks. Because WPA2 supports authentication, only authorized users can access the network. WEP should be replaced with either WPA or WPA2 to secure a Wi-Fi network. Though WPA and WPA2 incorporate protections against forgery and replay attacks, WPA3 can provide a more enhanced password-protection mechanism and secure IoT connections; further, it utilizes stronger encryption techniques. The below table compares WEP, WPA, WPA2, and WPA3 in terms of the encryption algorithm used, the encryption-key size, the initialization vector (IV) it produces, key management, and data integrity.

Encryption	Attributes				
	Encryption Algorithm	IV Size	Encryption Key Length	Key Management	Integrity Check Mechanism
WEP	RC4	24-bits	40/104-bits	None	CRC-32
WPA	RC4, TKIP	48-bits	128-bits	4-way handshake	Michael algorithm and CRC-32
WPA2	AES-CCMP	48-bits	128-bits	4-way handshake	CBC-MAC
WPA3	AES-GCMP 256	Arbitrary length 1 - 2^{64}	192-bits	ECDH and ECDSA	BIP-GMAC-256

Table 7.2: Comparison of WEP, WPA, WPA2, and WPA3

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Issues in WEP, WPA, and WPA2

Issues in WEP

WEP encryption is insufficient to secure wireless networks because of certain issues and anomalies, which include the following.

- **CRC32 is insufficient to ensure the complete cryptographic integrity of a packet**: By capturing two packets, an attacker can reliably flip a bit in the encrypted stream and modify the checksum so that the packet is accepted.
- **IVs are of 24 bits**: The IV is a 24-bit field, which is too small to be secure, and is sent in the cleartext portion of a message. An AP broadcasting 1500-byte packets at 11 Mbps would exhaust the entire IV space in five hours.
- **WEP is vulnerable to known plaintext attacks**: When an IV collision occurs, it becomes possible to reconstruct the RC4 keystream based on the IV and the decrypted payload of the packet.
- **WEP is vulnerable to dictionary attacks**: Because WEP is based on a password, it is prone to password-cracking attacks. The small IV space allows the attacker to create a decryption table, which is a dictionary attack.
- **WEP is vulnerable to DoS attacks**: This is because associate and disassociate messages are not authenticated.
- **An attacker can eventually construct a decryption table of reconstructed keystreams**: With approximately 24 GB of space, an attacker can use this table to decrypt WEP packets in real time.
- **A lack of centralized key management makes it difficult to change WEP keys regularly.**

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **IV is a value used to randomize the keystream value, and each packet has an IV value**: The standard IV allows only a 24-bit field, which is too small to be secure, and is sent in the cleartext portion of a message. All available IV values can be used up within hours at a busy AP. IV is a part of the RC4 encryption key and is vulnerable to an analytical attack that recovers the key after intercepting and analyzing a relatively small amount of traffic. Identical keystreams are produced with the reuse of the IV for data protection because the short IV keystreams are repeated within a short time. Furthermore, wireless adapters from the same vendor may all generate the same IV sequence. This enables attackers to determine the keystream and decrypt the ciphertext.
- **The standard does not require each packet to have a unique IV:** Vendors use only a small part of the available 24-bit possibilities. Consequently, a mechanism that depends on randomness is not random at all, and attackers can easily determine the keystream and decrypt other messages.
- **The use of RC4 was designed to be a one-time cipher and not intended for use with multiple messages.**

Issues in WPA

WPA is an improvement over WEP in many ways because it uses TKIP for data encryption and helps in secured data transfer. However, WPA has many security issues as well.

Some of the security issues of WPA are as described follows.

- **Weak passwords**: If users depend on weak passwords, the WPA PSK is vulnerable to various password-cracking attacks.
- **Lack of forward secrecy**: If an attacker captures a PSK, they can decrypt all the packets encrypted with that key (i.e., all the packets transmitted or being transmitted can be decrypted).
- **Vulnerability to packet spoofing and decryption**: Clients using WPA-TKIP are vulnerable to packet-injection attacks and decryption attacks, which further allows attackers to hijack Transmission Control Protocol (TCP) connections.
- **Predictability of the group temporal key (GTK)**: An insecure random number generator (RNG) in WPA allows attackers to discover the GTK generated by the AP. This further allows attackers to inject malicious traffic in the network and decrypt all the transmissions in progress over the Internet.
- **Guessing of IP addresses**: TKIP vulnerabilities allow attackers to guess the IP address of the subnet and inject small packets into the network to downgrade the network performance.

Issues in WPA2

Although WPA2 is more secure than WPA, it also has some security issues, which are discussed below.

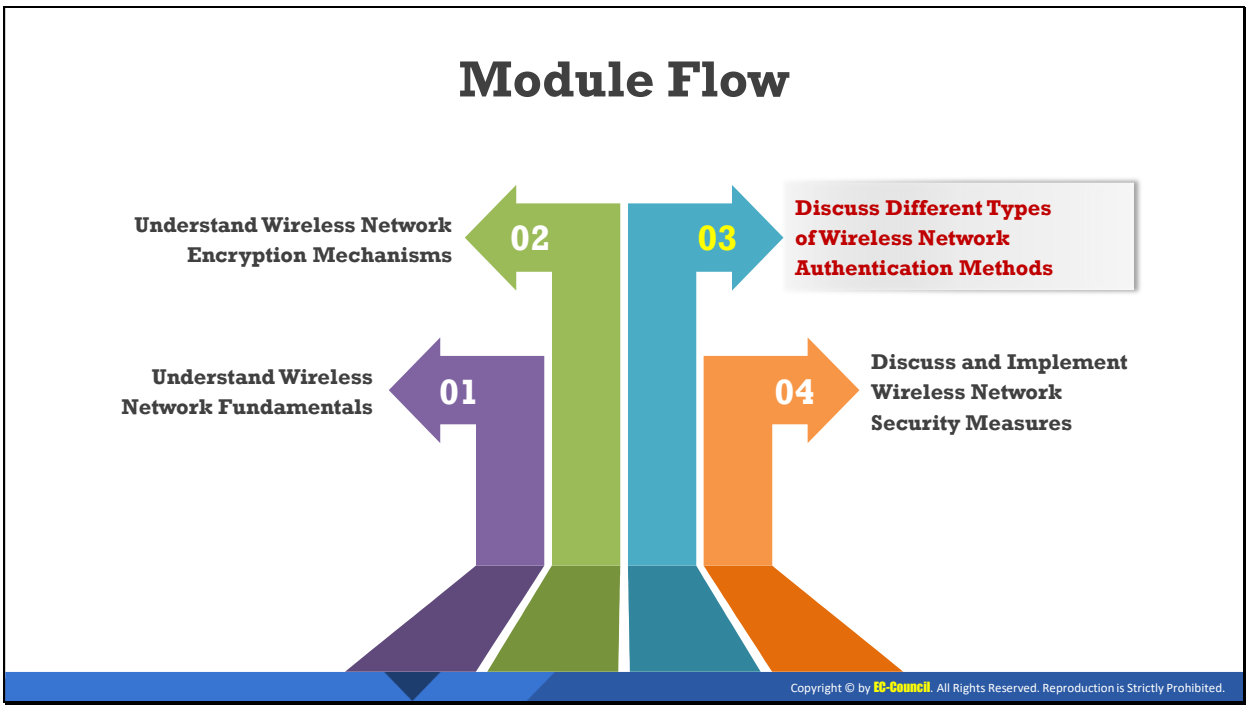
- **Weak passwords**: If users depend on weak passwords, the WPA2 PSK is vulnerable to various attacks such as eavesdropping, dictionary, and password-cracking attacks.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- **Lack of forward secrecy**: If an attacker captures a PSK, they can decrypt all the packets encrypted with that key (i.e., all the packets transmitted or being transmitted can be decrypted).
- **Vulnerability to man-in-the-middle (MITM) and denial-of-service (DoS) attacks**: The Hole96 vulnerability in WPA2 allows attackers to exploit a shared group temporal key (GTK) to perform MITM and DoS attacks.
- **Predictability of GTK**: An insecure random number generator (RNG) in WPA2 allows attackers to discover the GTK generated by the AP. This further allows attackers to inject malicious traffic in the network and decrypt all the transmissions in progress over the Internet.
- **KRACK vulnerabilities**: WPA2 has a significant vulnerability to an exploit known as key reinstallation attack (KRACK). This exploit may allow attackers to sniff packets, hijack connections, inject malware, and decrypt packets.
- **Vulnerability to wireless DoS attacks**: Attackers can exploit the WPA2 replay attack detection feature to send forged group-addressed data frames with a large PN to perform a DoS attack.
- **Insecure WPS PIN recovery**: In some cases, disabling WPA2 and WPS can be a time-consuming process, in which the attacker needs to control the WPA2 PSK used by the clients. When WPA2 and WPS are enabled, the attacker can disclose the WPA2 key by determining the WPS personal identification number (PIN) through simple steps.

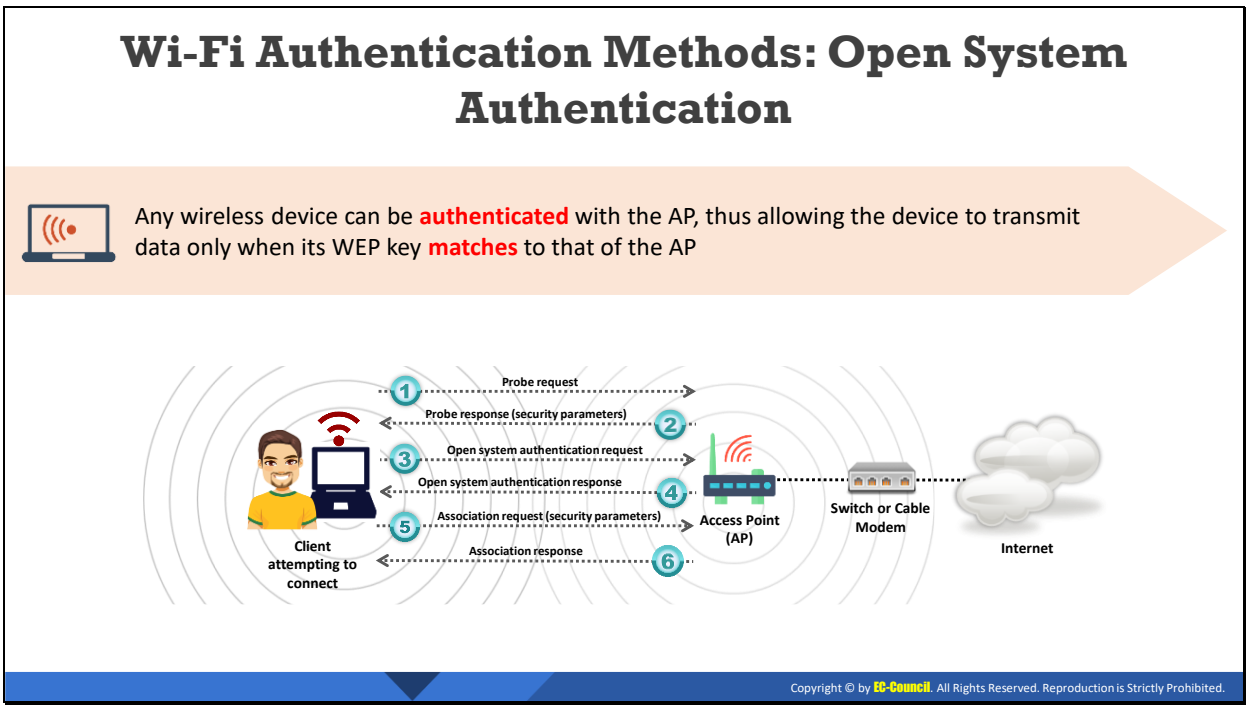
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

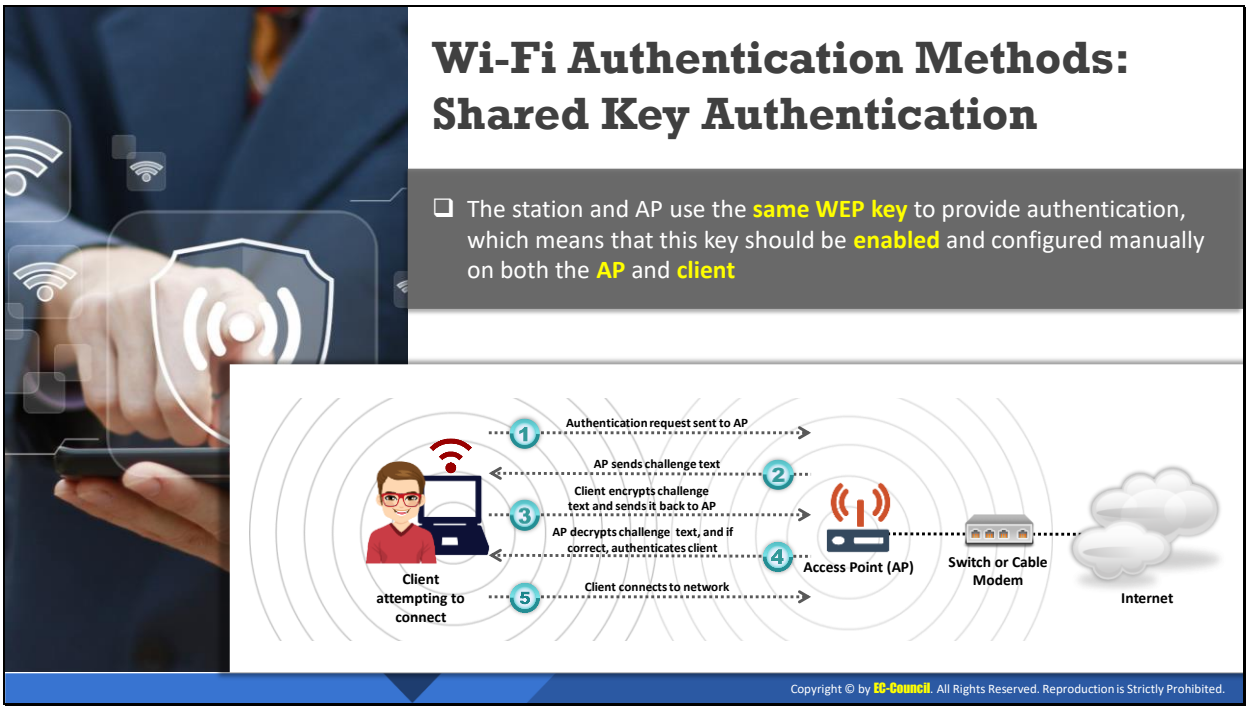


Discuss Different Types of Wireless Network Authentication Methods

The objective of this section is to explain the various authentication methods such as the open system authentication, shared key authentication, etc., used in wireless networks.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets





Wi-Fi Authentication Methods

Methods used to perform Wi-Fi authentication include open system authentication and shared key authentication.

- **Open system authentication process**: Open system authentication is a null authentication algorithm that does not verify whether it is a user or a machine requesting network access. It uses cleartext transmission to allow the device to

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

associate with an AP. In the absence of encryption, the device can use the SSID of an available WLAN to gain access to a wireless network. The enabled WEP key on the AP acts as an access control to enter the network. Any user entering the wrong WEP key cannot transmit messages via the AP even if the authentication is successful. The device can only transmit messages when its WEP key matches with the WEP key of the AP. This authentication mechanism does not depend on a RADIUS server on the network.

In the open system authentication process, any wireless client that wishes to access a Wi-Fi network sends a request to the wireless AP for authentication. In this process, the station sends an authentication management frame containing the identity of the sending station for authenticating and connecting with the other wireless stations. The AP then returns an authentication frame to confirm access to the requested station and completes the authentication process.

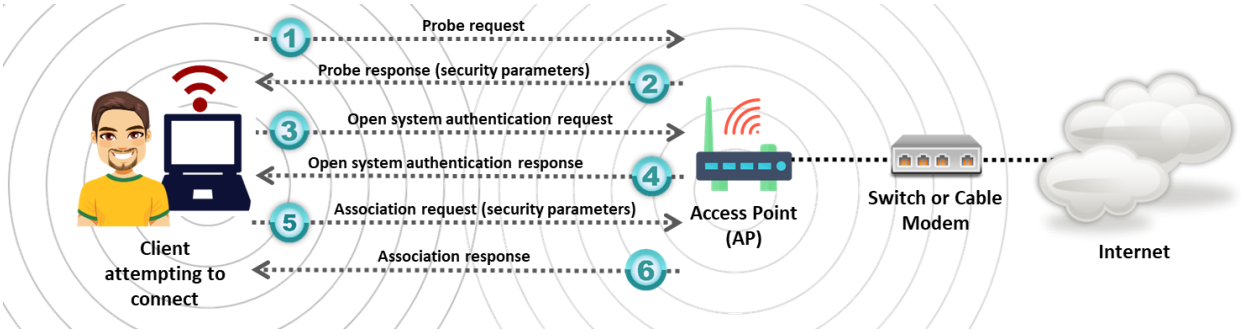


Figure 7.10: Open system authentication process

Advantage

- This mechanism can be used with wireless devices that do not support complex authentication algorithms.

Disadvantage

- There is no way to check whether someone is a genuine client or an attacker. Anyone who knows the SSID can easily access the wireless network.

- **Shared key authentication process**: In this process, each wireless station receives a shared secret key over a secure channel that is distinct from the 802.11 wireless network communication channels. The following steps illustrate the establishment of a network connection using the shared key authentication process:
  - The station sends an authentication frame to the AP.
  - The AP sends a challenge text to the station.
  - The station encrypts the challenge text using its configured 64-bit or 128-bit key and sends the encrypted text to the AP.
  - The AP uses its configured Wired Equivalent Privacy (WEP) key to decrypt the encrypted text. The AP compares the decrypted text with the original challenge text. If they match, the AP authenticates the station.
  - The station connects to the network.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

The AP can reject the station if the decrypted text does not match the original challenge text; then, the station will be unable to communicate with either the Ethernet network or the 802.11 networks.

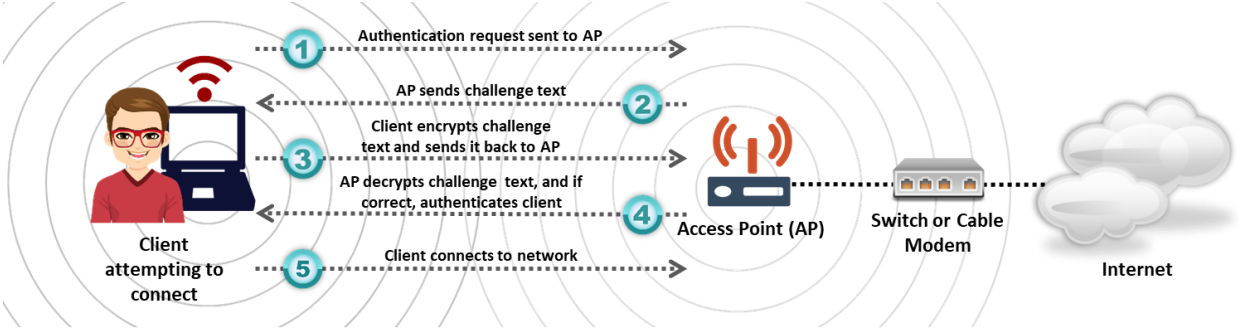
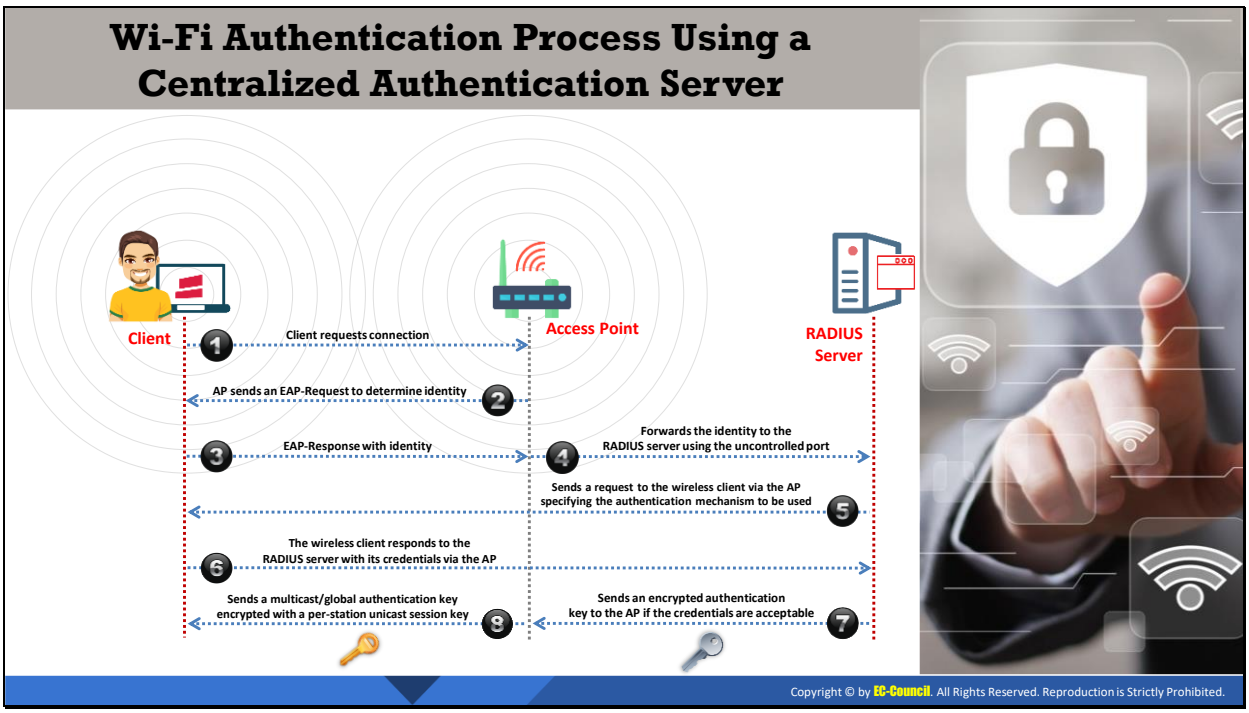


Figure 7.11: Shared key authentication process

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Wi-Fi Authentication Process Using a Centralized Authentication Server

The 802.1X standard provides centralized authentication. For 802.1X authentication to work in a wireless network, the AP must be able to securely identify the traffic from a specific wireless client. In this Wi-Fi authentication process, a centralized authentication server known as Remote Authentication Dial-in User Service (RADIUS) sends authentication keys to both the AP and the clients that attempt to authenticate with the AP. This key enables the AP to identify a particular wireless client.

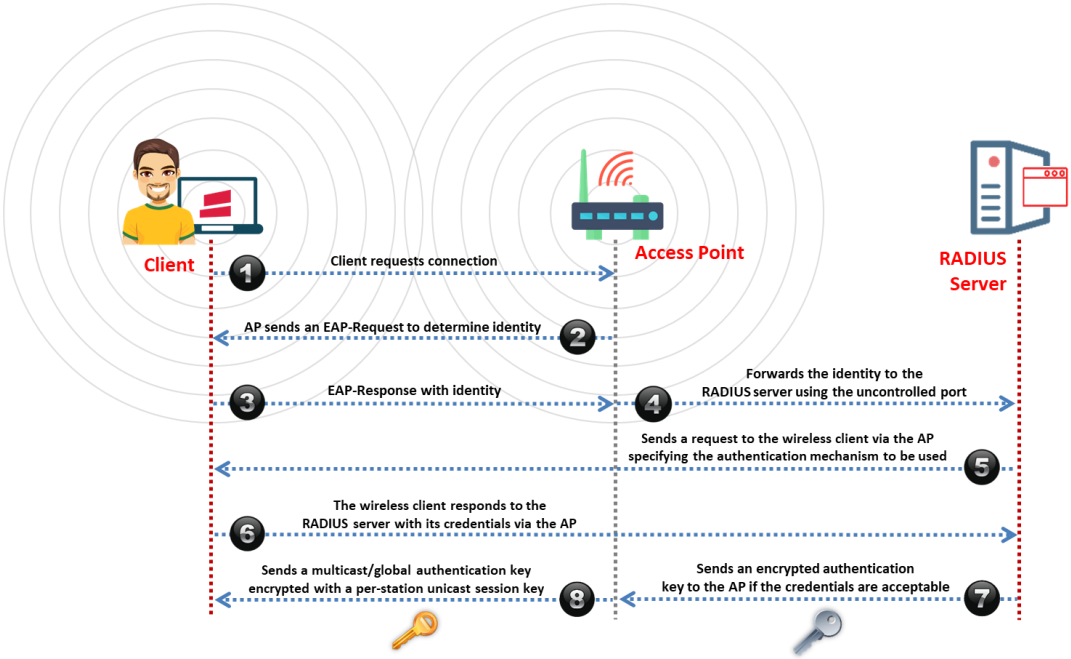
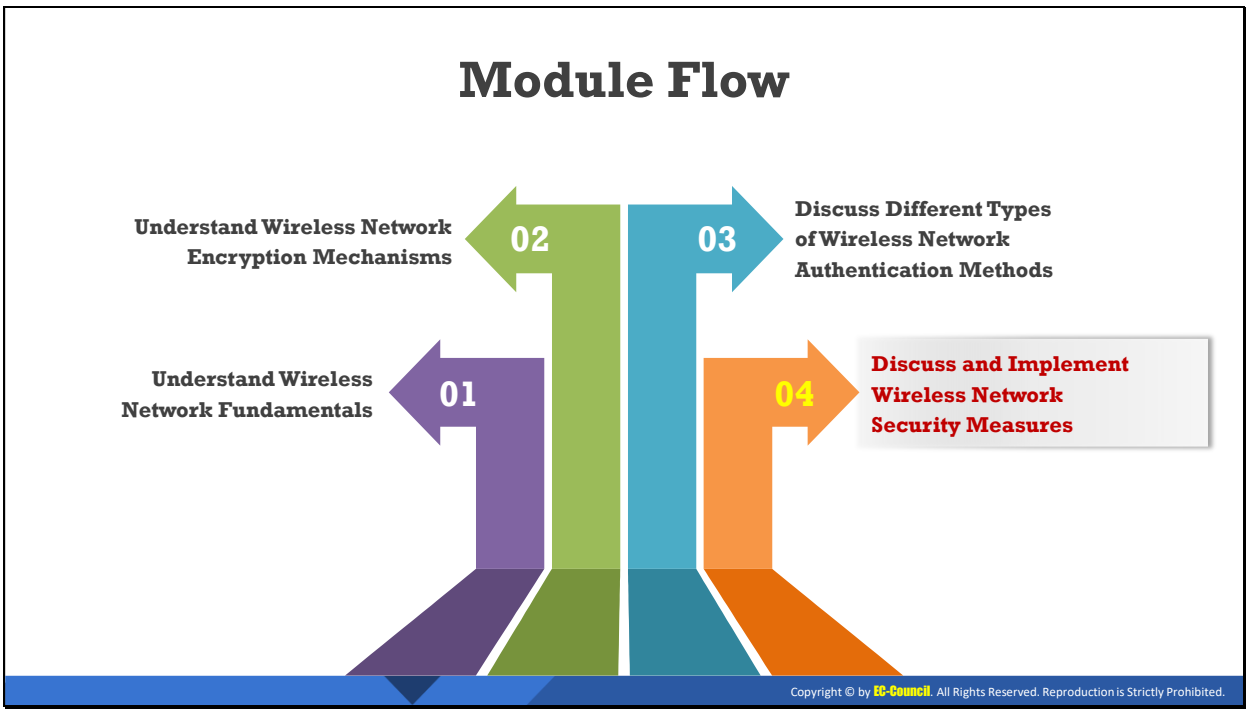


Figure 7.12: Wi-Fi authentication process using a centralized authentication server

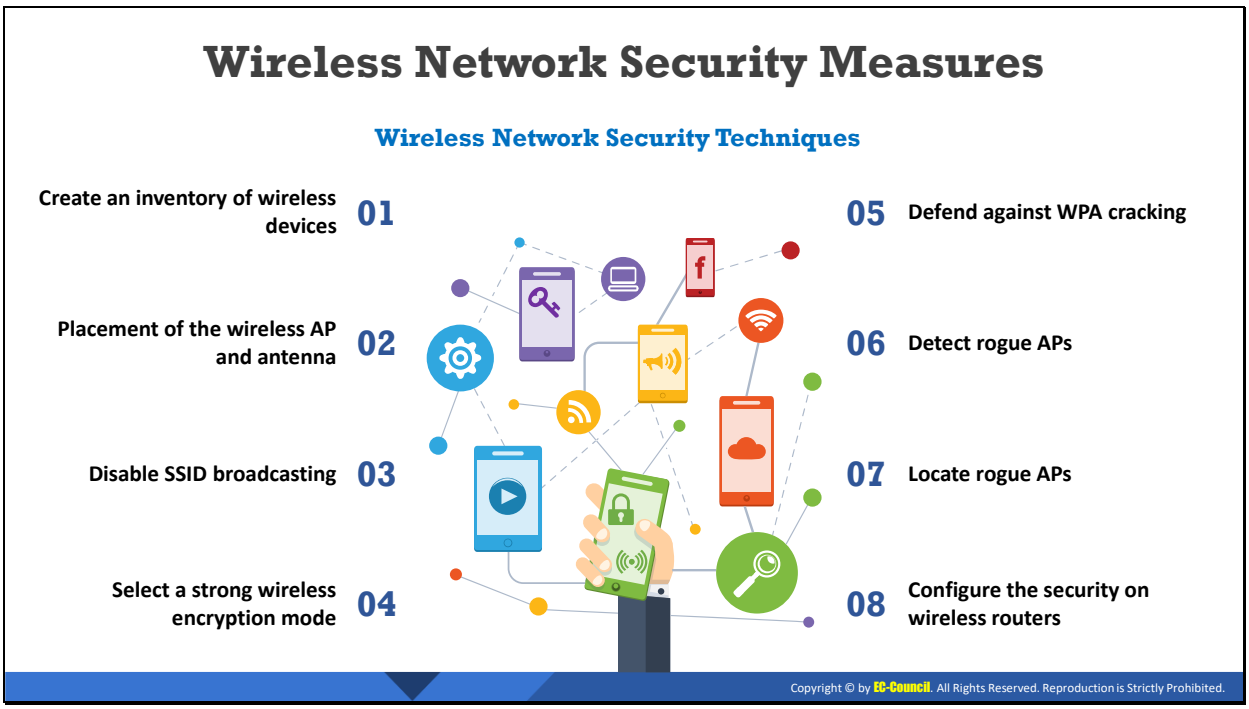
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Discuss and Implement Wireless Network Security Measures

The objective of this section is to explain the various security measures that must be implemented to secure the wireless network.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Wireless Network Security Measures

A wireless network can be insecure if proper care has not been taken while configuring it. Insecure configurations can pose a great risk to the wireless networks. Thus, a wireless network should be configured as per the wireless security policy of the organization.

The following points should be clearly stated in the organization's wireless security policy:

- Identity of the users who are using the network
- Determine whether the user is allowed access or not
- Clearly define who can and cannot install the APs and other wireless devices in the enterprise
- Describe the type of information that users are allowed to communicate over the wireless network
- Provide limitations on APs such as location, cell size, frequency, etc., in order to overcome the wireless security risks
- Clearly define the standard security settings for wireless components
- Describe the conditions in which wireless devices are allowed to use the network

Furthermore, a successful and effective wireless security implementation should involve the following:

- Centralized implementation of security measures for all wireless technology
- Security awareness and training programs for all employees

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

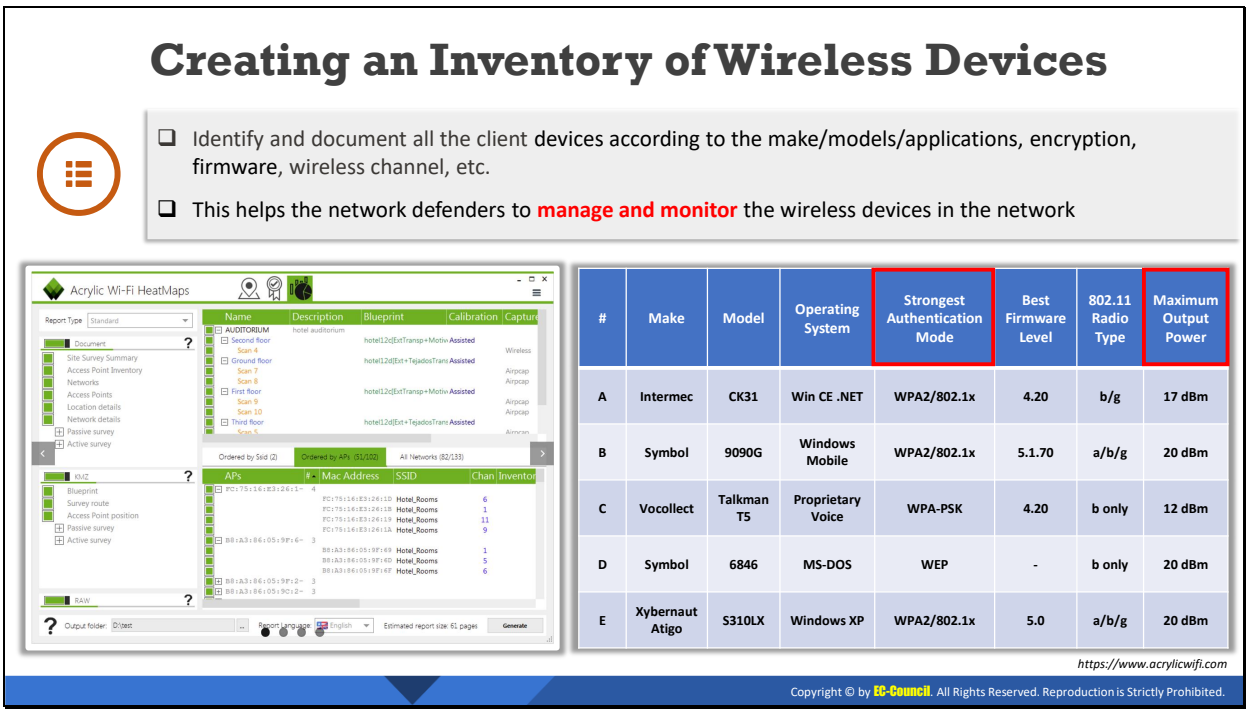
- Standardized configurations to reflect the security policies and procedures of the organization
- Configuration management and control to make sure the latest security patches and features are available on wireless devices.

The following activities help in defending and maintaining the security of a wireless network:

- Creating an inventory of the wireless devices
- Placement of the wireless AP and antenna
- Disable SSID broadcasting
- Selecting a strong wireless encryption mode
- Defending against WPA cracking
- Detecting rogue APs
- Locating rogue access points
- Configuring the security on wireless routers

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



#	Make	Model	Operating System	Strongest Authentication Mode	Best Firmware Level	802.11 Radio Type	Maximum Output Power
A	Intermec	CK31	Win CE .NET	WPA2/802.1x	4.20	b/g	17 dBm
B	Symbol	9090G	Windows Mobile	WPA2/802.1x	5.1.70	a/b/g	20 dBm
C	Vocollect	Talkman T5	Proprietary Voice	WPA-PSK	4.20	b only	12 dBm
D	Symbol	6846	MS-DOS	WEP	-	b only	20 dBm
E	Xybernaut Atigo	S310LX	Windows XP	WPA2/802.1x	5.0	a/b/g	20 dBm

Creating an Inventory of Wireless Devices

The use of wireless devices in various organizations is continuously growing. Therefore, it becomes increasingly important for organizations to track and manage their wireless assets for security purposes. Maintaining an accurate and up-to-date inventory of wireless devices is required for proper security.

A network device inventory helps in consolidating all the updated network data and devices. The inventory can help in quickly identifying the non-functioning devices as well as rogue network devices that are present on the network. A list of devices that are not connected to the network should also be added to the list. This helps in detecting unknown devices in the network. A regular scanning of the inventory is important. Through scanning, the administrators can determine the rogue network devices, problematic devices, potential vulnerabilities, devices that need a patch/update, etc., in a network. A network is only as secure as its weakest link. Information about all the devices should be maintained regardless of their configuration settings or the vendor.

An inventory should be maintained either manually or with the help of an effective inventory tracking solution. At times, an inventory tool may not auto-update the network device. In such scenarios, information of a device should be manually added in the inventory list.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

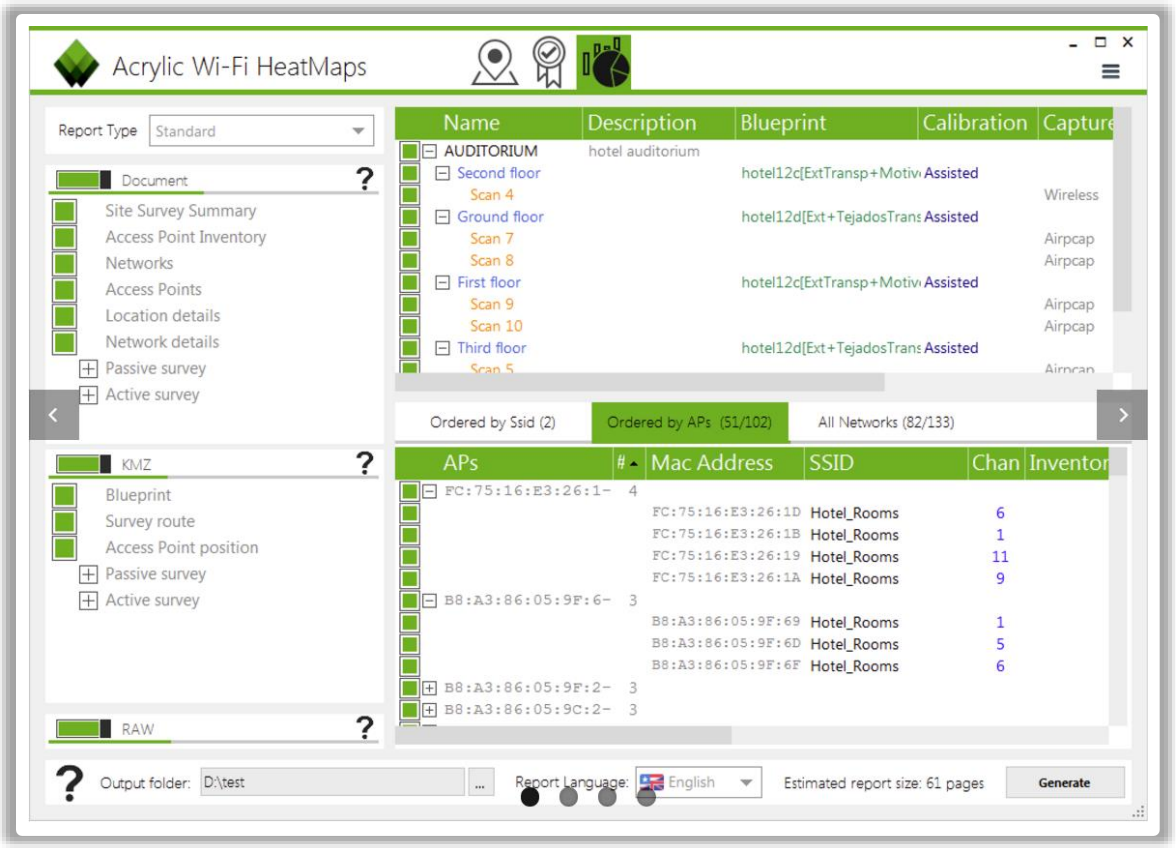
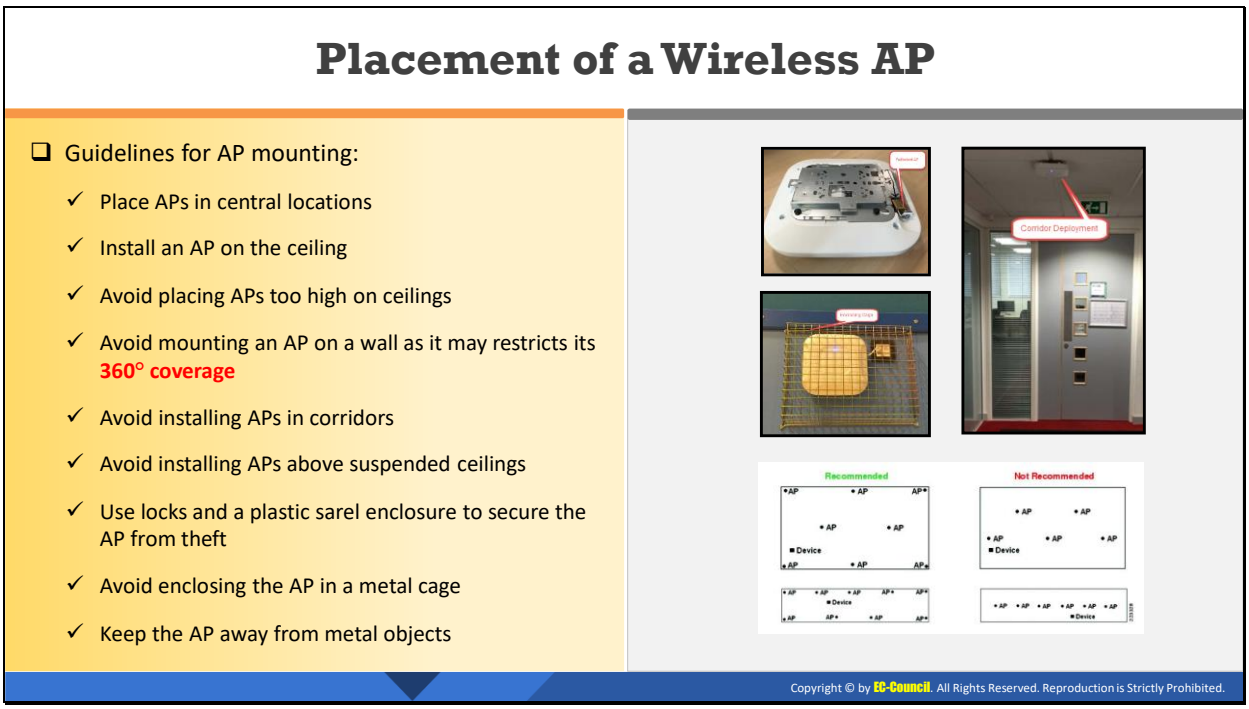


Figure 7.13: Screenshot of Acrylic Wi-Fi HeatMaps

#	Make	Model	Operating System	Strongest Authentication Mode	Best Firmware Level	802.11 Radio Type	Maximum Output Power
A	Intermec	CK31	Win CE .NET	WPA2/802.1x	4.20	b/g	17 dBm
B	Symbol	9090G	Windows Mobile	WPA2/802.1x	5.1.70	a/b/g	20 dBm
C	Vocollect	Talkman T5	Proprietary Voice	WPA-PSK	4.20	b only	12 dBm
D	Symbol	6846	MS-DOS	WEP	-	b only	20 dBm
E	XybernautAtigo	S310LX	Windows XP	WPA2/802.1x	5.0	a/b/g	20 dBm

Table 7.3: Wireless device inventory

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Placement of a Wireless AP

Choosing an appropriate location for an AP is very important as it plays a vital role in achieving a high network performance, coverage, and speed. Many organizations have their APs placed across their interior spaces. Every AP requires installation at a specific location and angle since their installation at random locations will restrict the network performance. In addition, the coverage area needs to be planned wisely. Overlap is good. Care must be taken to not create dead-zones.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

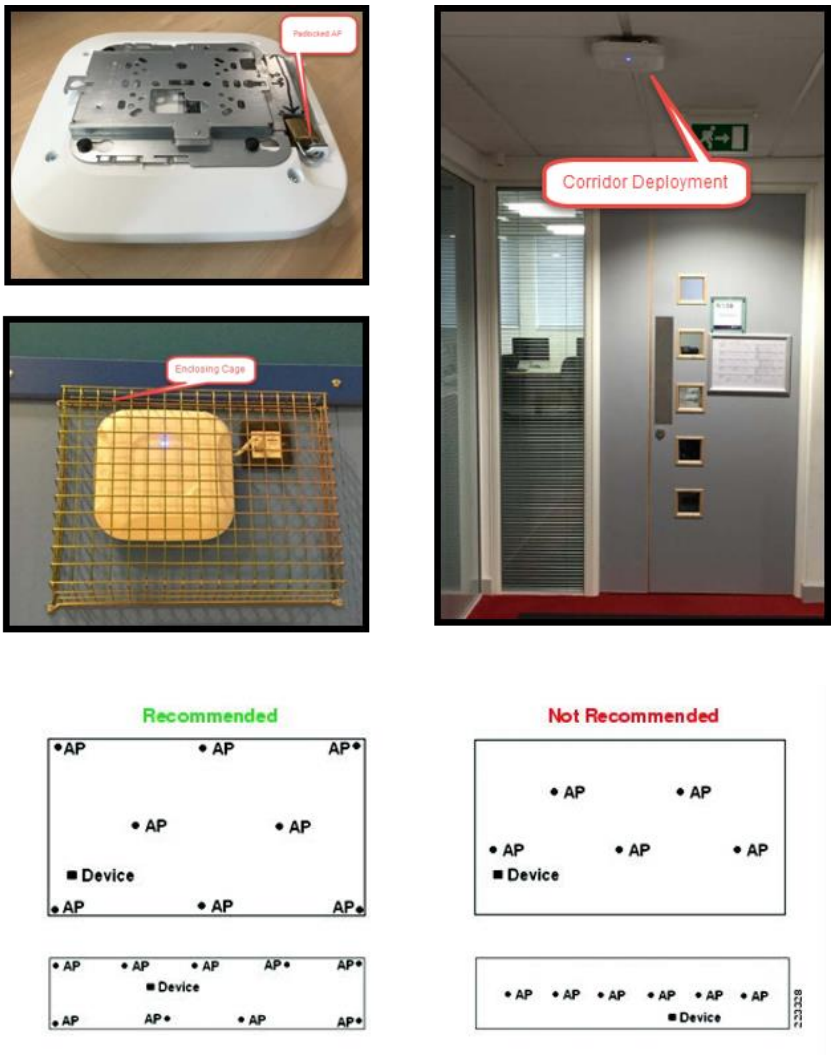
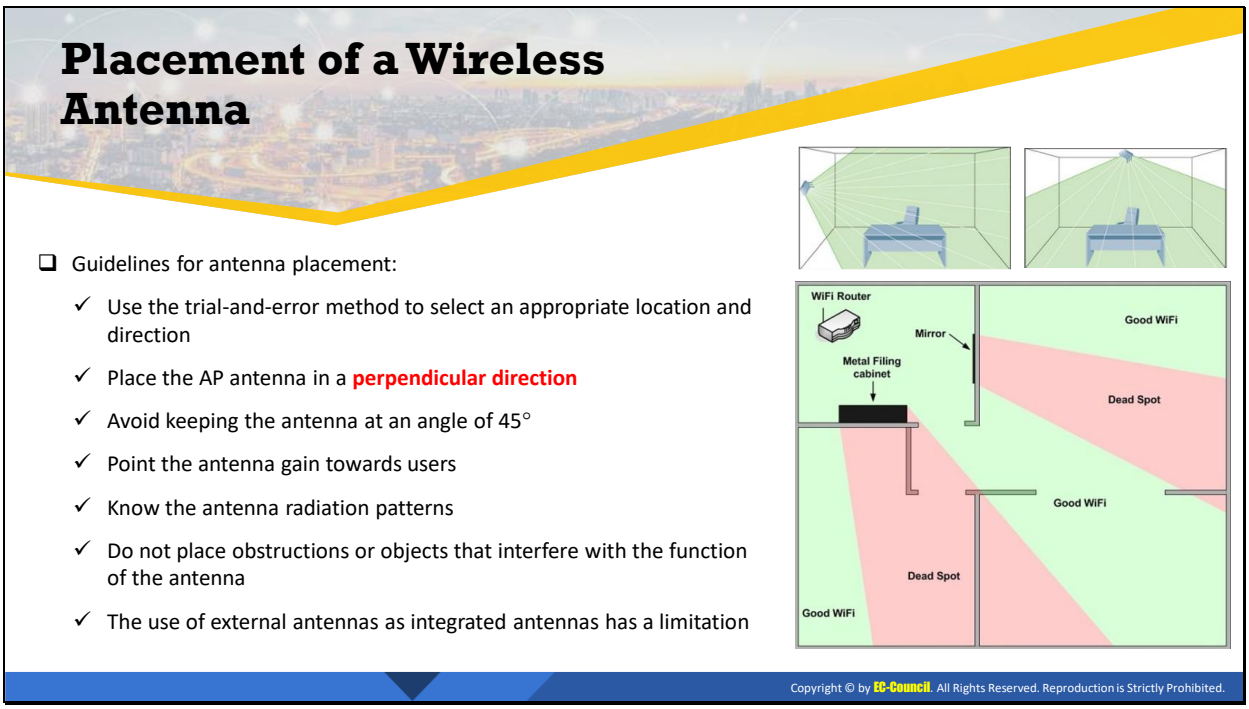


Figure 7.14: Placement of wireless AP

The following guidelines help in choosing the appropriate locations for APs and to achieve maximum coverage, performance, and speed:

- Place APs in central locations
- Install an AP on the ceiling
- Avoid placing APs too high on ceilings
- Avoid mounting an AP on a wall as it may restricts its 360° coverage
- Avoid installing APs in corridors
- Avoid installing APs above suspended ceilings
- Use locks and a plastic sarel enclosure to secure the AP from theft
- Avoid enclosing the AP in a metal cage
- Keep the AP away from metal objects

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Placement of a Wireless Antenna

Placement of an antenna depends on the type, angle, and location of the AP, and the coverage required.

Guidelines for the Placement of a Wireless Antenna

- Use the trial-and-error method to select an appropriate location and direction.
- Place the AP antenna in a perpendicular direction.
- Avoid keeping the antenna at an angle of 45°
- Point the antenna gain towards users
- Know the antenna radiation patterns
- Do not place obstructions or objects that interfere with the function of the antenna
- The use of external antennas as integrated antennas has a limitation
- Tilt the antennas downwards when installed on the ceiling
- Use omnidirectional antennas pointing downwards for attenuating the signals traveling up to the AP
- Avoid using simple dipole antennas as an optimal solution
- Use single frequency antenna elements rather than dual tuned elements

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

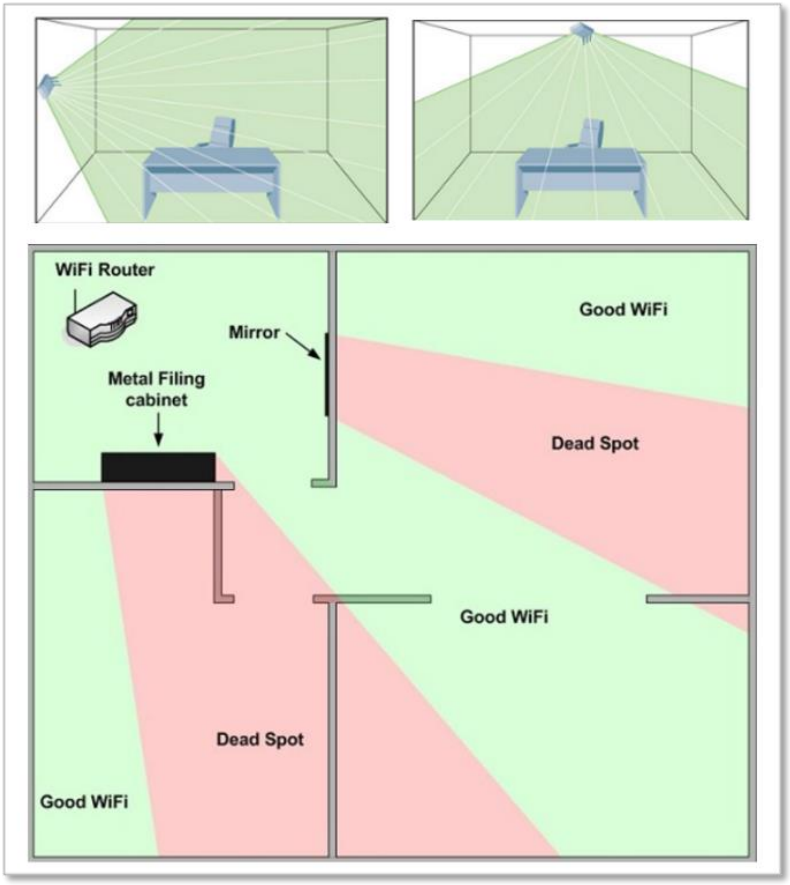
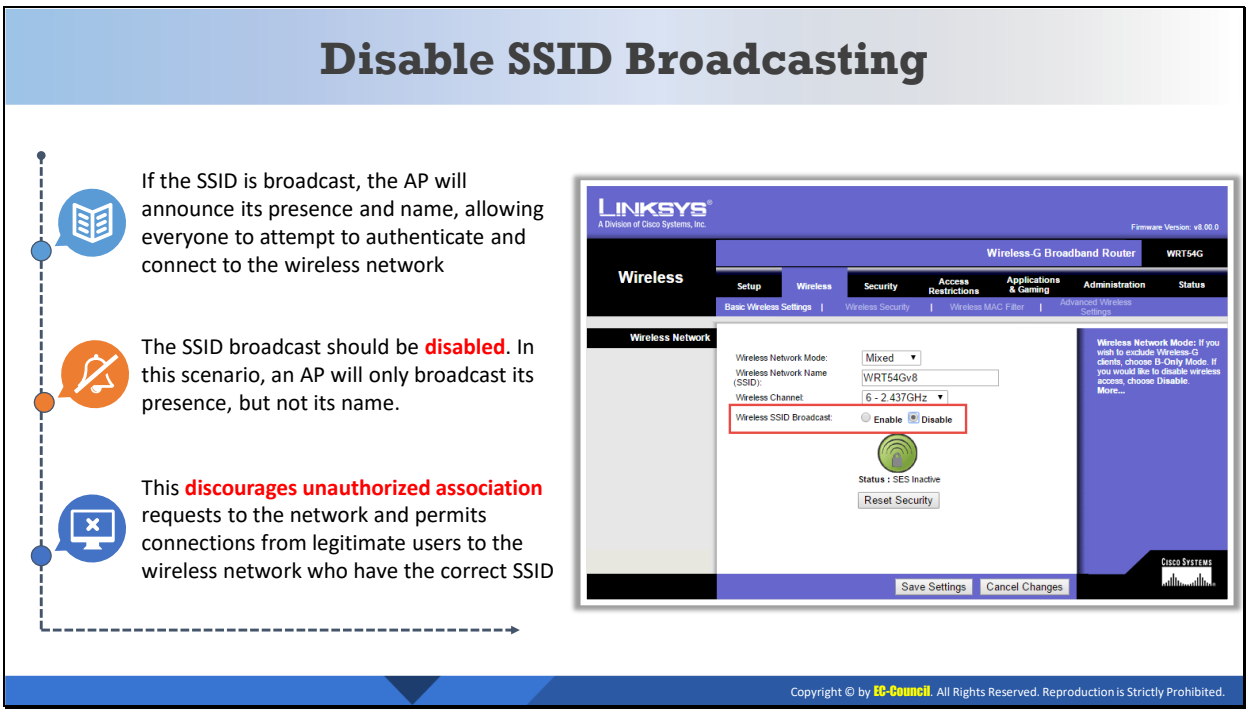


Figure 7.15: Placement of a wireless antenna

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Disable SSID Broadcasting

A wireless network SSID can either be broadcast or hidden. By broadcasting the SSID, anyone can find and access it. If the SSID is hidden, the user has to know the exact SSID in order to connect to the wireless network. Security professionals should always disable SSID broadcasting on their devices.

- **SSID Broadcast in the Enabled State**

  By enabling the SSID broadcast, the wireless router will broadcast its presence and name. When scanning for available wireless connections, if the SSID is broadcast, the name and presence of the network will be identified. It may be locked with a password, but anyone will be able to see it.

- **SSID Broadcast in the Disabled State**

  If the SSID broadcast is disabled, then the wireless router will broadcast its presence, but will not display the name. Instead "unnamed network" will be displayed as a connection present within a user's range. The user can connect to the wireless network after naming it and providing it with the correct authentication credentials.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

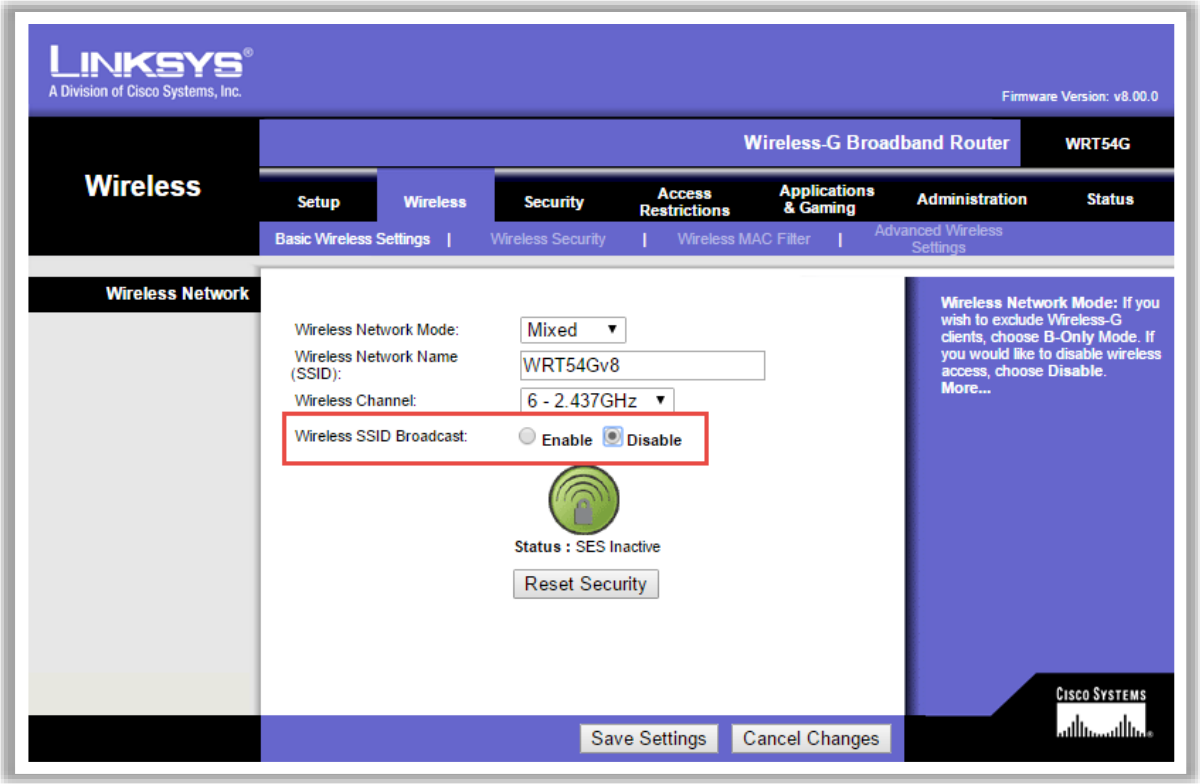
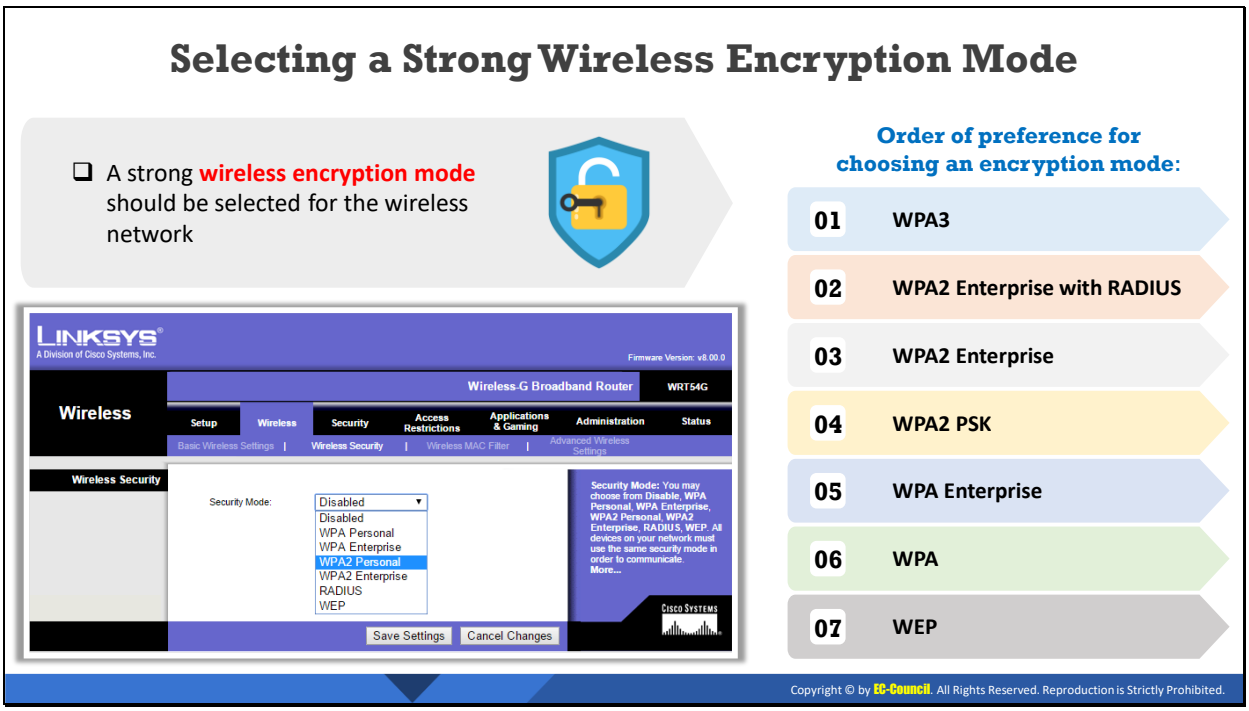


Figure 7.16: Disabling SSID broadcasting

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Selecting a Strong Wireless Encryption Mode

A strong wireless encryption mode should be used for keeping the wireless network safe from various types of attacks. There are various encryption modes that can be used for an organization's wireless network.

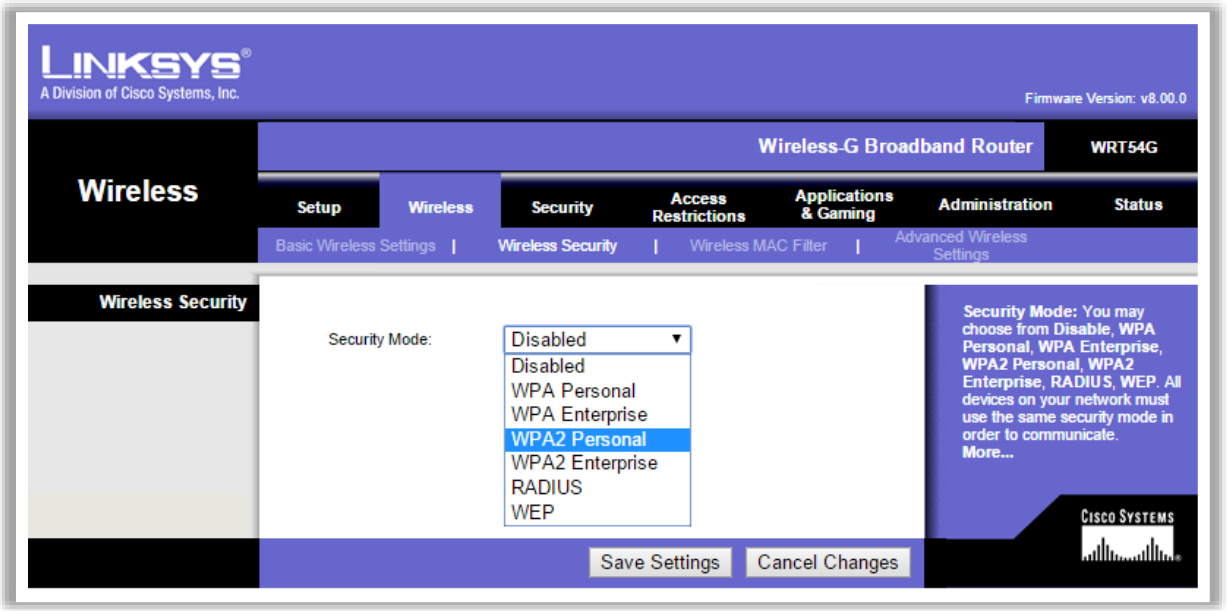


Figure 7.17: Selecting wireless encryption mode

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Order of preference for choosing an encryption mode

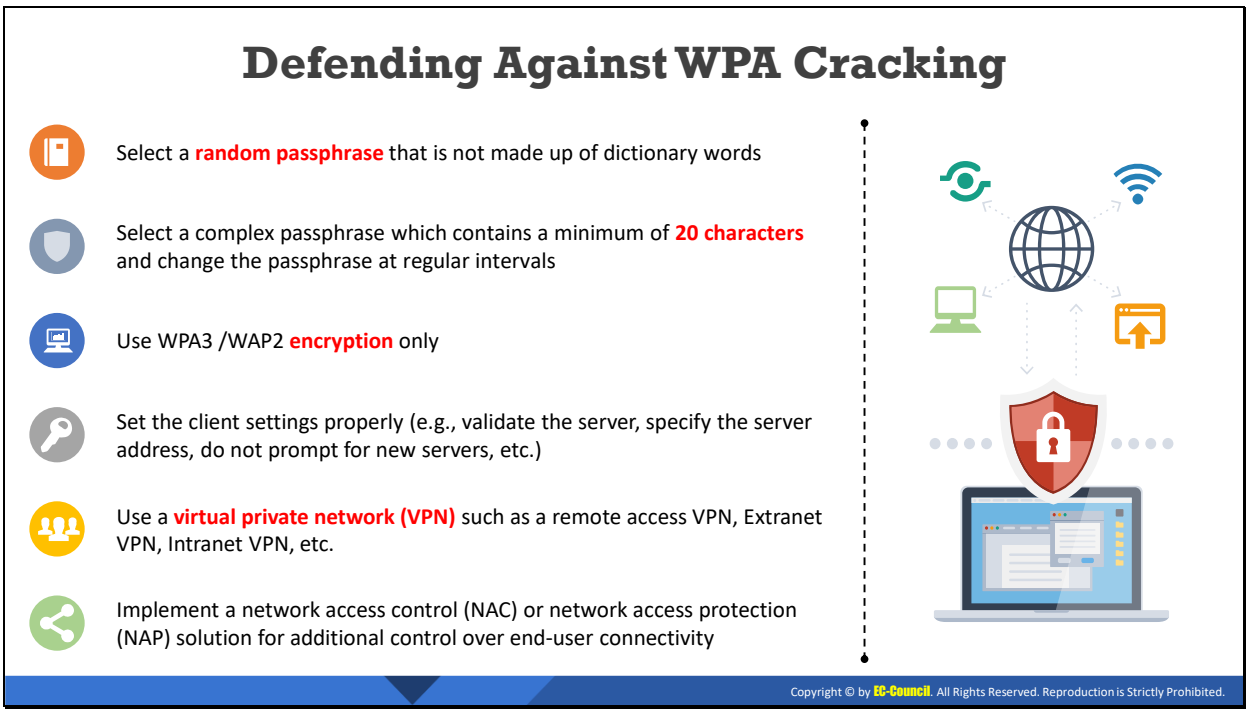
1. WPA3
2. WPA2 Enterprise with RADIUS
3. WPA2 Enterprise
4. WPA2 PSK
5. WPA Enterprise
6. WPA
7. WEP

Order of preference for choosing a Wi-Fi security method

1. WPA3
2. WPA2 + AES
3. WPA + AES
4. WPA + TKIP/AES
5. WPA + TKIP
6. WEP
7. Open Network (no security at all)

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Defending Against WPA Cracking

The only way to crack WPA is to sniff the password pairwise master key (PMK) associated with the "handshake" authentication process. If this password is extremely complicated, it might be almost impossible to crack.

The following countermeasures can help a user to defeat WPA cracking attempts:

- Select a random passphrase that is not made up of dictionary words.
- Select a complex passphrase which contains a minimum of 20 characters and change the passphrase at regular intervals
- Use WPA3 /WAP2 encryption only
- Set the client settings properly (e.g., validate the server, specify the server address, do not prompt for new servers, etc.)
- Use a virtual private network (VPN) such as a remote access VPN, Extranet VPN, Intranet VPN, etc.
- Implement a network access control (NAC) or network access protection (NAP) solution for additional control over end-user connectivity
- Do not use words from the dictionary.
- Do not use words with numbers appended at the end.
- Do not use double words or simple letter substitution such as p@55w0rd.
- Do not use common sequences from your keyboard such as qwerty.
- Do not use common numerical sequences.
- Avoid using personal information in the key/password.

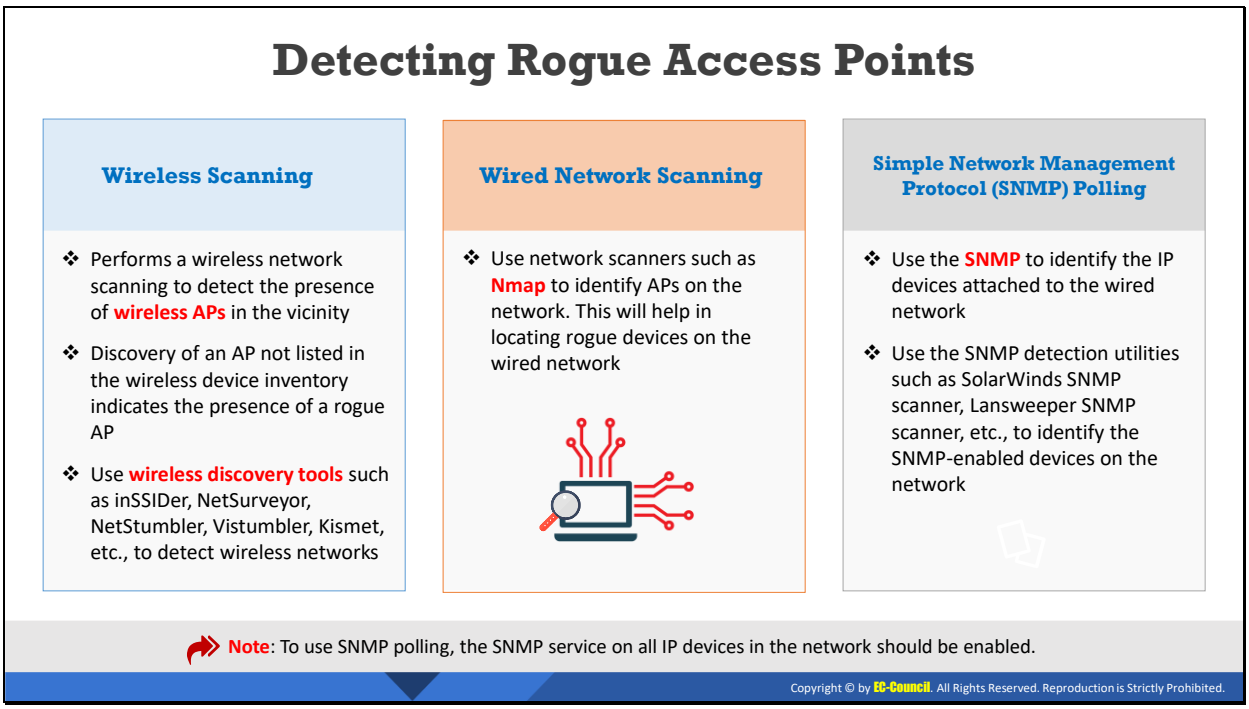
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

A WPA password should be constructed according to the following rules:

- It should have a random passphrase.
- It should have at least 12 characters in length.
- It should contain at least one uppercase letter.
- It should contain at least one lowercase letter.
- It should contain at least one special character such as @ or !
- It should contain at least one number.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Detecting Rogue Access Points

A wireless AP is termed as a rogue AP when it is installed on a trusted network without authorization. An inside or outside attacker can install rogue APs on a trusted network for their malicious intent.

Types of Rogue APs

1. Wireless router connected via a "trusted" interface
2. Wireless router connected via an "untrusted" interface
3. Installing a wireless card into a device that is already on a trusted LAN
4. Enabling wireless on a device that is already on a trusted LAN

The methods mentioned below should be used for detecting wireless networks in the vicinity of the network and the detected wireless APs should be compared with the wireless device inventory for the environment. If an AP that is not listed in the inventory is found, it can generally be considered as a rogue AP.

- **Wireless scanning:** It performs an active wireless network scanning to detect the presence of wireless APs in the vicinity. It helps in detecting unauthorized or hidden wireless APs that can be malicious. Discovery of an AP not listed in the wireless device inventory indicates the presence of a rogue AP. You can use wireless discovery tools such as inSSIDer, NetSurveyor, NetStumbler, Vistumbler, Kismet, etc., to detect wireless networks.
- **Wired network scanning:** Wired network scanners such as Nmap are used for identifying a large number of devices on a network by sending specially crafted TCP

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

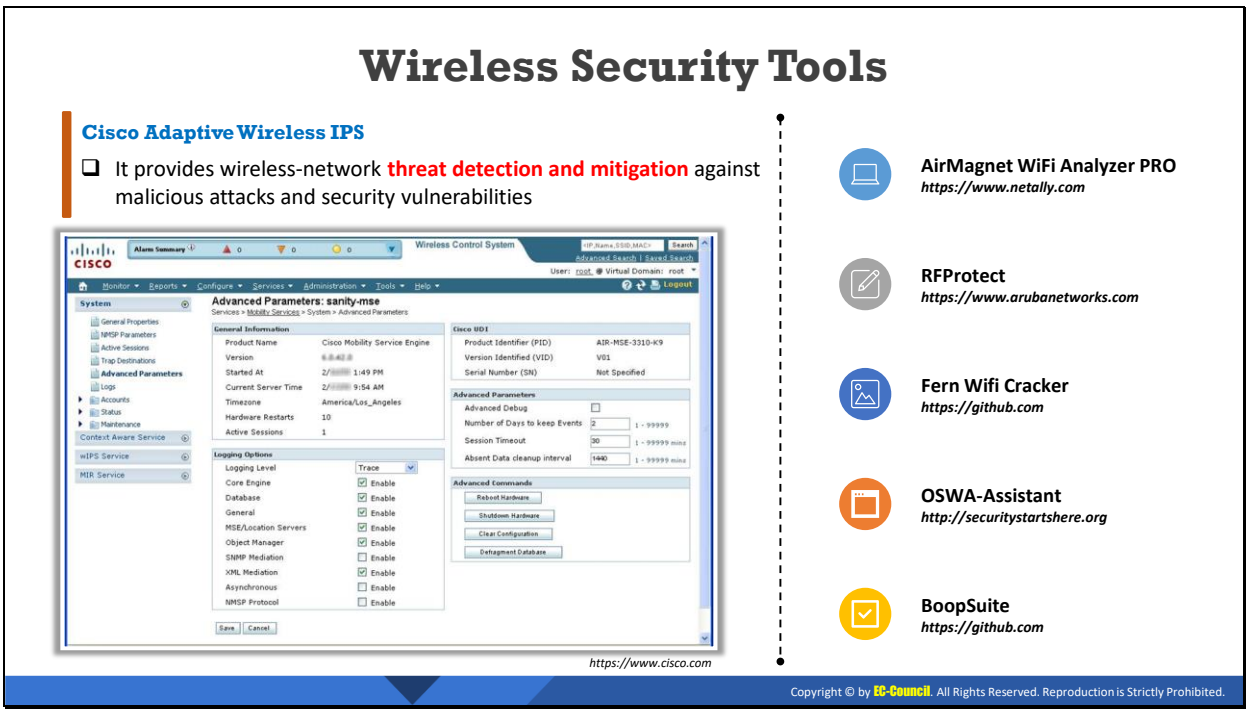
packets to the device (Nmap-TCP fingerprinting). It helps locate rogue APs attached to a wired network.

- **Simple Network Management Protocol (SNMP) polling:** Simple network management protocol (SNMP) polling is used for identifying the IP devices attached to a wired network. SNMP detection utilities such as SolarWinds SNMP Scanner, Lansweeper, etc., can be used for identifying SNMP enabled devices on the network.

Note: To use SNMP polling, the SNMP service on all IP devices in the network should be enabled.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Wireless Security Tools

- **Cisco Adaptive Wireless IPS**

  Source: *https://www.cisco.com*

  Cisco Adaptive Wireless Intrusion Prevention System (IPS) offers advanced network security for dedicated monitoring and detection of wireless network anomalies, unauthorized access, and RF attacks. Fully integrated with the Cisco Unified Wireless Network, this solution delivers integrated visibility and control across the network, without the need for an overlay solution. Adaptive WIPS provides wireless-network threat detection and mitigation against malicious attacks and security vulnerabilities. It also provides security professionals with the ability to detect, analyze, and identify wireless threats.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

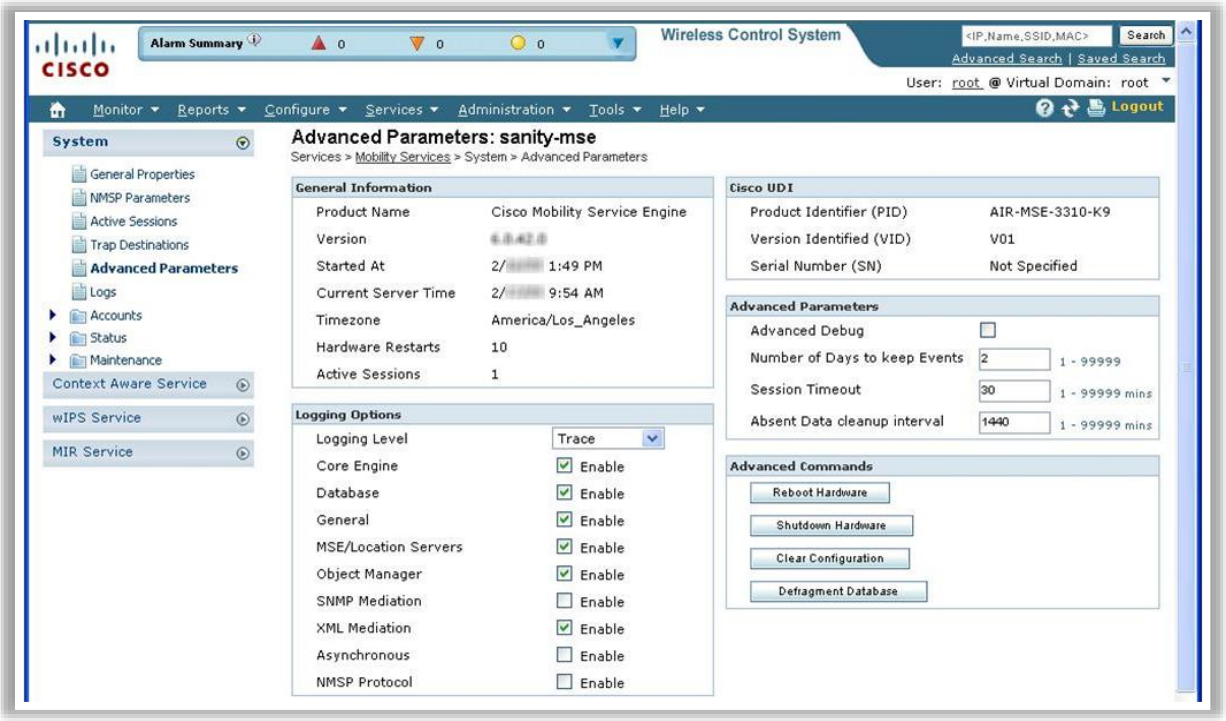
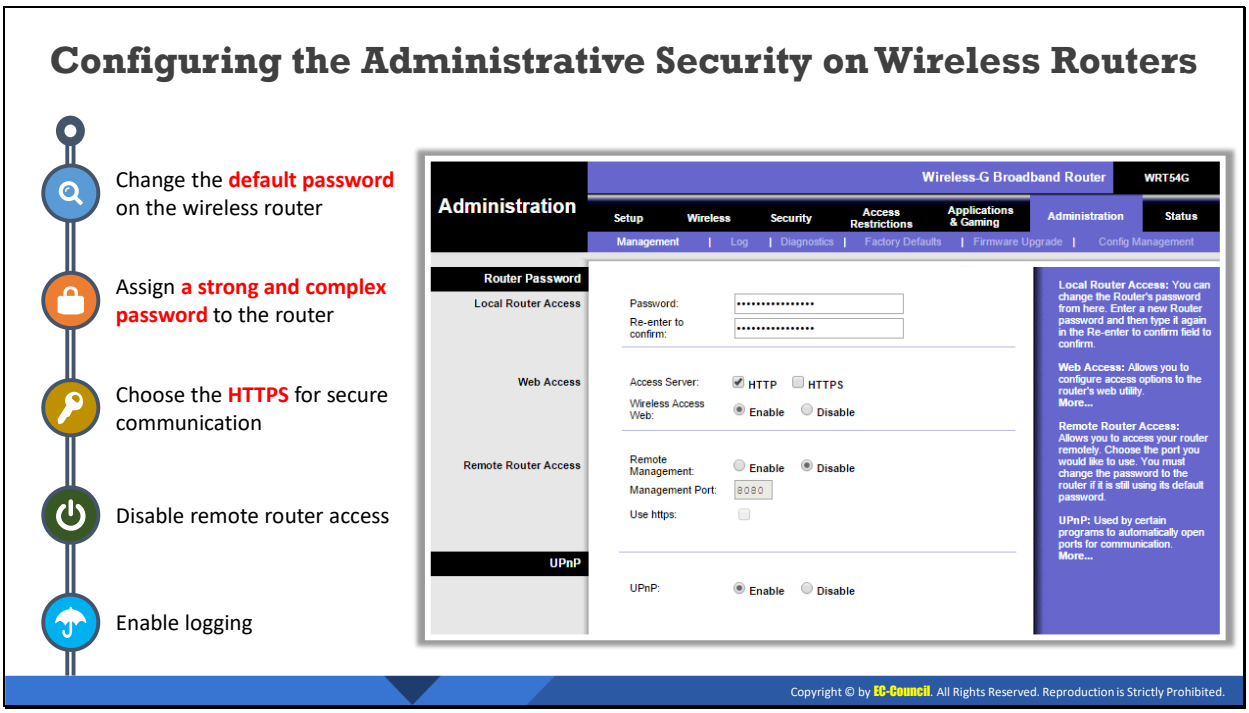


Figure 7.18: Screenshot of Cisco Adaptive Wireless IPS

The following are some additional Wi-Fi security auditing tools:

- AirMagnet WiFi Analyzer PRO (*https://www.netally.com*)
- RFProtect (*https://www.arubanetworks.com*)
- Fern Wifi Cracker (*https://github.com*)
- OSWA-Assistant (*http://securitystartshere.org*)
- BoopSuite (*https://github.com*)

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Configuring the Administrative Security on Wireless Routers

In order to harden the wireless router, the recommended security configurations should be applied on the wireless router. These security configuration settings help minimize any wireless attacks and provide the best performance, security, and reliability when using Wi-Fi.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

The following are the security recommendations that must be considered:

1. Changing the default password of the wireless router
2. Assigning a strong and complex password to the router
3. Choosing the hypertext transfer protocol secure (HTTPS) for secure communication
4. Disabling the remote router access
5. Enabling the firewall to block certain WAN requests
6. Configuring an internet access policy
7. Specifying the blocked services, URL, keywords, etc.
8. Disabling the demilitarized zone (DMZ) option
9. Configuring the QoS settings
10. Avoid using the default IP ranges
11. Keep the router firmware up-to-date

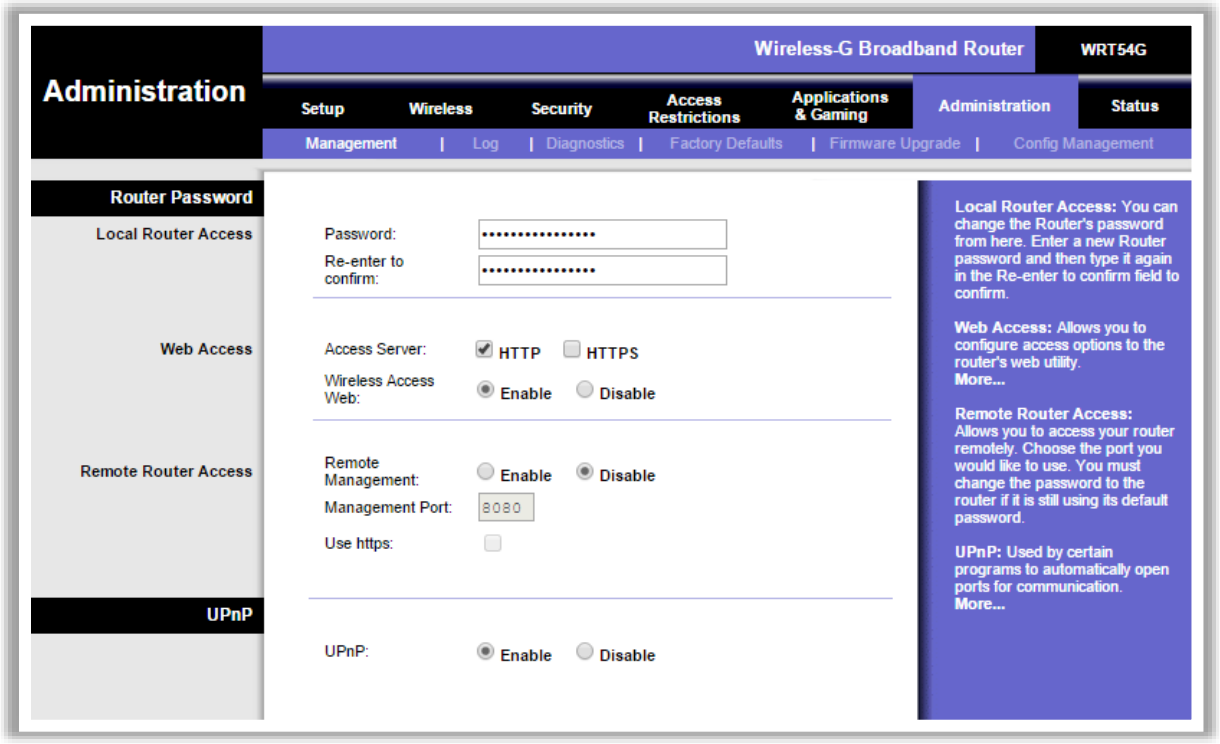


Figure 7.19: Strong password

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

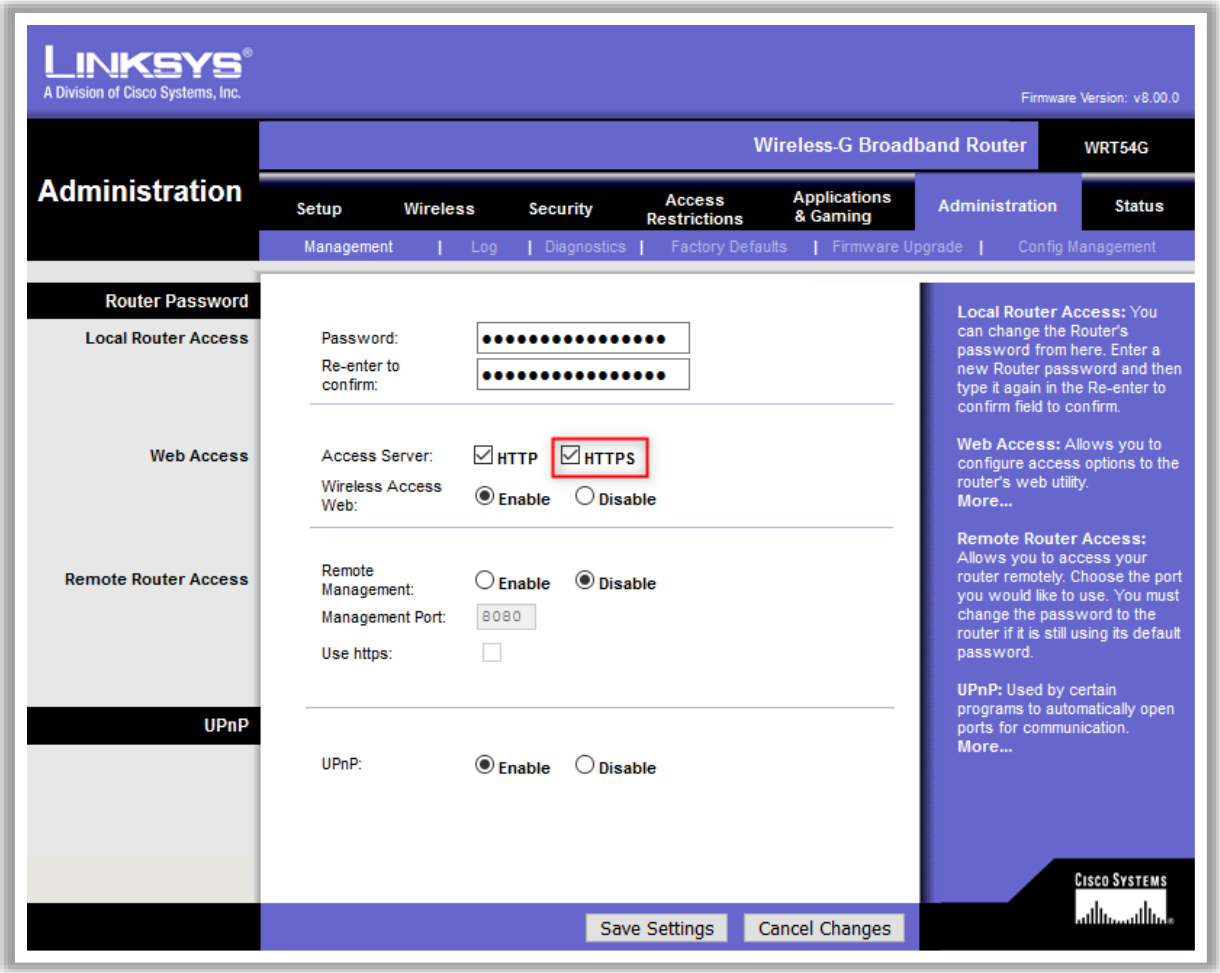


Figure 7.20: Enabling HTTPS

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

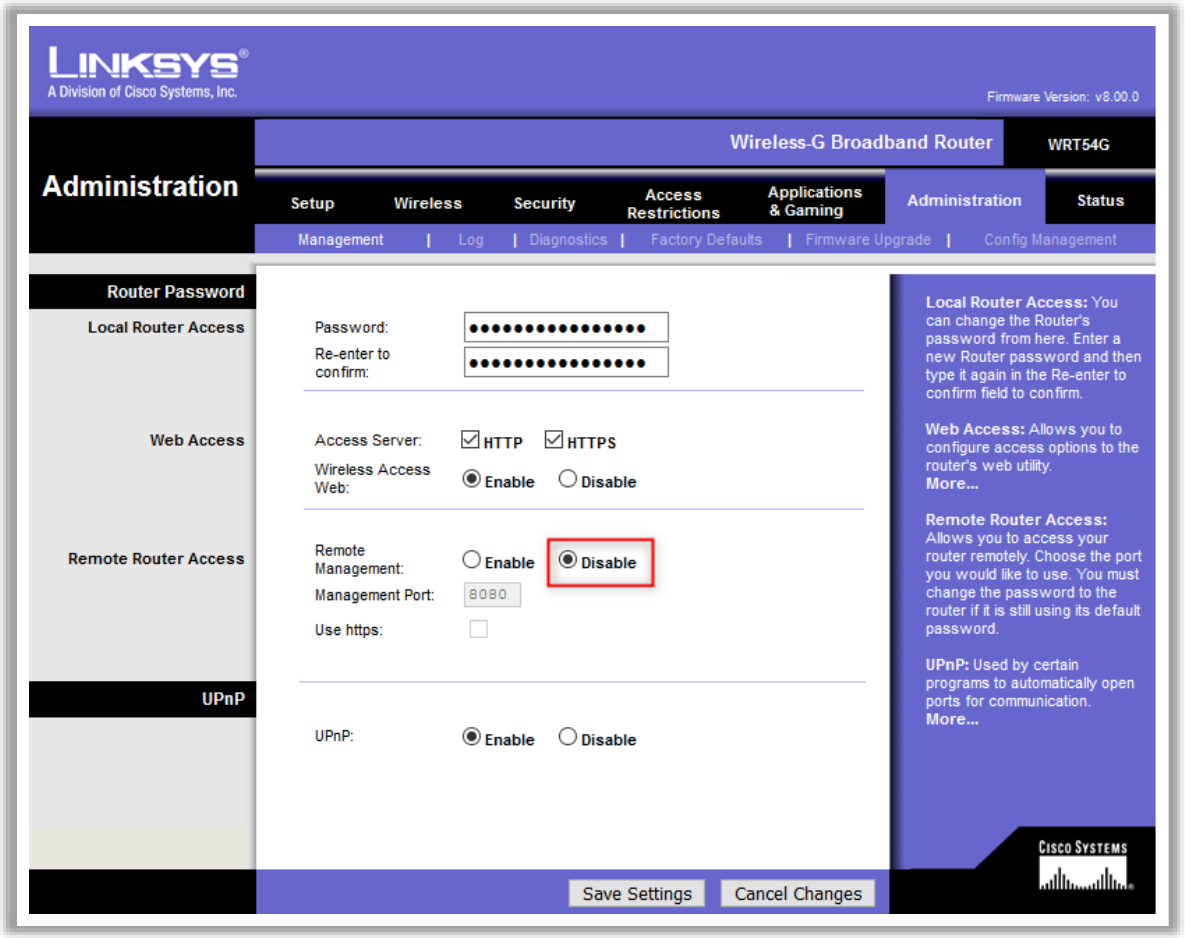


Figure 7.21: Disabling remote router access

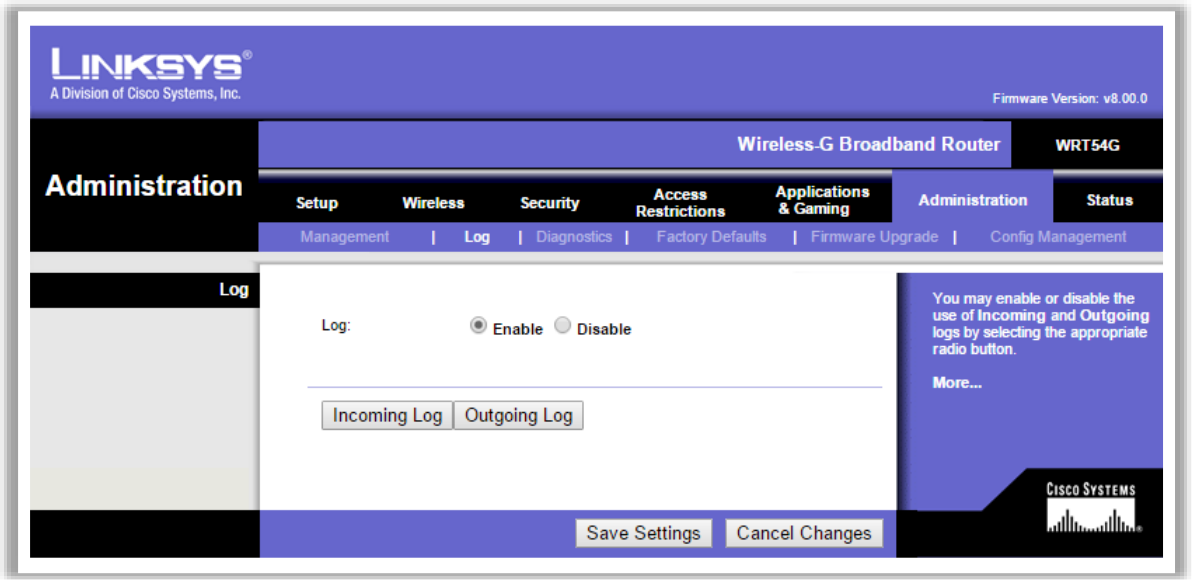
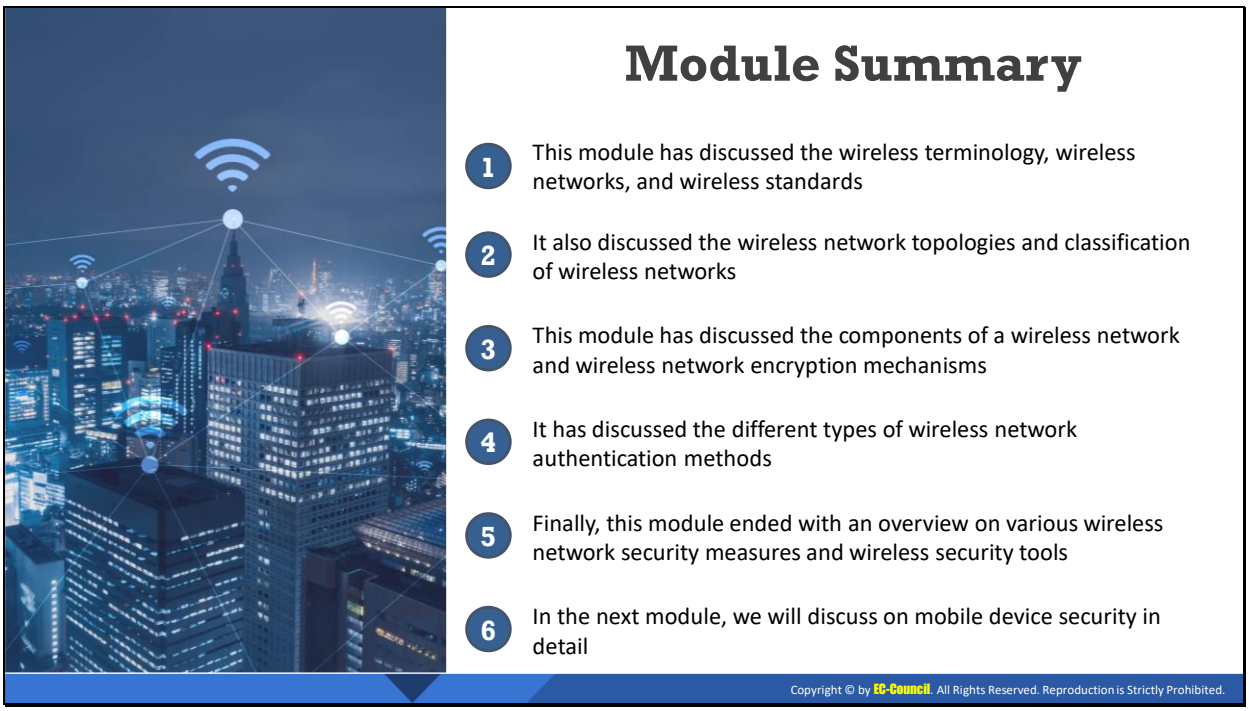


Figure 7.22: Enable logging

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Module Summary

This module discussed wireless terminology, wireless networks, and wireless standards. It also discussed the wireless network topologies and classification of wireless networks. Furthermore, this module explained the components of a wireless network and various wireless network encryption mechanisms. Moreover, it discussed the different types of wireless network authentication methods. Finally, this module presented an overview on various wireless network security measures and wireless security tools.

In the next module, we will discuss mobile device security in detail.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

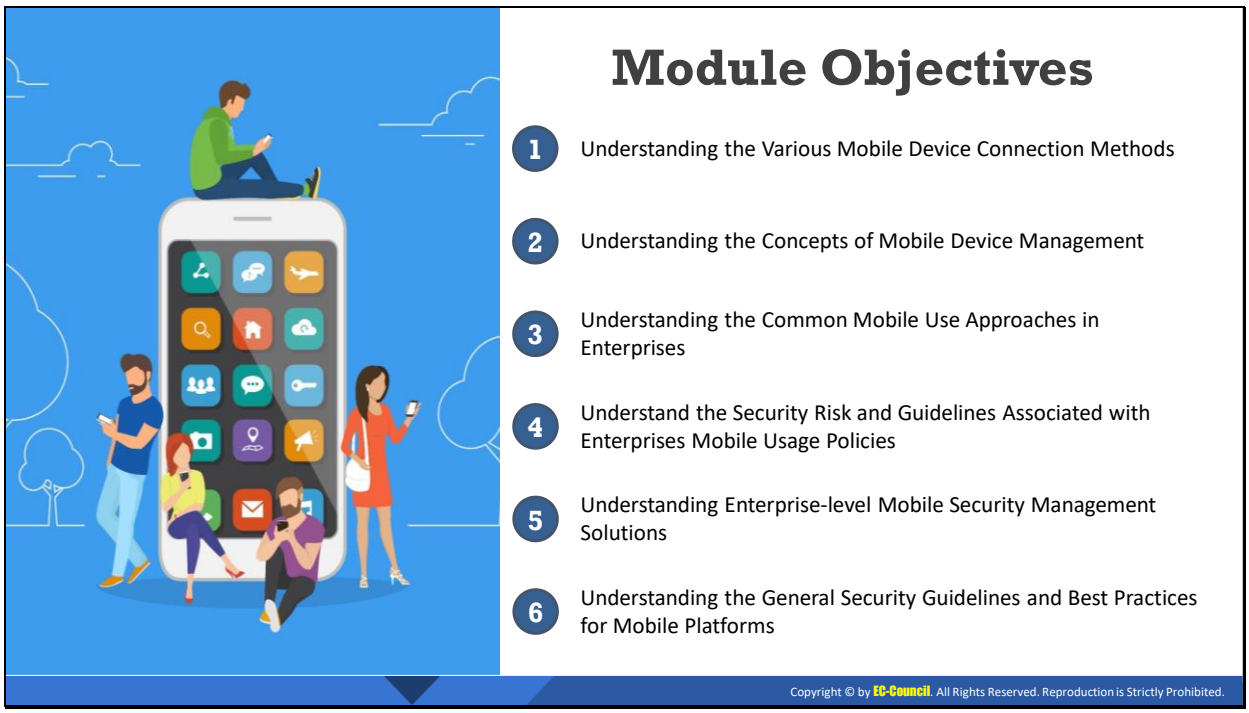
EC-Council

N|DE
Network Defense Essentials

Module 08

Mobile Device Security

https://t.me/learningnets



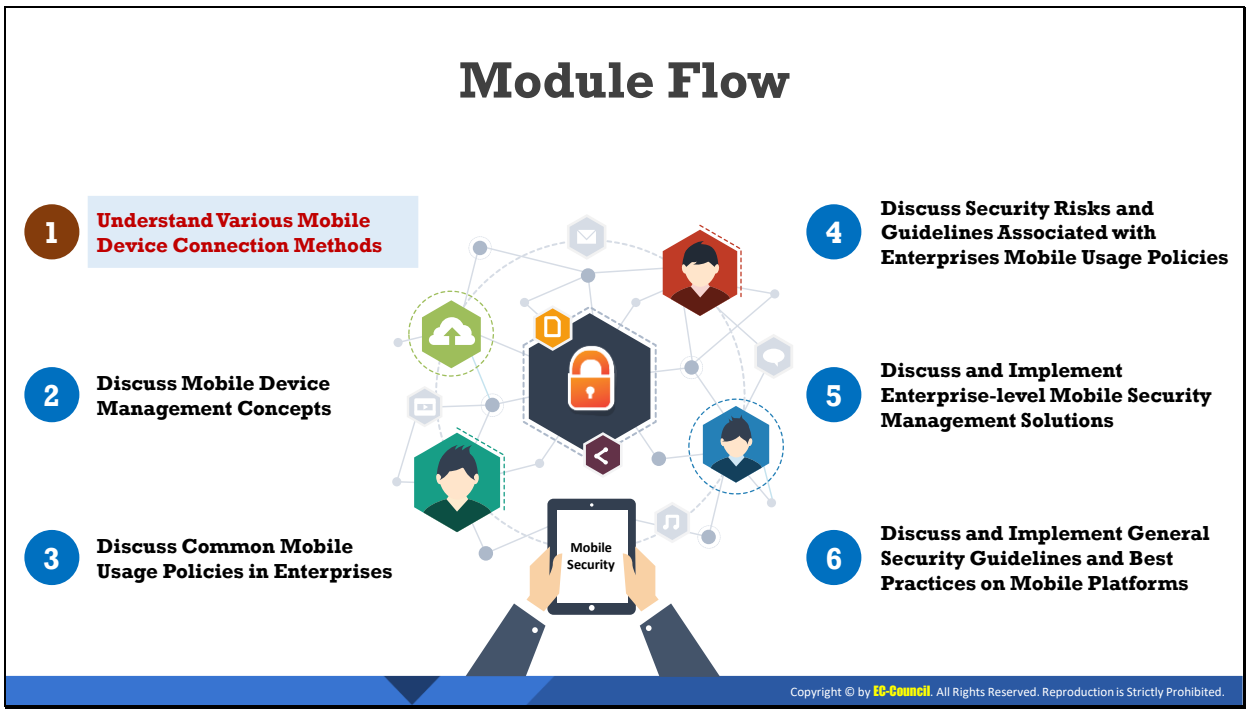
Module Objectives

With the introduction of mobile phones in enterprises, enterprise security has become more complex. Enterprise mobile security has become a major challenge for organizations. Therefore, it is important for organizations to address these security concerns to effectively manage the security of mobile devices.

At the end of this module, you will be able to do the following:

- Understand the various mobile device connection methods
- Understand the concepts of mobile device management
- Understand the common mobile use approaches in enterprises
- Understand the security risk and guidelines associated with enterprise mobile usage policies
- Understand enterprise-level mobile security management solutions
- Explain the general security guidelines and best practices for mobile platforms

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

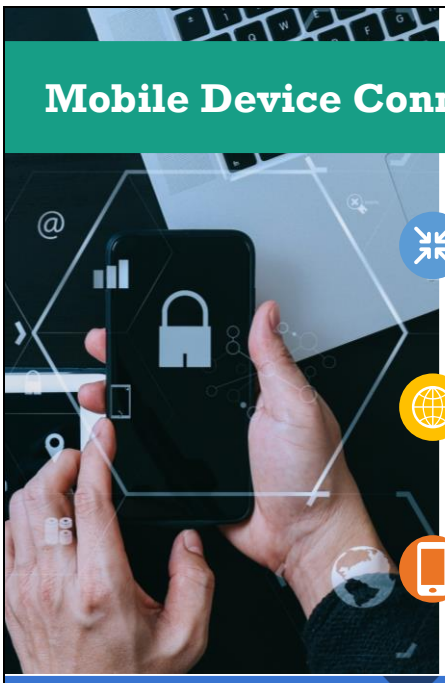


Understand Various Mobile Device Connection Methods

To secure mobile devices from various cyber-attacks, security professionals should be aware of different connection methods involved in mobile communications. They should also understand how devices gain access to the network and share their resources with other devices. There are many ways in which mobile networks can be connected; therefore, it is important for security professionals to be aware of the security concerns associated with each connection method and how to protect mobile networks from malicious intents. This section discusses various mobile device connection methods.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Mobile Device Connection Methods



Near-field Communication (NFC)

- It employs **electromagnetic induction** to enable communication between the devices connected within 10 cm

Satellite Communication (Satcom)

- It is an **artificial geostationary satellite** that provides services across the globe, but it is much slower and more expensive than other technologies

Cellular Communication

- It is based on a **single network tower** that serves devices located within a specific radius

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Device Connection Methods (Cont'd)

ANT

It is a **wireless sensor protocol** that enables communication between sensors and their controllers

Universal Serial Bus (USB)

It enables **wired communication** for devices. It can be used for power supply and serial data transmission between devices

Global Positioning System (GPS)

It is a **radio navigation** and **positioning system** based on satellite communication. It provides information related to geolocation and timing irrespective of weather conditions on the Earth

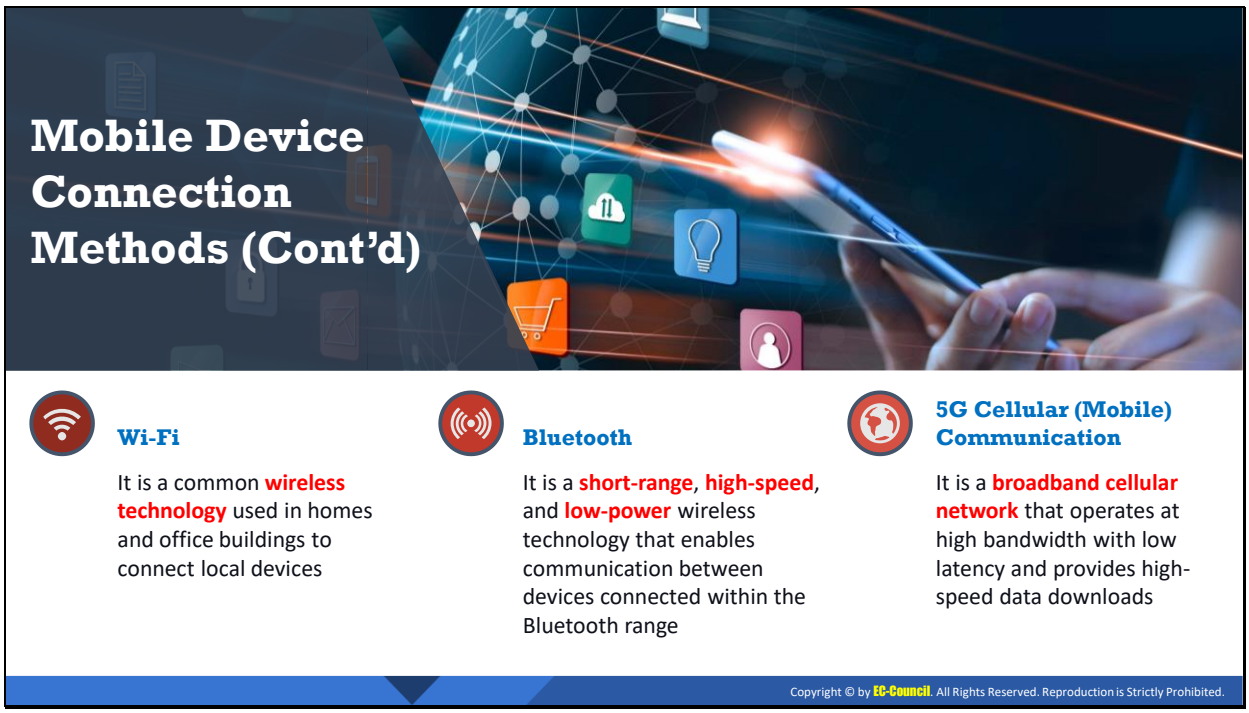
Infrared (IR)

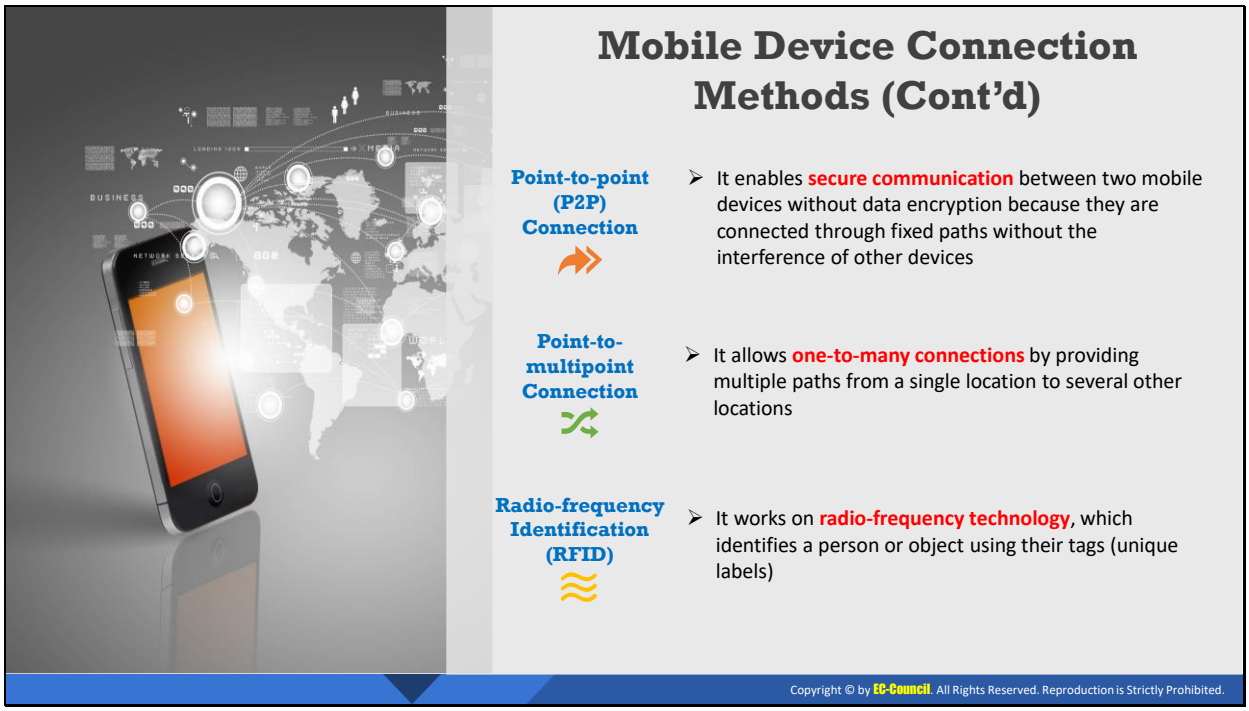
It is a wireless technology for transferring data between two devices in the digital form within a **short range** of up to 5 m

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets





Mobile Device Connection Methods

The following are some commonly used mobile connection methods.

- **Near-field communication (NFC):** NFC covers very short distances. It employs electromagnetic induction to enable communication between devices connected within 10 cm. Although it allows a very narrow range of communication, an attacker with a specialized antenna can intercept and capture the data by jamming the traffic. This

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

security issue may result from the improper configuration of NFC and non-encrypted data transmission.

- **Satellite communication (Satcom):** Satcom is an artificial geostationary satellite that provides services across the globe, but it is much slower and more expensive than other technologies. There are many technologies that utilize satellite technology; some employ a connection to geostationary satellites, while others connect to satellites that revolve around the Earth in a low orbit, through which voice and data can be transmitted. The technology also has security concerns such as remote code execution and OS vulnerabilities.
- **Cellular communication:** Cellular communication is based on a single network tower that serves devices located within a specific radius. They are installed in urban, suburban, and rural areas and cover a large distance. Mobile devices contain built-in antennas, which enable the device to communicate via a cellular network. Security concerns with cellular networks include location tracking, traffic monitoring, denial-of-service (DoS) attacks, channel jamming attacks, and illegitimate access.
- **ANT:** ANT is a wireless sensor protocol that enables communication between sensors and their controllers. This technology is used in Internet of Things (IoT) devices such as heart-rate or fitness monitoring equipment. It is not a Bluetooth or 802.11 wireless technology and has its own set of protocols developed for low-powered devices. It is susceptible to DoS or jamming attacks, and attackers can capture data in transit.
- **Universal Serial Bus (USB):** USB enables wired communication for devices. It can be used for power supply and serial data transmission between devices. It is also designed to enable hot-swapping and improve plug-and-play features. USB ports are commonly used in mobile devices for both data transmission and power supply. It is relatively more secure than other connection methods, but disgruntled employees can use a USB device to exfiltrate data from the organization's local network.
- **Global Positioning System (GPS):** GPS is a radio navigation and positioning system based on satellite communication. It provides information related to geolocation and timing irrespective of weather conditions on the Earth. Devices do not need to pass any data to satellites to establish a GPS connection; they only need to receive the signals from four or more satellites out of 28 to estimate their location. Security concerns with this technology include the fact that GPS signals can be intercepted and tampered with using specially designed GPS jammers.
- **Infrared (IR):** IR is a wireless technology for transferring data between two devices in the digital form within a short range of up to 5 m. It works only when there is no physical blockage or obstacle between the two devices. It is a type of networking feature integrated within devices such as tablets and smartphones that allows them to manage infrared devices. It can also be used to transfer files between devices. Any device with infrared accessibility can be managed using the infrared feature of a mobile device.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

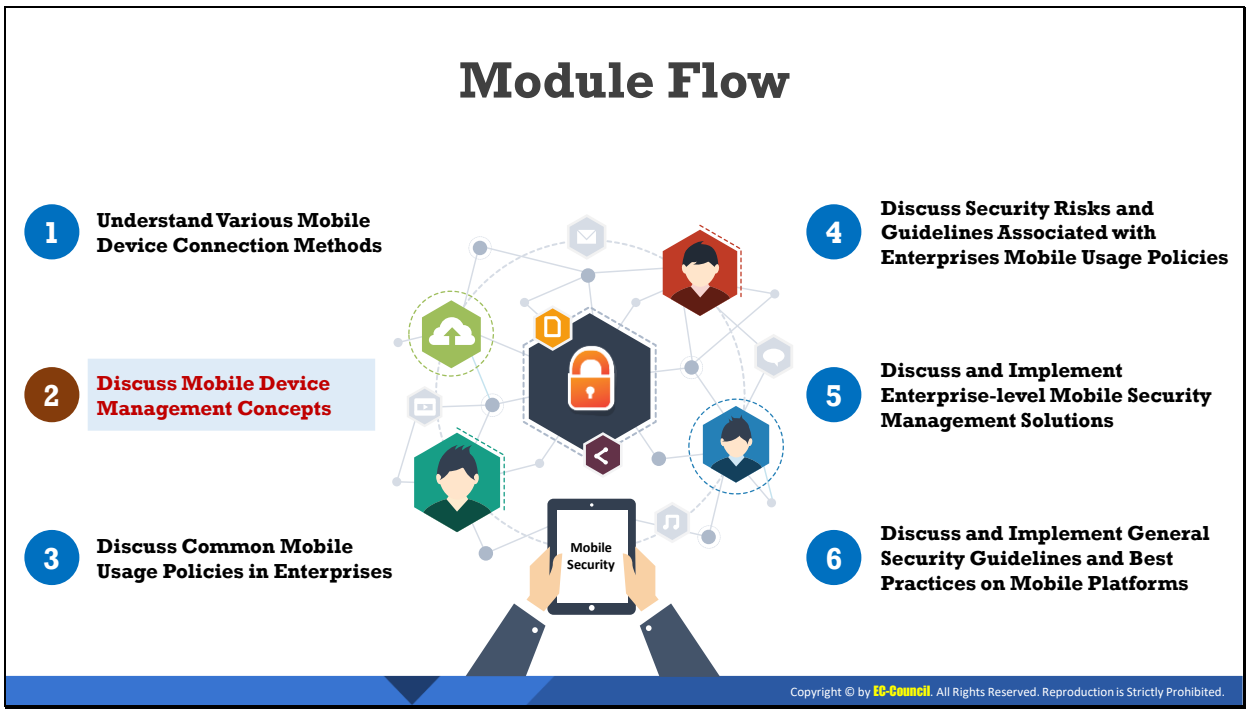
- **Wi-Fi:** A Wi-Fi network connects devices within a limited (Wi-Fi enabled) area with high bandwidth. It covers a shorter distance than a cellular network. It is a common wireless technology used in homes and office buildings to connect local devices. Furthermore, a mobile device can share its Internet service with other devices by using the hotspot tethering feature based on Wi-Fi technology. If clients do not use an encrypted channel or the channel does not use an appropriate protocol, then the clients can be targeted by main-in-the-middle (MITM) attacks, through which attackers can sniff the traffic between two communicating devices. Since the technology uses a set of 5 or 2.5 GHz frequencies, it can also be vulnerable to DoS attacks and frequency interferences.
- **Bluetooth:** Bluetooth technology covers a longer distance than NFC. It is a short-range, high-speed, and low-power wireless technology that enables communication between devices connected within the Bluetooth range. When a device enables a Bluetooth connection, it sends "pairing" requests to a certain number of devices located within range, following which the corresponding device pairs with it using the device name and ID. Security concerns with Bluetooth technology include interception, eavesdropping, DoS attacks, transmission of viruses or worms, Bluesnarfing, and Bluejacking.
- **5G cellular (mobile) communication:** 5G or fifth-generation communication technology is a broadband cellular network that operates at high bandwidth with low latency and provides high-speed data downloads. Some of the applications of 5G include the automobile industry, public safety, and fixed wireless access. The technology is designed to support IoT devices. Security concerns with this technology are associated with its management complexity. Attackers may attempt to take advantage of the increased number of devices connected to a 5G network to compromise and use them as botnets to paralyze the network through DDoS attacks.
- **Point-to-point (P2P) connection:** A P2P connection enables secure communication between two mobile devices without data encryption because they are connected through fixed paths without the interference of other devices. For example, in a scenario of mobile communication between two people, only the concerned device can hear the voice from the dialed device. Routing devices can also use this method to connect with each other by adopting the over-the-air encryption technique, which reduces the risk of eavesdropping.
- **Point-to-multipoint connection:** A point-to-multipoint (P2MP, PTMP, and PMP) connection allows one-to-many connections by providing multiple paths from a single location to several other locations. In this connection method, a central antenna broadcasts signals to multiple receiving antennas and devices through either time-division multiplexing (TDM) or frequency-division multiplexing (FDM) for bidirectional data transmission. One technology that uses PMP connections is Bluetooth, which can use the PMP method to connect one device with multiple devices such as headphones and media players. This type of connection does not provide high security or privacy, because the communication channel is broadcasted and shared.
- **Radio-frequency identification (RFID):** RFID works on radio-frequency technology, which identifies a person or object using their tags (unique labels). RFID operates in the

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

low-frequency (LF), high-frequency (HF), and ultra-high-frequency (UHF) bands. HF-RFID with a mobile device is communicated via servers by providing data history, data persistence, and data management. The RFID systems can be susceptible to attacks such as power analysis, reverse engineering, replay attacks, spoofing, sniffing, DoS, and cloning.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Discuss Mobile Device Management Concepts

This section discusses various mobile device management concepts.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Mobile Device Management (MDM)

MDM provides platforms for **over-the-air** or **wired distribution of applications**, **data** and **configuration settings** for all types of mobile devices, including mobile phones, smartphones, tablet computers, etc.

Mobile Application Management

- A software that is mostly used by IT admins to **control** and **secure organizational data**. It offers features such as the remote activation or deactivation of devices, remote wiping in case of theft or loss, etc.

Mobile Content Management

- A software that offers solutions to **safeguard the content** or data on the mobile devices. It provides features to store and deliver data, offer the required services, and permit employees to access the organizational data remotely

Context-aware Authentication

- It uses the contextual information of a user such as **geolocation**, **identity**, and **behavior** for enhancing data security decisions

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Device Management (MDM) (Cont'd)

Mobile Email Management

It offers **secure access** to organizational email infrastructure and data on an employee's mobile devices

Mobile Security Management

It involves **actions** and **precautionary steps** for securing the organizational data and mobile devices used by employees

Enterprise Mobility Management

It consists of **tools** and **technologies** used in an organization to secure the data in employees' personal (BYOD) and organizational devices

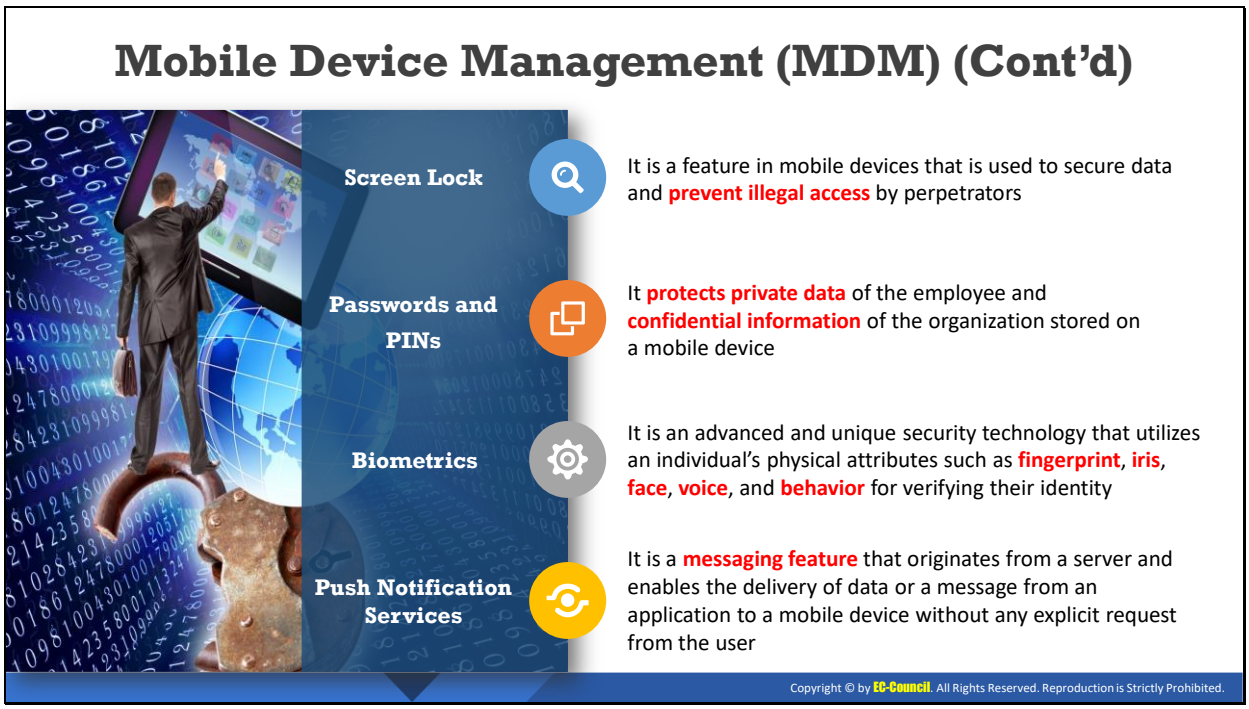
Remote Wipe

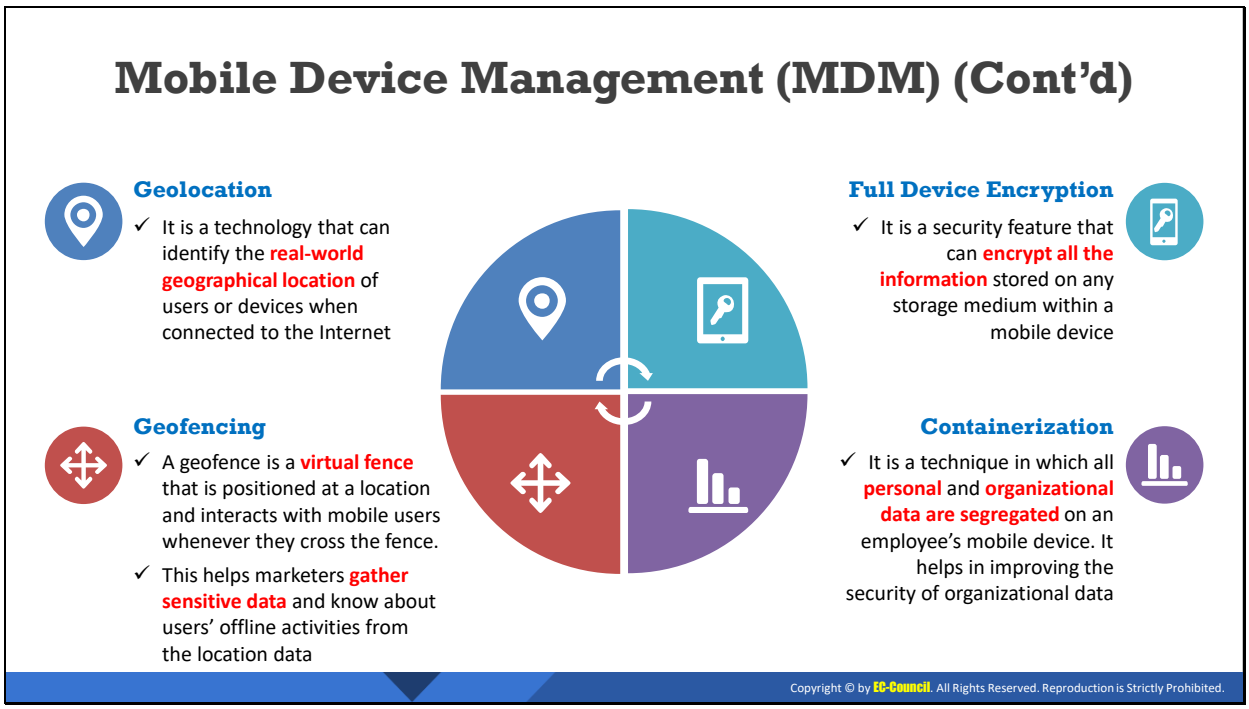
It is a technique used for securing and protecting data from miscreants if a mobile device used by an employee was lost. This feature allows the administrator to send a command that can **erase all the device data**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets





Mobile Device Management (MDM)

MDM provides platforms for over-the-air or wired distribution of applications, data, and configuration settings for all types of mobile devices, including mobile phones, smartphones, tablet computers, and so on. It helps in implementing enterprise-wide policies to reduce support costs, business discontinuity, and security risks. It helps system administrators to deploy and manage software applications across all enterprise mobile devices to secure,

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

monitor, manage, and support these devices. It can be used to manage both company-owned and employee-owned (BYOD) devices across the enterprise.

Discussed below are various concepts related to mobile device management:

- **Mobile application management**

  Mobile application management (MAM) is software that is mostly used by IT admins to control and secure organizational data. MAM offers features such as the remote activation or deactivation of devices, device registration in the organization, and remote wiping in case of theft or loss. These features are suitable for mobile devices that are used only for organizational purposes by the employees. For mobile devices that are used for both work and personal use, IT admins can implement and apply privacy policies on mobile applications by limiting organizational data sharing. They can also enable the partitioning of the applications used in the organization and personal data on the same mobile devices. MAM features also include software or application distribution to employees, license management, data encryption, configuration, and inventory management.

- **Mobile content management**

  Mobile content management (MCM) is software that forms a part of mobile device management (MDM). MCM offers solutions to safeguard the content or data on the mobile devices used in an organization. It provides features to store and deliver data, offer the required services, and permit employees to access the organizational data remotely and at any time necessary. MCM ensures that unauthorized data access is restricted or blocked, thereby protecting the confidential data of the organization. It oversees critical data management, access to work documents, email management, and digital asset management. It can also encrypt confidential data and use any strong password technique for data transmission and data storage.

- **Context-aware authentication**

  Context-aware authentication is a type of enhanced security technique that uses the contextual information of a user such as geolocation, identity, and behavior for enhancing data security decisions. It also uses the data about the user, requests made, connection, and location. All this data help in preventing malicious users from accessing the organizational data. This technique also allows employees to access the organizational network within the office perimeter and denies access when a device is connected to a public Wi-Fi network.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

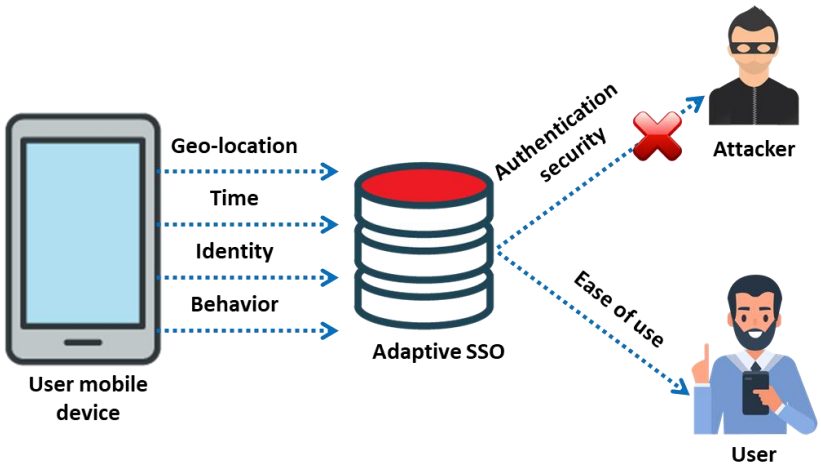


Figure 8.1: Context-aware authentication

- **Mobile email management**

  Mobile email management (MEM) offers secure access to organizational email infrastructure and data on an employee's mobile devices. It helps in the remote pre-configuration and pre-set up of organizational email accounts for employees. MEM can enforce compliance and thwart unauthorized access by allowing only approved and authorized devices and applications to access the email.

- **Enterprise mobility management**

  Enterprise mobility management (EMM) consists of tools and technologies used in an organization to secure the data in employees' personal (BYOD) and organizational devices. EMM acts as a comprehensive solution responsible for MDM, MAM, MTM, MCM, and MEM. It safeguards the enterprise data accessed and used by employee mobile devices. EMM can increase employee productivity as the IT admin can configure applications remotely and provide data access to employees.

- **Mobile security management**

  Mobile security management involves actions and precautionary steps for securing the organizational data and mobile devices used by employees. It can protect the organization's network access, helps in device and application security, and enables secure access to the organization's emails.

  The following are some of the features of mobile security management:

  - Generates separate logical containers on mobile devices to prevent private apps from accessing the organization's data
  - Employs strong passcode techniques to restrict third-party access
  - Automates updates of the devices and OS with the latest security patches
  - Blacklists malicious applications
  - Executes commands on lost mobile devices remotely
  - Configures a VPN specifically for the organization's data, resources, and applications

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **Remote wipe**

  Remote wipe is a technique used for securing and protecting data from miscreants if a mobile device used by an employee was stolen or lost. This feature allows the device owner or the organization's administrator to send a command that can delete or erase all the device data. This helps prevent perpetrators from compromising sensitive personal data or confidential organizational assets.

- **Screen lock**

  Screen lock is a feature in mobile devices that is used to secure data and prevent illegal access by perpetrators. Enabling screen lock in a mobile device can prevent access to private data in the mobile device even if it was lost or stolen. Screen lock can be set in a mobile device by using protection techniques such as a password, face lock, fingerprint lock, pattern, or PIN. Unlocking the screen involves a set of actions that needs to be performed correctly, failing which the device can lock out after a certain number of unsuccessful attempts.

- **Passwords and PINs**

  Passwords and PINs are basic security features used in all mobile devices. Using a secure PIN and complex password can protect private data of the employee and confidential information of the organization stored on a mobile device. A password or PIN acts as a simple but effective defense to safeguard the data from being accessed by any malicious user. A PIN consists of a sequence of numbers, without any letters or special characters. In contrast, a password comprises uppercase and lowercase letters, numerals, and special characters and are usually lengthier than a PIN.

- **Biometrics**

  Biometrics is an advanced and unique security technology that utilizes an individual's physical attributes such as fingerprint, iris, face, voice, and behavior for verifying their identity. These data are stored in a database, and whenever the mobile device needs to be accessed, the user-provided data are compared with the stored data; access is allowed only if there is a match. Biometrics can be used to authenticate a user very easily, quickly, and securely. It also prevents the need for remembering complex passwords.

- **Push notification services**

  A push notification service is a messaging feature that originates from a server and enables the delivery of data or a message from an application to a mobile device without any explicit request from the user. It is a great marketing tool for maintaining contact with users. This service does not require any application to be opened for receiving the notification, and the text message in the notification will be displayed on the mobile device even if the application is closed or the screen is locked.

- **Geolocation**

  Geolocation is a technology that can identify the real-world geographical location of users or devices when connected to the Internet. It works on mobile devices through

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

the GPS system and is accurate to the level of approximately one foot. Deploying geolocation in applications helps marketers in implementing their business and marketing techniques easily. Geolocation is also famous for offering a rich user experience for navigation through maps and for tracking people, devices, or vehicles having the GPS feature. Geolocation is also used in weather forecasting.

- **Geofencing**

  Geofencing is a technique through which mobile-application marketers utilize the location of the user to gather information. This technique can determine how close the user's mobile device is to an exact location by using the GPS feature. A geofence is a virtual fence that is positioned at a location and interacts with mobile users whenever they cross the fence. This helps marketers gather sensitive data and know about users' offline activities from the location data. It uses cellular triangulation for locating the user's device with an accuracy level of 50–50,000 m.

  The following are the main advantages of using geofencing for marketing:

  - Send promotions directly to clients
  - Improve sales locally
  - Reduce cost on paid advertising
  - Obtain data on user experience for further improvement

- **Full device encryption**

  Full disk encryption is a security feature that can encrypt all the information stored on any storage medium within a mobile device. This technique encodes the user's information stored on the mobile device by using an encryption key. It is useful for automatically encrypting data, which can be decrypted using the key. It employs encryption algorithms such as the 128-bit Advanced Encryption Standard (AES) with cipher-block chaining (CBC).

- **Containerization**

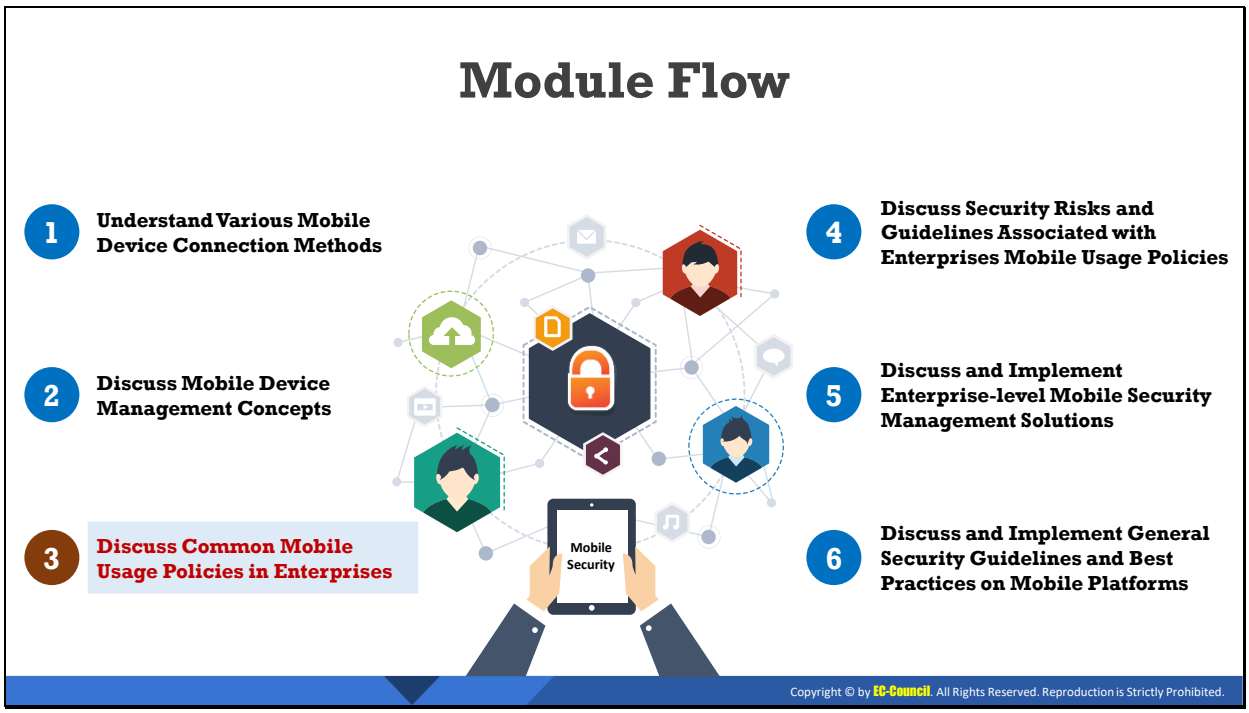
  Containerization is a technique in which all personal and organizational data are segregated on an employee's mobile device. With the increasing adoption of BYOD policies, using this technique substantially helps in improving the security of organizational data. It also improves productivity and enables the easy use of company resources and applications. These applications do not have any control of or communication with the private applications or data of the employees as they exist outside the container.

  The following are the benefits of containerization:

  - By default, containers are encrypted to secure corporate data.
  - Data cannot enter or exit the container.
  - Data are shared only between the apps within the container.
  - Containerization provides complete control over the container's workspace.
  - Containerization provides privacy to the user's data on the mobile device.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

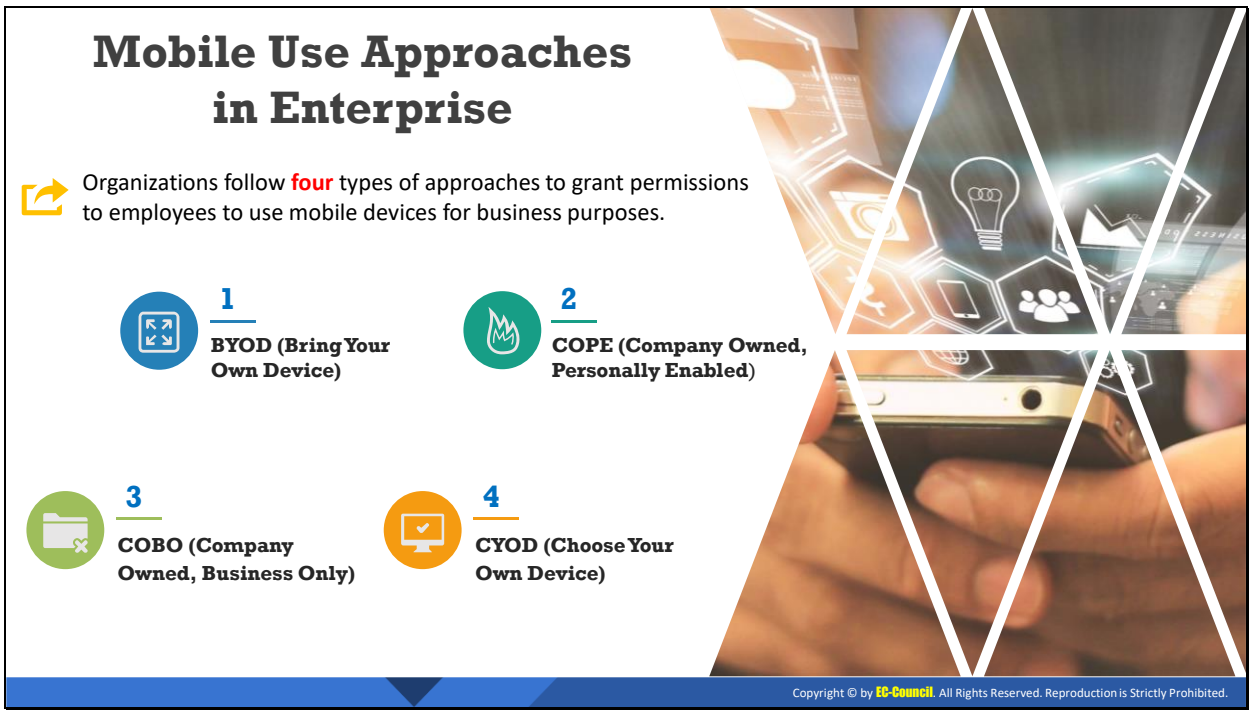
https://t.me/learningnets



Discuss Common Mobile Usage Policies in Enterprises

An organization that enables its employees to work remotely using a smartphone or tablet must design a policy to secure these devices and protect the company data. This section introduces the various mobile usage policies that can be implemented by an organization based on its requirements.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Mobile Use Approaches in Enterprise

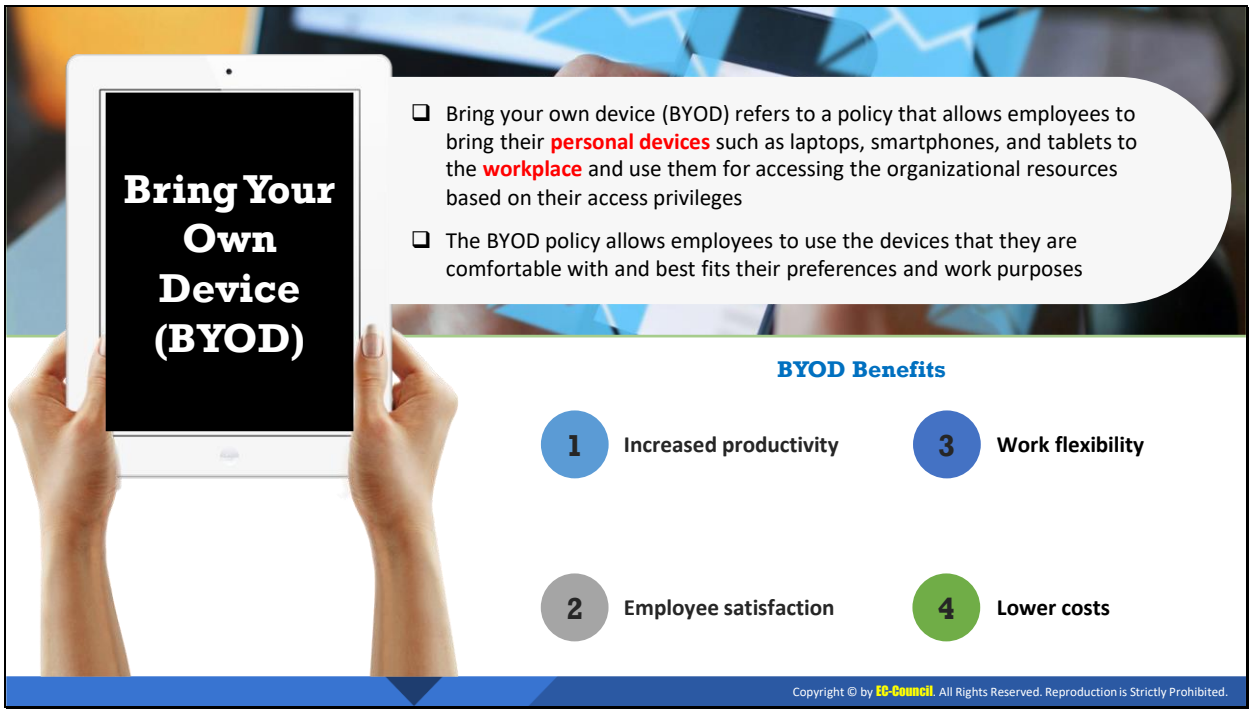
An organization can implement any of the following policies based on their requirements as well as the role and responsibilities of its employees to enable them to use mobile devices for business purposes.

- BYOD (Bring Your Own Device)
- COPE (Company Owned, Personally Enabled)
- COBO (Company Owned, Business Only)
- CYOD (Choose Your Own Device)

The following questions can help an organization to determine which approach to follow:

- **Device Specific**
  - Device type (which device to use (smartphone/phablet/laptop)?)
  - Selection of device (who uses which devices?)
  - Who pays for the device?
  - Service providers for cellular connectivity and monthly plans
- **Management and Support**
  - Who manages the device?
  - Who is responsible for support?
- **Describe Integration and Application**
  - Describe how closely the device is integrated and important for everyday workflow?
  - Describe the installed/running applications
  - Should personal applications be restricted?

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Bring Your Own Device (BYOD)

Bring Your Own Device (BYOD)/Bring Your Own Technology (BYOT)/Bring Your Own Phone (BYOP)/Bring Your Own PC (BYOPC) refers to a policy that allows employees to bring their devices such as laptops, smartphones, and tablets to the workplace and use them for accessing the organizational resources based on their access privileges.

The BYOD policy allows employees to use the devices they are comfortable with that best fit their preferences and work purposes. With the "work anywhere, anytime" strategy, the BYOD trend encounters challenges in securing the company data and satisfy compliance requirements.

BYOD Advantages

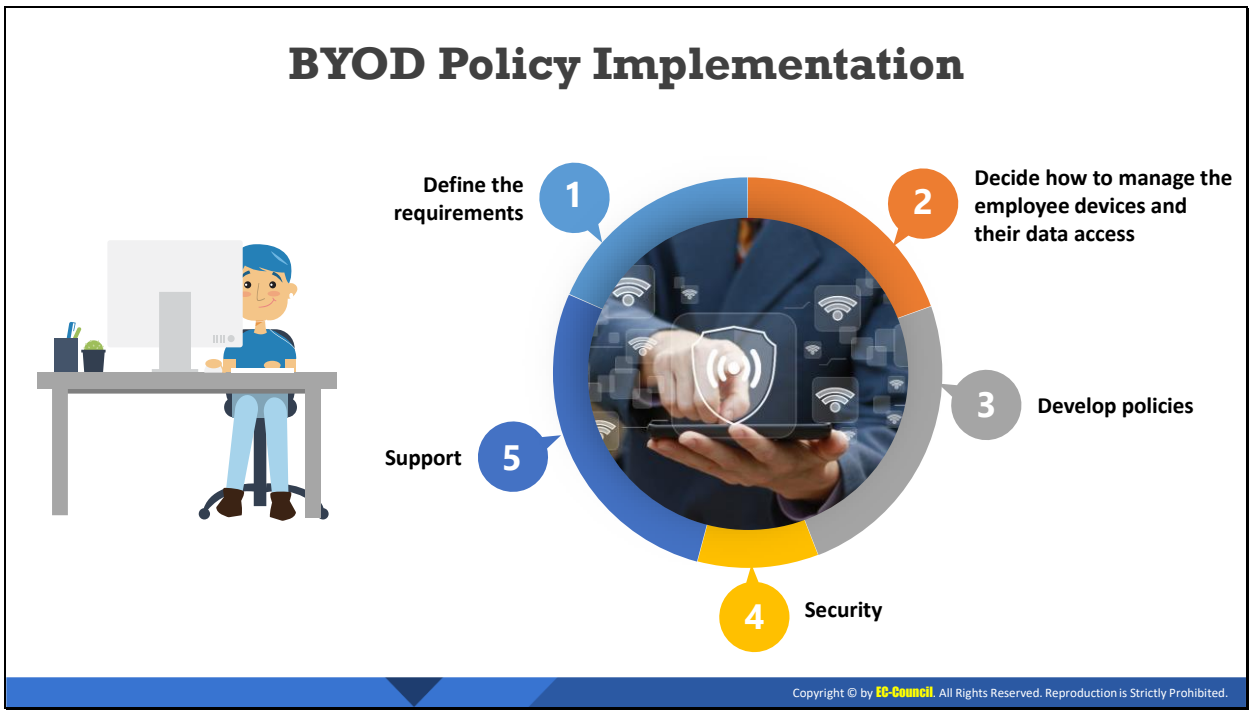
The adoption of BYOD is advantageous to the company as well as its employees. Its advantages include:

- Increased productivity and employee satisfaction
- Enhances work flexibility
- Lower IT Costs
- Increased availability of resources

BYOD Disadvantages

- Difficult to maintain security access in organizational networks
- Increased compatibility issues
- Reduced Scalability

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



BYOD Policy Implementation

For the implementation of the BYOD policy, the employee devices must be introduced to the corporate environment to minimize the risks associated with data security and privacy.

- **Define the requirements**

  Not all user requirements are similar. Thus, the employees must be grouped into segments considering the job criticality, time sensitivity, value derived from mobility, data access, and system access. Further, end user segments should be defined based on the location/type of worker (e.g., an employee working from home, full-time remote, day extender, part-time remote), and a technology portfolio should be assigned for each segment based on user needs.

  Privacy impact assessment (PIA) should also be performed at the beginning of each BYOD project in the presence of all relevant teams after assigning the responsibilities and collecting the requirements. It provides an organized procedure to document the facts, objectives, privacy risks, and risk mitigation approaches and decisions throughout the project lifecycle. It should be a central activity performed by the mobile governance committee (end users from each segment/line of business and IT management).

- **Decide how to manage the employee devices and their data access**

  Apart from the mobile device management (MDM) system that provides a minimum level of control, other options such as virtual desktops or on-device software can be used to improve the security and data privacy. Additionally, it should be ensuring that the corporate environment supports WLAN device connectivity and management.

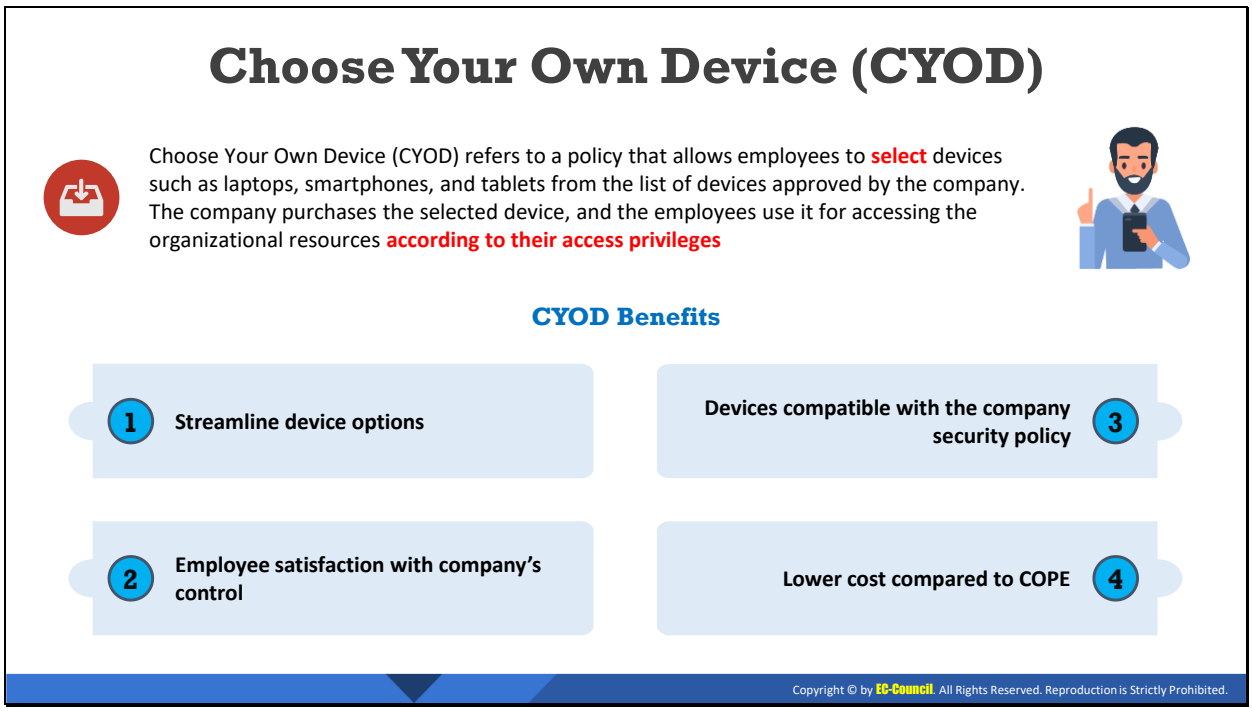
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **Develop policies**
  - A delegation of company resources should develop the policies, instead of just IT. It should include key participants such as the HR, legal, security, and privacy.
  - Each device (smartphone, PC, laptop, tablet, or even smartwatch) and OS in the BYOD policy of a company should be listed; devices with a poor security record should not be permitted. This involves only permitting devices with specific OSes or manufacturers.
  - Establish a policy to determine a reasonable, binding policy regarding BYOD to secure businesses and employees.
  - The IT staff of an organization should be trained about the various platforms, devices, and OSes to familiarize them with the risks associated with wrong device handling or to avoid the security threats imposed by a BYOD work environment.
  - The BYOD policy should also ensure that the devices are appropriately backed up to prevent the loss of critical data under unforeseen circumstances.
- **Security**

  The mobile management technology is effective only when suitable policies are established, implemented, and supported. The organizations must ensure sufficient security in the mobile ecosystem to make the BYOD programs work. This requires a thorough assessment of the operating environment and the development of a solution that provides the following.
  - Asset and identity management
  - Local storage controls
  - Removable media controls
  - Network access levels
  - Network application controls
  - Corporate versus personal app controls
  - Web and messaging security
  - Device health management
  - Data loss prevention
- **Support**

  The inconsistent nature of BYOD users will increase the frequency of support calls. Therefore, organizations should establish suitable processes and capabilities in the early stages to ensure success. Mobile committees should frequently reassess the support levels and ensure the productivity of their mobile employees.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Choose Your Own Device (CYOD)

Choose Your Own Device (CYOD) refers to a policy in the employees select their device of choice from a preapproved set of devices (laptops, smartphones, and tablets) to access company data according to the access privileges of an organization. For example, allowing employees to select an Apple device instead of Android devices. CYOD has recently garnered more attention than BYOD in the business world because securing BYOD systems can be difficult considering the various devices available in the market, and employees store personal and professional data irrespective of whether a device is personal or belongs to the employer.

CYOD Advantages

- Users are allowed to carry only one smartphone and one tablet.
- It reduces hardware costs compared to COPE.
- End users are still in control of their own technology.
- Procurement standards are stricter than those of BYOD.
- Its support standards are streamlined.
- Each security device is preinstalled with a security solution and predefined firewall and network settings of a dedicated administrator.
- Administration of a small number of different specifications makes record-keeping easy.
- Employees comply with data and information management requirements.

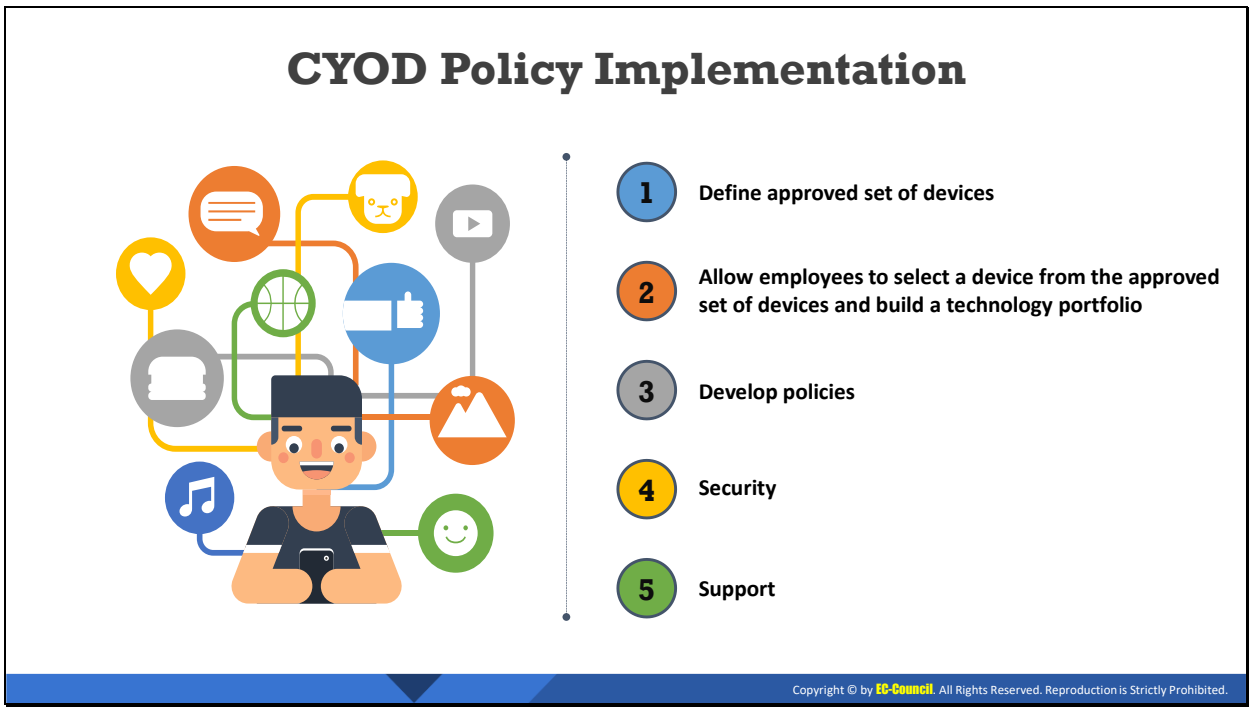
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

CYOD Disadvantages

- Some IT staff may not be happy with the choices.
- It involves a more complex procurement process than BYOD or COPE.
- End users face replacement and repair problems.
- It needs to be updated with the mobile technology / apps used by the organizations.
- It comprises a slower deployment timeframe.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



CYOD Policy Implementation

The key considerations before implementing a CYOD policy are

- **Define an approved set of devices:** Organizations must formulate a list of corporate-sanctioned devices and plans for their employees to access company data according to their access privileges.
- **Allow employees to work with company-owned devices (including personal work) and build a technology portfolio:** Allow employees to select devices (laptops, smartphones, and tablets) and plans from role-based corporate catalogs. Before delivery, set up the devices with apps, software, and settings required by each employee, thereby enabling them to operate the apps immediately. For example, set up devices with Outlook with the employee credentials.
- **Develop policies and device security:** Establish policies to ensure that the employees understand the responsibilities accompanying network access. The more granular the organizational policies are in terms of device types, different versions of OSes, and device model number, the more resources will need to be tested to support such devices. For example, allowing only a specific Android mobile model or a specific version of a mobile OS.

  Implement the following:

  - Virus protection
  - Encryption
  - Network access controls and authentication
  - Data wipes and remote locks in case devices are lost or stolen

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- Train the employees to inform them about their mobile responsibilities, including how data are accessed, used, and stored, and how to use apps and services.

- **Support:** Deploy expertise solutions (dedicated helpdesk that knows the policies and needs of the organization) to speedily resolve any mobility issues. They should address
  - Device troubleshooting
  - Service troubleshooting
  - Activating devices
  - Deactivating devices
  - Managing service requests

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Corporate Owned, Personally Enabled (COPE)

Corporate Owned, Personally Enabled (COPE) refers to a policy that allows employees to use and manage the devices purchased by the organizations. The devices include laptops, notebooks, smartphones, tablets, and/or software services. Larger enterprises are more likely to employ the COPE model.

COPE is a lesser expensive option than BYOD because the companies buy devices at a lower cost than the retail price. COPE reduces the risks associated with BYOD by implementing stringent policies and protecting devices.

COPE Advantages

- Work or life balance on a single device
- Fewer security concerns than BYOD and CYOD
- Personal apps
- Enhanced control and authority over devices
- Prevents employees from carrying two phones
- Retains ownership of devices
- Less expensive than BOYD
- Enables organizations to freely install management software and/or integrate devices in MDM systems
- Helps in solving regulatory and legal issues associated with deleting data on lost/stolen mobile devices

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

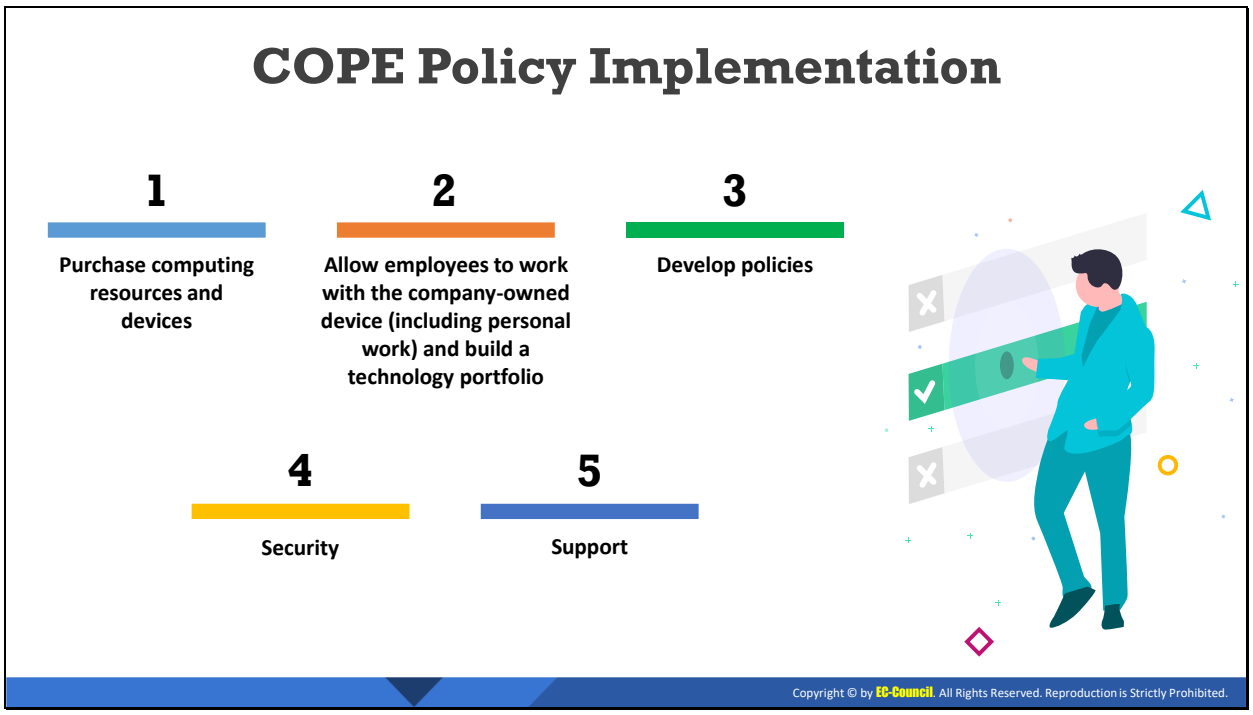
- Economizes the resources (save and time) of the IT department because the employees are responsible for the condition of their devices.

COPE Disadvantages

- Need to purchase devices
- Monitoring policies must be established
- Business is completely responsible for keeping up with the latest technologies
- Potential for productivity issues owing to less user freedom
- Slowest deployment timeframe

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



COPE Policy Implementation

The considerations for the implementation of a COPE strategy include:

- **Purchase computing resources and devices:** The organization purchases preapproved devices from vendors based on their centrally designed plan.
- **Allow employees to work with company-owned devices and build a technology portfolio:** These organization-owned devices allow employees to have COBO's conservatism and BYOD's freedom. The devices are designed for both office and personal works.
- **Develop policies**
  - Ensure that the **employees completely understand and sign-off on the policy** related to them leaving the company.
  - Decide whether the employees will be **allowed to procure or retain the device** after leaving the company and create a procedure for removing all corporate data and assets from the device.
- **Security:** To ensure device security, organizations apply security controls, restrict certain features to secure from malware and data leaks, and monitor devices for data breaches or jailbreaking.
- **Support:** Deploy expertise solutions (dedicated helpdesk that knows the policies and needs of the organization) to speedily resolve any mobility issues. They should address
  - Device troubleshooting
  - Service troubleshooting
  - Activating devices
  - Deactivating devices
  - Managing service requests

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Company Owned, Business Only (COBO)

Company Owned, Business Only (COBO) refers to a policy that allows employees to use and manage the devices purchased by the organization but restrict the use of the device for business use only. COBO is used to describe a device that runs a single application. For example,

- An inventory system with an embedded barcode scanner.
- Blackberry is the best example of devices used in a COBO environment.

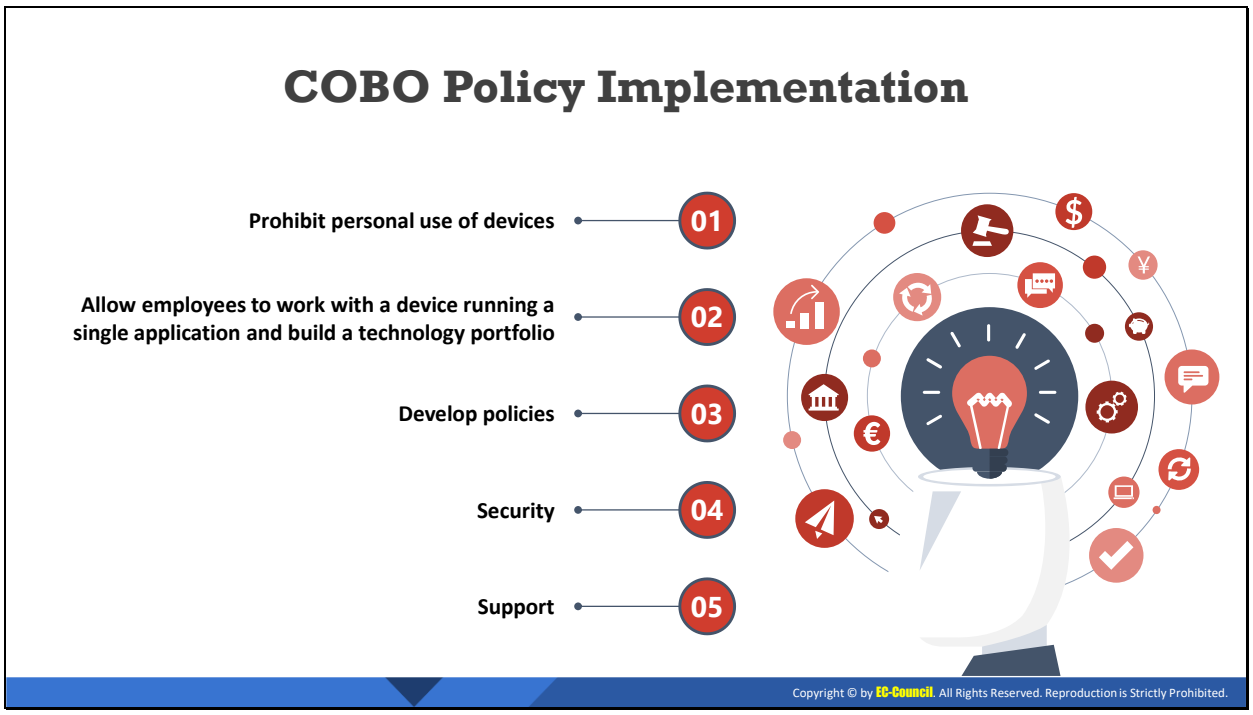
COBO Advantages

- The company retains full control over all apps on the device and its data.
- A uniform system landscape is adhered to because the organization purchases the device.
- Prevents data leakage.

COBO Disadvantages

- High purchase cost for devices.
- Employees do not really enjoy working with at least two devices in their pockets.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



COBO Policy Implementation

The considerations for the implementation of a COBO strategy are

- **Prohibit personal use of devices:** Enterprises prohibit the use of mobile devices as a part of their designing policy based on the COBO approach.
- **Allow employees to work with devices running single application and build a technology portfolio:** Enterprises allow employees to work with a device that runs a single application; for example, an inventory system with an embedded barcode scanner. Otherwise, they can allow the use of smartphones with prohibited personal use. Additionally, they should implement highly granular devices as well as app and data management to enable compliance.
- **Develop policies:** Ensure that the mobile device management **(MDM)** and mobile application management **(MAM)** solutions fully meet the requirements of the company's concept.
- **Security**
  - Ensure fully locked down devices to maintain control over granular policies and control the device usage
  - Prevent app downloads
- **Support**

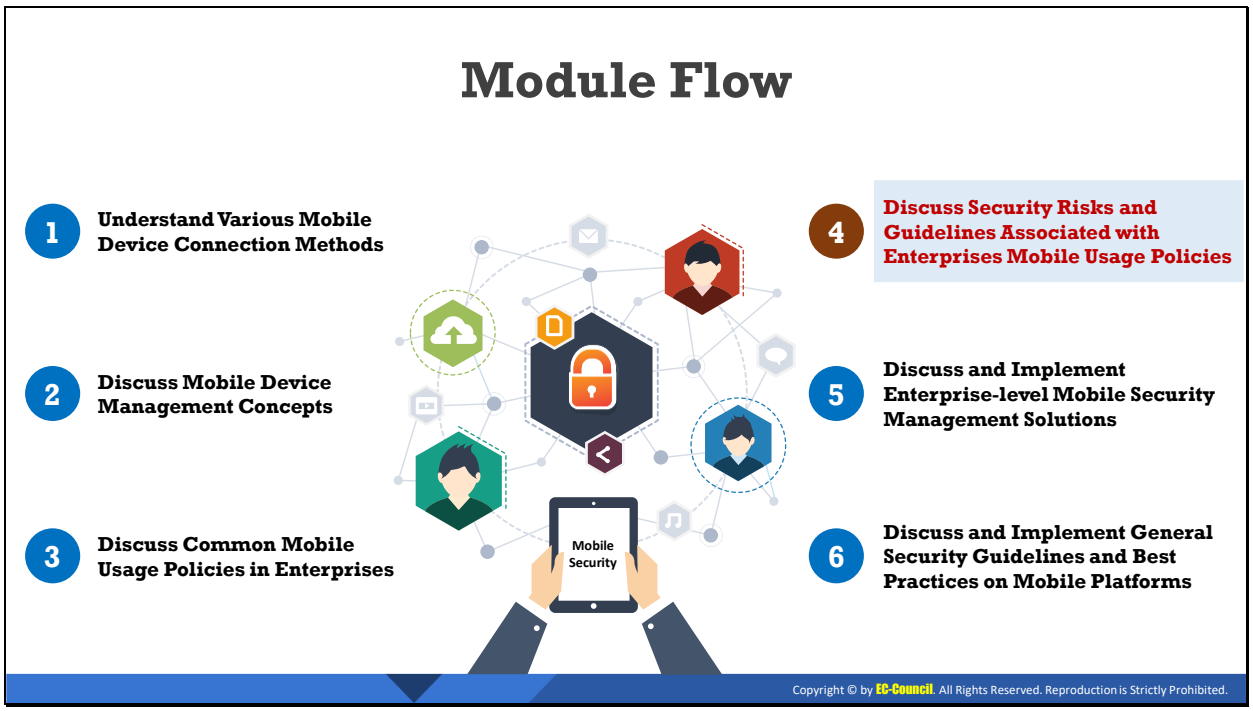
  Deploy expertise systems (dedicated helpdesk that knows the policies and needs of the organization) to speedily resolve any mobility issues. They should address
  - Device troubleshooting

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- Service troubleshooting
- Activating devices
- Deactivating devices
- Managing service requests

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

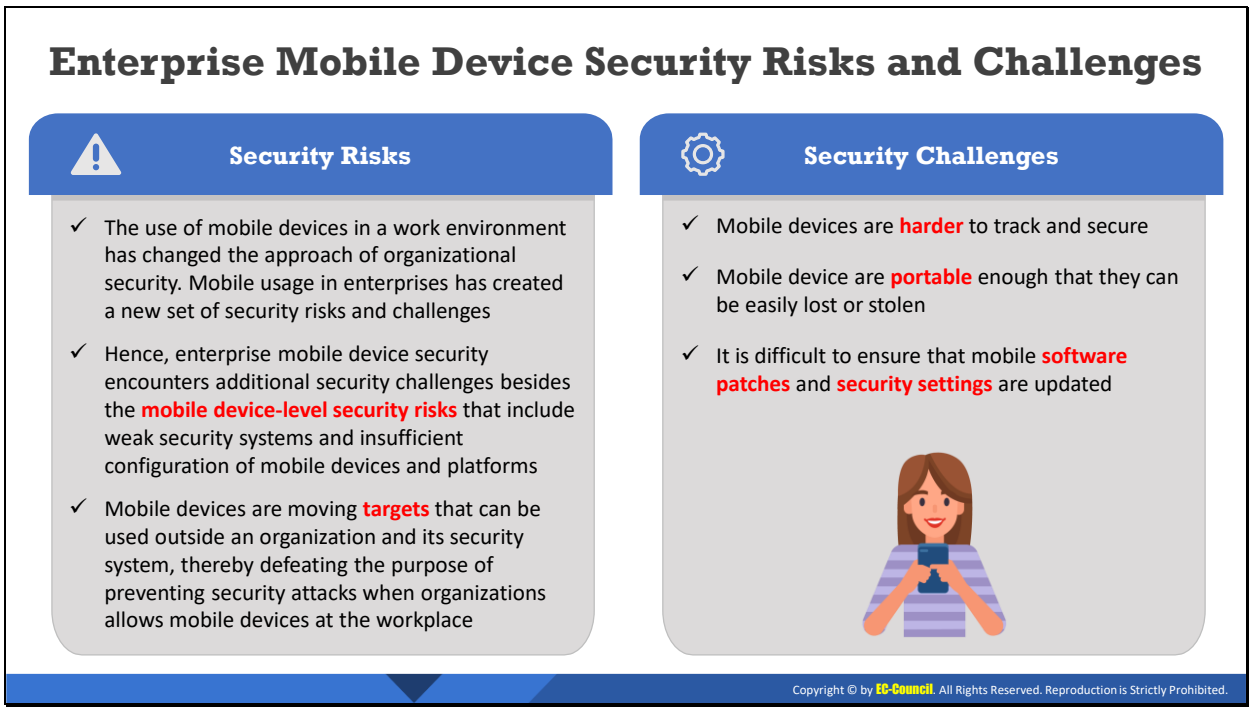
https://t.me/learningnets



Discuss Security Risks and Guidelines Associated with Enterprises Mobile Usage Policies

Creating a mobile usage policy that will enable smooth functioning and ensure security of the corporate assets is a major challenge. The objective of this section is to explain the security risks and challenges associated with the enterprise mobile usage policies. It describes the risks associated with the BYOD, CYOD, COPE, and COBO policies in detail along with the security guidelines to be implemented for them.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Enterprise Mobile Device Security Risks and Challenges

The use of mobile devices in work environments has changed the security approach of organizations. It has given rise to a new set of security risks and challenges in organizational security. In addition to the mobile device security risks that include weak security systems and insufficient configuration of mobile devices and platforms, enterprise mobile device security faces additional security challenges. Mobile devices are moving targets that can be used outside an organization and its security system, thereby defeating the purpose of preventing security attacks when organizations allow mobile devices at the workplace.

These challenges can be divided into the following categories:

- **Physical Risks and Challenges**

  This includes the loss or theft of a mobile device owing to their portability and lightweight. Attackers can perform malicious actions if they get physical access to a device such as flashing the device with a malicious system image that is connected to a computer to install a malicious application or conduct data extraction.

  Therefore, the devices should not be left unattended. Security measures such as device authentication and encryption must be enforced. Instead of using a simple password, enforce multiple forms of authentication to prevent unauthorized access to mobile devices.

- **Network-based Risks and Challenges**

  Mobile devices that use common wireless network interfaces (Wi-Fi, Bluetooth) for connectivity are vulnerable to wireless eavesdropping attempts.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Therefore, employees should connect to trusted networks using WPA21 or use secured network protocols (IPSec, SSL, SSH, HTTPS, Kerberos, etc.) to prevent mobile devices from network-based threats. Moreover, they can use special gateways with customized firewalls and security controls to direct the mobile traffic. For example, content filtering and data loss prevention tools.

- **System-based Risks and Challenges**

  Manufacturers may unintentionally introduce vulnerabilities in devices; for example, vulnerabilities in SwiftKey keyboards or mobile OSes. Therefore, the devices should be regularly updated to reduce threats.

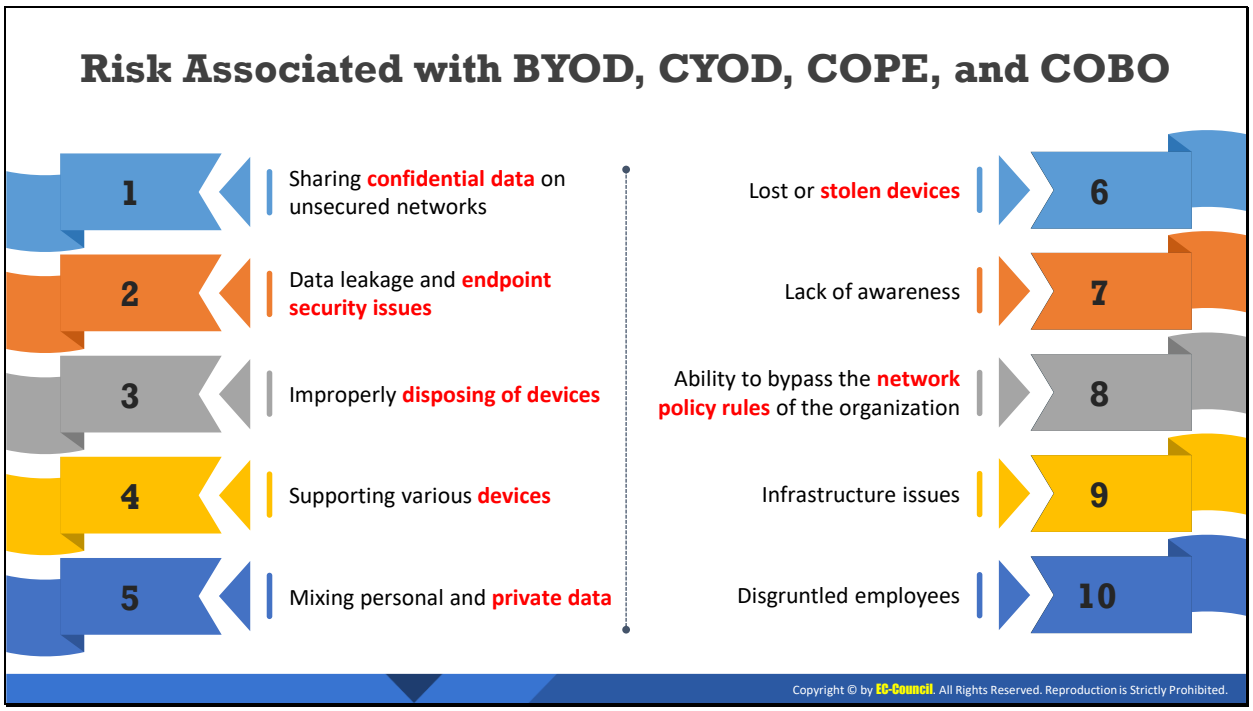
- **Application-based Risks and Challenges**

  Vendors may not release timely app updates and support for older OS versions or users may not update their apps regularly. Attackers can exploit the vulnerabilities in applications and attempt to steal data, download other malware, or control the device remotely, thereby resulting in financial loss and risk the reputation of an organization.

  Thus, strict controls must be enforced regarding downloading and installing applications on a device and using mobile anti-virus. Additionally, strong policies must be established to limit or block the use of third-party applications on devices.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Risk Associated with BYOD, CYOD, COPE, and COBO

Employees connecting to a corporate network or accessing corporate data using their own mobile devices pose security risks to an organization. Following are some security risks associated with the BYOD, CYOD, COPE, and COBO policies:

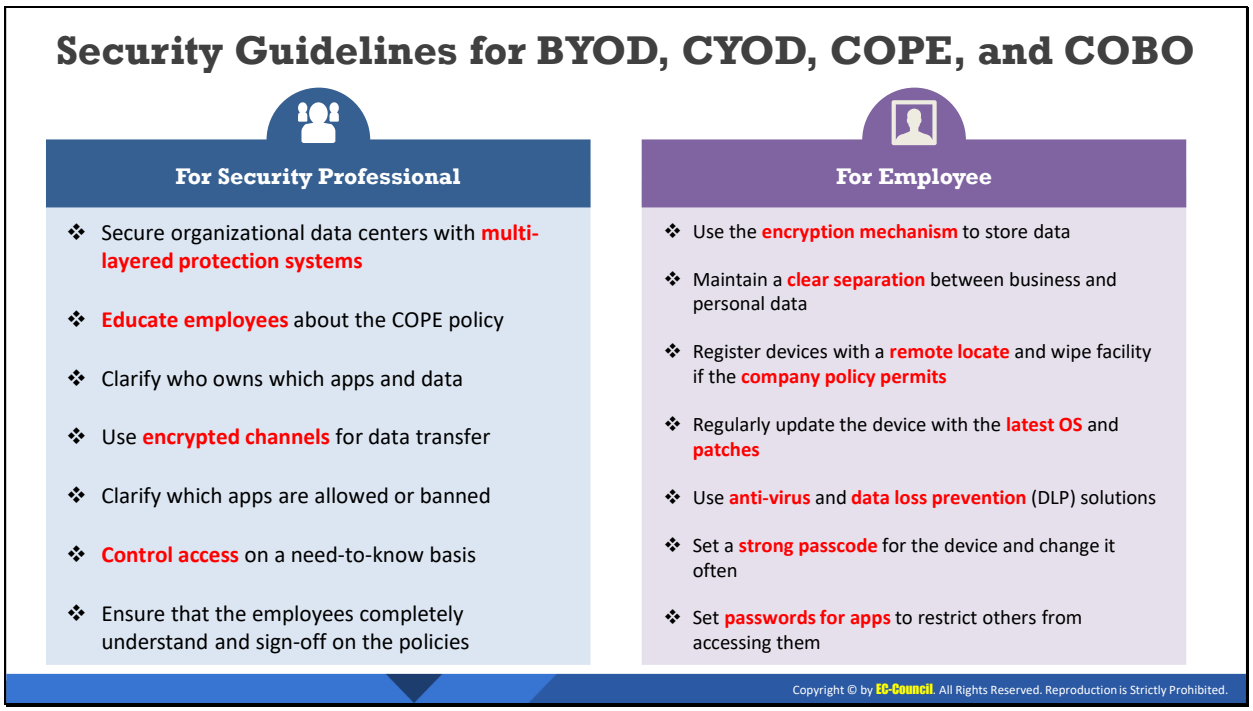
- **Sharing confidential data on an unsecured network:** Employees might access corporate data via a public network. These connections may not be encrypted and sharing confidential data via an unsecured network may lead to data leakage.
- **Data leakage and endpoint security issues:** In this cloud-computing era, mobile devices are insecure endpoints with cloud connectivity. By synchronizing with organizational email or other apps, these mobile devices carry confidential information. If a device is lost, it could potentially expose all corporate data.
- **Improperly disposing of devices:** An improperly disposed of device could contain a wealth of information such as financial information, credit card details, contact numbers, and corporate data. Therefore, it is important to ensure that devices do not contain any data before they are disposed or passed on to others.
- **Support of many different devices:** Organizations allow employees to access their resources from anywhere in the world, thereby enhancing productivity and driving employee satisfaction. Support for different devices and processes can increase the cost. Employee-owned devices have limited security that operate on different platforms. This deters the capabilities of the IT department to manage and control devices in a company.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **Mixing personal and private data:** Control over isolating business use from personal use is difficult. For example, managing employees that shop on compromised websites, use public Wi-Fi connections, or given their device to others.
- **Lost or stolen devices:** Owing to their small size, mobile devices are often lost or stolen. When an employee loses their mobile device that is used for both personal and official purposes, the organization might face a security risk because the corporate data on the lost device may be compromised.
- **Lack of awareness:** Failing to educate employees regarding these policy and security issues may compromise the corporate data stored in mobile devices.
- **Ability to bypass organizational network policy rules:** According to requirements, the policies imposed may differ for wired and wireless networks. The devices connected to wireless networks can bypass the network policies enforced only on wired LANs.
- **Infrastructure issues:** These policies involve dealing with various platforms and technologies. Not all employees carry the same device. Different devices, each running different OSes and programs, have security loopholes. This can be problematic for an IT department to set up and maintain an infrastructure that supports the requirements of different devices such as managing data, security, back up, and compatibility among devices.
- **Disgruntled employees:** Disgruntled employees in an organization can misuse the corporate data stored on their mobile devices. They may also leak sensitive information to competitors.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Security Guidelines for BYOD, CYOD, COPE, and COBO

The following are some of the security guidelines to be followed by network defender and employees when the BYOD, CYOD, COPE, and COBO policies are implemented.

- **For Security Professional**

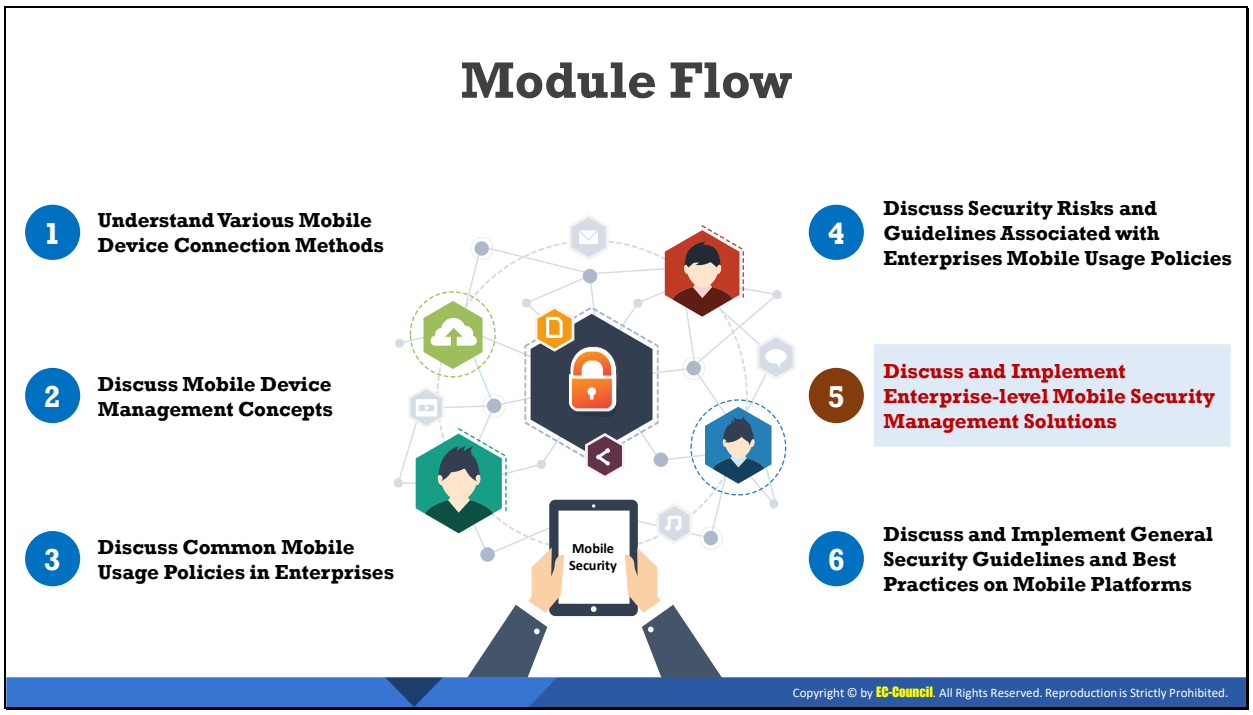
  With the increased use of tablets, smartphones, and other devices at work, mobile security has become a great concern. Listed below are the security guidelines that should be implemented to ensure the security of the network and data of an organization.

  - Secure the data centers in organizations with multi-layered protection systems.
  - Educate employees about these policies.
  - Clarify who owns which apps and data.
  - Use an encrypted channel for data transfer.
  - Clarify which apps are allowed or banned.
  - Control access on a need-to-know basis.
  - Do not allow jailbroken and rooted devices.
  - Apply session authentication and timeout policy on access gateways.
  - Ensure that the employees completely understand and sign-off on the policies.
  - Create a procedure for removing all corporate data and assets from the device if an employee leaves the company.
  - Ensure that the MDM and MAM solutions of company correspond its requirements.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **For Employees**
  - Impose company WLAN access when on-site.
  - Ensure the use of complex passcodes and change them frequently.
  - Ensure that mobile devices are registered and authenticated before allowing access to the organizational network.
  - Consider multi-factor authentication methods to enhance the security while remotely accessing the organization's information systems.
  - Make users agree and sign the policies before they can access the organization's information system.
  - When an employee leaves the organization, state whether total device wipe or selective wipe of certain apps and data is required and ensure that the organization and personal data are maintained separately.
  - Implement strong algorithms to encrypt the organization data stored in the devices; also use an encrypted channel for data transfer.
  - If a device is lost or stolen, remotely reset or wipe the device passwords to prevent unauthorized access to the sensitive data of an organization.
  - Implement an SSL-based VPN, which provides secure remote access.
  - Ensure that user devices are regularly updated with the latest OSes and other software, which could avoid and sometimes even fix any security vulnerabilities.
  - Do not provide offline access to the sensitive information of an organization, which should be accessible only via the company network.
  - Use anti-virus and data loss prevention (DLP) solutions.
  - Set passwords for apps to restrict others from accessing them.

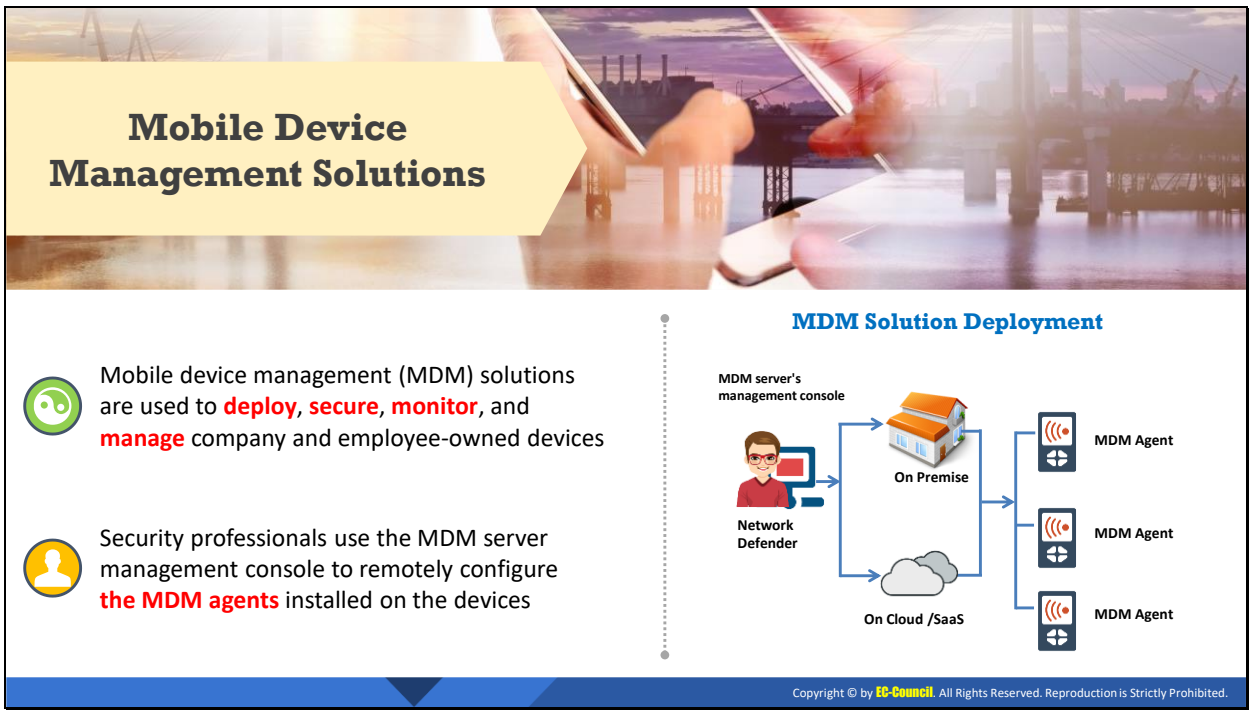
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

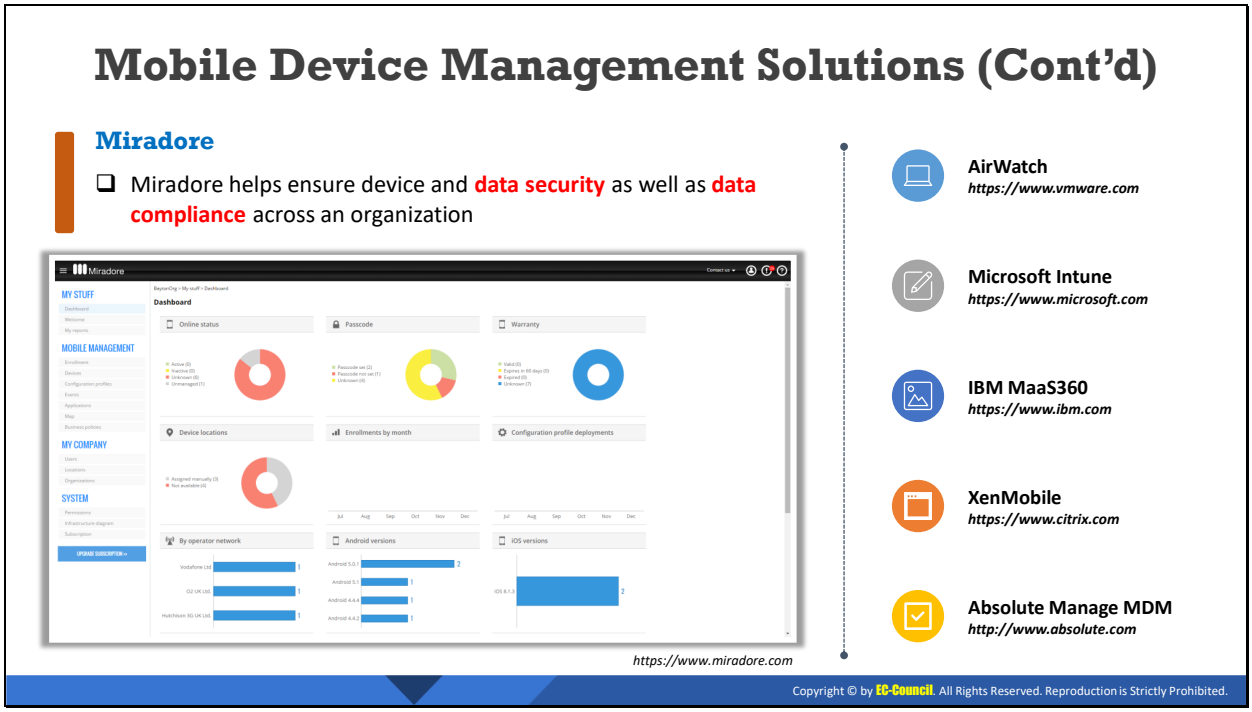


Discuss and Implement Enterprise-level Mobile Security Management Solutions

To handle the mobile security challenges in enterprises, organizations are implementing various mobile security management solutions. Mobile management solutions help an organization to manage mobiles devices across the organization from a central location. The objective of this section is to explain the benefits of such mobile management tools and solutions. It describes mobile devices management tools such as MDM solutions, MAM solutions, mobile content management (MCM) solutions, mobile threat defense (MTD) solutions, mobile email management (MEM) solutions, enterprise mobility management (EMM) solutions, and unified endpoint management (UEM) solutions.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets





Mobile Device Management Solutions

Mobile device management (MDM) is gaining significant importance with the adoption of policies such as BYOD across organizations. The increase in different types of mobile devices such as smartphones, laptops, and tablets has made it difficult for enterprises to make policies and manage the devices securely. MDM is a policy that helps in managing devices carefully while reducing support costs, mitigating security risks, and reducing business discontinuity.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Mobile device management (MDM) solutions are used to deploy, secure, monitor, and manage company and employee-owned devices. Network defenders use the MDM server management console to remotely configure the MDM agents installed on the devices.

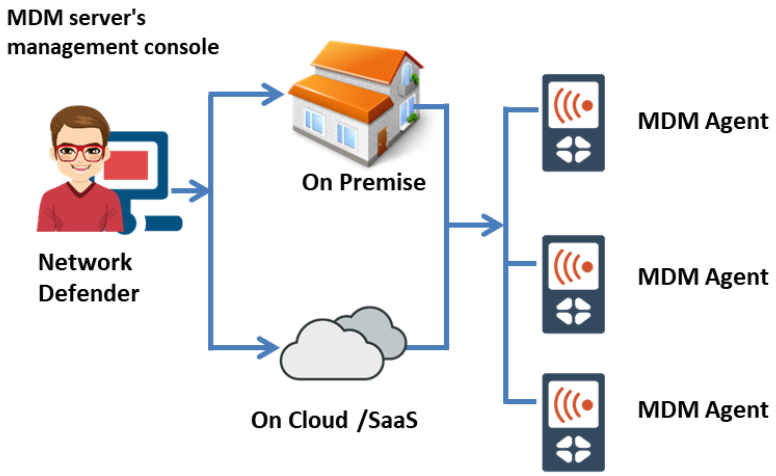


Figure 8.2: MDM Solution Deployment

Features of MDM Solutions

- Security Management
- Device Configuration Management
- Device Inventory and Tracking
- Over-the-Air Application Distribution
- Enterprise Policy Management
  - Password Enforcement
  - Data Encryption Enforcement
- Enterprise Network Integration
- Remote Data Wipe
- Blacklisting/Whitelisting Apps and Devices

Mobile Device Management (MDM) Solutions

- **Miradore**

  Source: *https://www.miradore.com*

  Miradore helps ensure device and data security as well as data compliance across an organization. It can easily encrypt all confidential data, separate business and personal use, enforce safe passcodes and screen locks, and prevent the use of unwanted applications.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

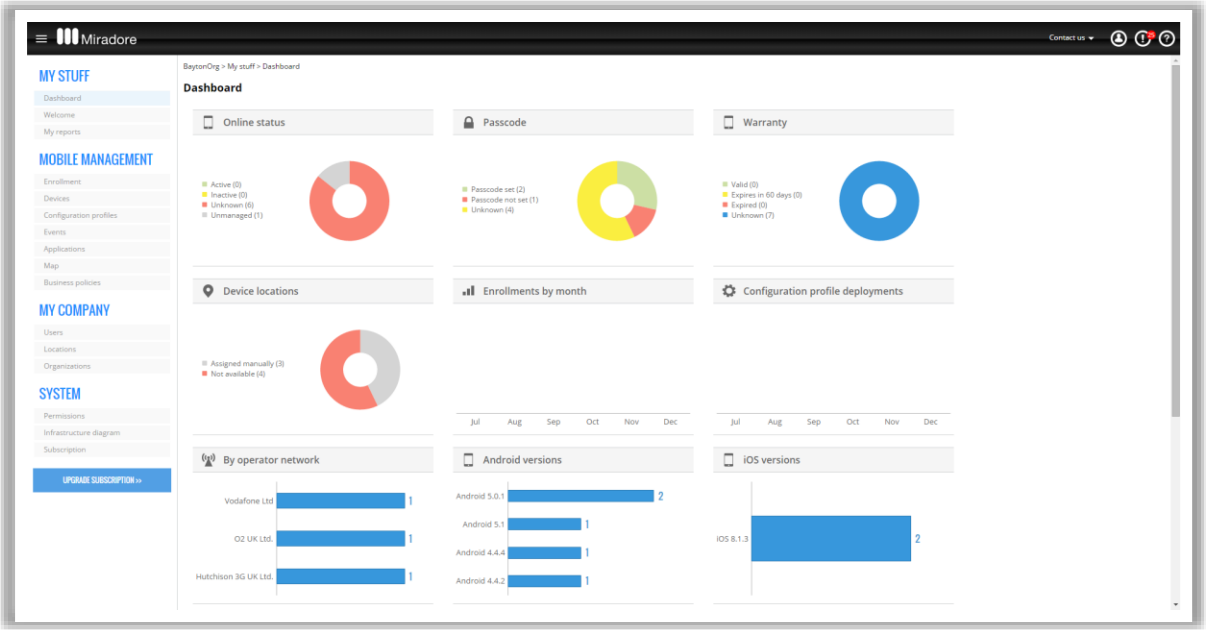
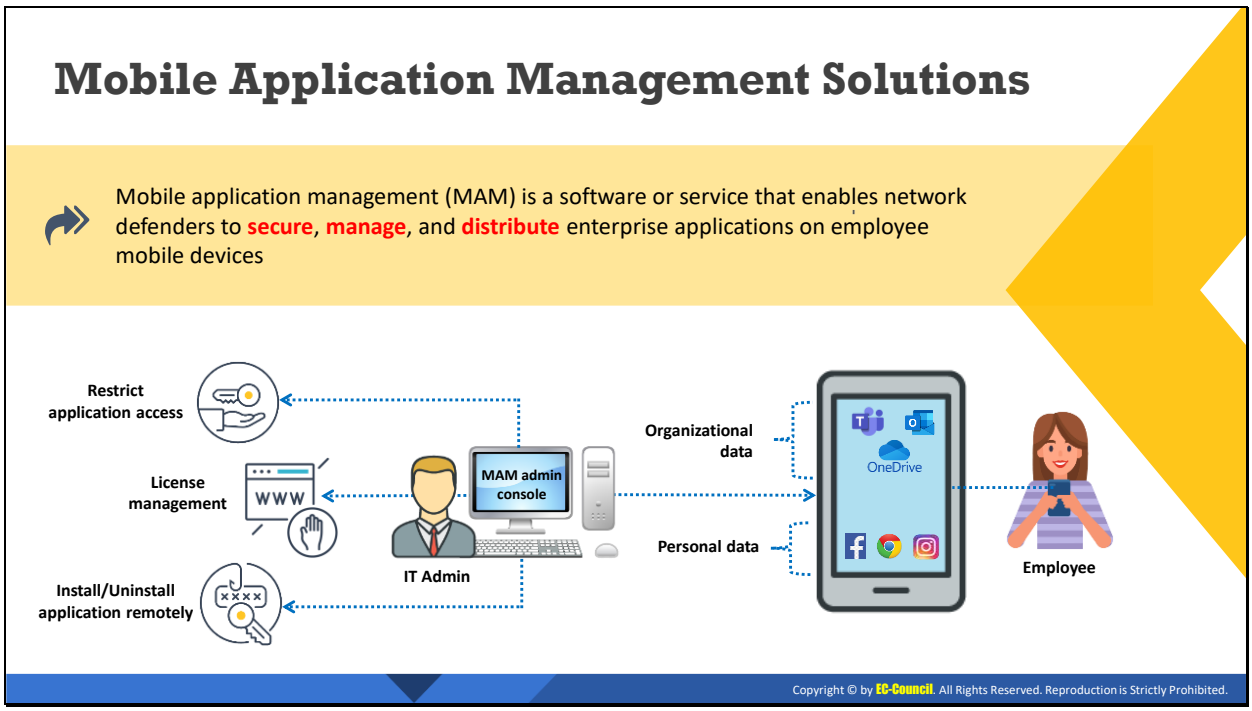


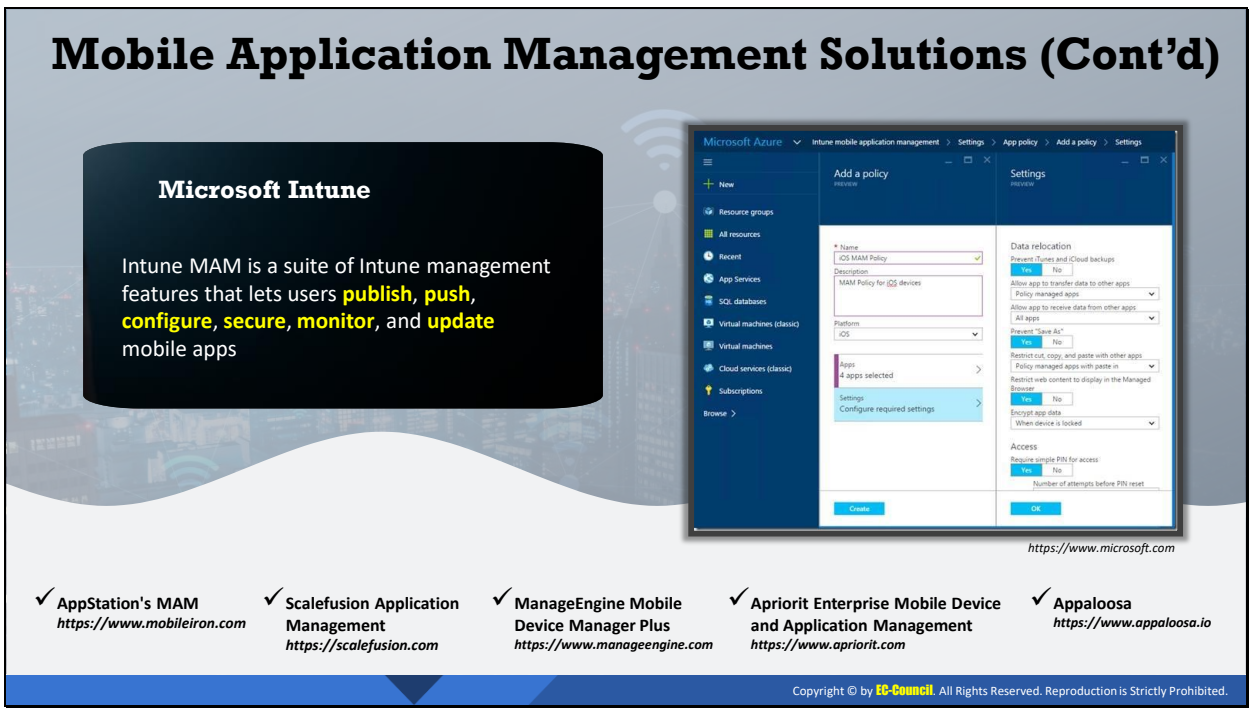
Figure 8.3: Screenshot of Miradore

Following are some examples of additional MDM solutions:

- AirWatch (*https://www.vmware.com*)
- Microsoft Intune (https://www.microsoft.com)
- IBM MaaS360 (*https://www.ibm.com*)
- XenMobile (*https://www.citrix.com*)
- Absolute Manage MDM (*http://www.absolute.com*)

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets





Mobile Application Management Solutions

Mobile application management (MAM) software and services enable an organization to secure, manage, and distribute enterprise applications on user mobile devices, without interfering with personal apps and data. Enterprise Application Management allows removing the access to a particular application for employees who left the organization. MAM can be applied to company-owned mobile devices and BYOD. It also enables the separation of enterprise apps and data from personal content on the same device.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

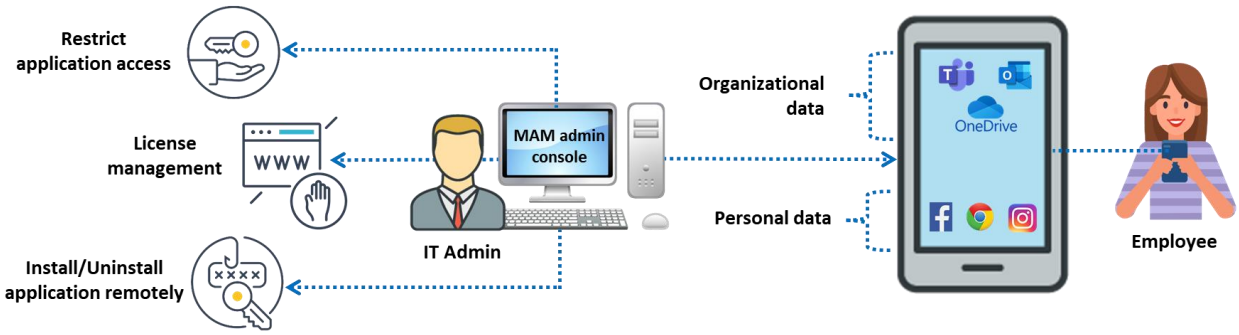


Figure 8.4: Mobile application management

Common features provided by MAM solutions:

- Device activation
- Enrollment and provisioning capabilities
- Remote wipe and other device-level functionalities
- Remote management does not require possession of the device
- Need minimal admin intervention and zero user action.

Services provided by Enterprise Application Management (MAM):

- Application delivery (enterprise app store)
- Software Licensing
- Application configuration
- Application authorization
- Application usage tracking
- Application lifecycle management
- Application updating
- Application performance monitoring
- User authentication
- Crash log reporting
- User and group access control
- App version management
- Push services
- Reporting and tracking
- Usage analytics
- Event management
- App wrapping

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Examples of Mobile Application Management (MAM)

- **Microsoft Intune**

  Source: *https://www.microsoft.com*

  Intune MAM is a suite of Intune management features that lets organizations publish, push, configure, secure, monitor, and update mobile apps for users.

  Intune MAM supports two configurations:

  - Intune MDM + MAM: Apps are managed using MAM and app protection policies on devices that are enrolled with Intune MDM.
  - MAM without device enrollment (MAM-WE): Apps are managed using MAM and app protection policies on devices that are not enrolled with Intune MDM.

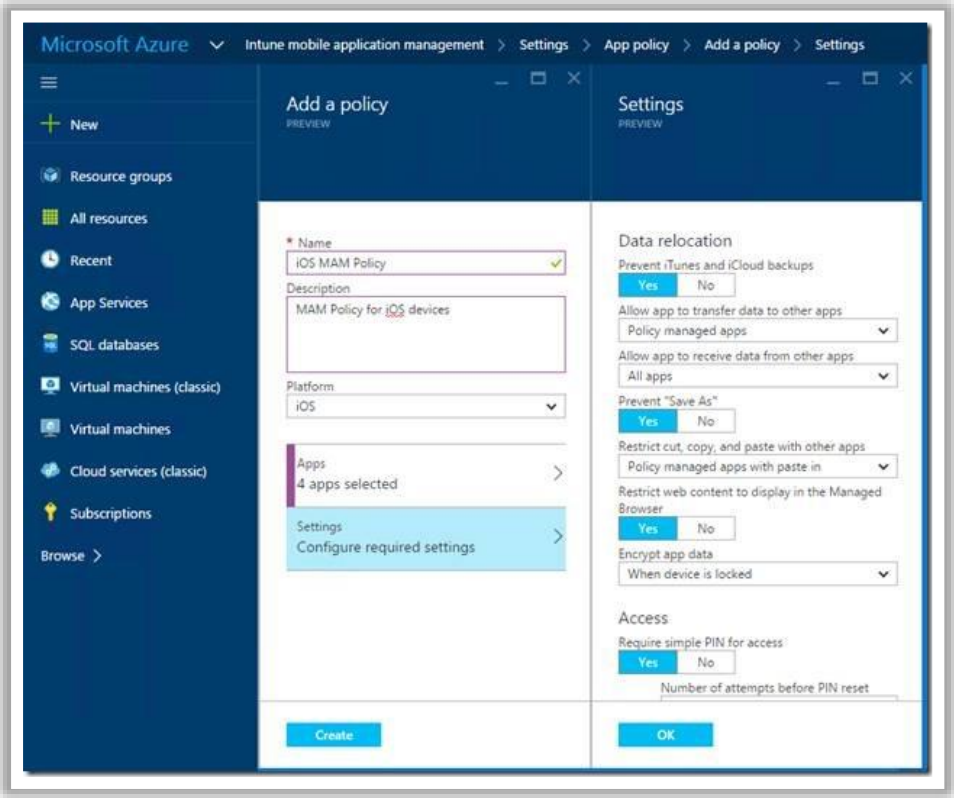
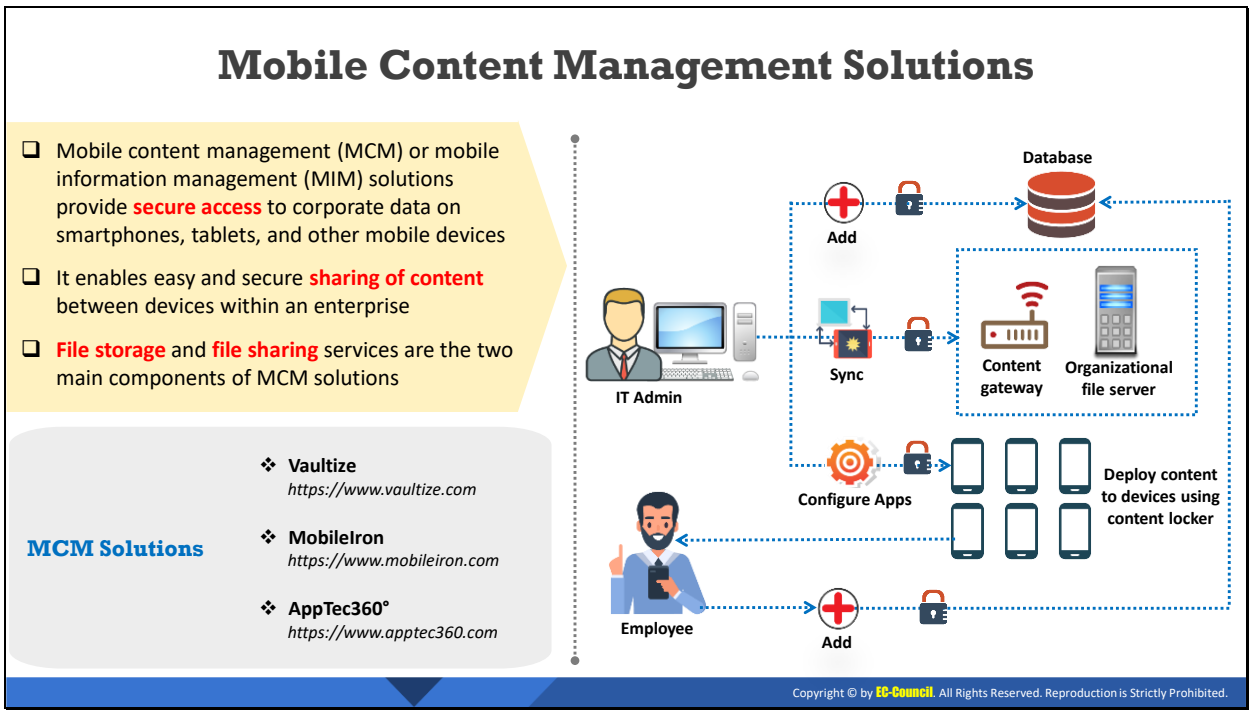


Figure 8.5: Microsoft Intune MAM

- AppStation's MAM (*https://www.mobileiron.com*)
- Scalefusion Application Management (*https://scalefusion.com*)
- ManageEngine Mobile Device Manager Plus (*https://www.manageengine.com*)
- Apriorit Enterprise Mobile Device and Application Management (*https://www.apriorit.com*)
- Appaloosa (*https://www.appaloosa.io*)

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Mobile Content Management Solutions

Mobile content management (MCM) or mobile information management (MIM) solutions provide secure access to corporate data (documents, spreadsheets, email, schedules, presentations, and other enterprise data) on mobile devices across the organizational networks without compromising with the speed. They enable easy and secure sharing of content between devices within an enterprise. File storage and file sharing services are the two main components of MCM solutions. MCM involves encrypting important information and allowing accessing, transmitting, or storing important information on only authorized apps using strong password protection policies.

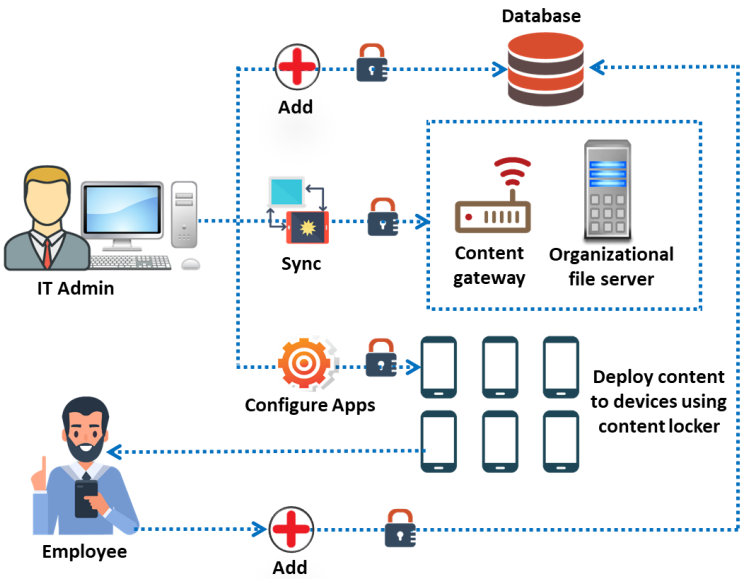


Figure 8.6: Mobile content management

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

MCM enables:

- **Multi-channel content delivery capabilities** that feature the management of a central content repository while delivering the content to devices simultaneously.
- **Content access control:** Access control to content includes
  - Authorization
  - Authentication
  - Access approval to content
  - Download control
  - Wipe-out for specific users
  - Time-specific access
- **Specialized templating system:** There are two approaches for adapting to mobile CMS templates.
  - **Multi-client approach** allows to view different versions of a site on the same domain and presents suitable templates based on the devices used by clients for viewing the website.
  - **Multi-site approach** displays mobile sites on a targeted sub-domain.
- **Location-based content delivery** provides content to mobile devices based on their current physical location.

Examples of MCM Solutions:

- Vaultize (*https://www.vaultize.com*)
- MobileIron (*https://www.mobileiron.com*)
- AppTec360° (*https://www.apptec360.com*)

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

Mobile Threat Defense Solutions

Mobile threat defense (MTD)/mobile threat management (MTM)/mobile threat prevention (MTP) protects organizations and their employees from threats on iOS and Android mobiles using different security technologies. The agents installed on the devices scan them for various mobile attacks using advanced threat intelligence. It uses machine learning and real-time analysis to protect mobile endpoints. MTD generate alerts for the enterprise mobility management (EMM) solutions to perform appropriate actions (switching mobiles into the quarantine state).

The MDM and MAM management tools only allow to set baseline management profiles for mobile devices and applications used within organizations. These two management tools lack insights related to app characteristics, protection against threats and user behaviors, reacting to threats dynamically, and providing continuous visibility of device health and trust. MTD extends EMM/MDM with additional security capabilities because it works with devices and secures them against the following attacks.

- It secures against device/physical threats by adding active threat detection and risk-based mobile management for more educated policy enforcement.
- It secures against malware.
- It secures against phishing.
- It secures against network attacks.

Factors to Consider Before Selecting an MTD solution:

The best suited MTD solution for an organization depends on

- The OS employed by the organization

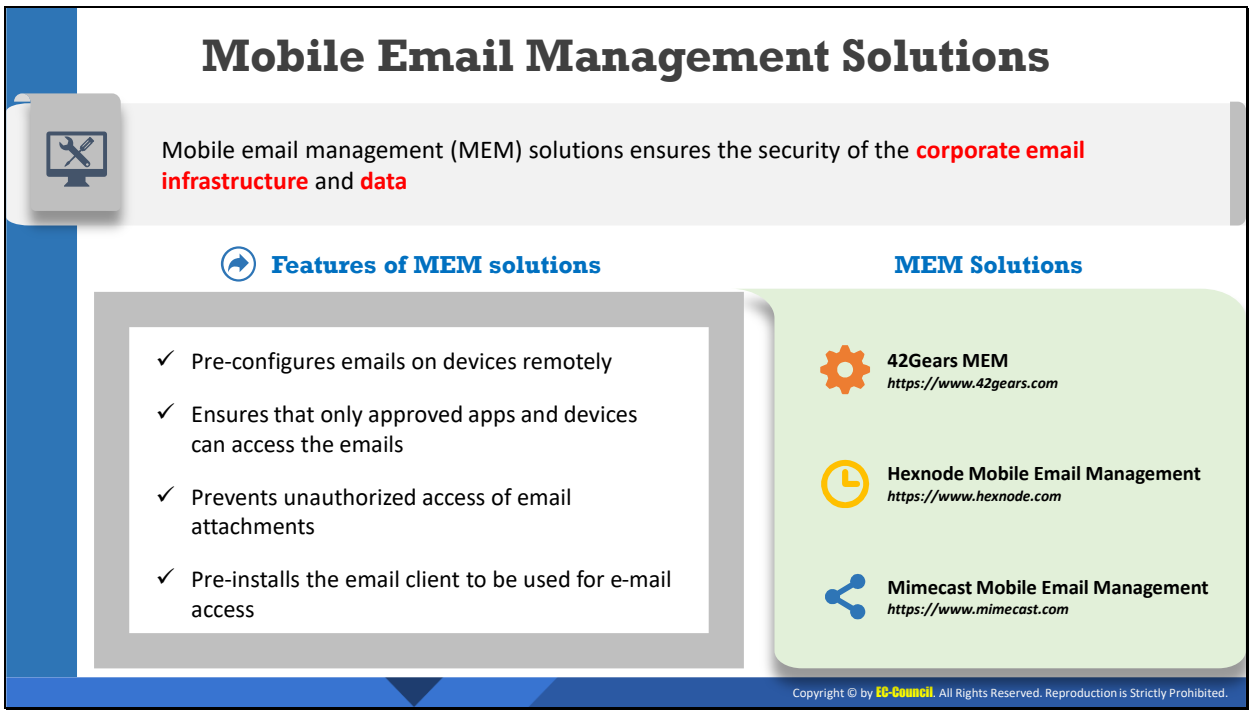
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- Mobile approach (BYOD or COPE)
- Type of access given to employees on their devices
- The EMM employed by the organization

Examples of MTD:

- MobileIron Threat Defense (MTD) (*https://www.mobileiron.com*)
- Pradeo Security Mobile Threat Defense (*https://www.pradeo.com*)
- Zimperium Mobile Threat Defense (MTD) (*https://www.zimperium.com*)
- Wandera Mobile Threat Defense (*https://www.wandera.com*)
- Lookout MTD (*https://www.lookout.com*)

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Mobile Email Management Solutions

Mobile email management (MEM) solutions ensure the security of the corporate email infrastructure and data on mobile devices. MEM allows

- Controlling mobile devices that access emails
- Prevention of data loss
- Enforcing strict compliance policies
- Encrypting sensitive corporate data

Common MEM Key Features:

- **Preconfiguring email on devices remotely:** Using MDM, MEM allows
  - Creating email accounts by associating an email policy with employee devices.
  - Configuring the email signature and setting up a default email account for users.
- **Ensure only approved apps and devices can access e-mail:** Using MDM, MEM provides
  - An additional layer of encryption through S/MIMEMDM.
  - Configuring Simple Certificate Enrollment Protocol (SCEP) for iOS and Windows devices to secure emails using certificates.
- **Prevent unauthorized access of email attachments:** Using MDM, MEM assures
  - Securing email attachments during transit and after downloading.
  - Ensuring secure viewing and storage of key attachments using the built-in document viewer of MEM, and MDM apps.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- Restricting document sharing to other devices or cloud services to prevent security breaches.

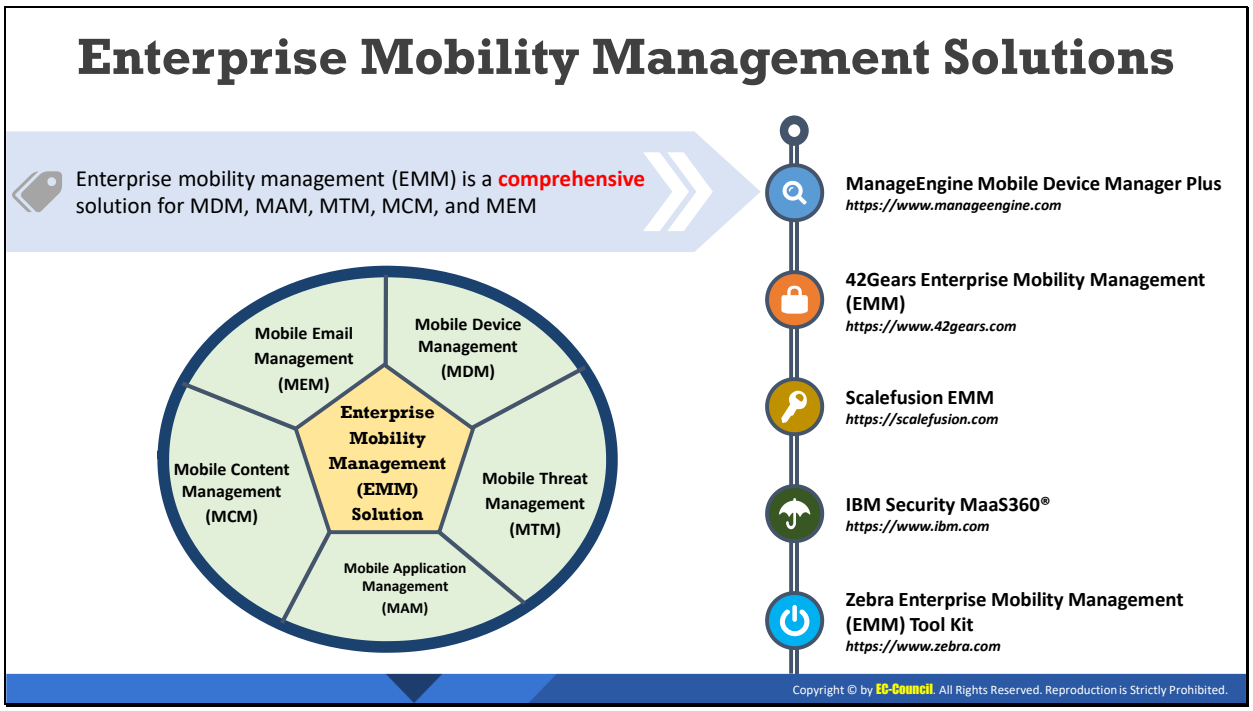
- **Pre-installing the email client to be used for email access:** The managed app configurations of MDM allow
  - Customizing the managed email app functionalities to suit the organizational requirements.
  - Distributing the app to devices.
  - Preconfiguring parameters (account type, domain name, and email signature) to make the app ready for corporate usage after installation.
  - Preconfiguring the app permissions.

Examples of MEM Solutions:

- 42Gears MEM (*https://www.42gears.com*)
- Hexnode Mobile Email Management (*https://www.hexnode.com*)
- Mimecast Mobile Email Management (*https://www.mimecast.com*)

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Enterprise Mobility Management Solutions

Enterprise mobility management (EMM) is a comprehensive solution responsible for MDM, MAM, MTM, MCM, and MEM. It safeguards the enterprise data accessed and used by employee mobile devices.

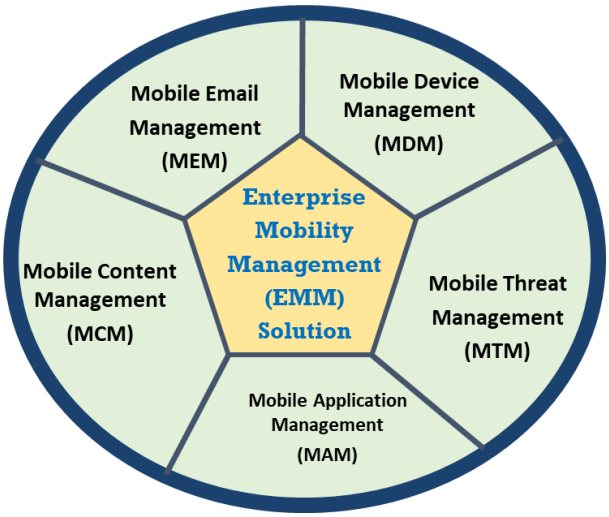


Figure 8.7: Enterprise Mobility Management Solution

Specifically, EMM is responsible for:

- Device management to provide the foundation for EMM solutions by
  - Enabling automatic device configuration
  - Allowing employees to be productive on the mobile devices they like to use

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

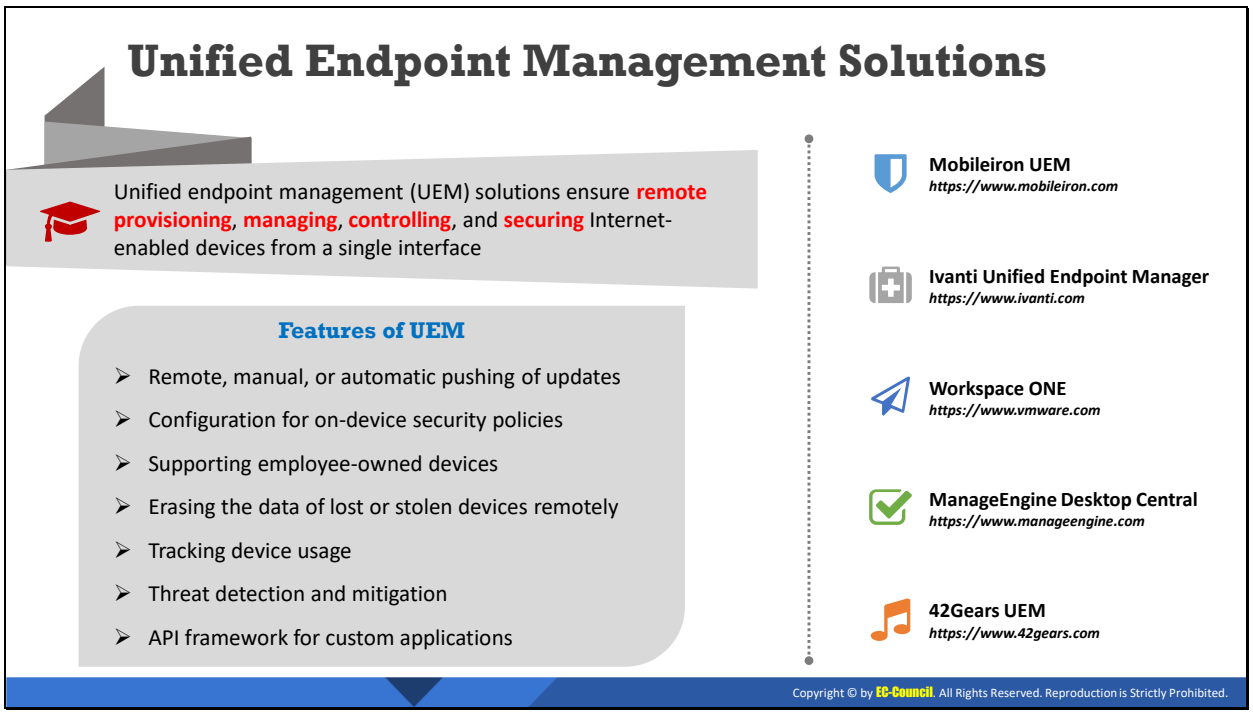
  - Wiping enterprise data from mobile devices selectively without interfering with personal data
  - Securing and managing mobile devices across multiple OSes (Android, iOS, macOS, and Windows 10)
- Content management
  - Encrypt email attachments
  - Establish DLP controls to secure corporate content
  - Secure corporate data distribution to mobile devices by applying content level policies (e.g., device-independent encryption keys, authentication, and file sharing)
- Application management
  - Protect applications on any device
  - Create and manage an enterprise app store
  - Provide authentication for end users on the device
  - Separate business and personal apps on mobile devices
  - User and identity management
- Mobile threat management
  - Protect organizations and their employees from threats on iOS and Android mobiles using different security technologies
- MEM
  - Provide security to the corporate email infrastructure and data on mobile devices

Examples of EMM Solutions:

- ManageEngine Mobile Device Manager Plus (*https://www.manageengine.com*)
- 42Gears Enterprise Mobility Management (EMM) (*https://www.42gears.com*)
- Scalefusion EMM (*https://scalefusion.com*)
- IBM Security MaaS360® (*https://www.ibm.com*)
- Zebra Enterprise Mobility Management (EMM) Tool Kit (*https://www.zebra.com*)

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Unified Endpoint Management Solutions

Unified endpoint management (UEM) solutions help in managing and controlling Internet-enabled mobile devices, desktops, applications, and content across the organization from a single interface. It provides security, management, and provisioning of mobile devices. UEM solutions address the problems of IT managers by extending MDM and EMM solutions.

Features and Capabilities of UEM

UEM solutions handle the unique security requirements in mobile enterprises by providing:

- App containerization
- Multi-OS environment
- Closed-loop automation features
- Certificate-based identity management
- Security for enterprise email, apps, and content
- Self-service features to simplify IT management
- DLP features to define open-in and copy/paste functions
- Help users maintain compliance with the corporate policies
- Secure multi-user profiles to securely allow users to share a single device
- Highly effective security measures that are invisible to the end users
- Per-app VPN technology that provides corporate network access to authorized apps only

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- Allow users to find and install critical enterprise apps (corporate email, calendar, etc.)
- Separate and manage highly sensitive personal and corporate data on mobile devices.
- Remote, manual, or automatic pushing of updates
- Configuration for on-device security policies
- Supporting employee-owned devices
- Erasing the data of lost or stolen devices remotely
- Tracking device usage
- Threat detection and mitigation
- API framework for custom applications

UEM Components

The key components that define the attributes of UEM solutions are:

- **CMT**

  CMT provides IT infrastructure to ensure the efficient working of mobile enterprises while enhancing the service to end users.

- **MDM**

  MDM provides a foundation for UEM solutions by allowing the IT team to

  - Secure corporate email
  - Certificate-based security
  - Automatic device configuration
  - Allow employees to be productive on the mobile devices they like to use
  - Wipe enterprise data from mobile devices selectively without interfering with personal data
  - Secure and manage mobile devices across multiple OSes (Android, iOS, macOS, and Windows 10)

- **MAM**

  MAM provides IT infrastructure to

  - Protect applications on any device
  - Create and manage an enterprise app store
  - Provide authentication for end users on a device
  - Separate business and personal apps on mobile devices

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- **MCM**

  MCM provides IT infrastructure to

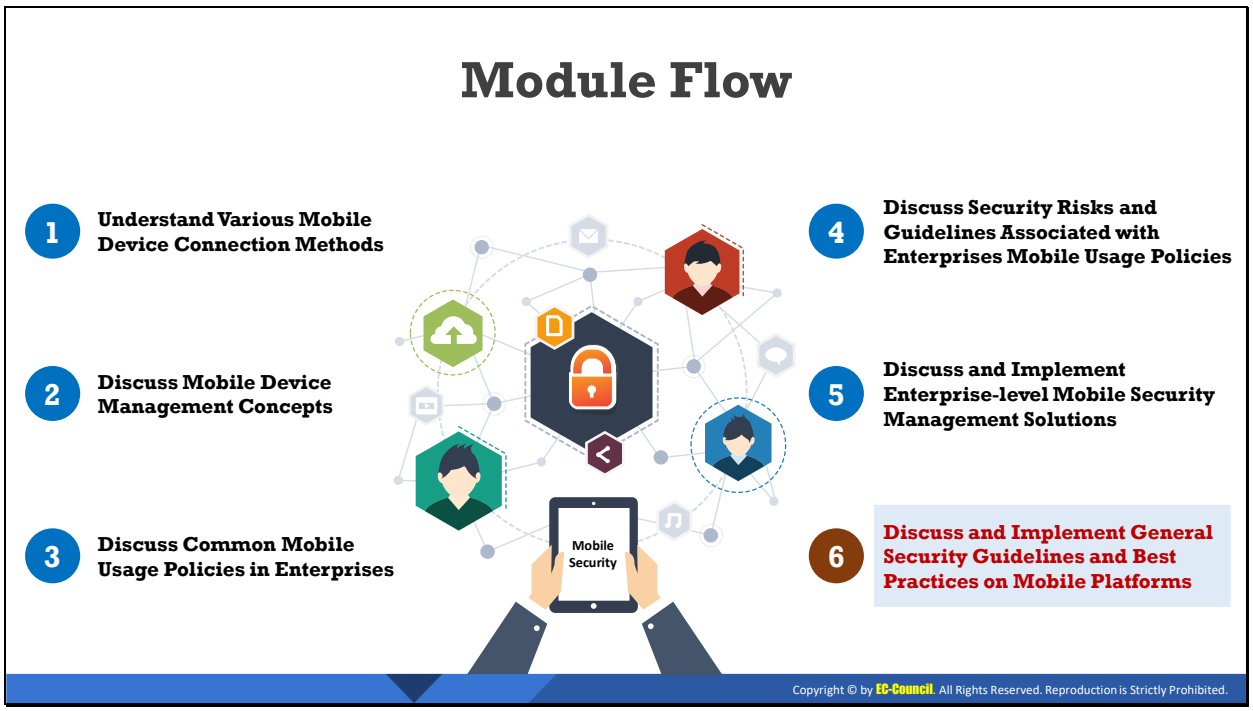
  - Encrypt email attachments
  - Establish DLP controls to secure corporate content
  - Secure corporate data distribution to mobile devices by applying content level policies (device-independent encryption keys, authentication, and file sharing)

Examples of UEM Solutions for Mobile Engagement:

- Mobileiron UEM (*https://www.mobileiron.com*)
- Ivanti Unified Endpoint Manager (*https://www.ivanti.com*)
- Workspace ONE UEM (*https://www.vmware.com*)
- ManageEngine Desktop Central (*https://www.manageengine.com*)
- 42Gears UEM (*https://www.42gears.com*)

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

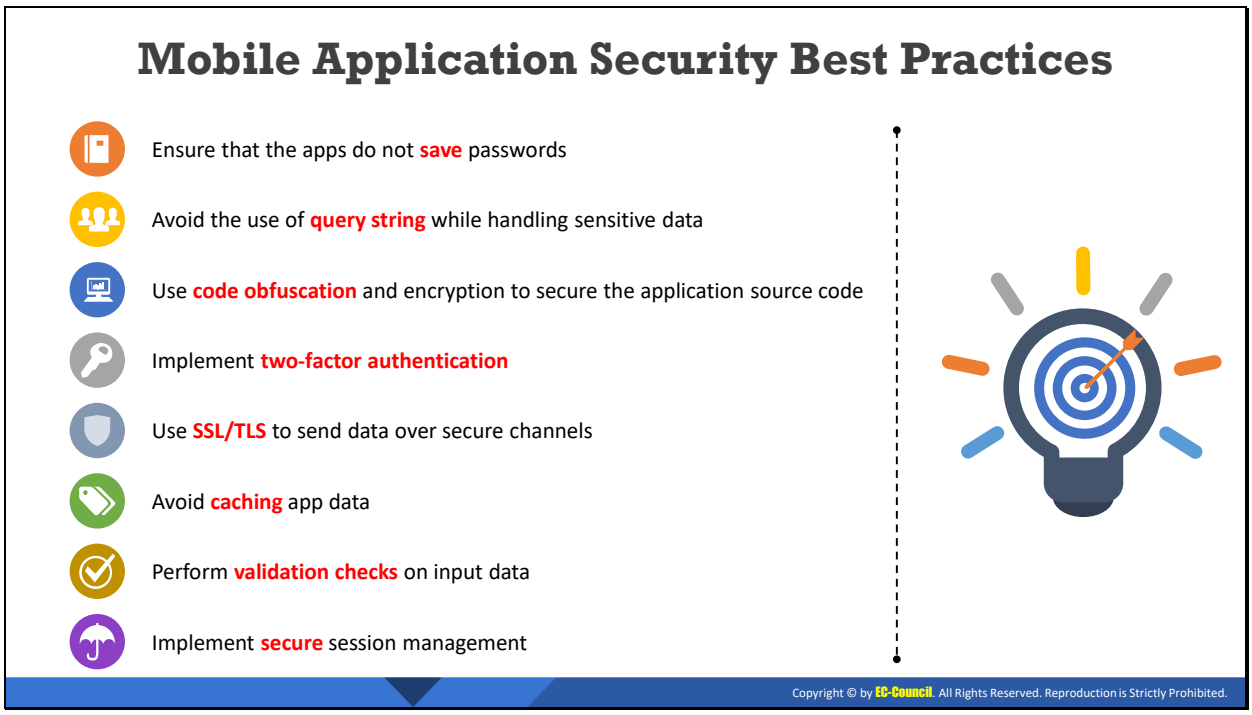
https://t.me/learningnets



Discuss and Implement General Security Guidelines and Best Practices on Mobile Platforms

Enterprise-level mobile security management solutions can only deliver their promised benefits if they are backed by strong mobile device security practices. The objective of this section is to explain the general security guidelines and best practices to be implemented for securing mobile platforms.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

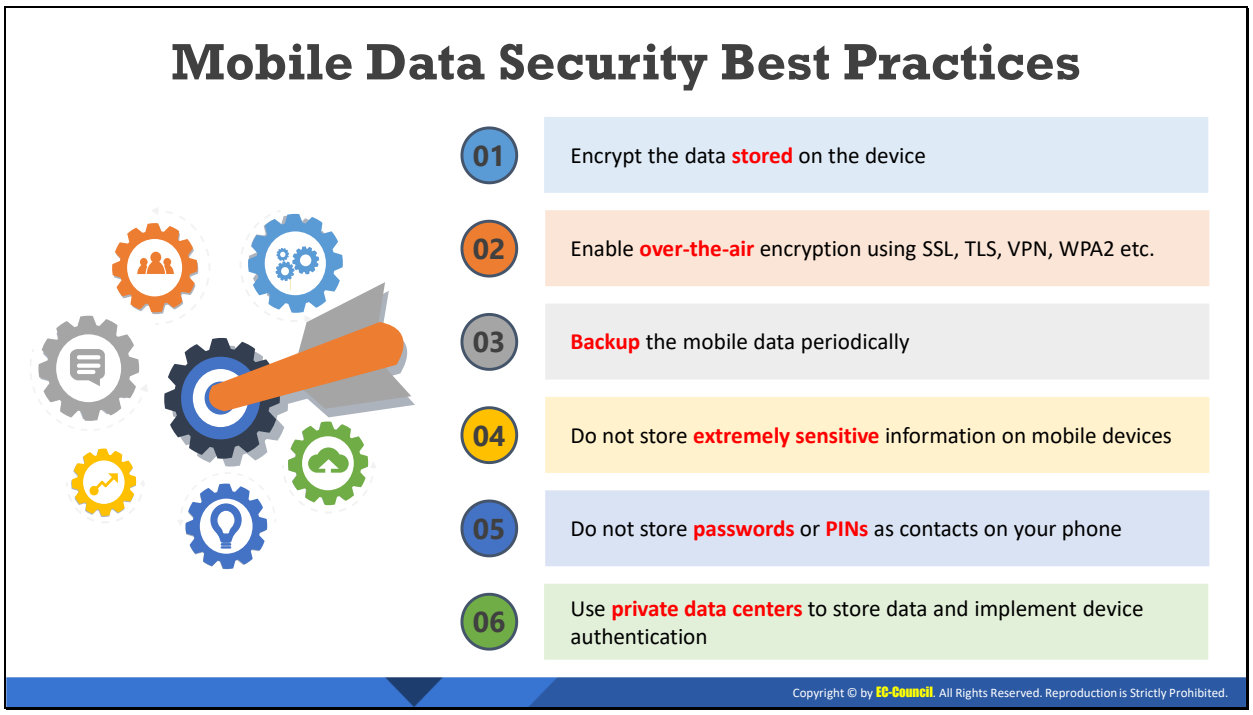


Mobile Application Security Best Practices

Security best practices that protect mobile applications:

- Ensure that the apps do not save passwords
- Avoid using query string while handling sensitive data
- Use code obfuscation and encryption to secure the application source code
- Implement two-factor authentication
- Use SSL/TLS to send data over a secure channel
- Avoid caching app data
- Perform validation checks on input data
- Implement secure session management
- Protect application setting
- Use server-side authentication
- Use cryptographic algorithms and key management
- Build threat models to defend data
- Ensure that employees download trusted apps from enterprise app stores
- Use containerization for critical corporate data
- Perform regular mobile security audits
- Regular software updates
- Implement jailbreak protection

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

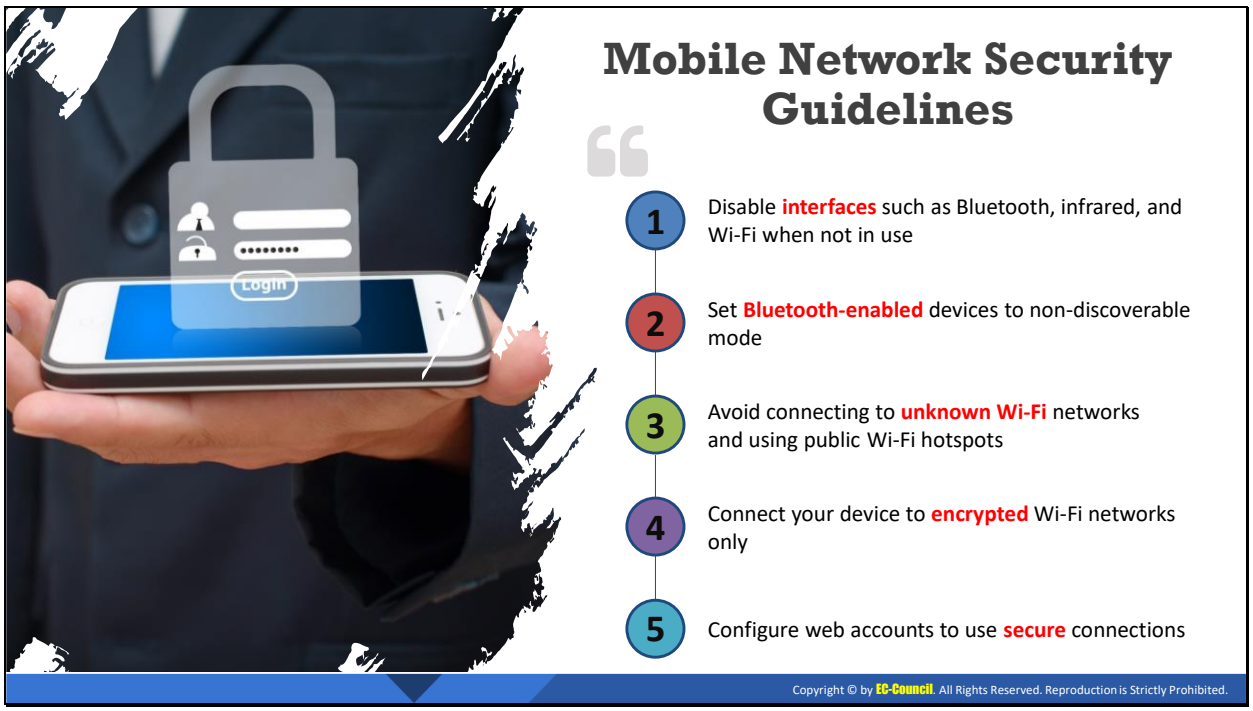


Mobile Data Security Best Practices

Security best practices that protect mobile data:

- Secure mobile infrastructure and strengthen the endpoints
- Encrypt the data stored on devices
- Enable over-the-air encryption using SSL, TLS, VPN, and WPA2
- Backup mobile data periodically
- Do not store extremely sensitive information on mobile devices
- Do not store passwords or PINs as contacts on your phone
- Use private data centers to store data and implement device authentication
- Maintain access control for devices and data
- Avoid public Wi-Fi networks
- Set automatic device locks when devices are not in use
- Ensure that users can access the corporate data from a secure central location
- Complete software updates and patches in a timely manner
- Educate employees to recognize suspicious emails
- Keep the antivirus and anti-malware software updated
- Train employees to encrypt hard drives and USBs before storing any work-related data on them

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Mobile Network Security Guidelines

Security best practices that protect mobile networks:

- Disable interfaces such as Bluetooth, infrared, and Wi-Fi when not in use
- Set Bluetooth-enabled devices to non-discoverable mode
- Avoid connecting to unknown Wi-Fi networks and using public Wi-Fi hotspots
- Connect the mobile devices to encrypted Wi-Fi networks only
- Configure web accounts to use secure connections
- Isolate a group of users using different SSIDs and segment the traffic for these groups to different VLANS
- Apply different firewall rules and filters to different combinations of user groups or devices
- Configure web accounts to use secure connections

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

General Guidelines for Mobile Platform Security

Given below are various guidelines that can help users to protect their mobile devices.

- Do not install too many applications and avoid auto-uploading photos to social networks
- Perform security assessment for the application architecture
- Maintain configuration control and management
- Install applications from trusted app stores
- Securely wipe or delete the data while disposing of devices
- Do not share any information within GPS-enabled apps unless required
- Never connect two separate networks such as Wi-Fi and Bluetooth simultaneously
- Disable wireless access such as Wi-Fi and Bluetooth if not in use
- Never connect two separate networks such as Wi-Fi and Bluetooth simultaneously
- Configure a strong passcode with the maximum possible length
- Update the OS and apps to keep them secure
- Enable Remote Management
- Do Not Allow Rooting or Jailbreaking
- Use remote wipe services such as Find My Device (Android) and Find My iPhone or Find My (Apple iOS) to locate your device if it is lost or stolen
- Encrypt the device and its backups
- Perform Periodic Backup and Synchronization

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- Filter emails by configuring the server-side settings of the corporate email system
- Strengthen Browser Permission Rules
- Design and Implement Mobile Device Policies
- Control devices and applications
- Prohibit USB keys
- Manage the operating and application environments
- Press the power button to lock the device when not in use

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

Android Security Tools

- **Kaspersky Internet Security for Android**

  Source: *https://my.kaspersky.com*

  Kaspersky Internet Security for Android blocks suspicious apps, websites, and files. It allows you to control access to specific apps and stops spyware monitoring calls, texts, and location. It includes anti-theft tools to protect mobiles and data. It uses machine learning to combat new threats.

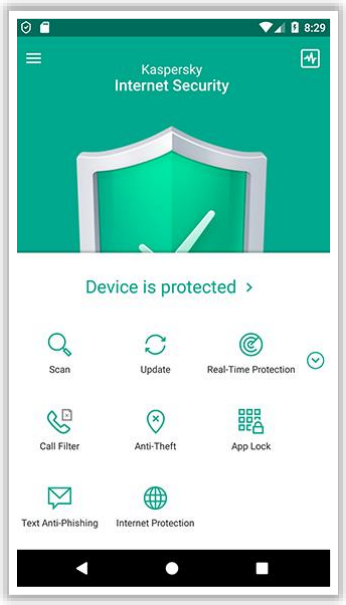


Figure 8.8: Screenshot of Kaspersky Mobile Antivirus

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Following are some additional Android security tools:

- Avira Antivirus Security (*https://www.avira.com*)
- Avast Mobile Security (*https://www.avast.com*)
- McAfee Mobile Security (*https://www.mcafeemobilesecurity.com*)
- Lookout Mobile Security and Antivirus (*https://www.lookout.com*)
- Sophos Mobile Security (*https://www.sophos.com*)

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

iOS Device Security Tools

- **Avira Mobile Security**

  Source: https://www.avira.com

  Avira Mobile Security provides features such as web protection and identity safeguarding, identifies phishing websites that target a specific user, tracks a device, organizes the device memory, and backs up all contacts and other data for all iOS devices.

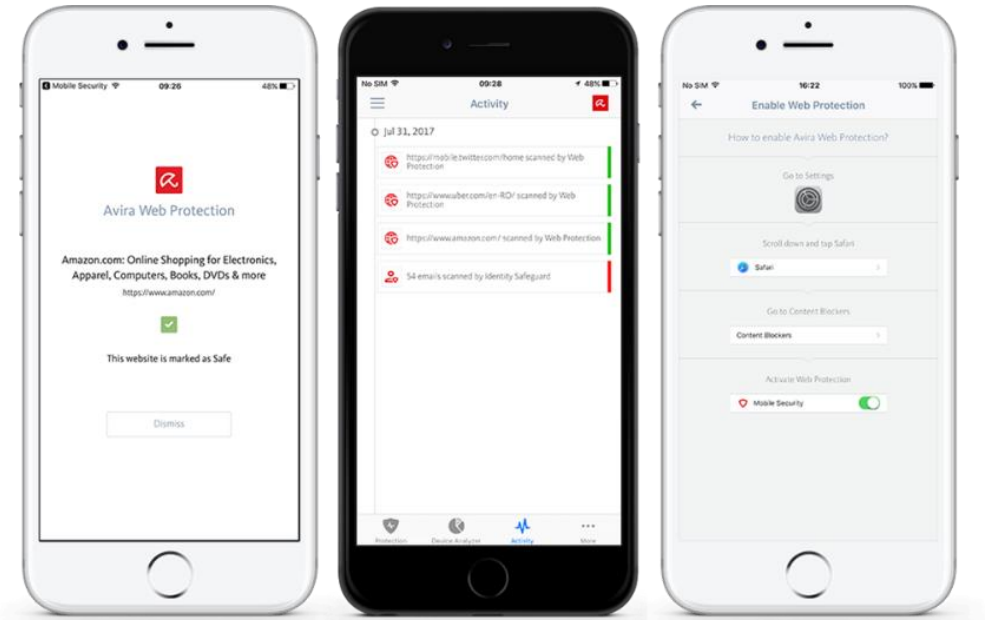


Figure 8.9: Screenshots of Avira Mobile Security

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Following are some additional iOS device security tools:

- Norton Mobile Security (*https://us.norton.com*)
- LastPass Password Manager (*https://www.lastpass.com*)
- Lookout Mobile Security (*https://www.lookout.com*)
- SplashID Safe Password Manager (*https://www.splashid.com*)
- Webroot Mobile Security (*https://www.webroot.com*)

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

Module Summary

This module discussed various mobile device connection methods. It discussed the concepts of mobile device management as well as the common mobile use approaches in enterprises. Furthermore, it discussed the security risk and guidelines associated with enterprise mobile usage policies. This module also introduced enterprise-level mobile security management solutions. Finally, this module presented an overview of general security guidelines and best practices for mobile platforms.

In the next module, we will discuss IoT device security in detail.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

EC-Council

N|DE™
Network Defense Essentials

Module 09

IoT Device Security

https://t.me/learningnets

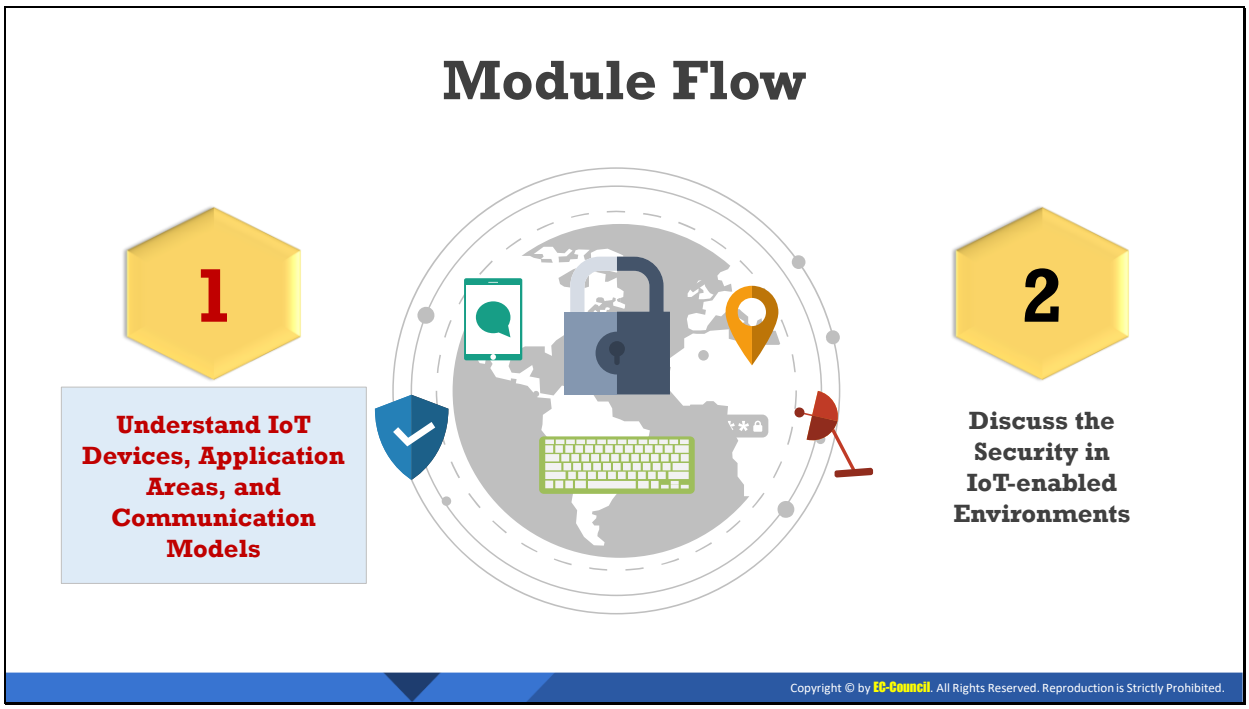
Module Objectives

The use of Internet of Things (IoT) devices in enterprise IT infrastructure has created a vast security perimeter. IoT devices use both networks and the cloud. However, they are highly vulnerable to malware, ransomware, and botnet attacks. Attackers can easily compromise IoT endpoints. Understanding the security measures will help in securing IoT-enabled environments.

At the end of this module, you will be able to do the following:

- Understand the IoT and why organizations opt for IoT-enabled environments
- Describe the IoT application areas and IoT devices
- Describe the IoT architecture and IoT communication models
- Understand the security in IoT-enabled environments and stack-wise IoT security principles
- Understand the security considerations of the IoT framework
- Understand IoT device management
- Understand the best practices and tools for IoT security

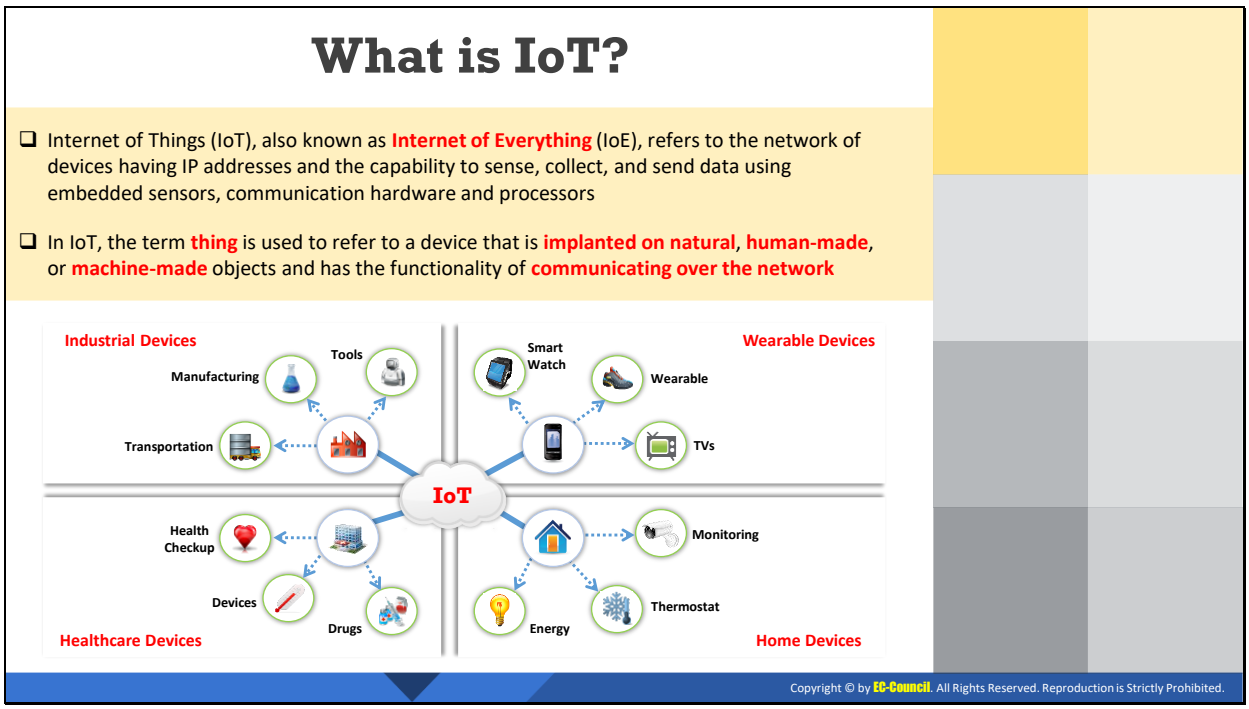
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Understand IoT Devices, Application Areas, and Communication Models

The objective of this section is to understand IoT devices and areas where IoT devices can be used in an enterprise.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



What is IoT?

The Internet of Things (IoT), also known as the Internet of Everything (IoE), refers to computing devices that are web-enabled and have the capability of sensing, collecting, and sending data using sensors, and the communication hardware and processors that are embedded within the device. In the IoT, a "thing" refers to a device that is implanted in a natural, human-made, or machine-made object and has the functionality of communicating over a network. The IoT utilizes existing emerging technology for sensing, networking, and robotics, therefore allowing the user to achieve deeper analysis, automation, and integration within a system.

With the increase in the networking capabilities of machines and everyday appliances used in different sectors like offices, homes, industry, transportation, buildings, and wearable devices, they open up a world of opportunities for the betterment of business and customer satisfaction. Some of the key features of the IoT are connectivity, sensors, artificial intelligence, small devices, and active engagement.

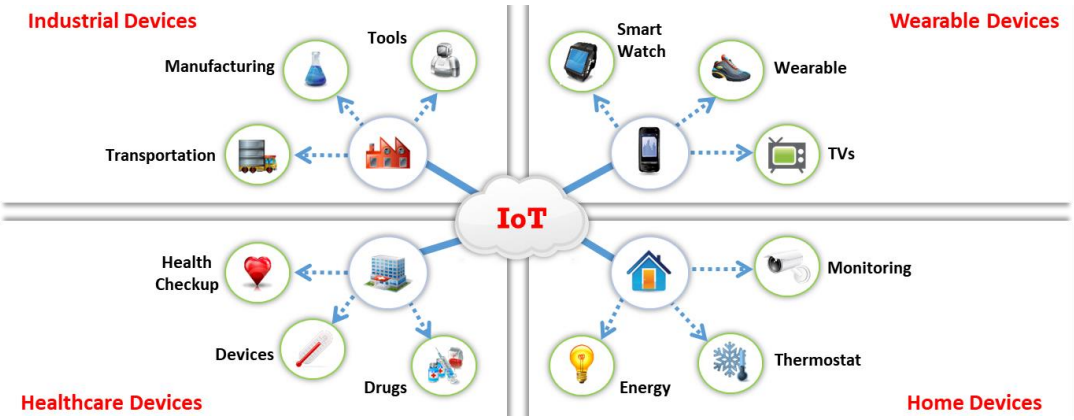
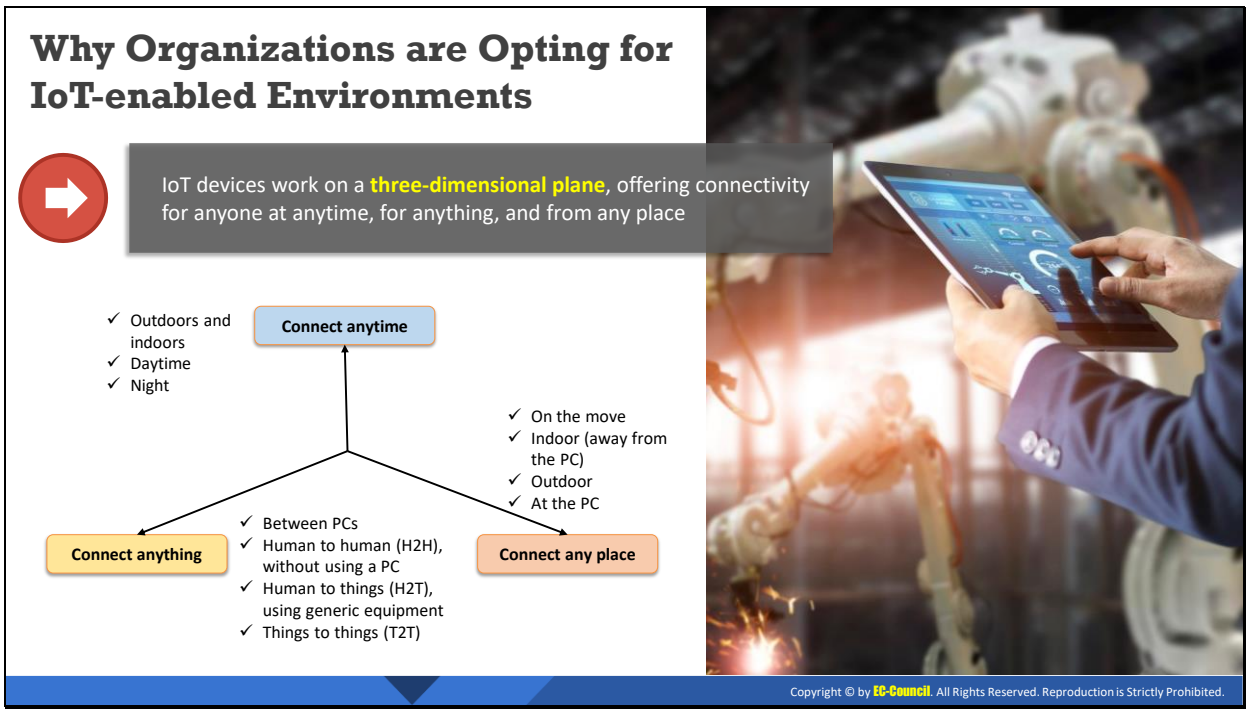


Figure 9.1: Illustration of IoT devices

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Why Organizations are Opting for IoT-enabled Environments

Organizations are opting for IoT-enabled environments because IoT devices work on a three-dimensional plane and provide connectivity for anyone at any time, for anything, and from any place. IoT devices facilitate connection to various objects; examples include Human-to-Thing (H2T) interactions using generic equipment, Thing-to-Thing (T2T) interactions between PCs, and Human-to-Human (H2H) interactions without using a PC. The user can connect to IoT devices at any place regardless of whether they are on the move, indoor (away from PC), outdoor, or at the PC. The working mechanism of IoT devices on the three-dimensional plane allows the user to continuously monitor their business, resolve concerns instantly, increase the efficiency of the business, enhance the growth of the organization, increase security, etc.

Some key features of IoT are connectivity, sensors, artificial intelligence, small devices, and active engagement. IoT technology includes four primary systems: IoT devices, gateway systems, data storage systems based on the cloud, and remote control using mobile apps. These systems together enable communication between two endpoints. Discussed below are some of the important components of IoT technology that play an essential role in the working of an IoT device.

- **Sensing technology:** Sensors embedded in devices acquire a wide variety of information from the surroundings such as the temperature, gases, location, working of industrial machines, and health data of a patient.
- **IoT gateways:** Gateways are used to bridge the gap between an IoT device (internal network) and the end user (external network), thereby allowing them to connect and communicate with each other. The data collected by the sensors in IoT devices are collected and sent to the concerned user or cloud through the gateway.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **Cloud server/data storage:** The collected data, after traveling through the gateway, arrives at the cloud, where it is stored and subjected to data analysis. The processed data is then transmitted to the user, who takes actions based on the information received.
- **Remote control using mobile apps:** The end user utilizes remote control devices such as mobile phones, tablets, and laptops installed with a mobile app to monitor, control, retrieve data from, and take actions on IoT devices from a remote location.

Example:

1. A smart security system is integrated with a gateway, which in turn helps connect the device to the Internet and cloud infrastructure.
2. The data storage in the cloud includes the information of every device connected to the network. The information includes the device IDs, the present status of the devices, who accessed the devices, and how many times they accessed the devices. It also includes information such as for how long the device was accessed the last time.
3. The connection with the cloud server is established through web services.
4. The user on the other side, who has the required app to access a device remotely on their mobile phone, interacts with the app and, in turn, with the device. Before accessing the device, they are asked to authenticate themselves. If the submitted credentials match those saved in the cloud, the user obtains access. Otherwise, access is denied, ensuring security. The cloud server identifies the device's ID and sends a request associated with that device using gateways.
5. If the security system recording footage senses any unusual activity, then it sends an alert to the cloud through the gateway, which matches the device's ID and the user associated with it. Finally, the end user receives an alert.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

IoT Application Areas and Devices

Service Sectors	Application Groups	Locations	Devices
Buildings	Commercial/Institutional	Office, Education, Retail, Hospitality, Healthcare, Airports, Stadiums	HVAC, Transport, Fire & Safety, Lighting, Security, Access, etc.
	Industrial	Process, Clean Room, Campus	
Energy	Supply/Demand	Power Gen, Trans & Dist, Low Voltage, Power Quality, Energy management	Turbines, Windmills, UPS, Batteries, Generators, Meters, Drills, Fuel Cells, etc.
	Alternative	Solar Wind, Co-generation, Electrochemical	
	Oil/Gas	Rigs, Derricks, Heads, Pumps, Pipelines	
Consumer and Home	Infrastructure	Wiring, Network Access, Energy management	Digital Cameras, Power Systems, MID, e-Readers, Dishwashers, Desktop Computers, Washing Machines/Dryers, Meters, Lights, TVs, MP3 Devices, Games Consoles, Alarms, etc.
	Awareness & Safety	Security/Alerts, Fire Safety, Elderly, Children, Power Protection	
	Convenience & Entertainment	HVAC/Climate, Lighting, Appliance, Entertainment	
Healthcare and Life Science	Care	Hospital, ER, Mobile, POC, Clinic, Labs, Doctor Office	MRI Machines, PDAs, Implants, Surgical Equipment, Pumps, Monitors, Telemedicine, etc.
	In Vivo/Home	Implants, Home, Monitoring Systems	
	Research	Drug Discovery, Diagnostics, Labs	
Transportation	Non-Vehicular	Air, Rail, Marine	Vehicles, Lights, Ships, Planes, Signage, Tolls, etc.
	Vehicles	Consumer, Commercial, Construction, Off-Highway	
	Trans Systems	Tolls, Traffic mgmt., Navigation	

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

IoT Application Areas and Devices (Cont'd)

Service Sectors	Application Groups	Locations	Devices
Industrial	Resource Automation	Mining, Irrigation, Agricultural, Woodland	Pumps, Valves, Vats, Conveyors, Fabrication, Assembly/Packaging, Vessels/Tanks, etc.
	Fluid/Processes	Petro-Chem, Hydro, Carbons, Food, Beverage	
	Converting/Discrete	Metals, Papers, Rubber/Plastic, Metalworking electronics, Assembly/Test	
	Distribution	Pipelines, Conveyance	
Retail	Specialty	Fuel Stations, Gaming, Bowling, Cinemas, Discos, Special Events	POS Terminals, Tags, Cash Registers, Vending Machines, Signs, etc.
	Hospitality	Hotels Restaurants, Bars, Cafes, Clubs	
	Stores	Supermarkets, Shopping Centers, Single Site, Distribution, Centers	
Security / Public Safety	Surveillance	Radar/Satellite, Environ., Military Security, Unmanned, Fixed	Tanks, Fighter Jets, Battlefields, Jeeps, Cars, Ambulance, Homeland Security, Environment, Monitor, etc.
	Equipment	Weapons, Vehicles, Ships, Aircraft, Gear	
	Tracking	Human, Animal, Postal, Food, Health, Baggage	
	Public Infrastructure	Water, Treatment, Building, Environ. Equip. & Personnel, Police, Fire, Regulatory	
	Emergency Services	Ambulance, Police, Fire, Homeland Security	
IT and Networks	Public	Services, E-Commerce, Data Centers, Mobile Carriers, ISPs	Servers, Storage, PCs, Routers, Switches, PBXs, etc.
	Private Enterprise	IT/Data Center Office, Privacy Nets	

http://www.beechamresearch.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

IoT Application Areas and Devices

IoT devices have a wide range of applications. They are used in almost every sector of society to assist in various ways to simplify routine work and personal tasks and, thus, improve the standard of living. IoT technology is included in smart homes and buildings, healthcare devices, industrial appliances, transportation, security devices, the retail sector, etc.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Some of the applications of IoT devices are as follows:

- Smart devices that are connected to the Internet, providing different services to end-users, include thermostats, lighting systems and security systems, and several other systems that reside in buildings.
- In the healthcare and life science sectors, devices include wearable devices, health monitoring devices such as implanted heart pacemakers, ECG, EKG, surgical equipment, telemedicine, etc.
- The Industrial Internet of Things (IIoT) is attracting growth through three approaches: increasing production to boost revenue, using intelligent technology that is entirely changing the way goods are made, and the creation of new hybrid business models.
- Similarly, use of IoT technology in the transportation sector follows the concept of vehicle-to-vehicle, vehicle-to-roadside, and vehicle-to-pedestrian communication, thus improving traffic conditions, navigation systems, and parking schemes.
- IoT in retail is mainly used in payments, advertisements, and tracking or monitoring products to protect them from theft and loss, thereby increasing revenue.
- In IT and networks, IoT devices mainly include various office machines such as printers, fax machines, and copiers as well as PBX monitoring systems; these serve to improve communication between endpoints and provide ease of sending data across long distances.

Source: *http://www.beechamresearch.com*

Service Sectors	Application Groups	Locations	Devices
Buildings	Commercial/ Institutional	Office, Education, Retail, Hospitality, Healthcare, Airports, Stadiums	Heating, Ventilation, and Air Conditioning (HVAC), Transport, Fire and Safety, Lighting, Security, Access, etc.
	Industrial	Process, Clean Room, Campus	
Energy	Supply/ Demand	Power Generation, Transport, and Distribution, Low Voltage, Power Quality, Energy Management	Turbines, Windmills, UPS, Batteries, Generators, Meters, Drills, Fuel Cells, etc.
	Alternative	Solar Wind, Co-generation, Electrochemical	
	Oil/Gas	Rigs, Derricks, Heads, Pumps, Pipelines	
Consumer and Home	Infrastructure	Wiring, Network Access, Energy Management	Digital Cameras, Power Systems, MID, e-Readers, Dishwashers, Desktop Computers, Washing Machines / Dryers, Meters, Lights, TVs, MP3 Devices, Games Consoles, Alarms, etc.
	Awareness and Safety	Security/Alerts, Fire Safety, Elderly, Children, Power Protection	
	Convenience and Entertainment	HVAC/Climate, Lighting, Appliances, Entertainment	

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

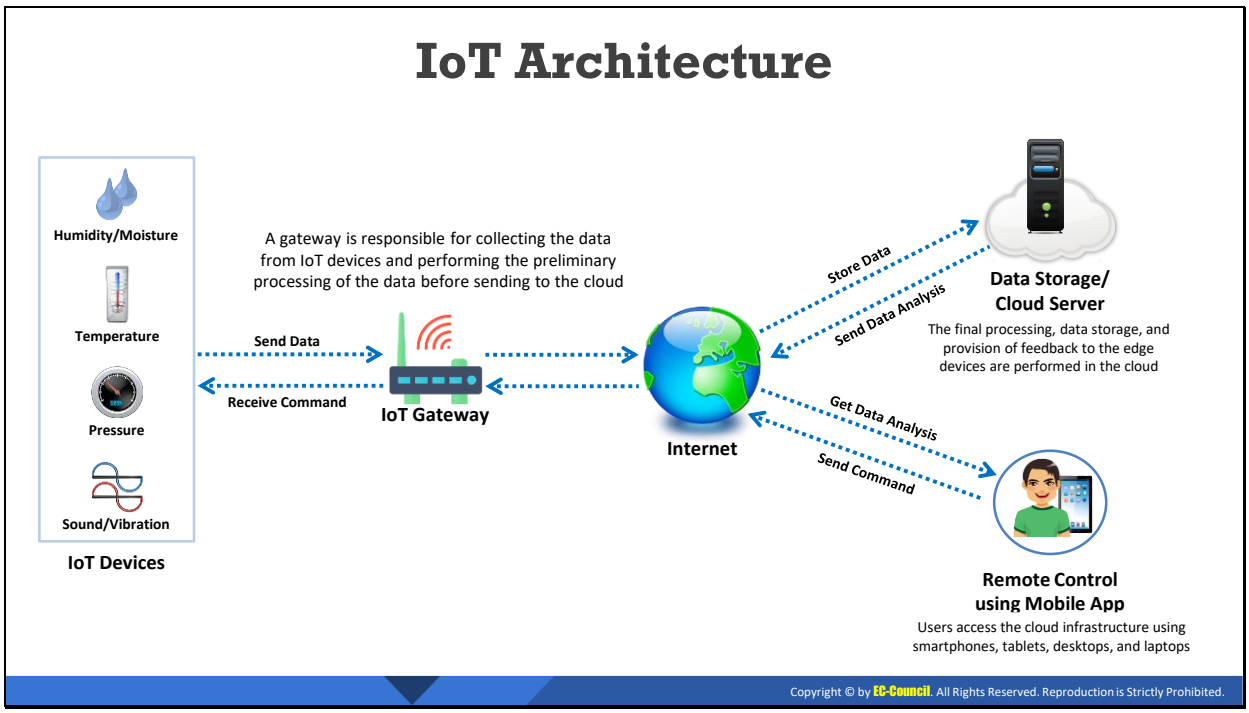
https://t.me/learningnets

Healthcare and Life Science	Care	Hospital, ER, Mobile, POC, Clinic, Labs, Doctors' Offices	MRI Machines, PDAs, Implants, Surgical Equipment, Pumps, Monitors, Telemedicine, etc.
	In Vivo/Home	Implants, Home, Monitoring Systems	
	Research	Drug Discovery, Diagnostics, Labs	
Transportation	Non-Vehicular	Air, Rail, Marine	Vehicles, Lights, Ships, Planes, Signage, Tolls, etc.
	Vehicles	Consumer, Commercial, Construction, Off-Highway	
	Transport Systems	Tolls, Traffic Management, Navigation	
Industrial	Resource Automation	Mining, Irrigation, Agricultural, Woodland	Pumps, Valves, Vats, Conveyors, Fabrication, Assembly/Packaging, Vessels/Tanks, etc.
	Fluid/ Processes	Petrochemicals, Hydro, Carbons, Food, Beverages	
	Converting/ Discrete	Metals, Papers, Rubber/Plastic, Metalworking, Electronics, Assembly/Test	
	Distribution	Pipelines, Conveyance	
Retail	Specialty	Fuel Stations, Gaming, Bowling, Cinemas, Discos, Special Events	POS Terminals, Tags, Cash Registers, Vending Machines, Signs, etc.
	Hospitality	Hotels Restaurants, Bars, Cafes, Clubs	
	Stores	Supermarkets, Shopping Centers, Single Site, Distribution, Centers	
Security / Public Safety	Surveillance	Radar/Satellite, Environment, Military Security, Unmanned, Fixed	Tanks, Fighter Jets, Battlefields, Jeeps, Cars, Ambulance, Homeland Security, Environment, Monitor, etc.
	Equipment	Weapons, Vehicles, Ships, Aircraft, Gear	
	Tracking	Human, Animal, Postal, Food, Health, Baggage	
	Public Infrastructure	Water, Treatment, Building, Environment, Equipment and Personnel, Police, Fire, Regulatory	
	Emergency Services	Ambulance, Police, Fire, Homeland Security	
IT and Networks	Public	Services, E-Commerce, Data Centers, Mobile Carriers, ISPs	Servers, Storage, PCs, Routers, Switches, PBXs, etc.
	Private Enterprise	IT/Data Center Office, Privacy Nets	

Table 9.1: IoT application areas and devices

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



IoT Architecture

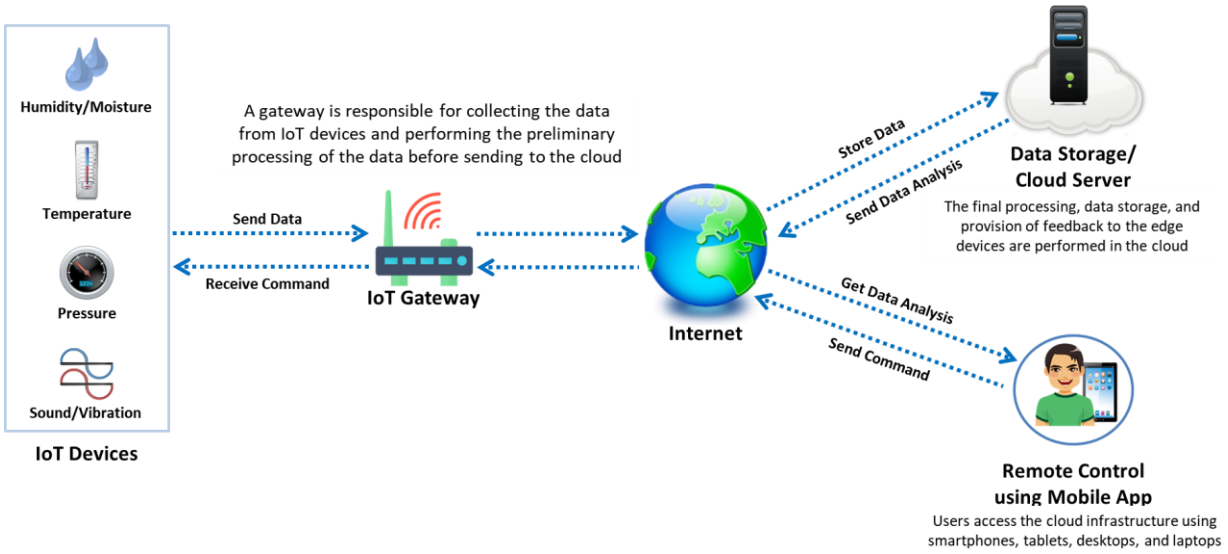


Figure 9.2: IoT Architecture

The IoT architecture includes several layers. These layers are designed in such a manner that they can meet the requirements of various sectors such as societies, industries, enterprises, and governments. The layers of the IoT architecture are connected to gather, save, and process data. The functions performed by various building blocks are as follows.

- **Gateways** are devices through which data are transmitted from things to the cloud and vice versa. They provide the following functions:
  - Pre-processing and filtering of data before transmitting them to the cloud, enabling lesser data volumes for detailed processing and storing

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- Sending control commands from the cloud to things to let the things execute the commands using their actuators

- **Cloud gateways** have the following features:
  - Data compression
  - Securing data transfer between field gateways and cloud IoT servers
  - Ensuring compatibility with different protocols
  - Communicating with field gateways through various protocols based on the protocol supported by gateways
- **Streaming data processors** ensure that no data can be lost or corrupted by providing the following features:
  - Effective input data transition to a data lake
  - Application control
- **Data lakes** store the data produced by the connected devices in the natural format. If the data are required for meaningful insights, the data will be extracted from a data lake and loaded to a big data warehouse.
- **Big data warehouses** contain only cleaned, structured, and matched data. They can store the following:
  - Context information about the things and devices; examples include the locations of sensors
  - Commands sent by control applications to things
- **Data analytics** help data analysts find trends and obtain actionable insights by using the data in the big data warehouse. The analysis of the data in the form of schemas, diagrams, and infographics reveals the following:
  - Device performance
  - Inefficiencies of the IoT system and ways to enhance it

  Moreover, manually found correlations and patterns further help create algorithms for control applications.
- **Machine learning** allows data analysts to create models for control applications. These models are updated regularly depending on the data in a big data warehouse. Examples include models for recognizing the patterns of an organization's employee behavior in terms of when they leave and return to the organization and adjusting the lights in the premises accordingly. After completing the phase of testing the applicability and efficiency of these models, they start to be used by control applications.
- **Control applications** send automatic commands and alerts to actuators. For example, if a pre-failure situation arises in an organization's equipment/devices, the sensors

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

monitor the state of the devices, and the IoT system sends automatic notifications to system engineers.

The stored commands in a big data warehouse sent by control applications to actuators help in the following:

- Investigating problematic cases; for example, checking the connectivity, gateways, and actuators if the actuators fail to execute the commands sent by a control application
- Enhancing security by identifying security breaches (possible when detecting unusual or huge amounts of commands)

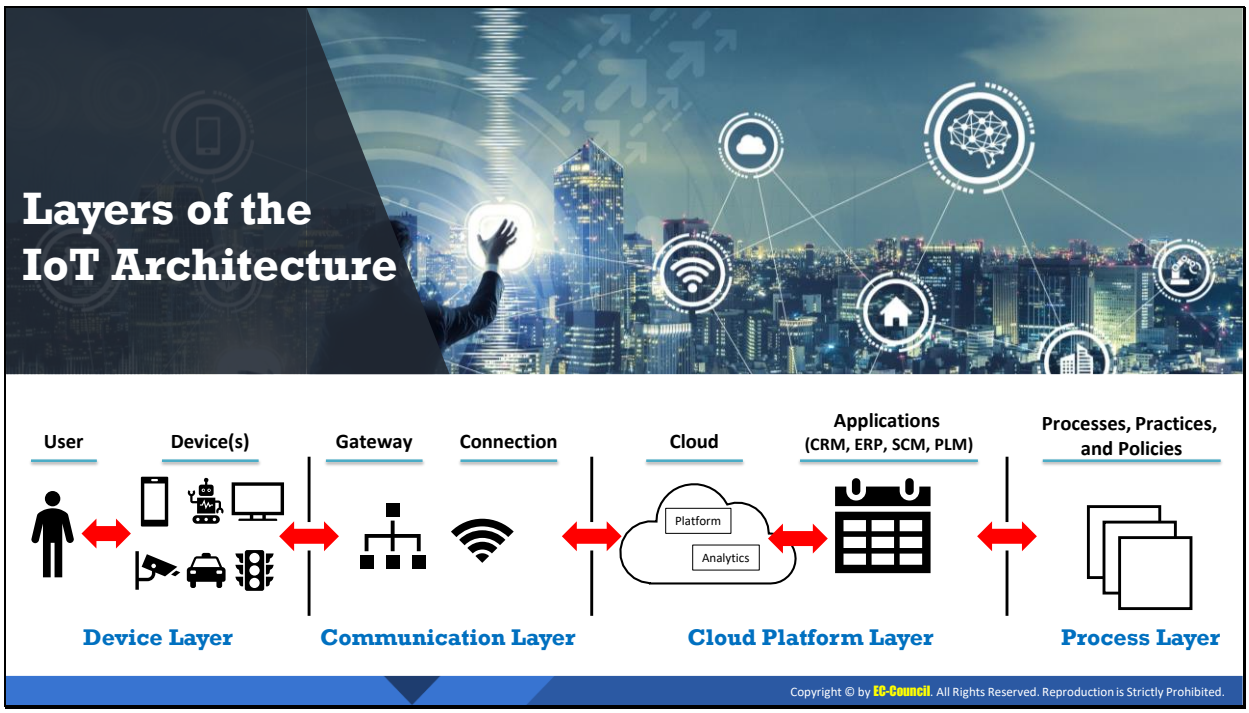
The control applications can be of the following two types:

- Rule-based control applications that operate based on the rules set by specialists
- Machine-learning-based control applications that use models, which can be updated regularly with the data stored in a big data warehouse

- **User applications (web or mobile applications)** help change the behavior of the application controls. For example, if an IoT system performs certain actions poorly, user applications allow users to do the following:
  - Connect to an IoT system
  - Monitor and control (by sending commands to control applications and setting options for automatic behavior) smart things while they are connected to a network of similar things.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Layers of the IoT Architecture

An IoT ecosystem is a combination of multiple IoT layers and comprises the components that allow organizations to connect to their IoT devices. Specifically, an ecosystem includes dashboards, remotes, gateways, analytics, networks, data storage, and security. The general architecture of an IoT ecosystem is different for different organizations. The ecosystem model that many organizations refer to when attempting to understand the IoT architecture includes the IoT layers.

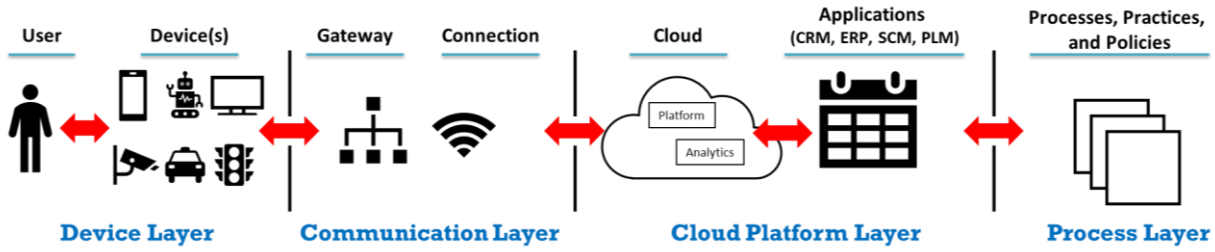


Figure 9.3: Layers of IoT Architecture

Layer 1: Device Layer

The device or thing layer of IoT includes the hardware that constitutes IoT devices. All the connected devices are the endpoint for an IoT ecosystem, and they acquire data based on a particular use case. The devices include the following:

- Sensors (temperature, gyroscope, pressure, light sensors, Global Positioning System (GPS), electrochemical, radio-frequency identification (RFID), etc.)
- Mobile devices (smartphones/tablets)
- Microcontroller units

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- Networking gear
- Single-board computers

Layer 2: Communication Layer

The communication (connectivity/edge computing) layer includes the components of communication protocols and networks used for connectivity and edge computing. A use case is successfully executed with seamless connectivity between IoT devices.

- **Protocols:** For Internet-based IoT applications, a Transmission Control Protocol (TCP)/Internet Protocol (IP)-based architecture is used. Intranet-based IoT use cases utilize LAN, RF, Wi-Fi, Li-Fi, etc.
- **Gateway:** Gateways help manage traffic between IoT devices and connected networks. To maintain and monitor the traffic, the level-5 gateways are helpful.

Layer 3: Cloud Layer

Servers hosted in the cloud accept, store, and process the sensor data received from IoT gateways. Many IoT solutions are integrated with cloud services. With a comprehensive set of integrated services and solutions, IoT cloud provides the required insights and perspectives for customers. It provides dashboards for monitoring, analyzing, and implementing proactive decisions.

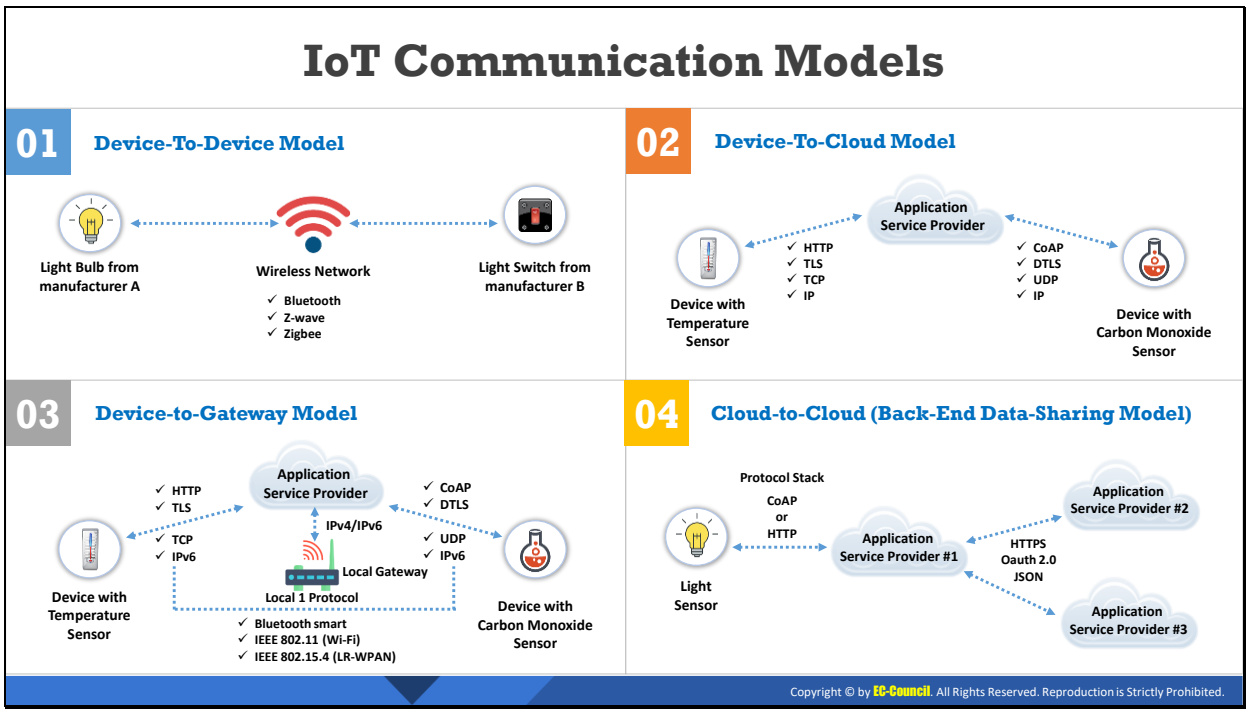
Layer 4: Process Layer

The process layer gathers information and processes the received information. It includes the following:

- People
- Businesses
- Collaborations
- Decision making based on the information derived from policies and procedures of IoT computing.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



IoT Communication Models

IoT technology uses various technical communication models, each with its own characteristics. These models highlight the flexibility with which IoT devices can communicate with each other or with the client. Discussed below are four communication models and the key characteristics associated with each model:

- **Device-to-Device Communication Model**

  In this type of communication, inter-connected devices interact with each other through the Internet, but they predominantly use protocols such as ZigBee, Z-Wave or Bluetooth. Device-to-device communication is most commonly used in smart home devices such as thermostats, light bulbs, door locks, CCTV cameras, and fridges, which transfer small data packets to each other at a low data rate. This model is also popular in communication between wearable devices. For example, an ECG/EKG device attached to the body of a patient will be paired to his/her smartphone and will send him/her notifications during an emergency.

Figure 9.4: IoT device-to-device communication model

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **Device-to-Cloud Communication Model**

  In this type of communication, devices communicate with the cloud directly, rather than directly communicating with the client to send or receive data or commands. It uses communication protocols such as Wi-Fi or Ethernet, and sometimes uses Cellular as well.

  An example of Wi-Fi-based device-to-cloud communication is a CCTV camera that can be accessed on a smartphone from a remote location. In this scenario, the device (here, the CCTV camera) cannot directly communicate with the client; rather, it first sends data to the cloud, and then, if the client inputs the correct credentials, he/she is then allowed to access the cloud, which in turn allows him/her to access the device at his/her home.

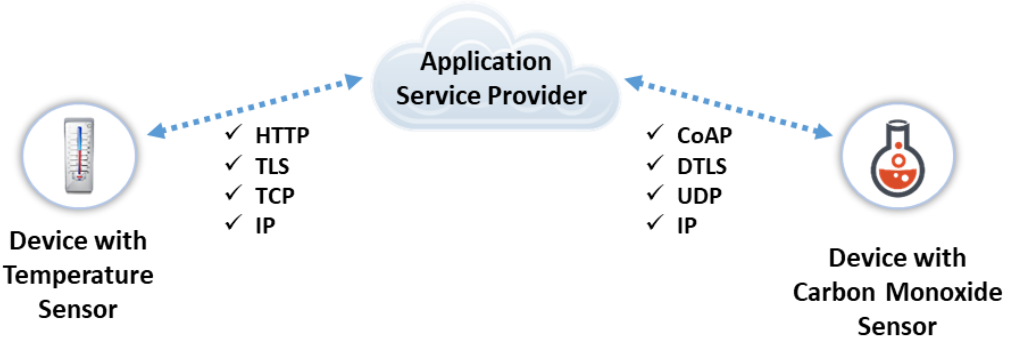


Figure 9.5: IoT device-to-cloud communication model

- **Device-to-Gateway Communication Model**

  In the device-to-gateway communication model, the IoT device communicates with an intermediate device called a gateway, which in turn communicates with the cloud service. This gateway device could be a smartphone or a hub that is acting as an intermediate point, which also provides security features and data or protocol translation. The protocols generally used in this mode of communication are ZigBee and Z-Wave.

  If the application layer gateway is a smartphone, then it might take the form of an app that interacts with the IoT device and with the cloud. This device might be a smart TV that connects to the cloud service through a mobile phone app.

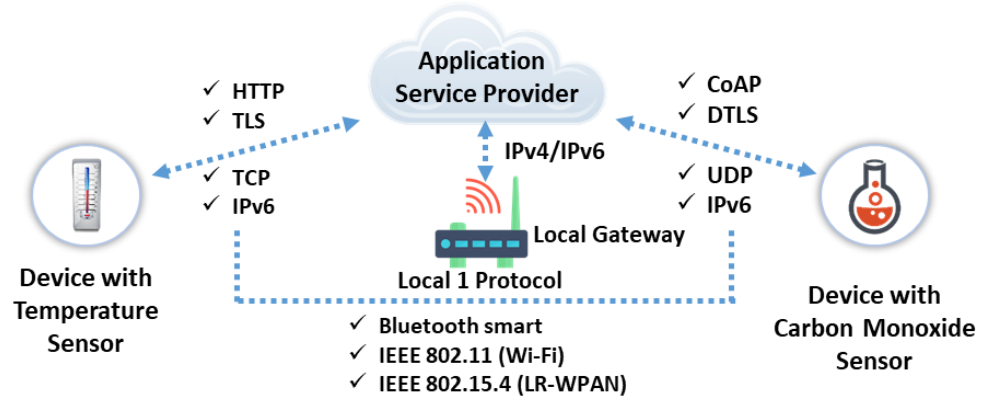


Figure 9.6: IoT device-to-gateway communication model

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **Cloud-to-Cloud (Back-End Data-Sharing) Communication Model**

  This type of communication model extends the device-to-cloud communication type such that the data from the IoT devices can be accessed by authorized third parties. Here, devices upload their data onto the cloud, which is later accessed or analyzed by third parties. An example of this model would be an analyzer of the yearly or monthly energy consumption of a company. Later, the analysis can be used to reduce the company's expenditure on energy by following certain energy-harvesting or saving techniques.

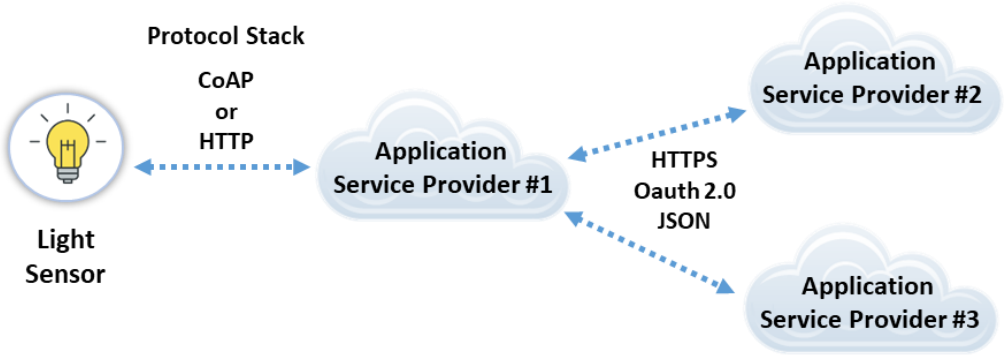
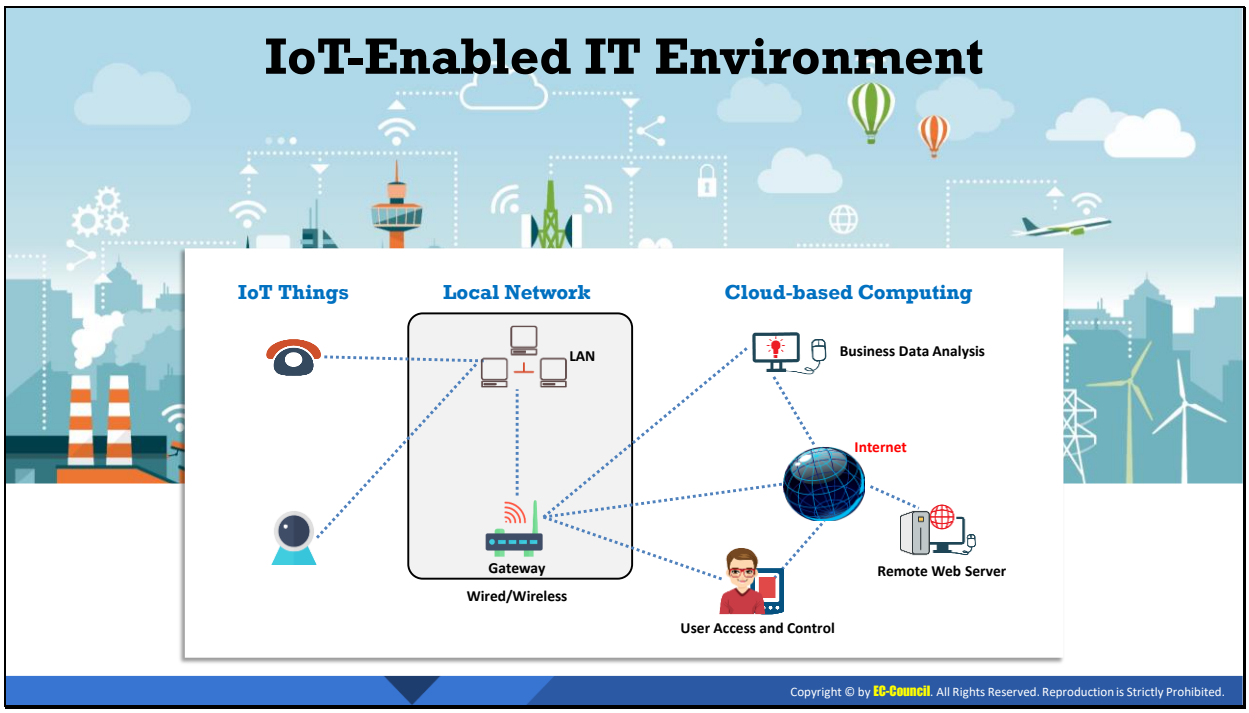
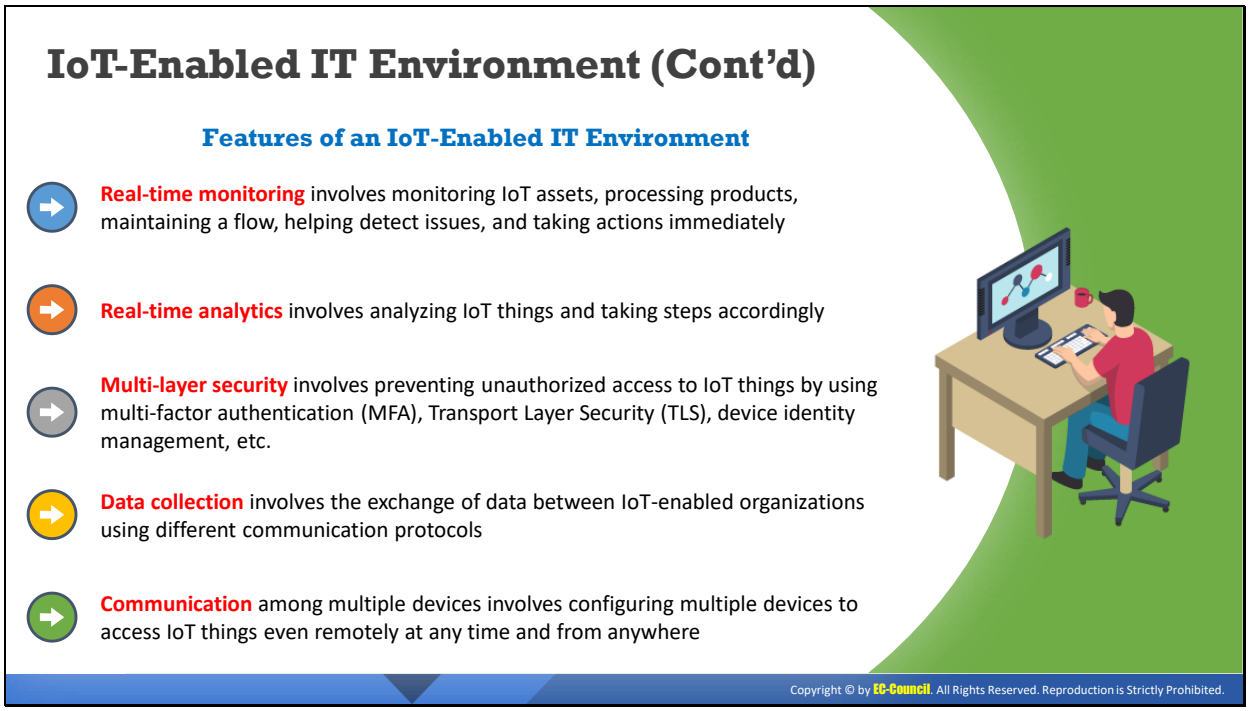


Figure 9.7: IoT back-end data-sharing model

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets





IoT-Enabled IT Environment

A typical IoT-enabled IT environment comprises devices/things that use a gateway for communicating over a network to access an organization's back-end servers running an IoT cloud platform. This IoT platform allows integrating the IoT information into the organization.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

The different tiers of an IoT-enabled IT environment are discussed below.

- **Things/Devices Tier**

  The things/devices tier include smartphones, wearable devices, autonomous machines, and tags (RFID, NFC, QR codes) that can gather data using their embedded sensors, which can track key parameters related to the physical environment. Some examples for these parameters are air quality, humidity, light, and pressure. To transfer these telemetry data/command and control requests from IoT devices through a gateway to the cloud, protocols based on wired and wireless networking standards are used. Moreover, the command and control data are transferred from the cloud through the gateway to the devices. These devices can control the state of another device. For example, they can switch off faulty devices or raise an alarm about them. Thus, these IoT devices allow remote control.

- **Gateway/Control Tier**

  The gateway/control tier focuses on communication, offload processing functions, and the driving of required actions. The gateway pre-processes the huge amount of data generated by sensors before sending it to the cloud tier; thus, it reduces the amount of unwanted data forwarded to the cloud tier. This process can reduce the costs of network transmission and allow the application of rules based on incoming data. The gateway can issue control information such as configuration changes to the devices while responding to the data tier's command and control requests such as authentication requests (bidirectional functioning). Moreover, the gateway acts as a proxy/edge device to legacy and low-power devices that cannot directly register and communicate with the IoT platform. In particular, the gateway can route commands received from the back-end to the respective device. All the new IoT devices, legacy devices, and edge devices form the IoT device layer.

  A typical control tier facilitates efficient communication through a personal area network (PAN), a local area network (LAN), Bluetooth, Zigbee, Message Queuing Telemetry Transport (MQTT)/TCP, etc., and micro-computing (micro-multi core chips).

- **Communication/Data Center/Cloud IOT Platform/Cloud Tier**

  The communication/data center/cloud IoT platform/cloud tier focuses on data computation to deliver insights and thereby generate business value. It acts as middleware by orchestrating the entire IoT workflow. It provides back-end business analytics to run event processes such as data analysis for creating and adapting business rules based on historical trends and then spreads business rules downstream. It needs to scale horizontally (for supporting an increasing number of IoT devices) and vertically (for addressing different IoT solutions). The cloud tier's key functions include the following:

  - Event processing and analysis
  - Data storage
  - Message and connectivity routing

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- Application integration and enablement

A typical cloud tier comprises software as a service (SaaS), business data analysis, user access controls, remote web servers, etc., and open/small operating systems (OSes) such as Linux.

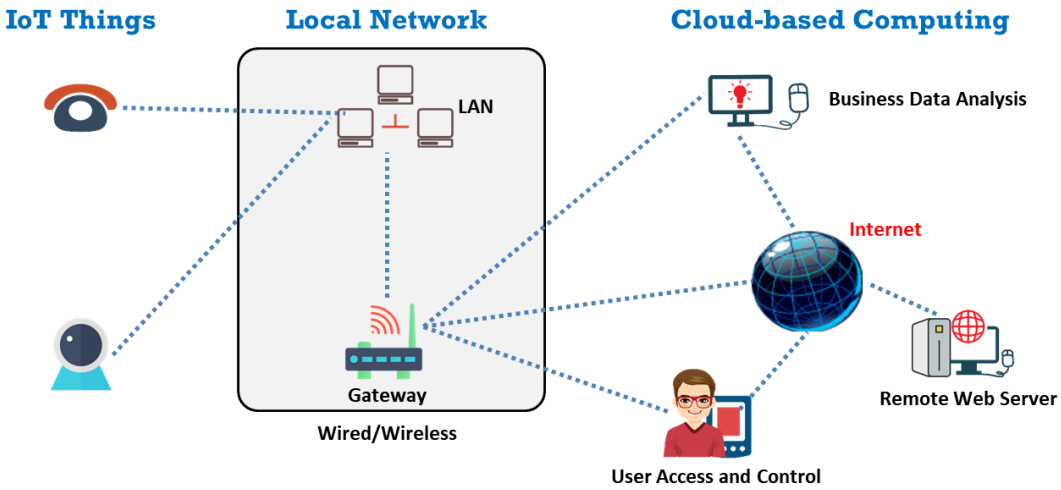


Figure 9.8: Schematic of an IoT-enabled environment

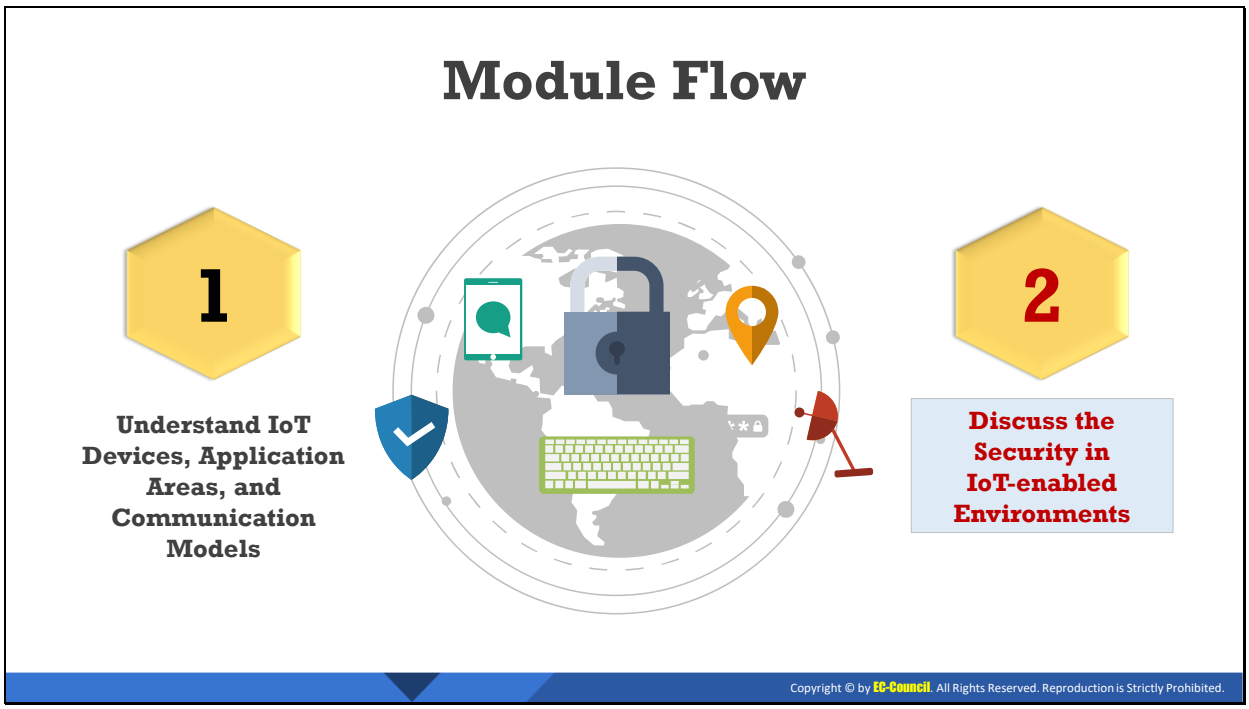
In the figure, the IoT things/devices layer communicates with a cloud gateway. Here, the gateway authenticates and authorizes the devices to participate in the workflow and thereby ensures secure communication between the devices and the centralized command center. Furthermore, the gateway can deal with different protocols and data formats. The devices and local gateways with different protocols (SOAP, REST, AMQP, etc.) register with the cloud gateway. Here, without considering the inbound protocol, the cloud gateway can provide a view of the device layer to the remaining IoT components.

Features of an IoT-Enabled IT Environment

The following features of IoT platforms help an IT environment reach its targets quickly:

- Real-time monitoring involves monitoring IoT assets, processing products, maintaining a flow, helping detect issues, and taking actions immediately.
- Real-time analytics involves analyzing IoT things and taking steps accordingly. For example, it provides graphs and real-time streaming analytics, allowing the business to overview its performance and production.
- Multi-layer security involves preventing unauthorized access to IoT things by using multi-factor authentication (MFA), Transport Layer Security (TLS), device identity management, etc.
- Data collection involves the exchange of data between IoT-enabled organizations using different communication protocols. These protocols should be lightweight and should provide low-network-bandwidth functionality.
- Communication among multiple devices involves configuring multiple devices to access IoT things even remotely at any time and from anywhere.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Discuss the Security in IoT-enabled Environments

The objective of this section is to explain the security principles in IoT-enabled environments.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Security in IoT-enabled Environments

Because IoT devices are vastly different from each other, the security of devices relies on their type and model. With no or inadequate focus on IoT device security by manufacturers, security measures used for IoT devices often fall short. Therefore, an organization should focus on securing IoT devices and countering attack scenarios in IoT-enabled environments.

An organization can secure IoT devices by changing the default passwords, disabling unused features, updating firmware and applications, and using a legitimate application developed by a reliable vendor in the case of IoT devices that rely on third-party applications.

An adversary uses a compromised IoT device as an entry point to a network and performs a lateral movement attack. For example, a compromised smart printer can infect other systems and devices connected to the same network. A compromised router can spread malware to all the IoT devices connected to it. Therefore, organizations should focus on securing network devices and routers in an IoT-enabled environment.

To secure an IoT network and router, the user should map and monitor all the devices, apply network segmentation, ensure a secure network architecture, use routers with in-built firewalls, and disable unnecessary services such as Universal Plug and Play (UPnP). This helps in restricting the attacker from accessing other parts of the network and performing targeted attacks.

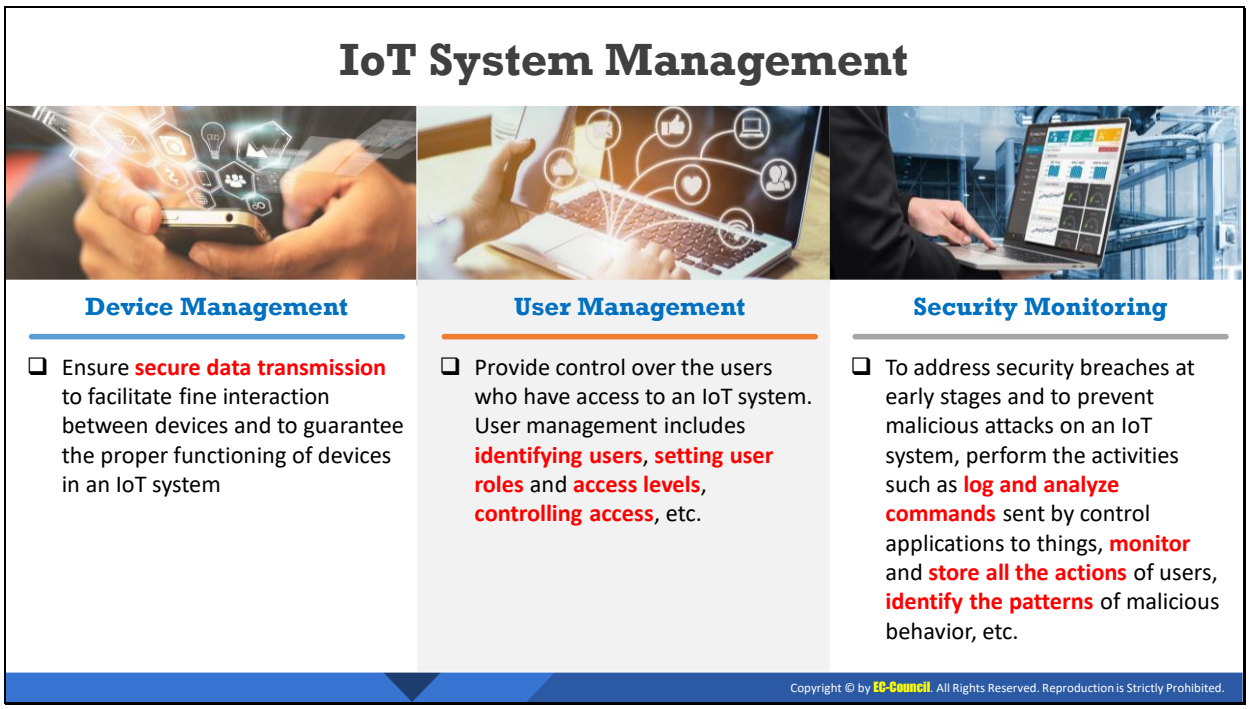
An organization should use multi-layered management. To secure all the different IoT devices, an overarching multi-layered security plan and constant maintenance are required. The organization should enforce security solutions that safeguard the IoT devices and detect malware at the endpoint level. It should also use security software that checks the network traffic between routers and connected devices to protect the IoT devices. Further, it should

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

utilize network appliances to monitor all the ports and network protocols for detecting advance threats and safeguard the IoT devices from targeted attacks. Company-wide collaboration and synchronization are required to secure an IoT-enabled environment.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



IoT System Management

IoT system management involves the following.

- **Device management**

  Ensure secure data transmission to facilitate fine interaction between devices and to guarantee the proper functioning of devices in an IoT system.

  - **Identify the identity of devices** to ensure a trusted device with genuine software transmitting reliable data.
  - **Configure devices and control them** as per the requirements of an IoT system. For example, provide IDs for devices.
  - **Monitor and diagnose devices** to ensure the smooth and secure functioning of IoT devices.
  - **Update software and maintain it** to add functionality, fix bugs, and address vulnerabilities.

- **User management**

  Provide control over the users who have access to an IoT system. User management includes the following:

  - Identify users.
  - Set user roles (owners, guests, etc.).
  - Set access levels for users.
  - Control the access of a few users to specific information.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

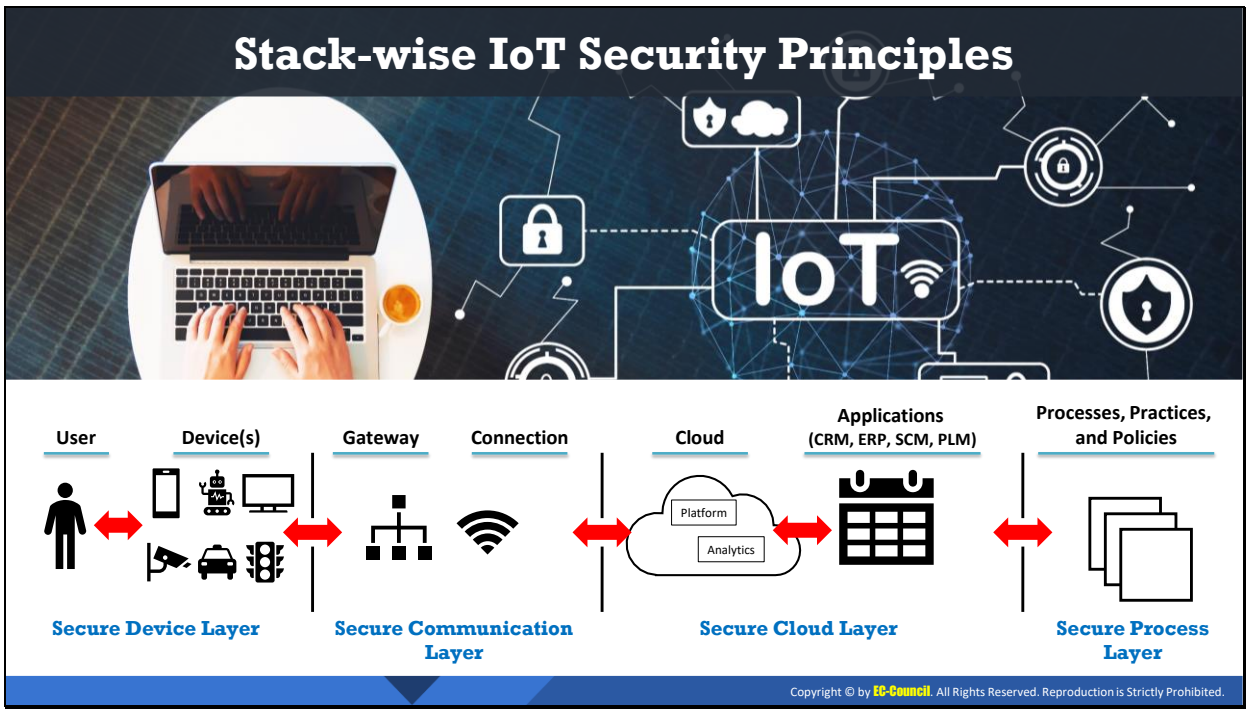
- Set user ownership.
- Add and remove users.
- Manage user settings.
- Allow permissions to perform certain operations within an IoT system (for example, controlling and recording user activities).

- **Security monitoring**

  To address security breaches at early stages and to prevent malicious attacks on an IoT system, the following should be performed:

  - Log and analyze commands sent by control applications to things.
  - Monitor the actions of users.
  - Store all actions in the cloud.
  - Identify the patterns of malicious behavior.
  - Store samples of malicious activity and compare them with the logs generated by the IoT system to avoid attacks and their impact.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Stack-wise IoT Security Principles

Several IoT devices are connected to the network and eventually to the cloud, which causes vulnerability to many threat vectors. To develop end-to-end (E2E) IoT solutions, the device, communication, cloud, and process layers should be secured. For this purpose, the following stack-wise IoT security principles should be implemented.

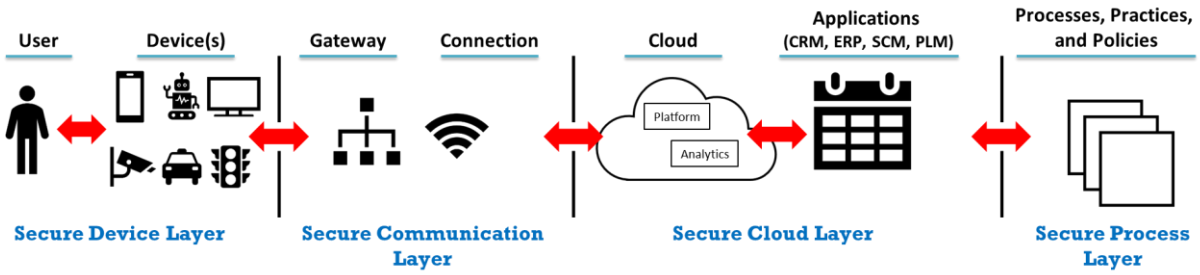


Figure 9.9: Stack-wise IoT security principles

IoT Security Principles on the Device Layer

- **Need for device intelligence to handle complex security tasks:** Most IoT devices communicate with services, the cloud, servers, etc., through the Internet or Wi-Fi. As these devices are powered by microprocessors, they are unable to handle the complexity of Internet connectivity and should not be utilized for front-line duty in IoT applications. Smart devices are secure and robust. They have embedded security features and can handle security, encryption, authentication, etc. Hence, smart devices should be used for front-line duty in IoT applications.
- **Security advantage of processing at the edge:** Smart IoT devices have an edge processing feature that processes data locally before sending the data to the cloud, thus

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

eliminating the need to forward a large quantity of data to the cloud. Edge processing enhances security by processing the data, packing the data into separate packets, and sending the data securely to the desired location. It allows users to keep sensitive information with them.

IoT Security Principles on the Communication Layer

- **Initiate a connection to the cloud but not from the cloud**: Instead of connecting IoT devices with the Internet, they should be connected to the cloud. Incoming connections should be disallowed. Connection to the cloud establishes a bi-directional channel, through which the user can control the IoT device remotely.
- **Inherent security of a message**: All communications with IoT devices should be carefully handled. The user must enforce lightweight message-based protocols for IoT devices that consist of options for double encryption, filtering, queuing, etc. With proper labeling, the messages will be handled securely. For example, double encryption secures client data when the data pass through the message switch.

IoT Security Principle on the Cloud Layer

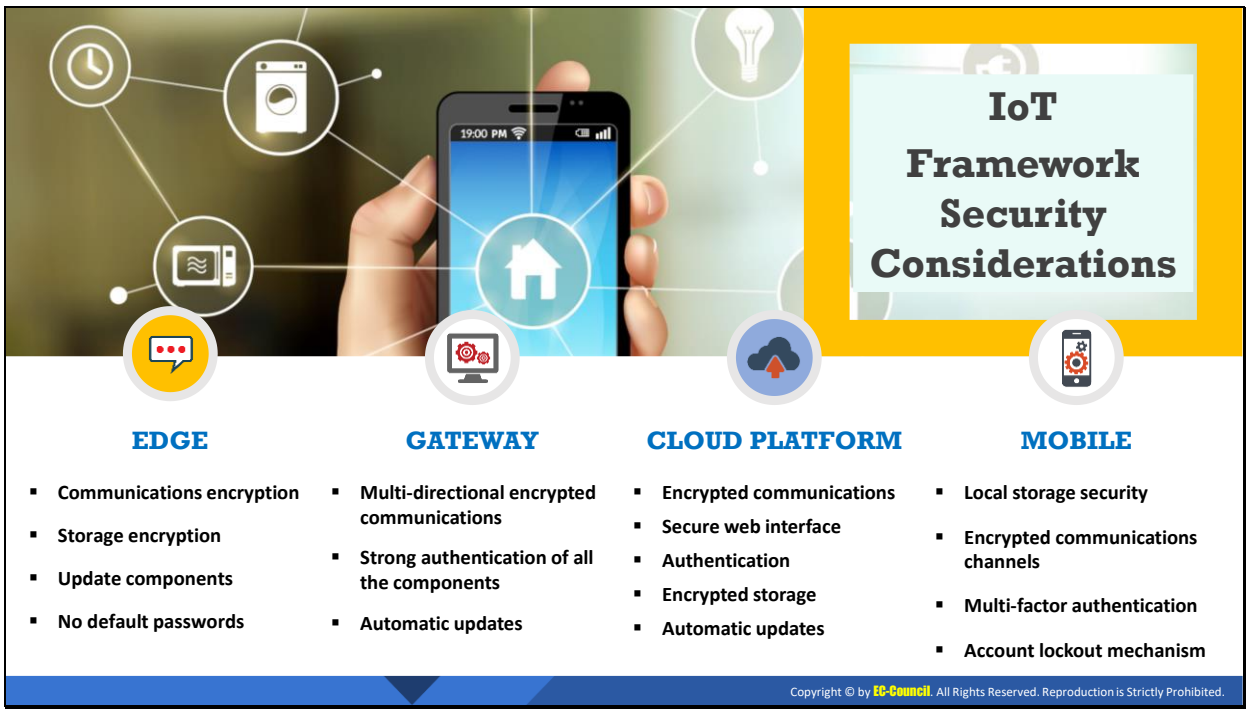
- **Identification, authentication, and encryption for machines, rather than humans**: Users access cloud services with a password. Occasionally, cloud services use two-factor authentication consisting of a password and a one-time password generator. For humans, passwords are the accepted method of authentication, but machines handle digital certificates while accessing cloud services. The system of digital certificates is used not only to authenticate transactions but also to encrypt the channel from the device to the cloud before the transaction. The cryptographic identification provided by the digital certificate cannot be achieved with a user ID and password.

IoT Security Principle on the Process Layer

- **Security of remote control and updates**: The remote control of an IoT device allows the user to perform remote diagnostics of the device, set new configurations, retrieve files, etc. The key to secure updates and remote control is to ensure that incoming connections to the device are disallowed; however, the device should establish a secure bi-directional connection with the cloud and utilize a message switch as a communication channel.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



IoT Framework Security Considerations

To design secure and protected IoT devices, security issues should be properly considered. One of the most important considerations is the development of a secure IoT framework for building the device. Ideally, a framework should be designed in a way that provides default security, so that the developers do not have to consider it later.

Security evaluation criteria for the IoT framework are broken down into four parts. Each part has its own security-related concerns that are discussed in the evaluation criteria for each part. The security evaluation criteria for the IoT devices are discussed below:

- **Edge**

  The edge is the main physical device in the IoT ecosystem that interacts with its surroundings and contains various components like sensors, actuators, operating systems, hardware and network, and communication capabilities. It is heterogeneous and can be deployed anywhere and in any condition. Therefore, an ideal framework for an edge would be such that it provides cross-platform components so that it can be deployed and work in any physical condition possible.

  Other framework considerations for an edge would be proper communications and storage encryption, no default credentials, strong passwords, use of the latest up-to-date components, etc.

- **Gateway**

  The gateway acts as the first step for an edge into the world of the Internet as it connects smart devices to cloud components. It is referred to as a communication aggregator that allows communication with a secure and trusted local network as well

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

as a secure connection with an untrusted public network. It also provides a layer of security to all the devices connected to it. The gateway serves as an aggregation point for the edge; therefore, it has a crucial security role in the ecosystem.

An ideal framework for the gateway should incorporate strong encryption techniques for secure communications between endpoints. In addition, the authentication mechanism for the edge components should be as strong as any other component in the framework. Wherever possible, the gateway should be designed in such a way that it authenticates multi-directionally to carry out trusted communication between the edge and the cloud. Automatic updates should also be provided to the device for countering vulnerabilities.

- **Cloud Platform**

  In an IoT ecosystem, the cloud component is referred to as the central aggregation and data management point. Access to the cloud must be restricted. The cloud component is usually at higher risk, as it is the central point of data aggregation for most of the data in the ecosystem. It also includes a command and control (C2) component, which is a centralized computer that issues various commands for the distribution of extensions and updates.

  A secure framework for the cloud component should include encrypted communications, strong authentication credentials, a secure web interface, encrypted storage, automatic updates, etc.

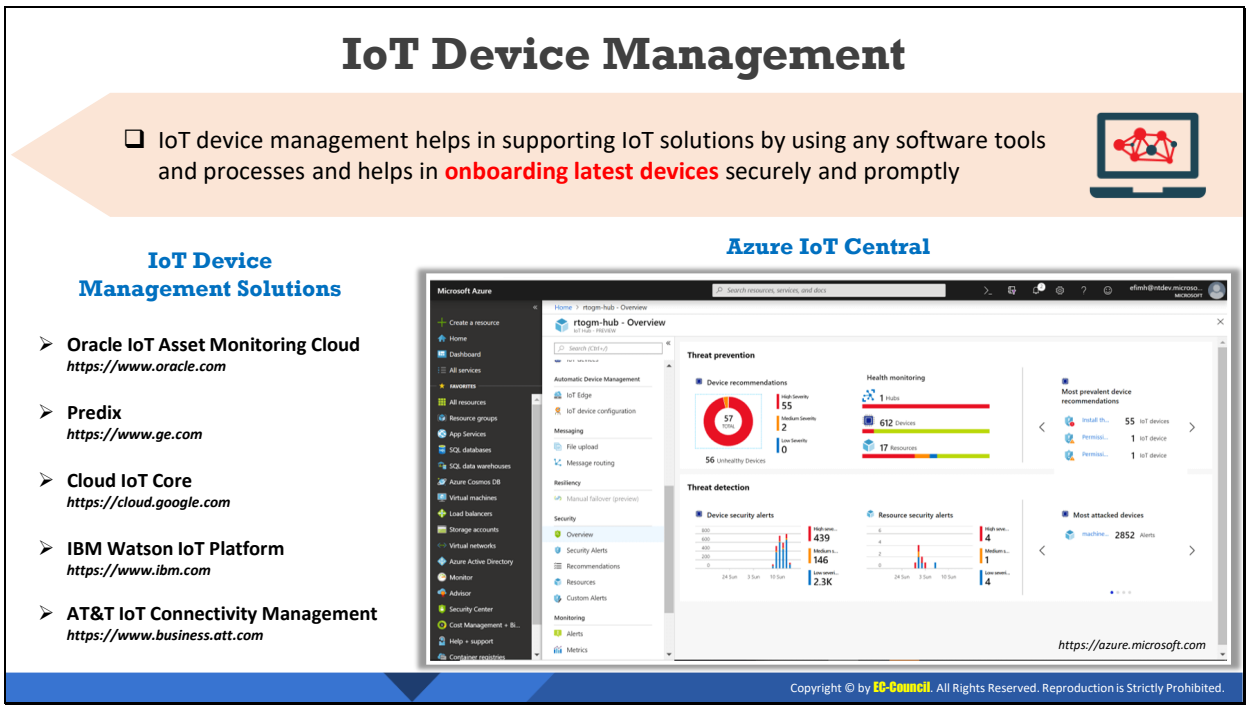
- **Mobile**

  In an IoT ecosystem, the mobile interface plays an important part, particularly where the data needs to be collected and managed. Using mobile interfaces, users can access and interact with the edge in their home or workplace from miles away. Some mobile applications provide users with only limited data from specific edge devices, while others allow complete manipulation of the edge components. Proper attention should be given to the mobile interface, as they are prone to various cyber-attacks.

  An ideal framework for the mobile interface should include a proper authentication mechanism for the user, an account lockout mechanism after a certain number of failed attempts, local storage security, encrypted communication channels, and security of data transmitted over the channel.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



IoT Device Management

IoT device management helps security professionals to track, monitor, and manage physical IoT devices from a remote location. Security professionals can use solutions such as Azure IoT Central, Oracle IoT Asset Monitoring Cloud, and Predix to perform IoT device management. These solutions allow security professionals to update the firmware remotely. Further, IoT device management helps in providing permissions and enhancing security capabilities to ensure protection against various vulnerabilities.

IoT device management can be very supportive in preventing IoT attacks as it can provide:

- Proper authentication, as only trusted and secure devices with proper credentials are enrolled
- Accurate configuration, controlling devices to ensure proper functionality and improved performance. It can also reset the factory settings during device decommissioning.
- Proper monitoring to detect flaws and diagnose operational issues and software bugs through program logs
- Secure maintenance of remote devices and frequent device updates with the latest security patches

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

IoT Device Management Solutions

IoT device management solutions are used by security professionals, IT admin, or IoT administrators for onboarding, organizing, monitoring, and managing IoT devices. Discussed below are some IoT device management solutions:

- **Azure IoT Central**

  Source: *https://azure.microsoft.com*

  Azure IoT Central is a hosted, extensible software-as-a-service (SaaS) platform that simplifies the setup of IoT solutions. It helps to easily connect, monitor, and manage IoT assets at scale. Azure IoT Central can simplify the initial setup of an IoT solution and can reduce the management burden, operational costs, and overheads of a typical IoT project.

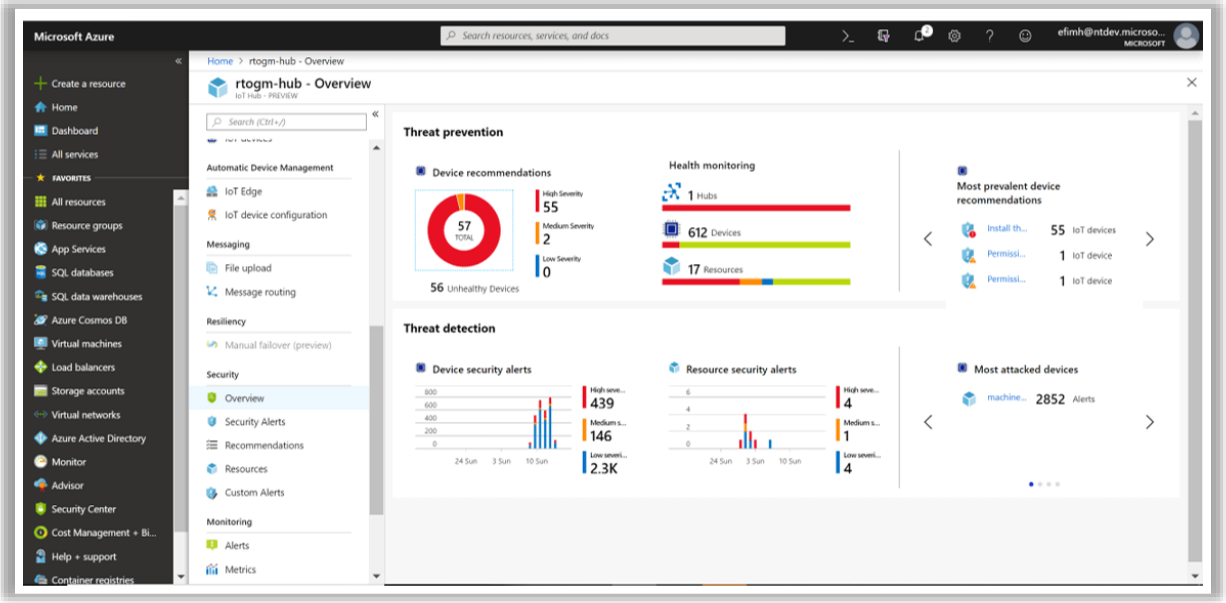
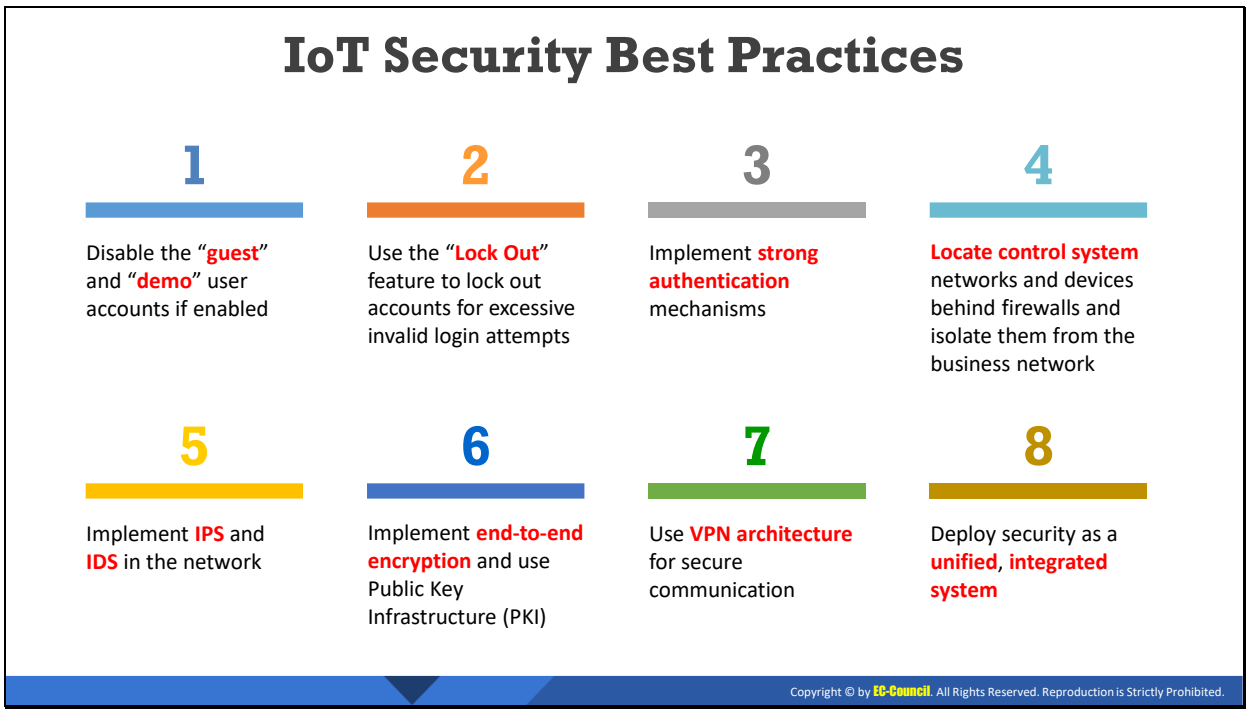


Figure 9.10: Screenshot of Azure IoT Central

Listed below are some of the additional solutions for IoT device management:

- Oracle IoT Asset Monitoring Cloud (*https://www.oracle.com*)
- Predix (*https://www.ge.com*)
- Cloud IoT Core (*https://cloud.google.com*)
- IBM Watson IoT Platform (*https://www.ibm.com*)
- AT&T IoT Connectivity Management (*https://www.business.att.com*)

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



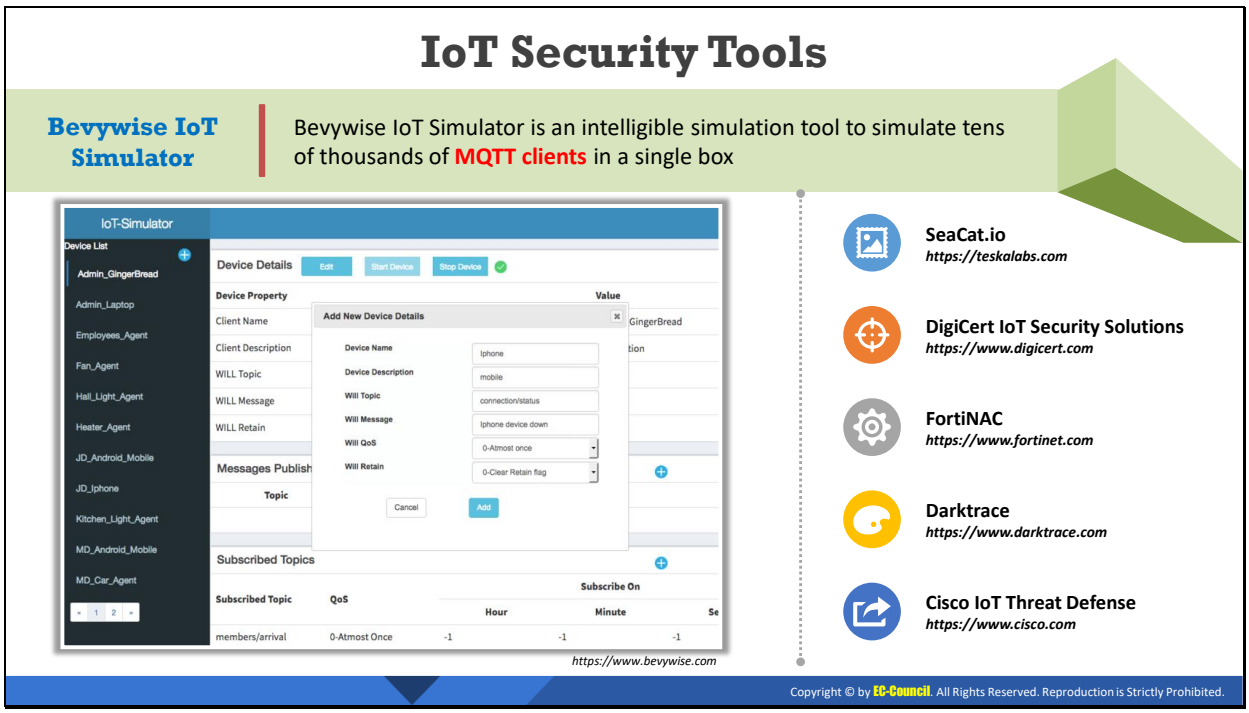
IoT Security Best Practices

- Disable the "guest" and "demo" user accounts if enabled
- Use the "Lock Out" feature to lock out accounts for excessive invalid login attempts
- Implement a strong authentication mechanism
- Locate control system networks and devices behind firewalls, and isolate them from the business network
- Implement IPS and IDS in the network
- Implement end-to-end encryption and use public key infrastructure (PKI)
- Use VPN architecture for secure communication
- Deploy security as a unified, integrated system
- Allow only trusted IP addresses to access the device from the Internet
- Disable telnet (port 23)
- Disable the UPnP port on routers
- Protect the devices against physical tampering
- Patch vulnerabilities and update the device firmware regularly
- Monitor traffic on port 48101, as infected devices attempt to spread the malicious file using port 48101
- Position of mobile nodes should be verified with the aim of referring one physical node with one vehicle identity only, which means one vehicle cannot have two or more identities

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- Data privacy should be implemented; therefore, the user's account or identity should be kept protected and hidden from other users
- Data authentication should be performed to confirm the identity of the original source node
- Maintain data confidentiality using symmetric key encryption
- Implement a strong password policy requiring a password at least 8–10 characters long with a combination of letters, numbers, and special characters
- Use CAPTCHA and account lockout policy methods to avoid brute-force attacks
- Use devices made by manufacturers with a track record of security awareness
- Isolate IoT devices on protected networks

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



IoT Security Tools

The IoT is not the only range of devices connected to the Internet, but it is also a very complex, rapidly growing technology. To understand and analyze various risk factors, proper security solutions must be incorporated to protect the IoT devices. The use of IoT security tools helps organizations to significantly limit security vulnerabilities, thereby protecting the IoT devices and networks from different kinds of attacks.

- **Bevywise IoT Simulator**

  Source: *https://www.bevywise.com*

  Bevywise IoT Simulator is an intelligible simulation tool to simulate tens of thousands of MQTT clients in a single box. It can be used to develop, test, and demonstrate IoT servers and managers. IoT Simulator can be configured to send real-time messages within a range or from a random set of values based on the time and client. Further, it can simulate dynamic messages in two message formats, namely, TXT and JSON, like real-world IoT devices. For flexibly varying the data published in every sequence and to make the data in sync with the real device, IoT Simulator supports four types of dynamic values to be sent as a part of messages: system variable timestamp and client identifier, random, range, linear, and constant. IoT events can be configured with a predefined dataset by uploading a CSV file.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

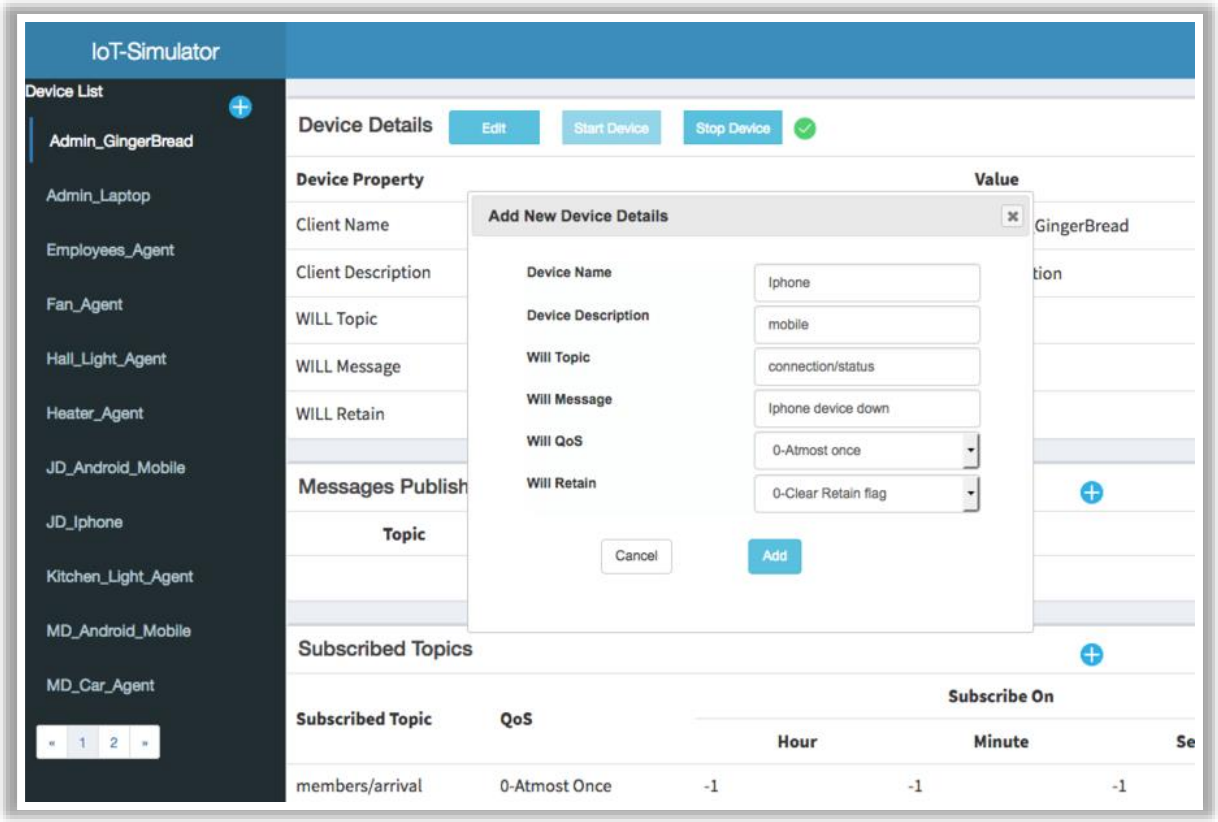
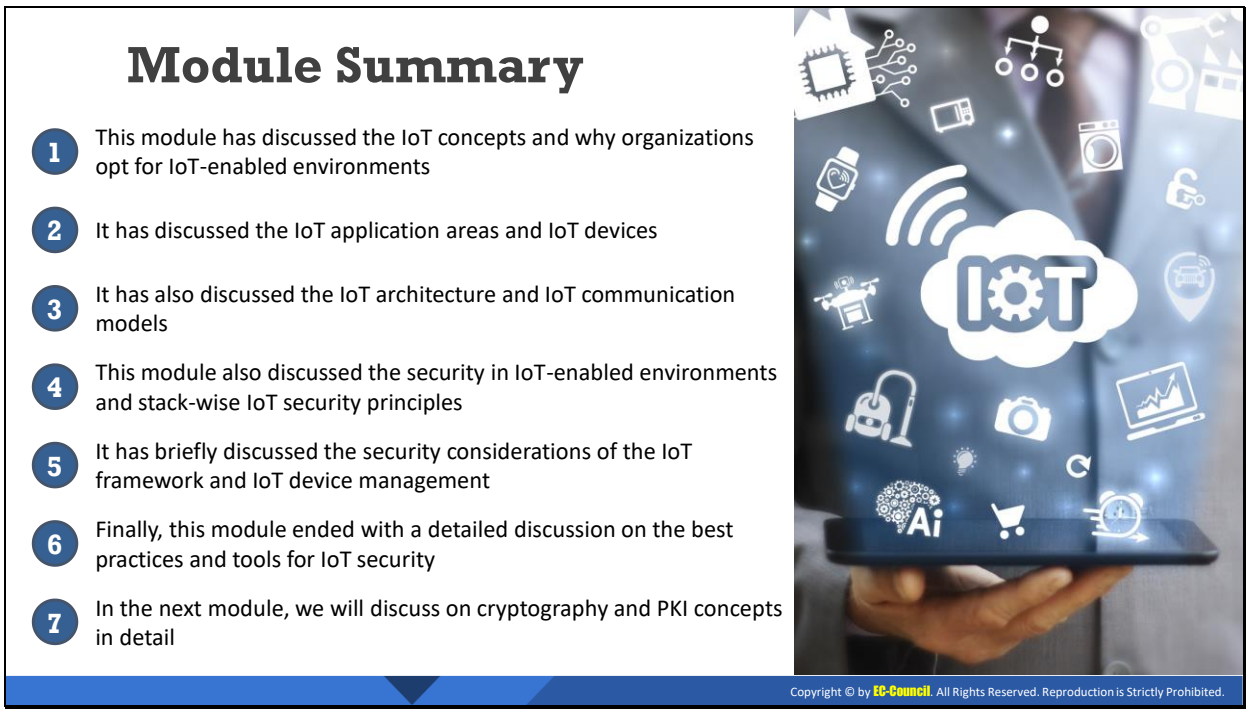


Figure 9.11: Screenshot of Bevywise IoT Simulator

Listed below are some of the additional IoT security tools and solutions:

- SeaCat.io (*https://teskalabs.com*)
- DigiCert IoT Security Solutions (*https://www.digicert.com*)
- FortiNAC (*https://www.fortinet.com*)
- Darktrace (*https://www.darktrace.com*)
- Cisco IoT Threat Defense (*https://www.cisco.com*)

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Module Summary

This module discussed IoT concepts and why organizations opt for IoT-enabled environments. It discussed IoT application areas, IoT devices, IoT architectures, and IoT communication models. Furthermore, this module discussed the security in IoT-enabled environments and stack-wise IoT security principles. It also briefly discussed the security considerations of the IoT framework and IoT device management. Finally, this module presented a detailed discussion on the best practices and tools for IoT security.

In the next module, we will discuss cryptography and PKI concepts in detail.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

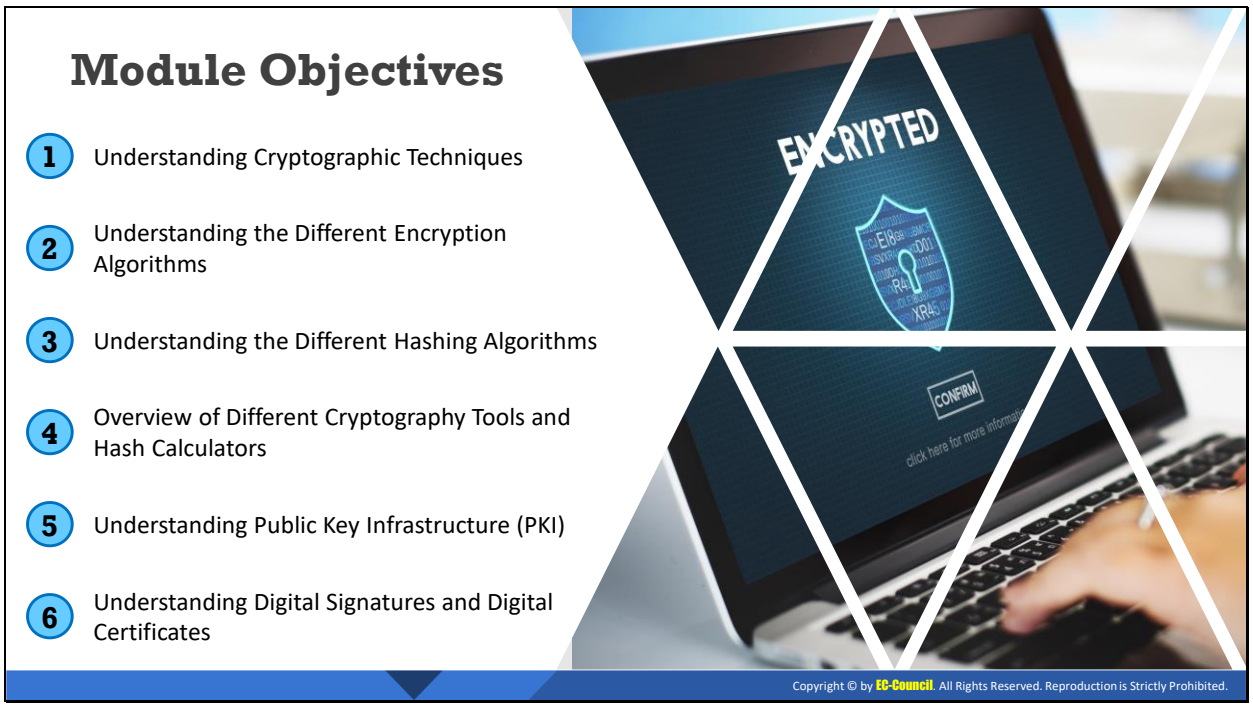
EC-Council

N|DE™
Network Defense Essentials

Module 10

Cryptography and PKI

https://t.me/learningnets



Module Objectives

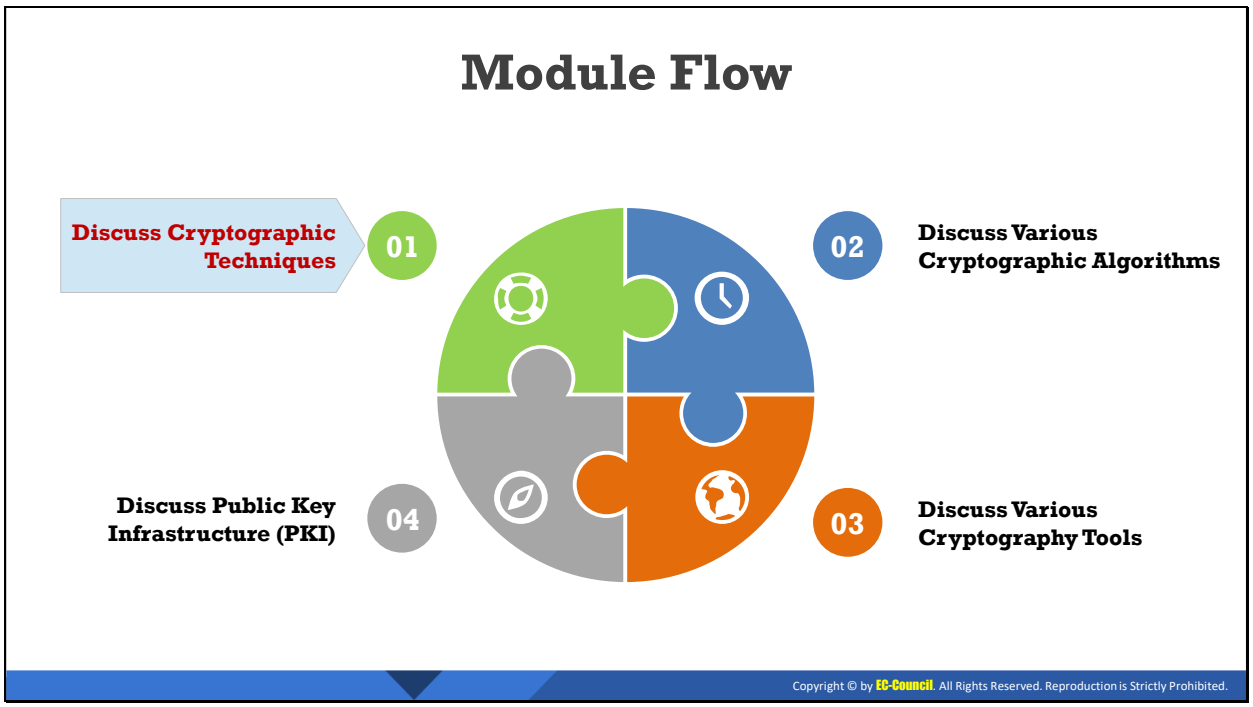
With the increasing adoption of the Internet (World Wide Web) for business and personal communication, securing sensitive information such as credit card details, PINs, bank account numbers, and private messages is becoming increasingly important, albeit more difficult to achieve. Today's information-based organizations extensively use the Internet for e-commerce, market research, customer support, and a variety of other activities. Data security is critical to online business and communication privacy.

Cryptography and cryptographic ("crypto") systems help in securing data against interception and compromise during online transmissions. This module provides a comprehensive understanding of different cryptosystems and algorithms, one-way hash functions, and public-key infrastructures (PKIs). It also covers various tools used to encrypt sensitive data.

At the end of this module, you will be able to do the following:

- Describe cryptographic techniques
- Understand the different encryption algorithms
- Understand the different hashing algorithms
- Use different cryptography tools and hash calculators
- Explain public key infrastructure (PKI)
- Understand digital signatures and digital certificates

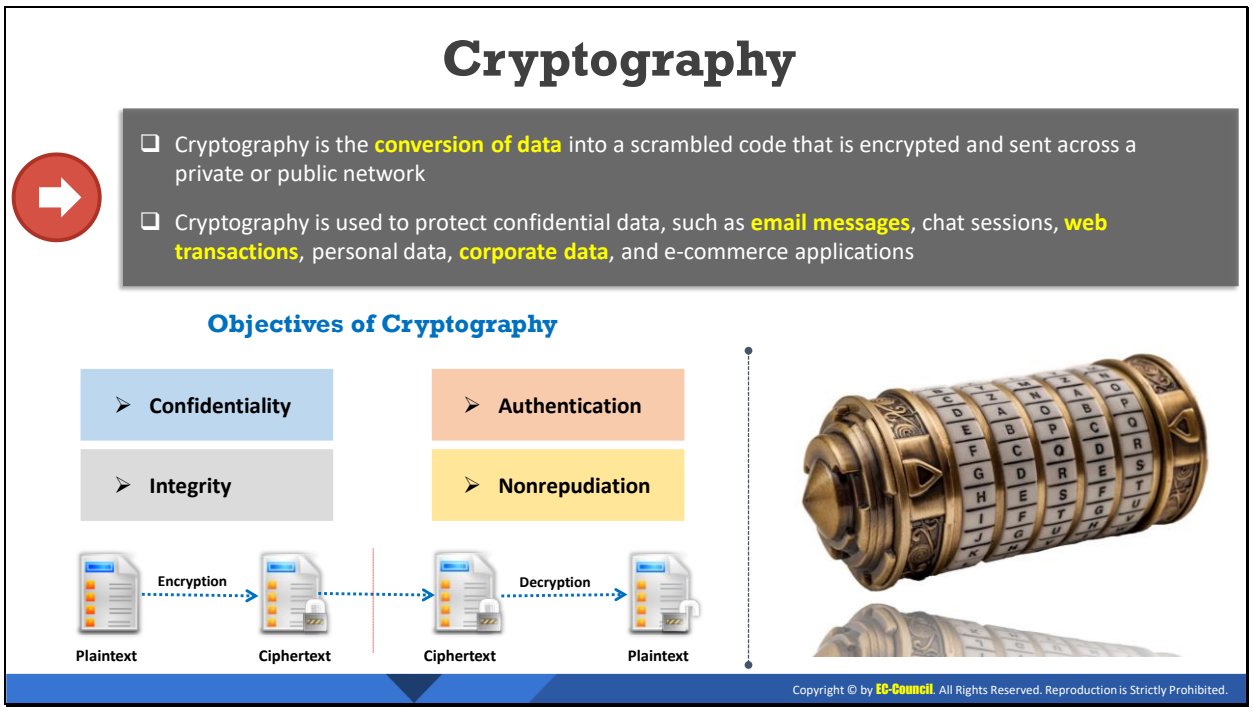
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Discuss Cryptographic Techniques

Cryptography enables one to secure transactions, communications, and other processes performed in the electronic world. This section deals with cryptography and its associated concepts, which will enable you to understand the other topics covered later in this module.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Cryptography

"Cryptography" comes from the Greek words ***kryptos***, meaning "concealed, hidden, veiled, secret, or mysterious," and ***graphia***, meaning "writing"; thus, cryptography is "the art of secret writing."

Cryptography is the practice of concealing information by converting plaintext (readable format) into ciphertext (unreadable format) using a key or encryption scheme. It is the process of converting data into a scrambled code that is encrypted and sent across a private or public network. Cryptography protects confidential data such as email messages, chat sessions, web transactions, personal data, corporate data, e-commerce applications, and many other types of communication. Encrypted messages can, at times, be decrypted by cryptanalysis (code breaking), even though modern encryption techniques are virtually unbreakable.

Objectives of Cryptography

- **Confidentiality**: Assurance that the information is accessible only to those authorized to access it.
- **Integrity**: Trustworthiness of data or resources in terms of preventing improper and unauthorized changes.
- **Authentication**: Assurance that the communication, document, or data is genuine.
- **Nonrepudiation**: Guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Cryptography Process

Plaintext (readable format) is encrypted by means of encryption algorithms such as RSA, DES, and AES, resulting in a ciphertext (unreadable format) that, on reaching the destination, is decrypted into readable plaintext.

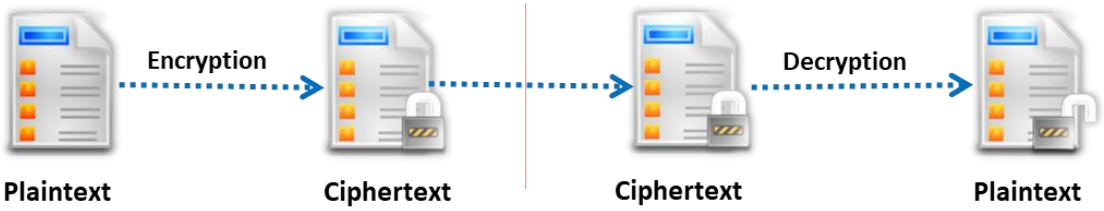
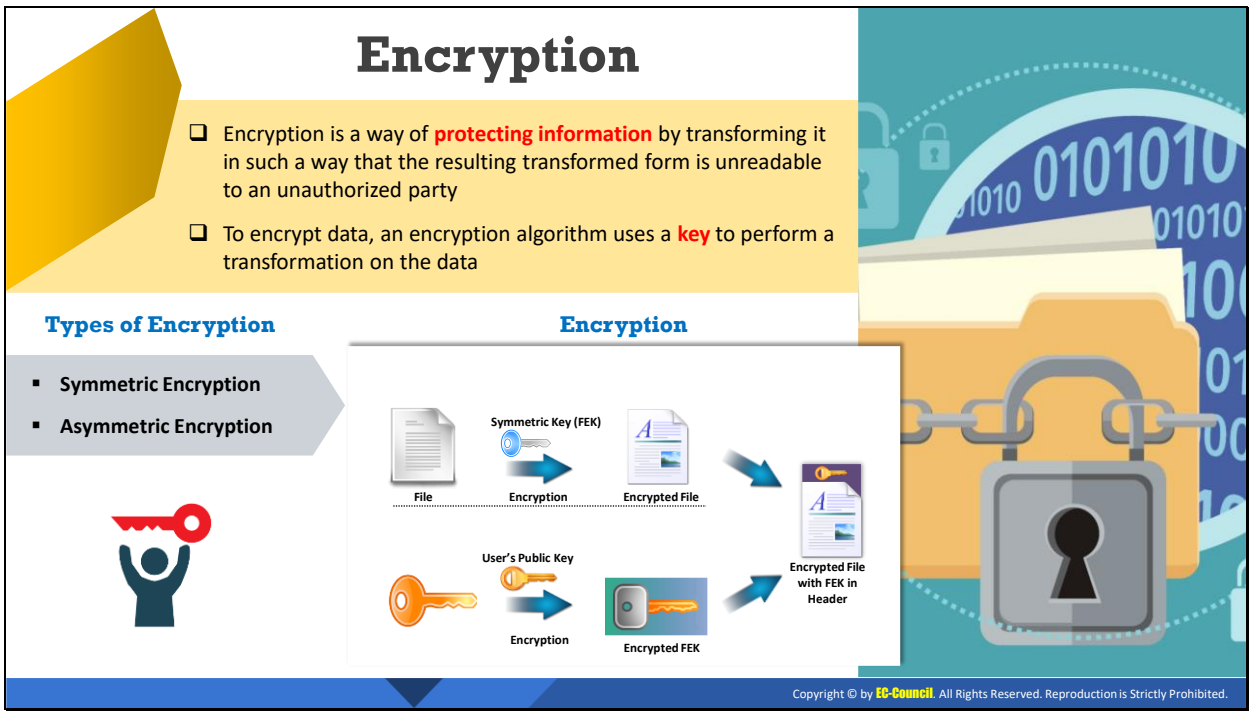


Figure 10.1: Example of Cryptography

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Encryption

Encryption is the practice of concealing information by converting a plain text (readable format) into a cipher text (unreadable format) using a key or an encryption scheme. Encryption guarantees the confidentiality and integrity of the organization's data, at rest or in transit.

The encryption algorithm encrypts the plain text with the help of an encryption key. The encryption process creates a cipher text that needs decrypting with the help of a key. The process of decryption involves the same steps except for the usage of keys in the reverse order.

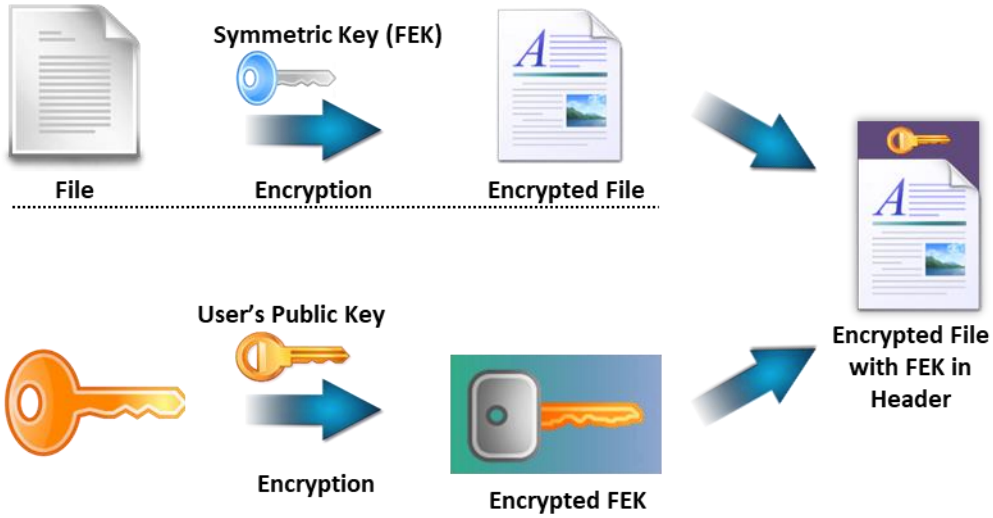


Figure 10.2: Encryption

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

The encryption process is generally applied while transmitting data through a network, mobile phones, wireless transmission, and in Bluetooth devices.

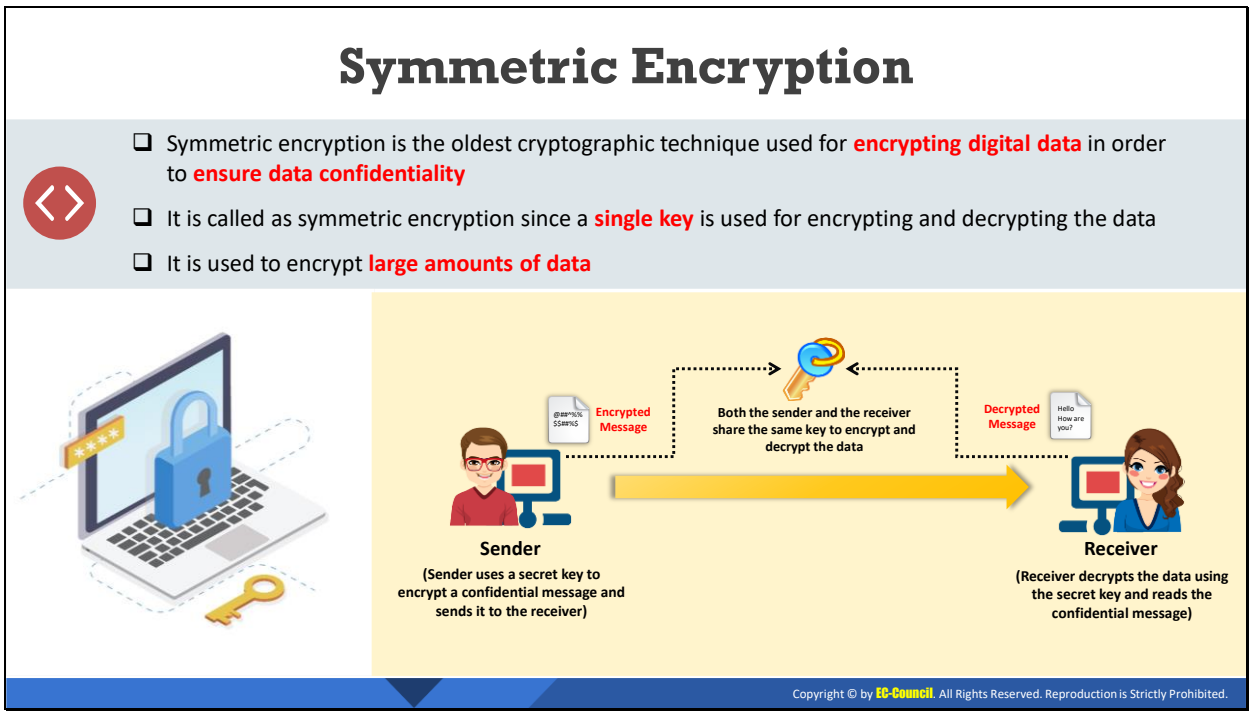
Types of Encryption

There are two types of encryption.

- Symmetric Encryption
- Asymmetric Encryption

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Symmetric Encryption

Symmetric encryption requires that both the sender and the receiver of the message possess the same encryption key. The sender uses a key to encrypt the plain text and sends the resulting cipher text to the recipient, who uses the same key to decrypt the cipher text into plain text. Symmetric encryption is also known as secret key cryptography since it uses only one secret key to encrypt and decrypt the data. This type of cryptography works well when one is communicating with only a few people.

Because the sender and receiver must share the key prior to sending any messages, this technique is of limited use over the Internet in the case where individuals who have not had prior contact frequently require a secure means of communication. The solution to this problem is the public-key cryptography.

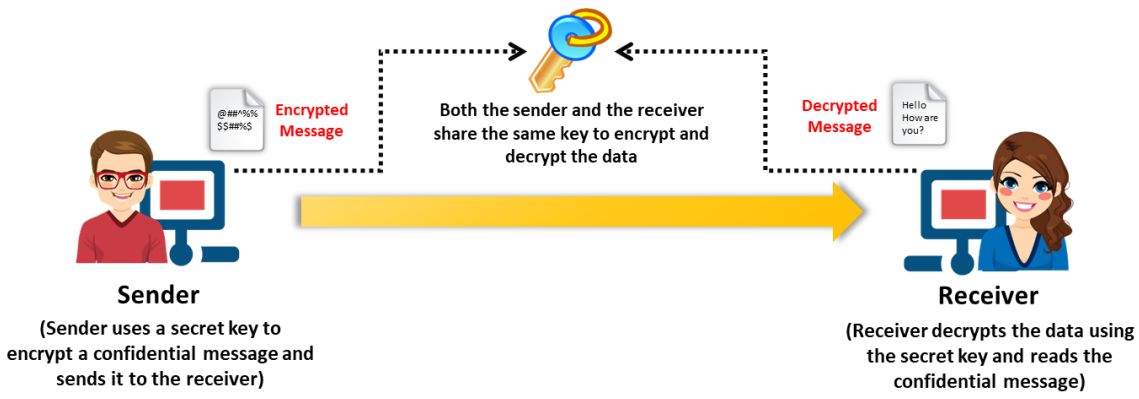


Figure 10.3: Symmetric Encryption

The symmetric key encryption can use either stream ciphers or block ciphers. Stream ciphers encrypt the bits of a message one at a time, whereas block ciphers encrypt blocks of bits.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Advantages:

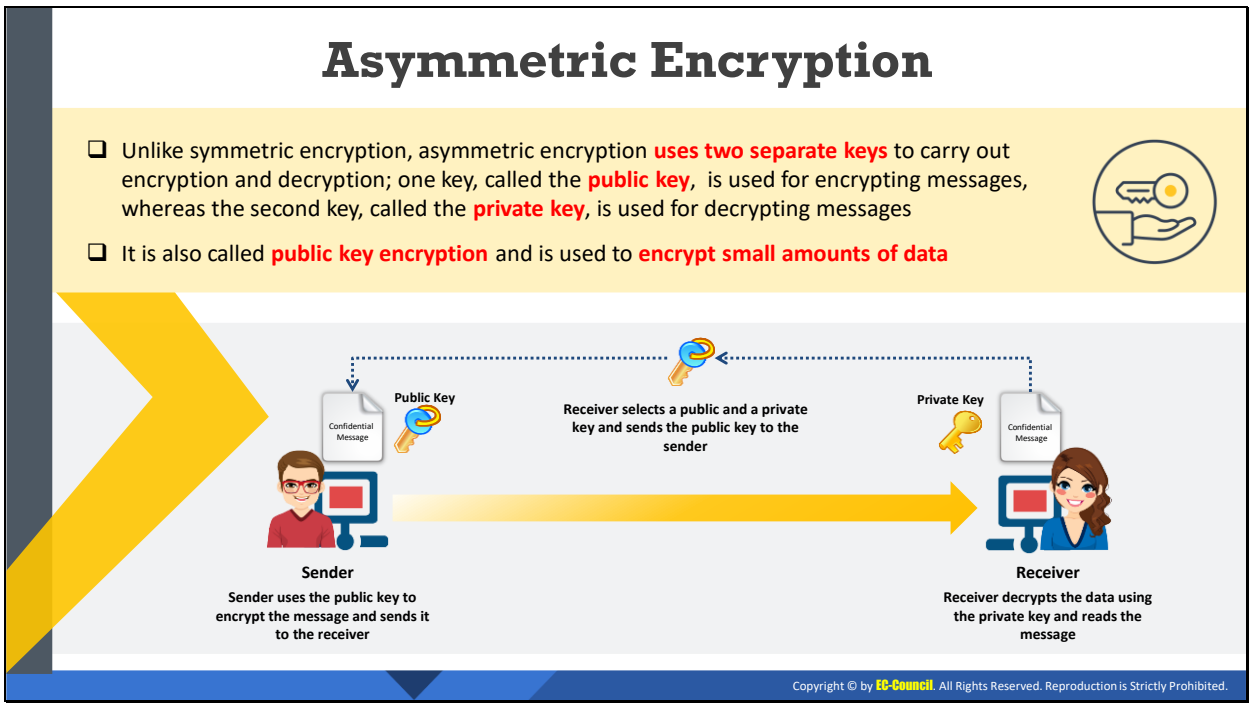
- It is easy to encrypt and decrypt a message
- It is faster than asymmetric encryption
- It is used to encrypt large amounts of data

Disadvantages:

- The communicating parties need to share the key used for transmitting the data
- Unauthorized access to a symmetric key leads to the compromise of data at both ends

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Asymmetric Encryption

Asymmetric encryption was introduced for solving key-management problems. Asymmetric encryption involves a public key and a private key. The public key is publicly available, whereas the sender keeps the private key a secret. It is also called public key encryption and is used to encrypt small amounts of data.

Asymmetric encryption uses the following sequence to send a message:

1. An individual finds the public key of the person they want to contact in a directory.
2. This public key is used for encrypting a message that is sent to the intended recipient.
3. The receiver uses the private key to decrypt the message for reading it.

No one except the holder of the private key can decrypt a message composed with the corresponding public key. This increases the security of the information because all communications involve only public keys; the message sender never transmits or shares the private keys. The sender must link the public keys with the usernames in a secured method to ensure that unauthorized individuals, claiming to be the intended recipient, do not intercept the information. To meet the requirement of authentication, one can use digital signatures.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

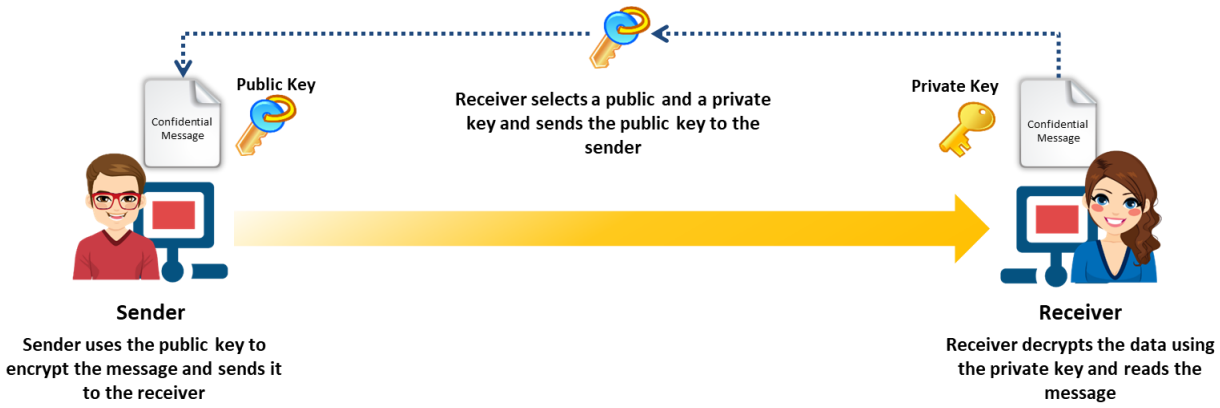


Figure 10.4: Asymmetric Encryption

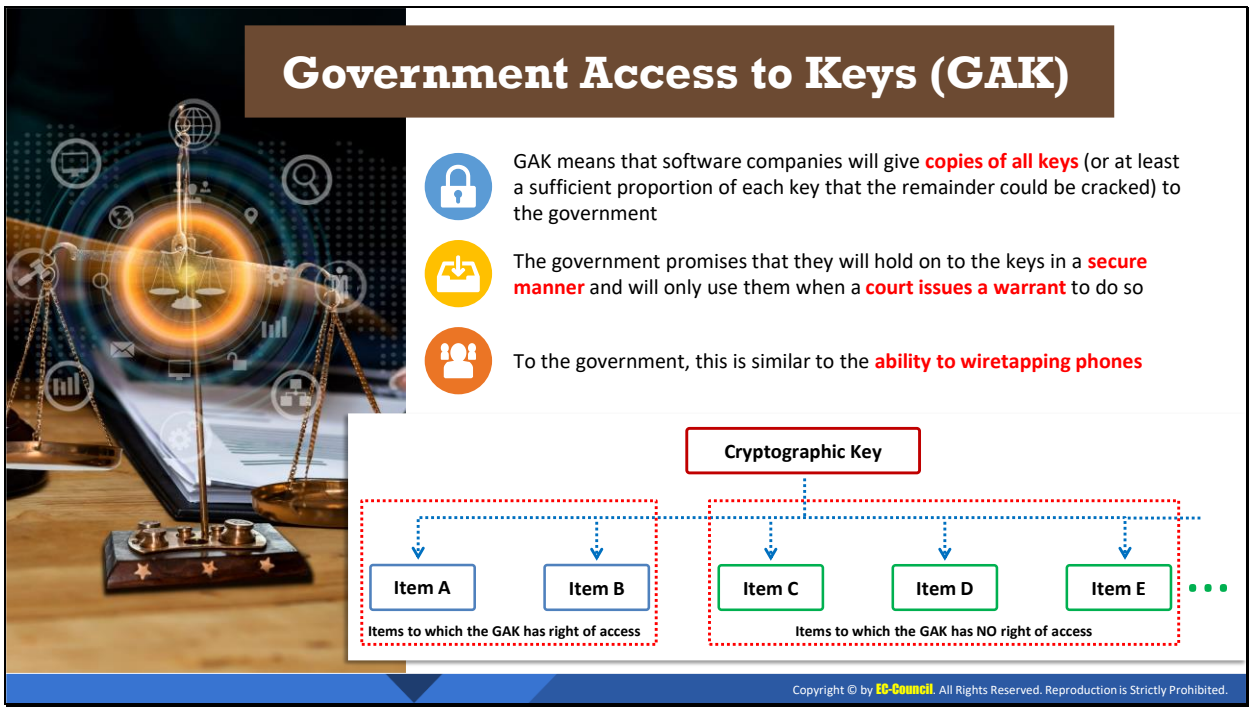
Advantages:

- It is more secure than symmetric encryption.
- There is no need to distribute the keys.

Disadvantages:

- It takes a longer processing time than symmetric encryption since it involves various combinations of secret keys and public keys.
- Various complex algorithms involved in the process of asymmetric encryption also increase the time taken to implement it.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Government Access to Keys (GAK)

Government Access to Keys (GAK) refers to the statutory obligation of individuals and organizations to disclose their cryptographic keys to government agencies. It means that software companies will give copies of all keys (or at least enough of the key such that the remainder can be cracked) to the government. Law enforcement agencies around the world acquire and use these cryptographic keys to monitor suspicious communication and collect evidence of cybercrimes in the interests of national security. The government promises that it will hold on to the keys in a secure manner and only use them when a court issues a warrant to do so. To the government, this issue is similar to the ability to wiretap phones.

Government agencies often use key escrow for uninterrupted access to keys. Key escrow is a key exchange arrangement in which essential cryptographic keys are stored with a third party in escrow. The third party can use or allow others to use the encryption keys under certain predefined circumstances. The third party, with regard to GAK, is generally a government agency that may use the encryption keys to decipher digital evidence under authorization or a warrant from a court of law. However, there is growing concern about the privacy and security of cryptographic keys and information. Government agencies are responsible for protecting these keys. Such agencies generally use a single key to protect other keys, which is not a good idea, as revealing a single key could expose the other keys.

These agencies are not aware of how confidential the information protected by the keys is, which makes it difficult to judge how much protection is required. In cases where seized keys also protect other information that these agencies have no right to access, the consequences of key revelation cannot be determined, because government agencies are not aware of the information that the keys protect. In such cases, the key owner is liable for the consequences of key revelation. Before owners hand over their keys to government agencies, they need to be

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

assured that the government agencies will protect these keys according to a sufficiently strong standard to protect their interests.

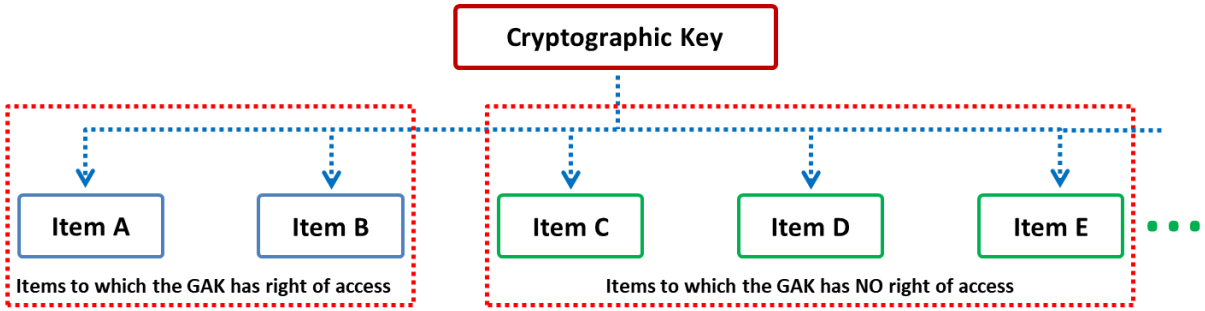
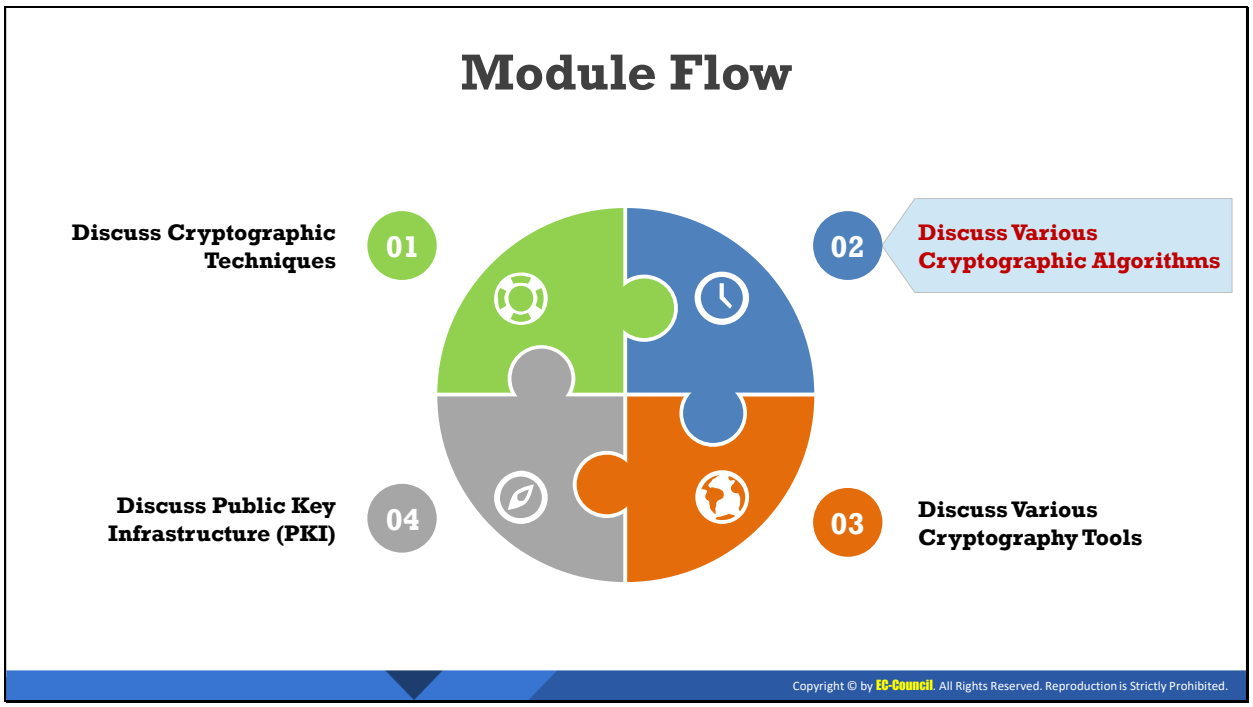


Figure 10.5: Illustration of GAK

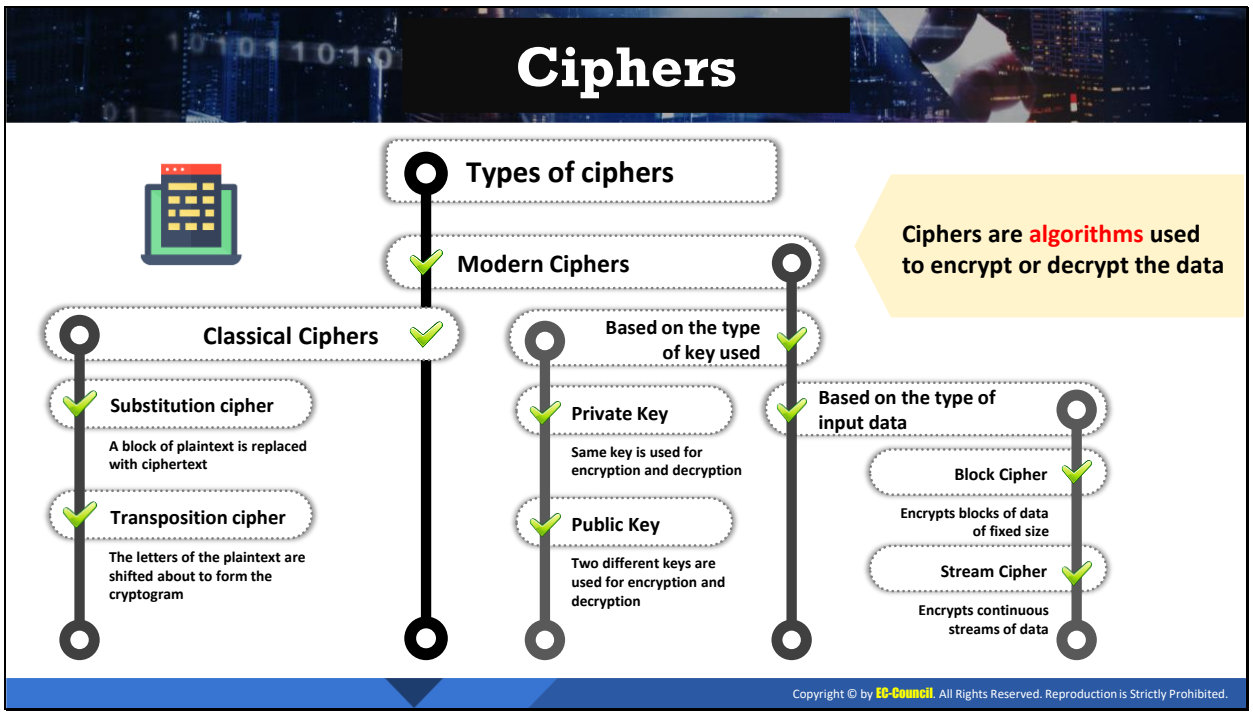
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Discuss Various Cryptographic Algorithms

Encryption is the process of converting readable plaintext into an unreadable ciphertext using a set of complex algorithms that transform the data into blocks or streams of random alphanumeric characters. This section deals with ciphers and various encryption algorithms such as DES, AES, RC4, RC5, RC6, DSA, RSA, MD5, MD6, SHA, etc.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Ciphers

In cryptography, a cipher is an algorithm (a series of well-defined steps) for performing encryption and decryption. Encipherment is the process of converting plaintext into a cipher or code; the reverse process is called decipherment. A message encrypted using a cipher is rendered unreadable unless its recipient knows the secret key required to decrypt it. Communication technologies (e.g., Internet, cell phones) rely on ciphers to maintain both security and privacy. Cipher algorithms may be open-source (the algorithmic process is in the public domain while the key is selected by a user and is private) or closed-source (the process is developed for use in specific domains, such as the military, and the algorithm itself is not in the public domain). Furthermore, ciphers may be free for public use or licensed.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Types of ciphers

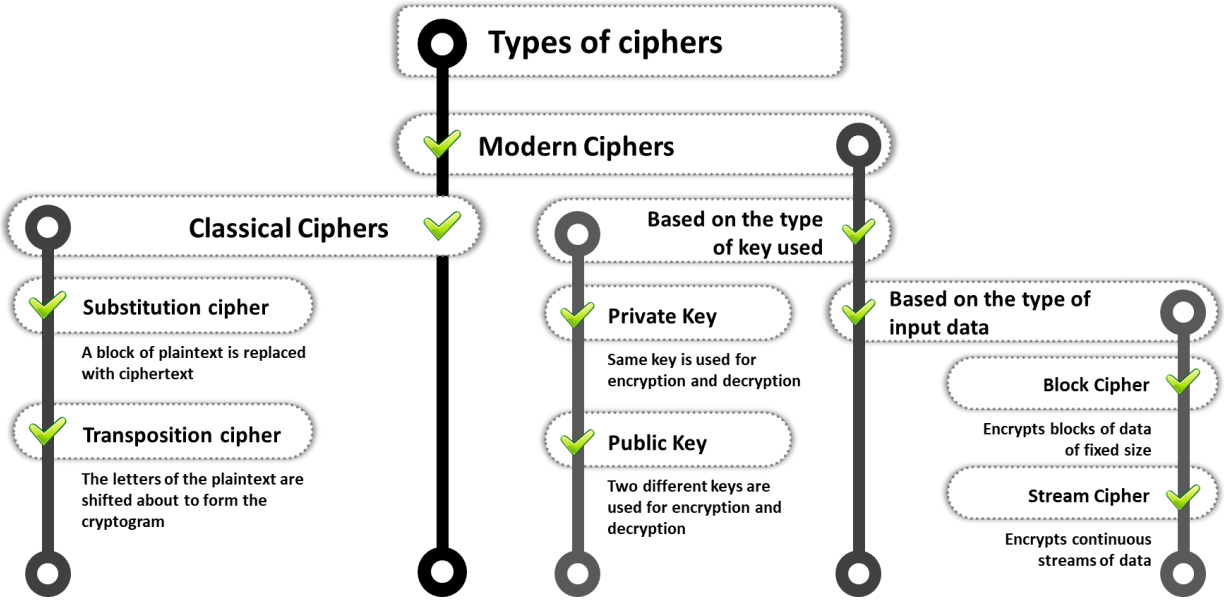


Figure 10.6: Classification of ciphers

Ciphers are of two main types: classical and modern.

- **Classical Ciphers**

  Classical ciphers are the most basic type of ciphers, which operate on letters of the alphabet (A–Z). These ciphers are generally implemented either by hand or with simple mechanical devices. Because these ciphers are easily deciphered, they are generally unreliable.

  Types of classical ciphers

  - **Substitution cipher**: The user replaces units of plaintext with ciphertext according to a regular system. The units may be single letters, pairs of letters, or combinations of them, and so on. The recipient performs inverse substitution to decipher the text. Examples include the Beale cipher, autokey cipher, Gronsfeld cipher, and Hill cipher.

    For example, "**HELLO WORLD**" can be encrypted as "**PSTER HGFST**" (i.e., H=P, E=S, etc.).

  - **Transposition cipher**: Here, letters in the plaintext are rearranged according to a regular system to produce the ciphertext. For example, "**CRYPTOGRAPHY**" when encrypted becomes "**AOYCRGPTYRHP**." Examples include the rail fence cipher, route cipher, and Myszkowski transposition.

- **Modern Ciphers**

  Modern ciphers are designed to withstand a wide range of attacks. They provide message secrecy, integrity, and authentication of the sender. A user can calculate a modern cipher using a one-way mathematical function that is capable of factoring large prime numbers.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Types of Modern ciphers

- **Based on the type of key used**
  - **Symmetric-key algorithms (Private-key cryptography)**: Use the same key for encryption and decryption.
  - **Asymmetric-key algorithms (Public-key cryptography)**: Use two different keys for encryption and decryption.
- **Based on the type of input data**
  - **Block cipher**: Deterministic algorithms operating on a block (a group of bits) of fixed size with an unvarying transformation specified by a symmetric key. Most modern ciphers are block ciphers. They are widely used to encrypt bulk data. Examples include DES, AES, IDEA, etc. When the block size is less than that used by the cipher, padding is employed to achieve a fixed block size.
  - **Stream cipher**: Symmetric-key ciphers are plaintext digits combined with a key stream (pseudorandom cipher digit stream). Here, the user applies the key to each bit, one at a time. Examples include RC4, SEAL, etc.

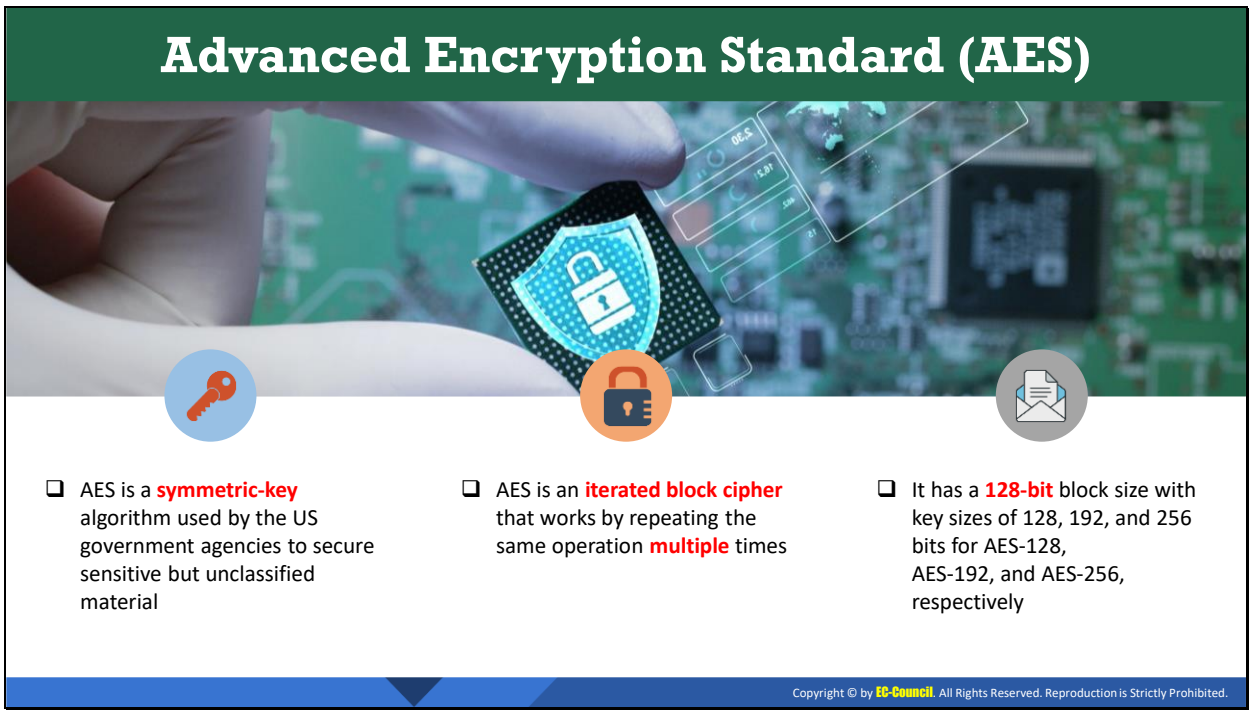
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Data Encryption Standard (DES)

DES is a standard for data encryption that uses a secret key for both encryption and decryption (symmetric cryptosystem). DES uses a 64-bit secret key, of which 56 bits are generated randomly and the other 8 bits are used for error detection. It uses a data encryption algorithm (DEA), a secret key block cipher employing a 56-bit key operating on 64-bit blocks. DES is the archetypal block cipher—an algorithm that takes a fixed-length string of plaintext bits and transforms it into a ciphertext bit string of the same length. The design of DES allows users to implement it in hardware and use it for single-user encryption, such as to store files on a hard disk in encrypted form.

DES provides 72 quadrillion or more possible encryption keys and chooses a random key for the encryption of each message. Because of the inherent weakness of DES vis-à-vis today's technologies, some organizations use triple DES (3DES), in which they repeat the process three times for added strength until they can afford to update their equipment to AES capabilities.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

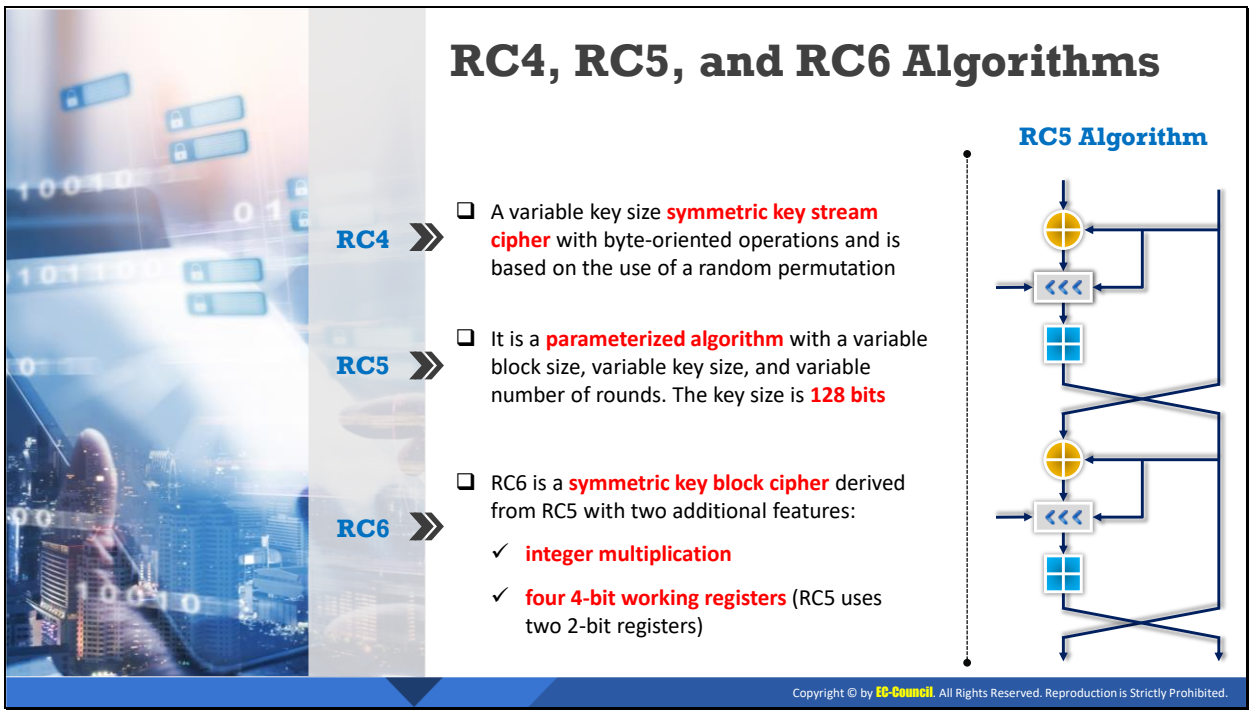


Advanced Encryption Standard (AES)

The advanced encryption standard (AES) is a National Institute of Standards and Technology (NIST) specification for the encryption of electronic data. It also helps to encrypt digital information such as telecommunications, financial, and government data. US government agencies have been using it to secure sensitive but unclassified material.

An AES consists of a symmetric-key algorithm in which the encryption as well as decryption is performed using the same key. It is an iterated block cipher that works by repeating the defined steps multiple times. It has a 128-bit block size, having key sizes of 128, 192, and 256 bits respectively for AES-128, AES-192, and AES-256. The design of AES makes its use efficient in both software and hardware. It works at multiple network layers simultaneously.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



RC4, RC5, and RC6 Algorithms

Symmetric encryption algorithms developed by RSA Security are discussed below.

- **RC4**

  RC4 is a variable key-size symmetric-key stream cipher with byte-oriented operations, and it is based on the use of a random permutation. According to some analyses, the period of the cipher is likely to be greater than 10,100. Each output byte uses 8 to 16 system operations; thus, the cipher can run fast when used in software. RC4 enables safe communications such as for traffic encryption (which secures websites) and for websites that use the SSL protocol.

- **RC5**

  RC5 is a fast symmetric-key block cipher designed by Ronald Rivest for RSA Data Security (now RSA Security). The algorithm is a parameterized algorithm with a variable block size, a variable key size, and a variable number of rounds. The block sizes can be 32, 64, or 128 bits. The range of the rounds can vary from 0 to 255, and the size of the key can vary from 0 to 2,040 bits. This built-in variability can offer flexibility at all levels of security. The routines used in RC5 are key expansion, encryption, and decryption.

  In the key expansion routine, the secret key that a user provides is expanded to fill the key table (the size of which depends on the number of rounds). RC5 uses a key table for both encryption and decryption. The encryption routine has three fundamental operations: integer addition, bitwise XOR, and variable rotation. The intensive use of data-dependent rotation and the combination of different operations make RC5 a secure encryption algorithm.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

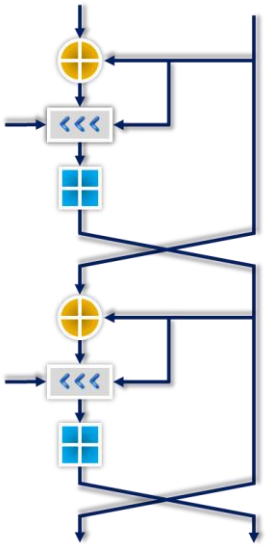


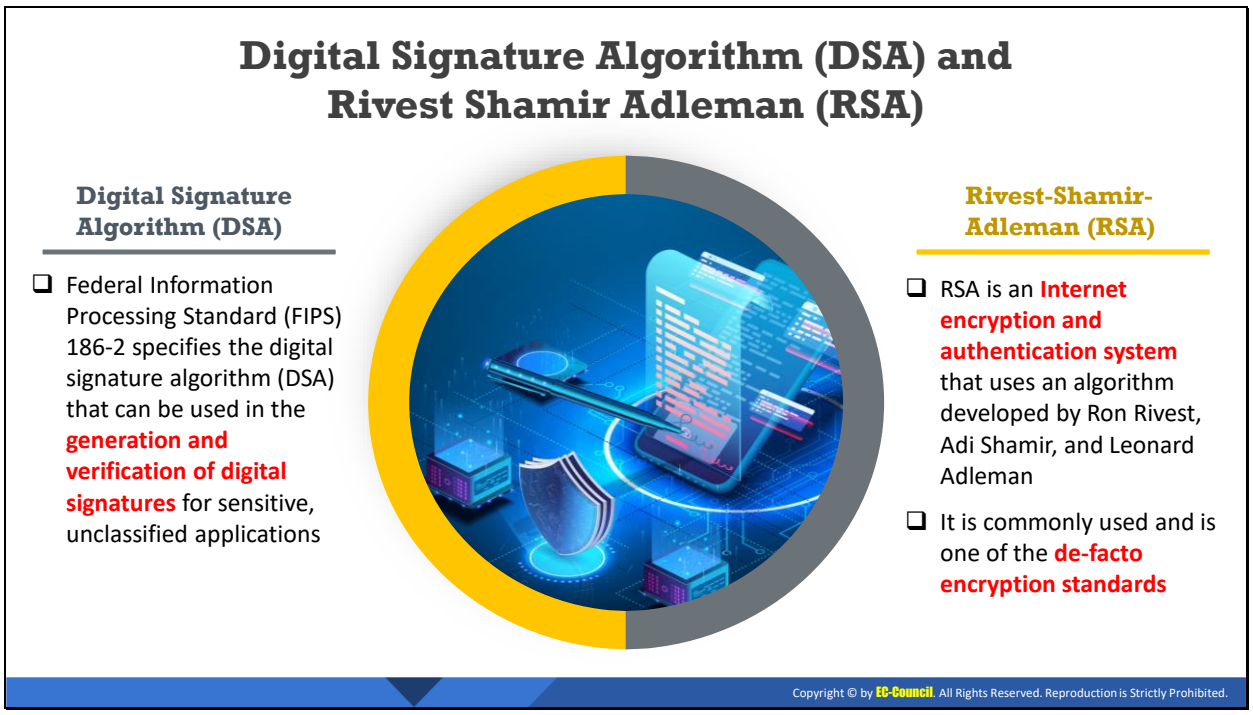
Figure 10.7: Block diagram of the RC5 algorithm

- **RC6**

  RC6 is a symmetric-key block cipher derived from RC5. It is a parameterized algorithm with a variable block size, key size, and number of rounds. Two features that differentiate RC6 from RC5 are integer multiplication (which is used to increase the diffusion, achieved in fewer rounds with increased speed of the cipher) and the use of four 4-bit working registers rather than two 2-bit registers. RC6 uses four 4-bit registers instead of two 2-bit registers because the block size of the AES is 128 bits.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Digital Signature Algorithm (DSA)

The digital signature algorithm (DSA) is a Federal Information Processing Standard (FIPS) for digital signatures. The NIST proposed the DSA for using it in the digital signature standard (DSS), adopted as a FIPS 186. The DSA helps in the generation and verification of digital signatures in sensitive and unclassified applications. It creates a 320-bit digital signature with a 512–1024 bit security.

A digital signature is a mathematical scheme used for the authenticating digital messages. Computation of a digital signature uses a set of rules (i.e., the DSA) and a set of parameters, using which a user can verify the identity of the signatory and the integrity of the data.

Processes involved in DSA:

- **Signature generation process**: A private key is used to sign the digital message.
- **Signature verification process**: A public key is used to verify whether the given digital signature is genuine.

DSA is a public-key cryptosystem as it involves the use of both private and public keys.

Benefits of DSA:

- Less chances of forgery than in the case of a written signature
- Quick and easy method for business transactions
- Fake currency problem can be drastically reduced

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Rivest Shamir Adleman (RSA)

Ron Rivest, Adi Shamir, and Leonard Adleman formulated RSA, a public-key cryptosystem for Internet encryption and authentication. RSA uses a modular arithmetic and elementary number theory for performing computations using two large prime numbers. The RSA system is widely used in a variety of products, platforms, and industries and is one of the de-facto encryption standards. Companies such as Microsoft, Apple, Sun, and Novell incorporate the RSA algorithm in their operating systems. RSA can also be found on hardware secured telephones, ethernet network cards, and smart cards.

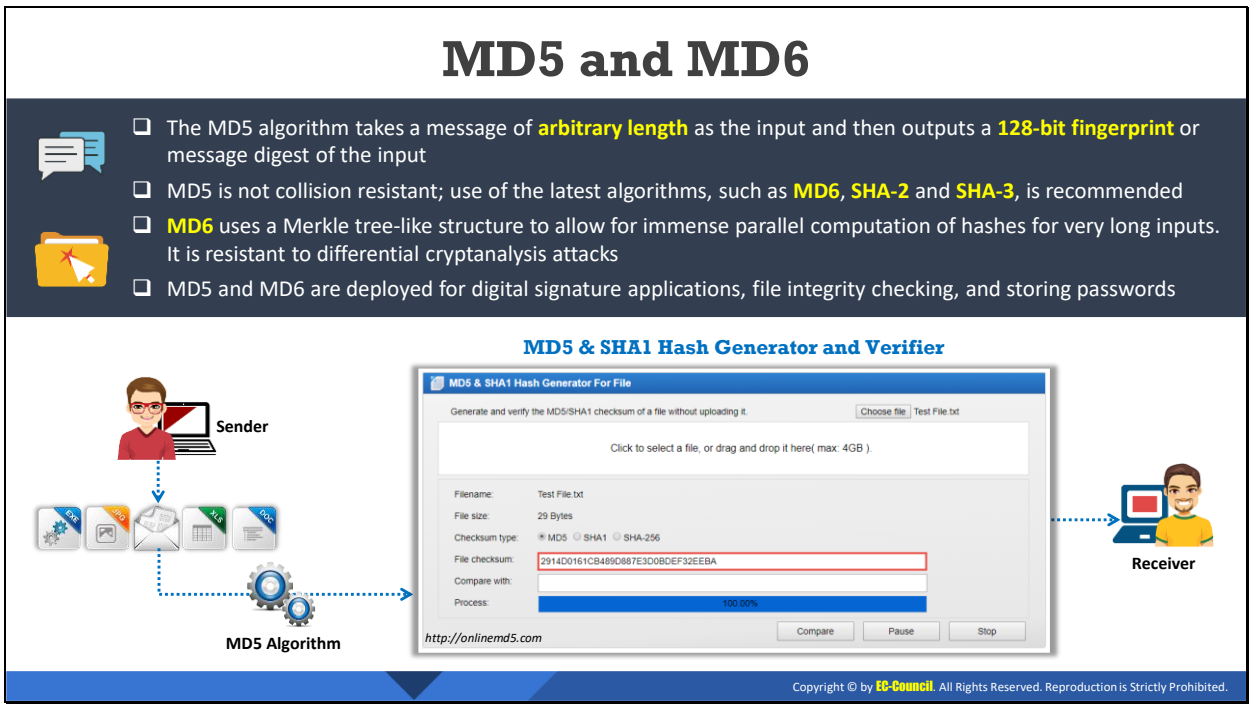
The following sequence is an example of how cryptography uses the RSA algorithm in a practical exchange:

- The sender encrypts a message using a randomly chosen DES symmetric key. DES is a relatively insecure symmetric-key system that uses 64-bit encryption (56 bits for key-length, 8 bits for cyclic redundancy check) to encrypt data.
- The sender then looks up the recipient's public key and uses it to encrypt the DES key using the RSA system.
- The sender transmits an RSA digital envelope, consisting of a DES-encrypted message and an RSA-encrypted DES key, to the recipient.
- The recipient decrypts the DES key using his/her RSA private key and uses it to decrypt the message itself.

This system combines the high speed of DES with the key management convenience of the RSA system.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



MD5 and MD6

MD2, MD4, MD5, and MD6 are **message digest algorithms** used in digital signature applications to compress a document securely before the system signs it with a private key. The algorithms can be of variable length, but the resulting message digest always has a size of 128 bits.

The structures of all three algorithms (MD2, MD4, and MD5) appear similar, although the design of MD2 is reasonably different from that of MD4 and MD5. MD2 supports 8-bit machines, while MD4 and MD5 support 32-bit machines. The algorithm pads the message with extra bits to ensure that the number of bits is divisible by 512. The extra bits may include a 64-bit binary message.

Attacks on versions of MD4 have become increasingly successful. Research has shown how an attacker launches collision attacks on the full version of MD4 within a minute on a typical PC. MD5 is slightly more secure but is slower than MD4. However, both the message digest size and the padding requirements remain the same.

MD5 is a widely used cryptographic hash function that takes a message of arbitrary length as input and outputs a 128-bit (16-byte) fingerprint or message digest of the input. MD5 can be used in a wide variety of cryptographic applications and is useful for digital signature applications, file integrity checking, and storing passwords. However, MD5 is not collision resistant; therefore, it is better to use the latest algorithms, such as MD6, SHA-2, and SHA-3.

MD6 uses a Merkle-tree-like structure to allow for large-scale parallel computation of hashes for very long inputs. It is resistant to differential cryptanalysis attacks.

To calculate the effectiveness of hash functions, check the output produced when the algorithm randomizes an arbitrary input message.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

The following are examples of minimally different message digests:

- echo “There is CHF1500 in the blue bo” | md5sum
  e41a323bdf20eadafd3f0e4f72055d36
- echo “There is CHF1500 in the blue box” | md5sum
  7a0da864a41fd0200ae0ae97afd3279d
- echo “There is CHF1500 in the blue box.” | md5sum
  2db1ff7a70245309e9f2165c6c34999d

Even minimally different texts produce radically different MD5 codes.

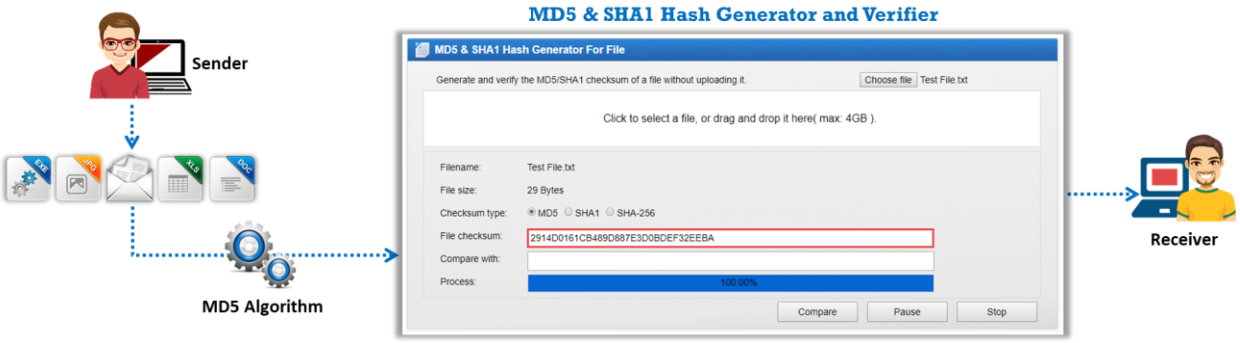


Figure 10.8: Verifying MD5 Hash

Note: Message digests are also called as one-way hash functions because they cannot be reversed.

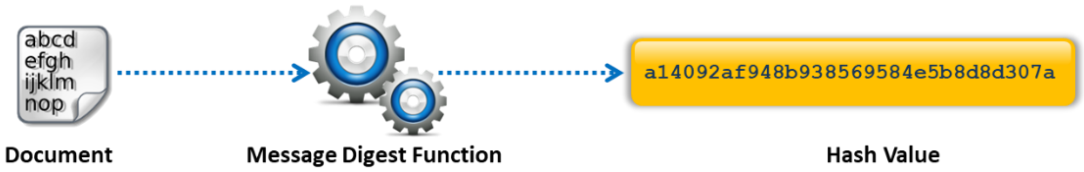
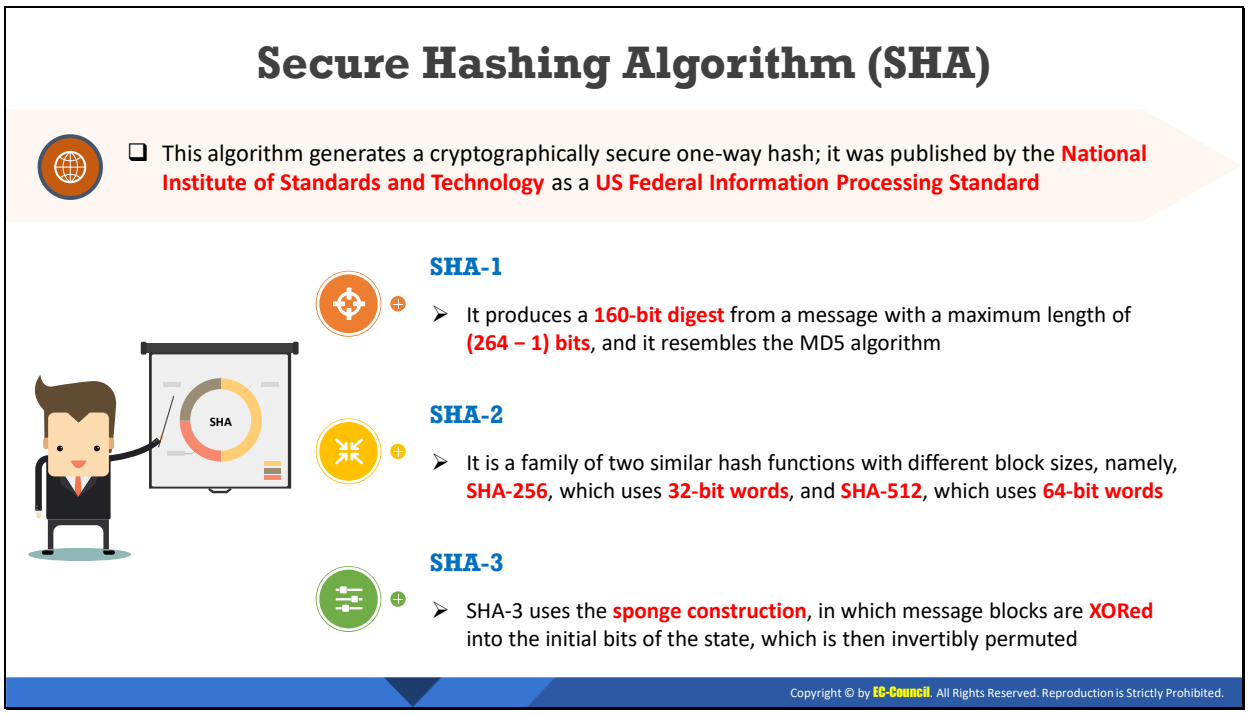


Figure 10.9: Working of Message Digests

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Secure Hashing Algorithm (SHA)

The NIST has developed the Secure Hash Algorithm (SHA), specified in the **Secure Hash Standard** (**SHS**) and published as a federal information-processing standard (FIPS PUB 180). It generates a cryptographically secure one-way hash. Rivest developed the SHA, which is similar to the message digest algorithm family of hash functions. It is slightly slower than MD5, but its larger message digest makes it more secure against brute-force collision and inversion attacks.

SHA encryption is a series of five different cryptographic functions, and it currently has three generations: SHA-1, SHA-2, and SHA-3.

- **SHA-0**: A retronym applied to the original version of the 160-bit hash function published in 1993 under the name SHA, which was withdrawn from trade due to an undisclosed "**significant flaw**" in it. It was replaced with a slightly revised version, namely SHA-1.
- **SHA-1**: It is a 160-bit hash function that resembles the former MD5 algorithm developed by Ron Rivest. It produces a 160-bit digest from a message with a maximum length of (264 − 1) bits. It was designed by the National Security Agency (NSA) to be part of the Digital Signature Algorithm (DSA). It is most commonly used in security protocols such as PGP, TLS, SSH, and SSL. As of 2010, SHA-1 is no longer approved for cryptographic use because of its cryptographic weaknesses.
- **SHA-2**: SHA2 is a family of two similar hash functions with different block sizes, namely SHA-256, which uses 32-bit words, and SHA-512, which uses 64-bit words. The truncated versions of each standard are SHA-224 and SHA-384.
- **SHA-3**: SHA-3 uses sponge construction in which message blocks are XORed into the initial bits of the state, which the algorithm then invertibly permutes. It supports the

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

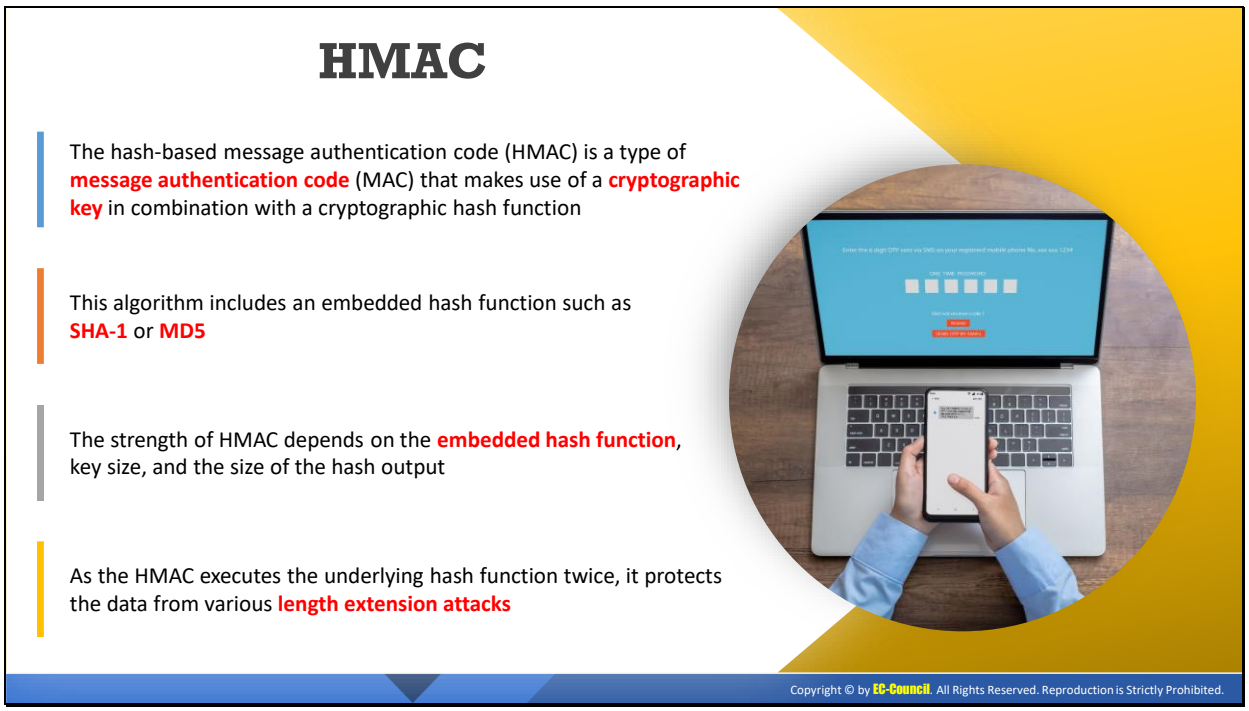
same hash lengths as SHA-2 but differs in its internal structure considerably from the rest of the SHA family.

Comparison of SHA functions (SHA-0, SHA-1, SHA-2, and SHA-3).

Algorithm and variant		Output size (bits)	Internal state size (bits)	Block Size (bits)	Maximum message size (bits)	Rounds	Operations	Security (bits)
MD5 (as reference)		128	128 (4*32)	512	2^{64}-1	64	Add mod 2^{32}, and, or, xor, rot	<=18 (collisions found)
SHA-0		160	160 (5*32)	512	2^{64}-1	80	Add mod 2^{32}, and, or, xor, rot	<34 (collisions found)
SHA-1		160	160 (5*32)	512	2^{64}-1	80	Add mod 2^{32}, and, or, xor, rot	<63 (collisions found)
SHA-2	SHA-224 SHA-256	224 256	256 (8*32)	512	2^{64}-1	64	Add mod 2^{32}, and, or, xor, shr, rot	112 128
	SHA-384 SHA-512 SHA-512/224 SHA-512/256	384 512 224 256	512 (8*64)	1024	2^{128}-1	80	Add mod 2^{64}, and, or, xor, shr, rot.	192 256 112 128
SHA-3	SHA3-224 SHA3-256 SHA3-384 SHA3-512 SHAKE128 sHAKE256	224 256 384 512 d(arbitrary) d(arbitrary)	1600 (5*5*64)	1152 1088 832 576 1344 1088	∞	24	And, xor, not, rot	112 128 192 256 Min(d/2,128) Min(d/2,256)

Table 10.1: Comparison between SHA functions

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



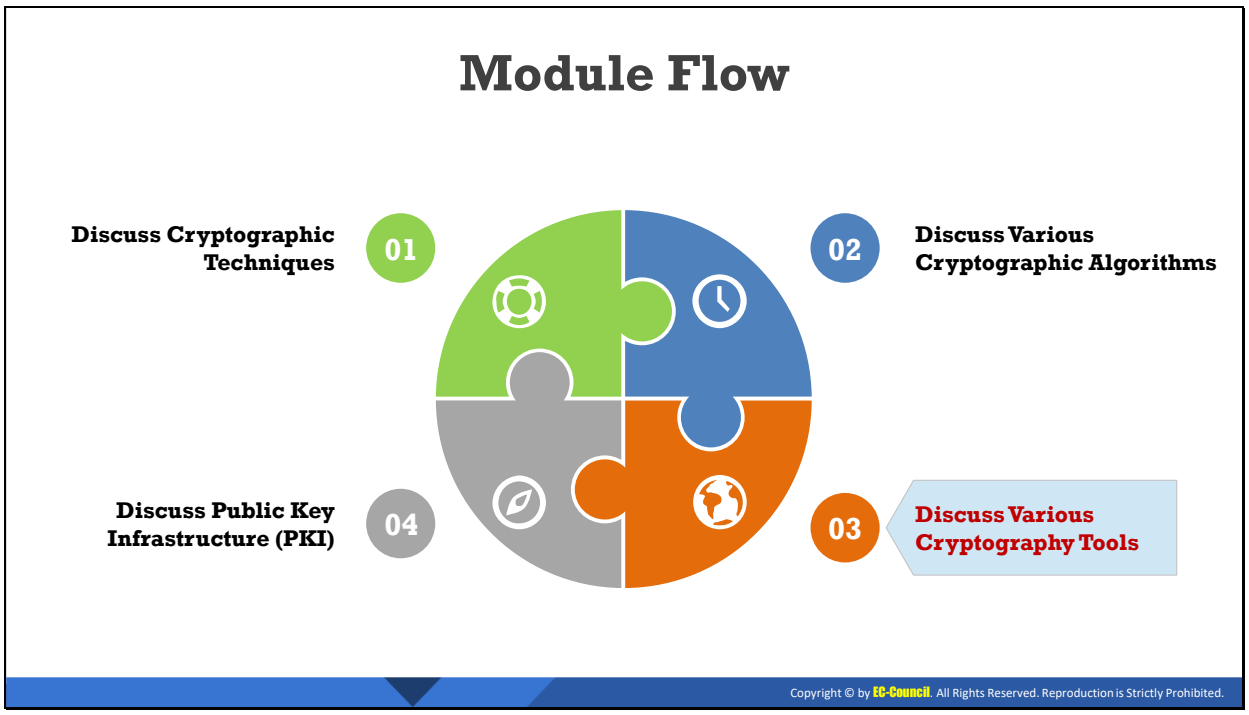
HMAC

Hash-based message authentication code (HMAC) is a type of message authentication code (MAC) that uses a cryptographic key along with a cryptographic hash function. It is widely used to verify the integrity of data and authentication of a message. This algorithm includes an embedded hash function such as SHA-1 or MD5. The strength of HMAC depends on the embedded hash function, key size, and size of the hash output.

HMAC includes two stages for computing the hash. The input key is processed to produce two keys, namely the inner key and the outer key. The first stage of the algorithm inputs the inner key and message to produce an internal hash. The second stage of the algorithm inputs the output from the first stage and outer key and produces the final HMAC code.

As HMAC executes the underlying hash function twice, it offers protection against various length extension attacks. The size of the key and the output depends on the embedded hash function, e.g., 128 or 160 bits in the case of MD5 or SHA-1, respectively.

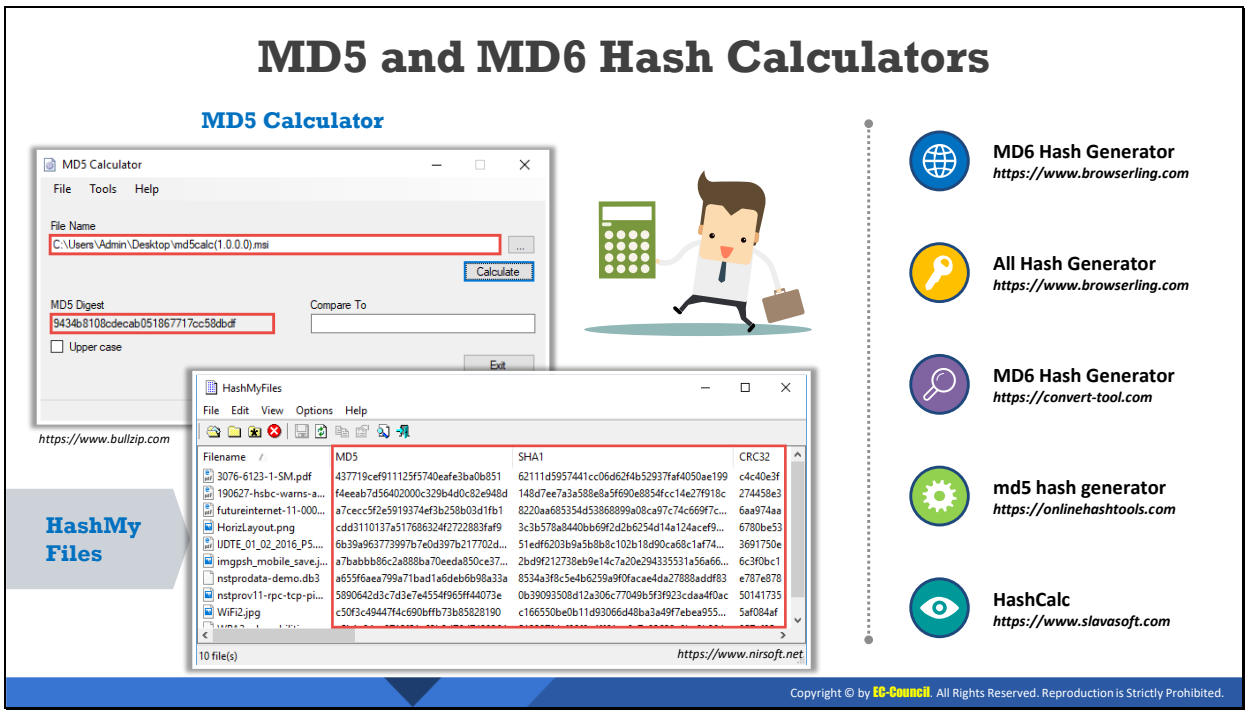
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Discuss Various Cryptography Tools

This section deals with various cryptography tools that you can use to encrypt sensitive data to protect it from unauthorized access by any party other than the person for whom it is intended.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



MD5 and MD6 Hash Calculators

MD5 and MD6 hash calculators that use different hash algorithms to convert plaintext into its equivalent hash value are discussed below.

- **MD5 Calculator**

  Source: *https://www.bullzip.com*

  MD5 Calculator is a simple application that calculates the MD5 hash of a given file. It can be used with large files (e.g., several gigabytes in size). It features a progress counter and a text field from which the final MD5 hash can be easily copied to the clipboard. MD5 Calculator can be used to check the integrity of a file.

  It allows you to calculate the MD5 hash value of the selected file. Right-click the file and choose "**MD5 Calculator**;" the program will calculate the MD5 hash. The MD5 Digest field contains the calculated value. To compare this MD5 digest with another, one can paste the other value into the Compare To field. Obviously, an equal to sign ("=") appears between the two values if they are equal; otherwise, the less than ("<") or greater than (">") sign will tell you that the values are different.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

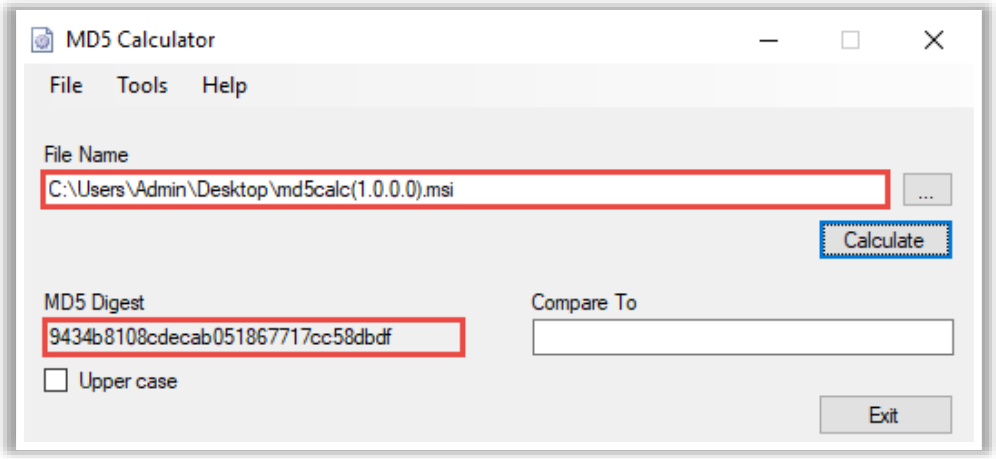


Figure 10.10: Screenshot of MD5 Calculator

- **HashMyFiles**

  Source: *https://www.nirsoft.net*

  HashMyFiles is a utility that allows you to calculate the MD5 and SHA1 hashes of one or more files in the system. It allows you to copy the MD5/SHA1 hash list to the clipboard or save it in a text/html/xml file. You can launch HashMyFiles from the context menu of Windows Explorer and display the MD5/SHA1 hashes of the selected files or folders.

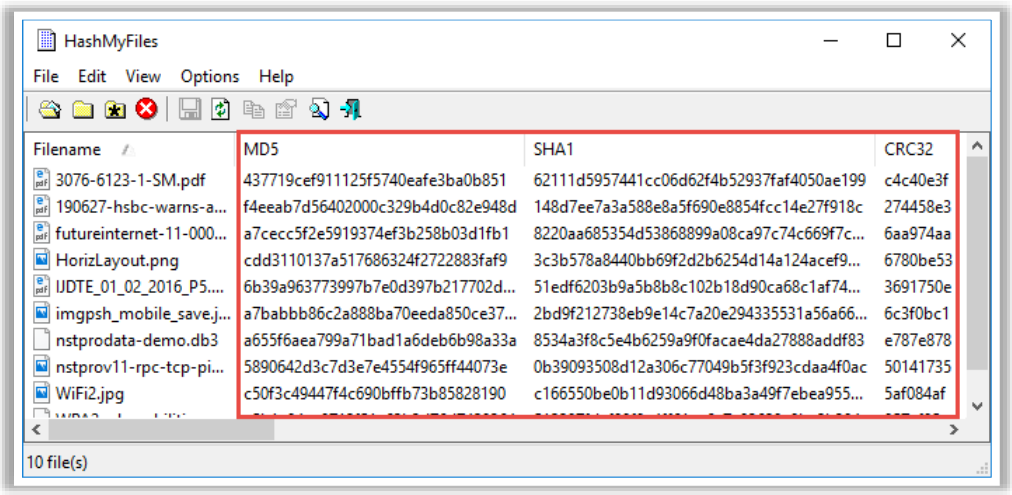
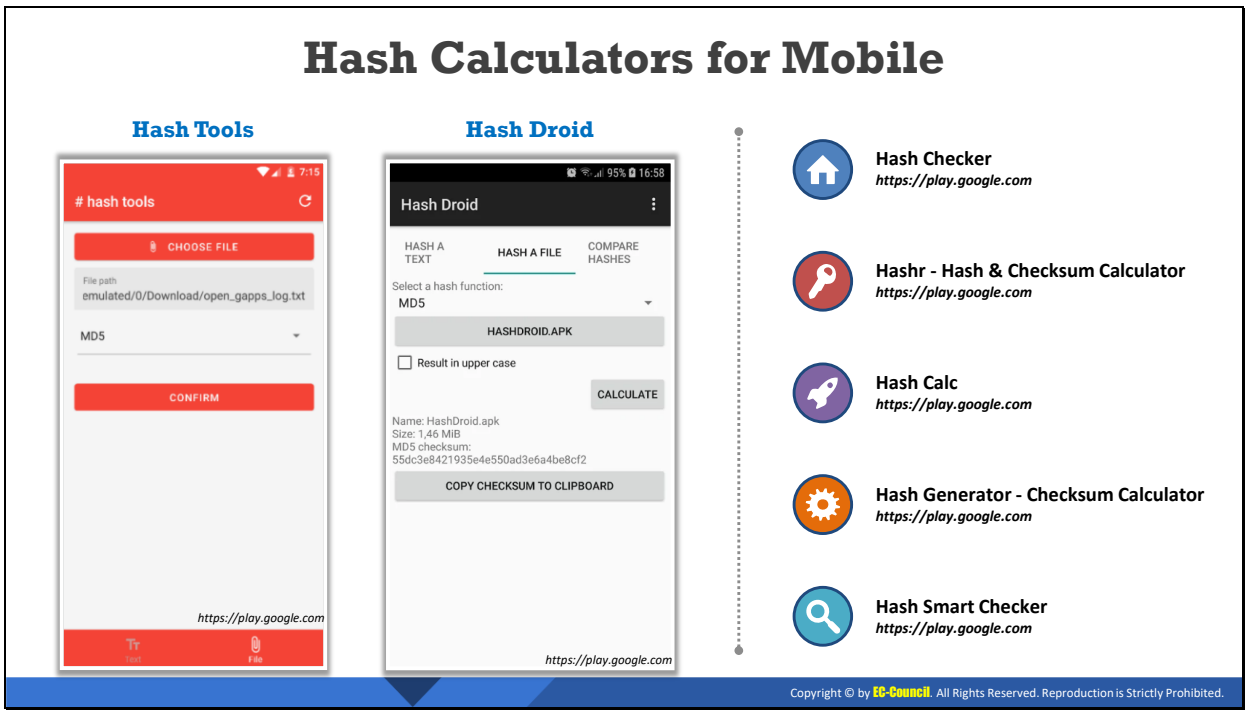


Figure 10.11: Screenshot of HashMyFiles

Some additional MD5 and MD6 hash calculators are as follows:

- MD6 Hash Generator (*https://www.browserling.com*)
- All Hash Generator (*https://www.browserling.com*)
- MD6 Hash Generator (*https://convert-tool.com*)
- md5 hash generator (*https://onlinehashtools.com*)
- HashCalc (*https://www.slavasoft.com*)

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Hash Calculators for Mobile

Some hash calculators for mobile devices are discussed below.

- **Hash Tools**

  Source: *https://play.google.com*

  Hash Tools is a utility for calculating a hash from a given text or decrypting a hash to its original text. In this application, the available hash functions are MD5, SHA-1, SHA-256, SHA-384, and SHA-512.

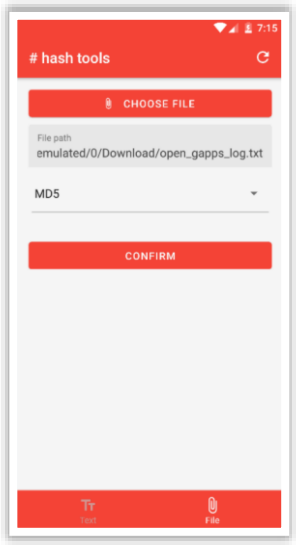


Figure 10.12: Screenshot of Hash Tools

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **Hash Droid**

  Source: *https://play.google.com*

  The Hash Droid utility helps to calculate a hash from a given text or a file stored on the device. In this application, the available hash functions are Adler-32, CRC-32, Haval-128, MD2, MD4, MD5, RIPEMD-128, RIPEMD-160, SHA-1, SHA-256, SHA-384, SHA-512, Tiger, and Whirlpool.

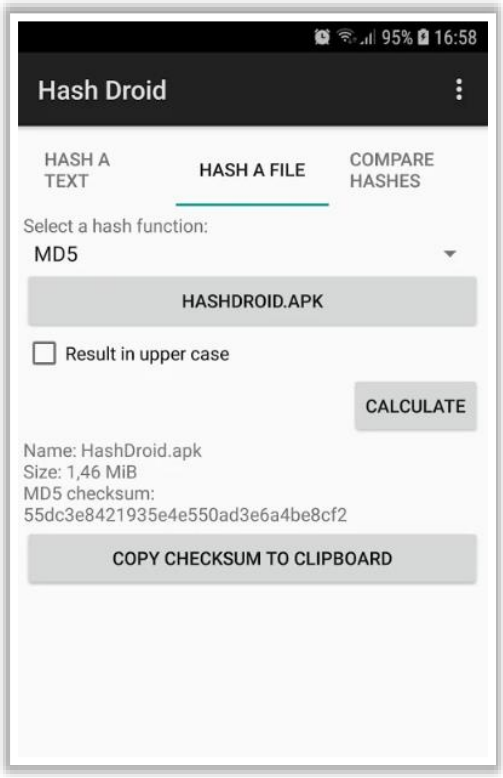
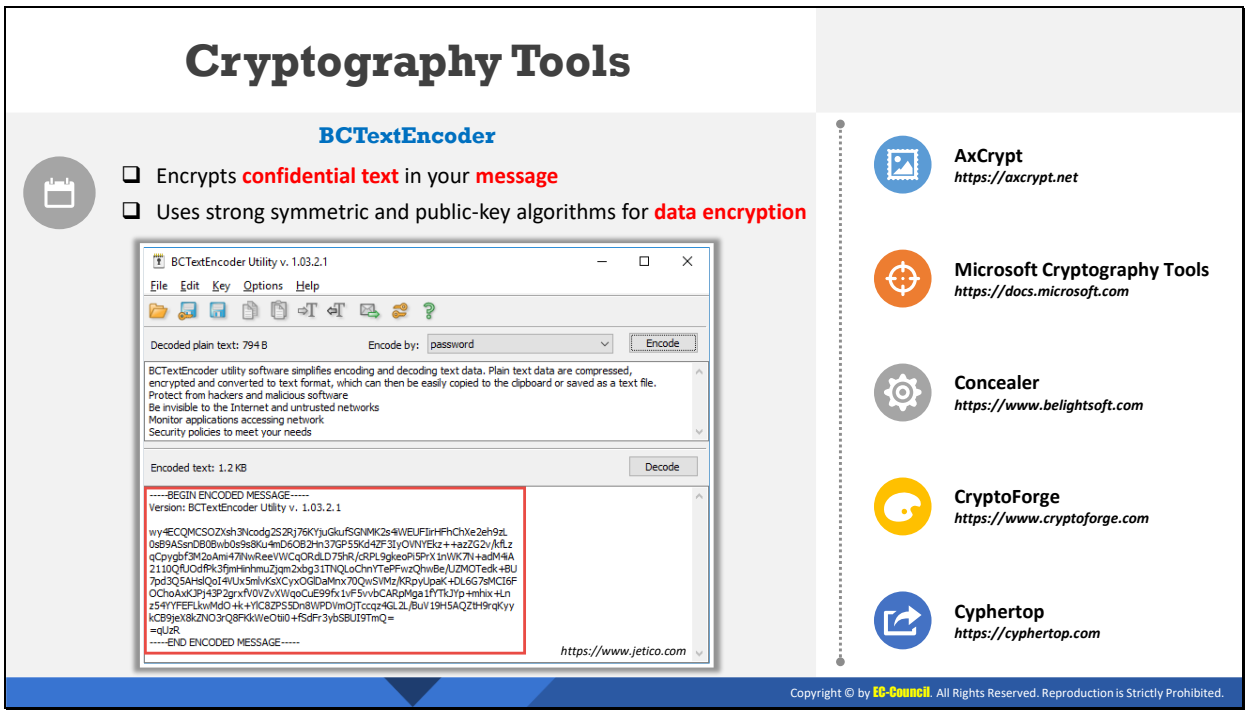


Figure 10.13: Screenshot of Hash Droid

Some additional MD5 hash calculators are as follows:

- Hash Checker (*https://play.google.com*)
- Hashr - Hash & Checksum Calculator (*https://play.google.com*)
- Hash Calc (*https://play.google.com*)
- Hash Generator - Checksum Calculator (*https://play.google.com*)
- Hash Smart Checker (*https://play.google.com*)

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Cryptography Tools

You can use various cryptographic tools for encrypting and decrypting your information, files, etc. These tools implement different types of encryption algorithms.

- **BCTextEncoder**

  Source: *https://www.jetico.com*

  The BCTextEncoder utility simplifies the encoding and decoding of text data. It compresses, encrypts, and converts plaintext data into text format, which the user can then copy to the clipboard or save as a text file. It uses public key encryption methods as well as password-based encryption. Furthermore, it uses strong and approved symmetric and public-key algorithms for data encryption.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

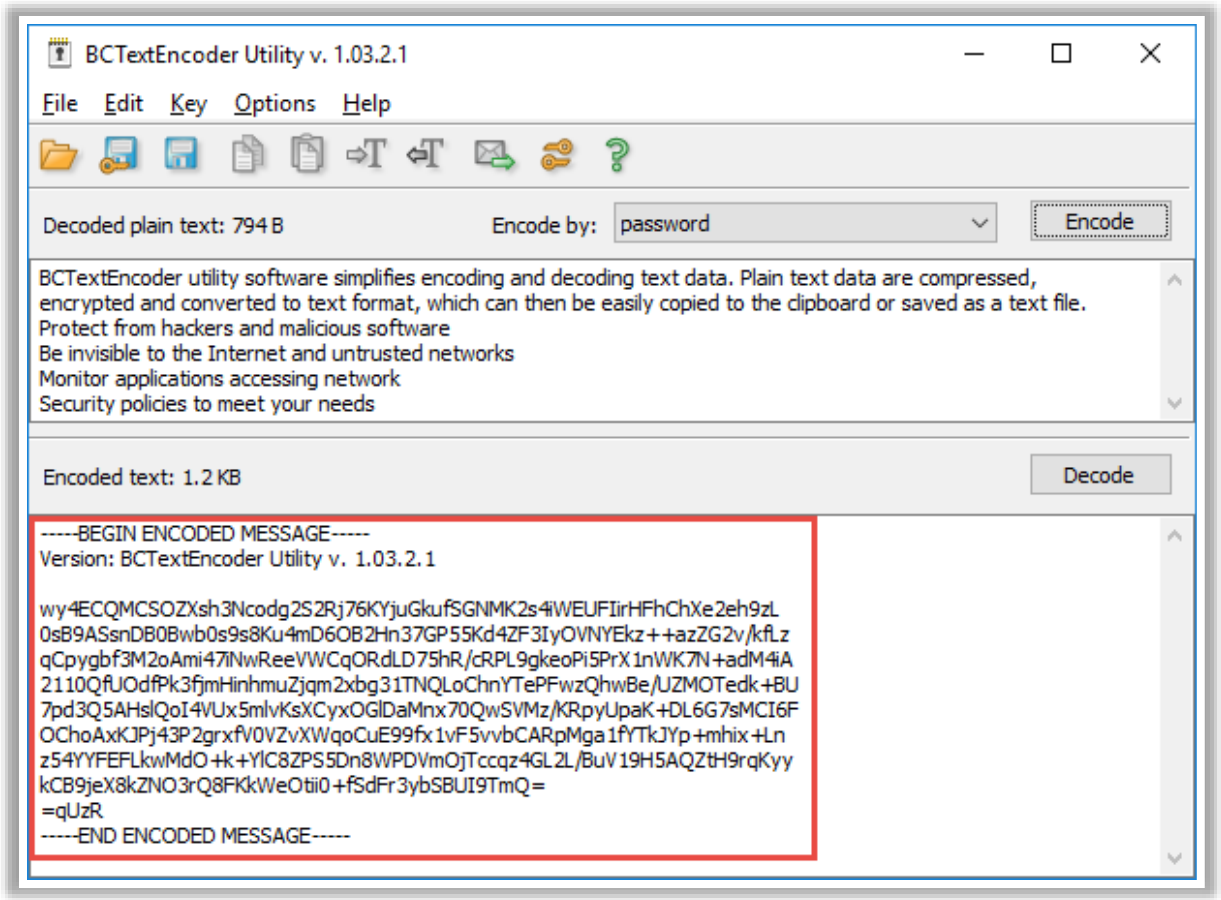
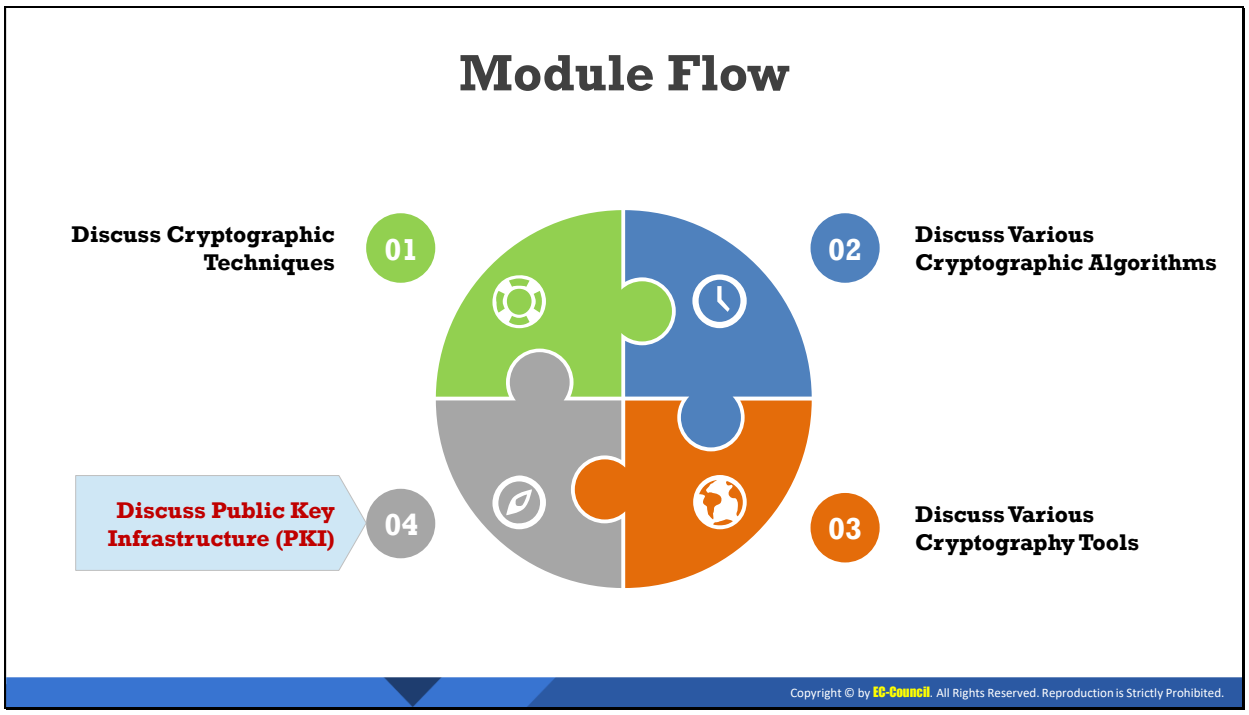


Figure 10.14: Screenshot of BCTextEncoder

Some additional cryptography tools are as follows:

- AxCrypt (*https://axcrypt.net*)
- Microsoft Cryptography Tools (*https://docs.microsoft.com*)
- Concealer (*https://www.belightsoft.com*)
- CryptoForge (*https://www.cryptoforge.com*)
- Cyphertop (*https://cyphertop.com*)

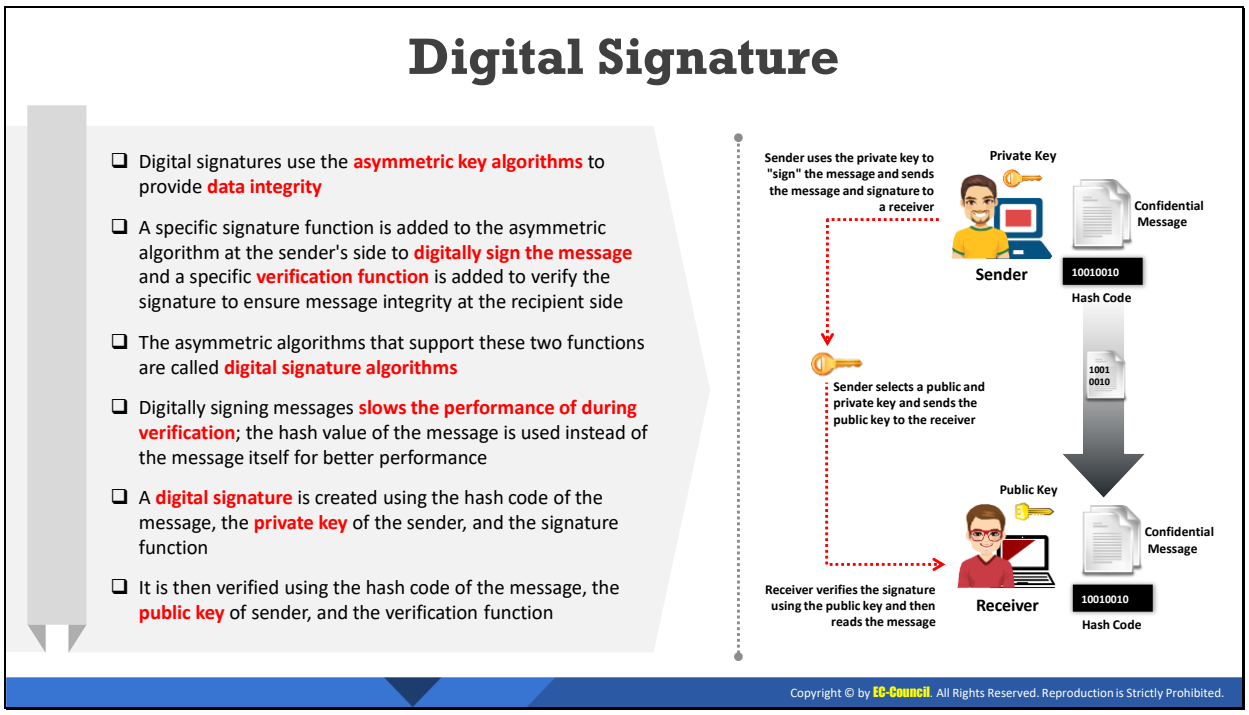
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

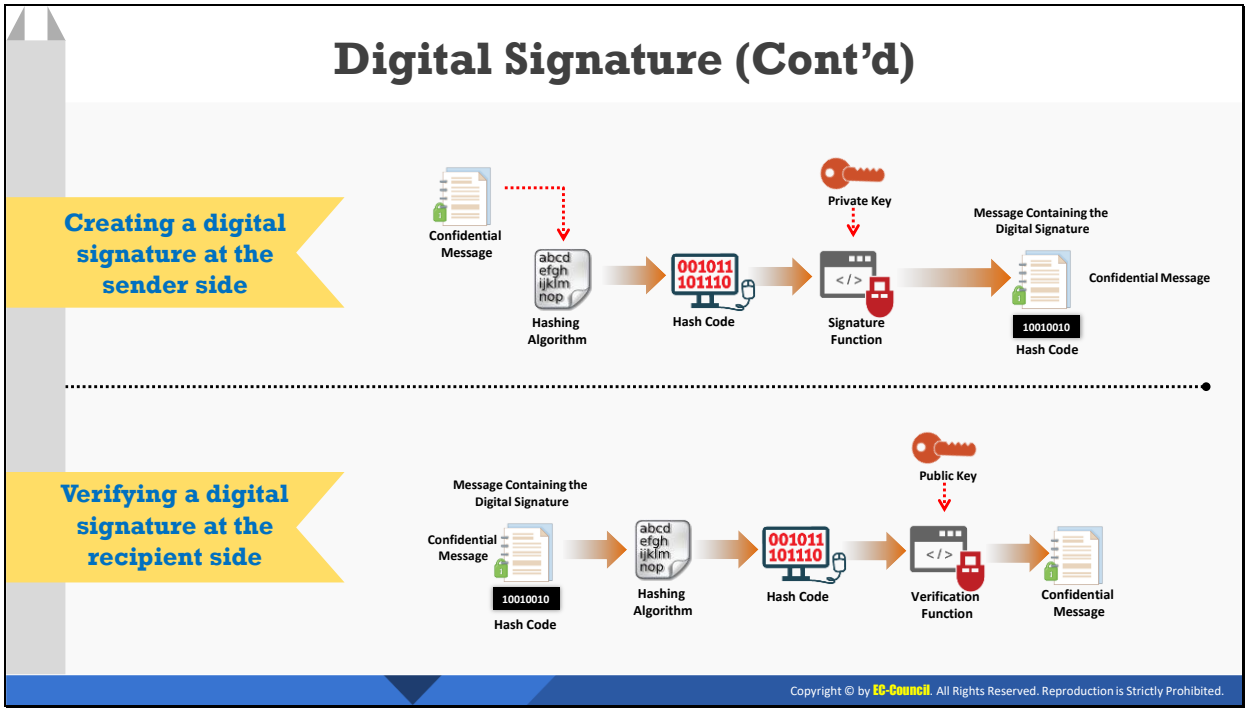


Discuss Public Key Infrastructure (PKI)

This section deals with public key infrastructure (PKI) and the role of each component of PKI, and certification authorities.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets





Digital Signature

A digital signature is a cryptographic means of authentication. Public-key cryptography uses asymmetric encryption and helps the user to create a digital signature.

A specific signature function is added to the asymmetric algorithm at the sender's side to digitally sign the message and a specific verification function is added to verify the signature to

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

ensure message integrity at the recipient side. The asymmetric algorithms that support these two functions are called digital signature algorithms.

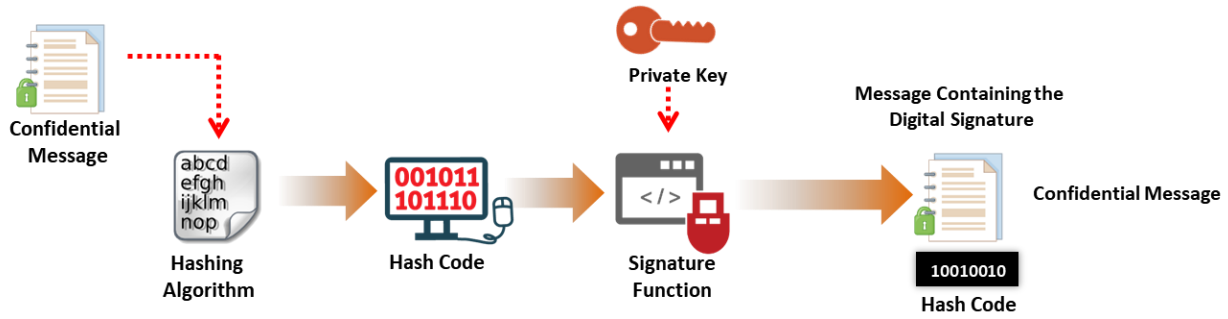


Figure 10.15: Creating a digital signature at the sender side

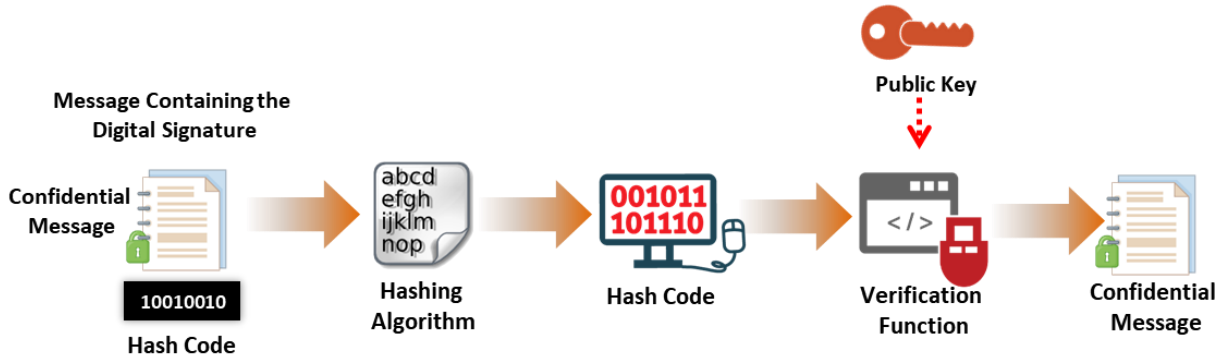


Figure 10.16: Verifying a digital signature at the recipient side

A hash function is an algorithm which helps users to create and verify digital signatures. This algorithm creates a digital representation, also known as a message fingerprint. This fingerprint has a hash value that is much smaller than the message, but one that is unique. If an attacker changes the message, the hash function will automatically produce a different hash value.

In order to verify a digital signature, one requires the hash value of the original message and the hash function used for creating the digital signature. With the help of the public key and the new result, the verifier checks whether the digital signature was created with the related private key and whether the new hash value is the same as the original or not. Digitally signing messages slows the performance of during verification; the hash value of the message is used instead of the message itself for better performance.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

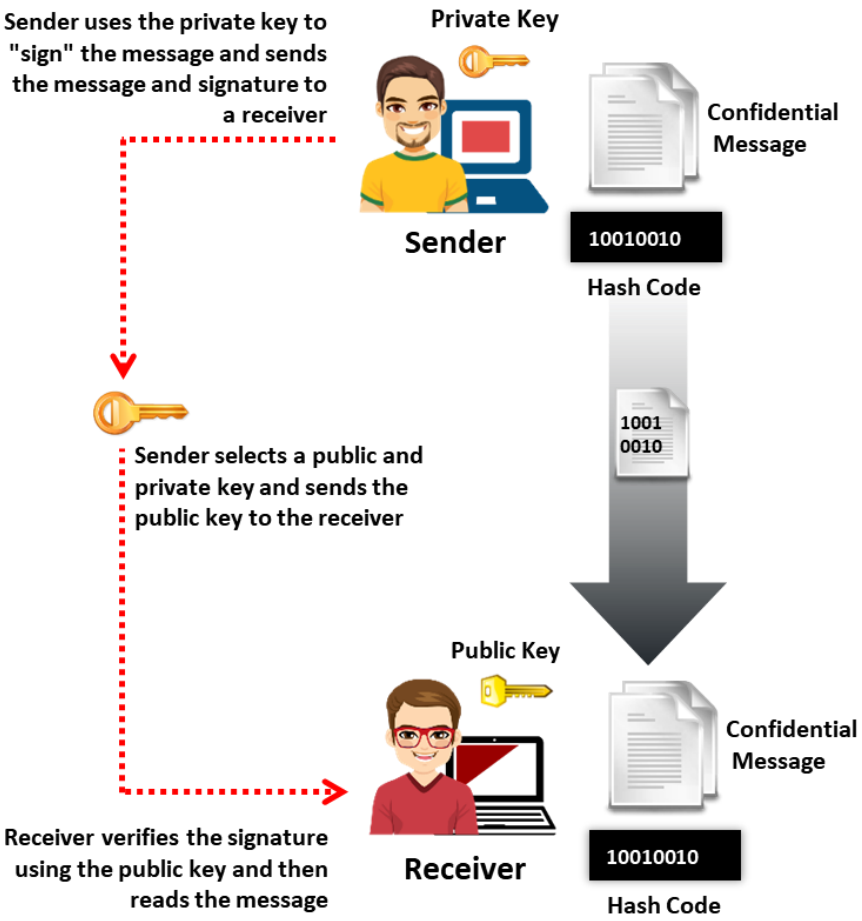
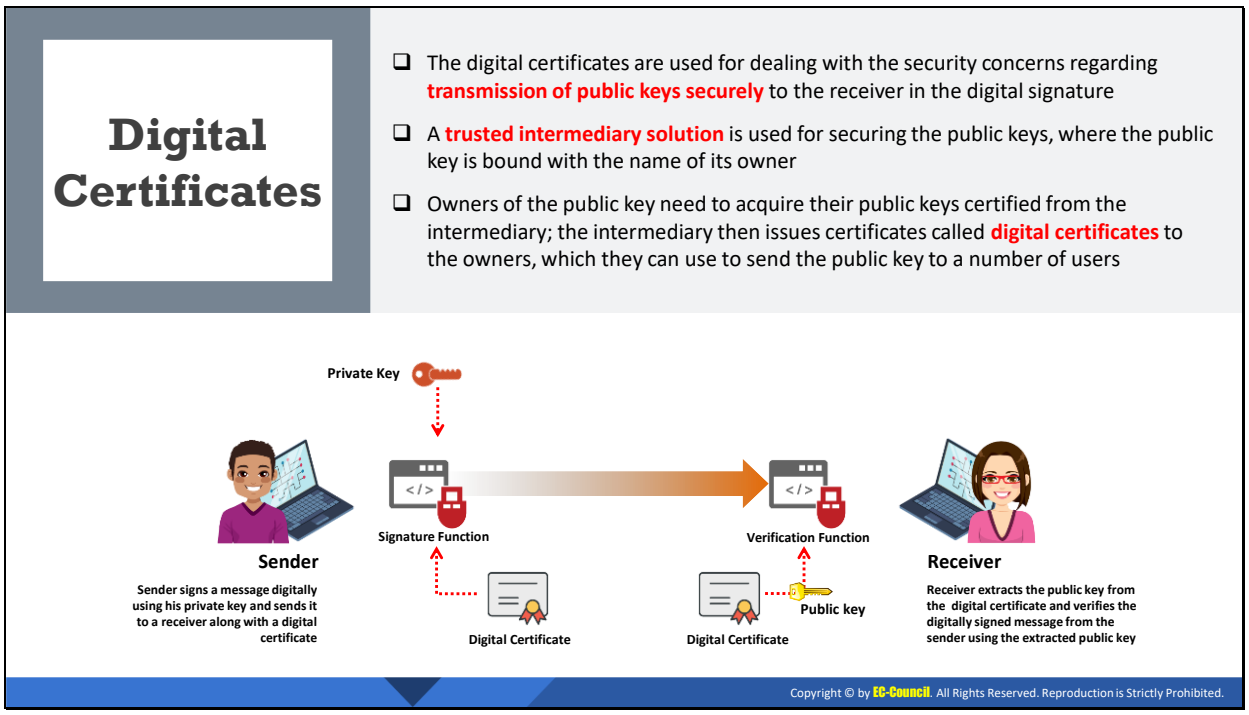
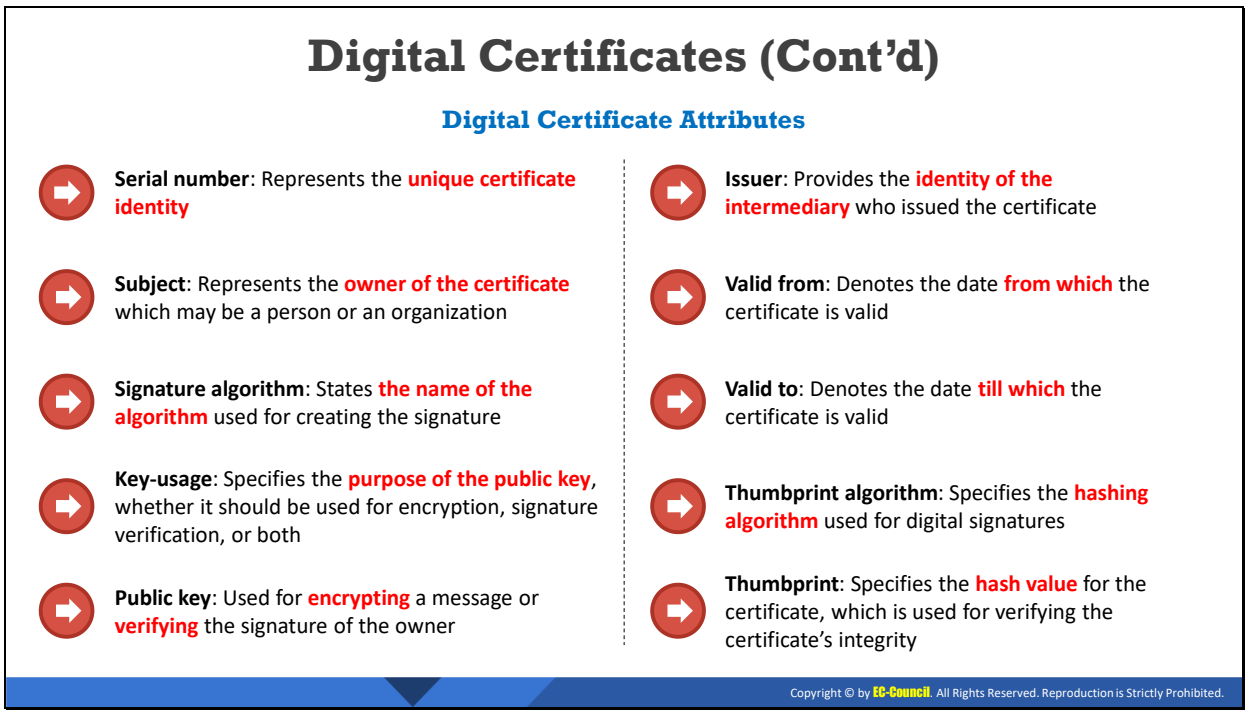


Figure 10.17: Working of Digital Signature

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets





Digital Certificates

Digital certificates allow a secure exchange of information between a sender and a receiver. This enables the use of a public key by the sender to the receiver. A trusted intermediary solution is used for securing the public keys, where the public key is bound with the name of its owner. Owners of the public key need to acquire their public keys certified from the intermediary; the intermediary then issues certificates called digital certificates to the owners, which they can use to send the public key to a number of users.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

The sender applies for a digital certificate from the certificate authority (CA). Along with the encrypted message and the public key, the CA provides other identity validating information. The receiver accepts the encrypted message and uses the CA's public key to decode the digital certificate. This allows the receiver to identify the digital signature and obtain the sender's public key and other identification details.

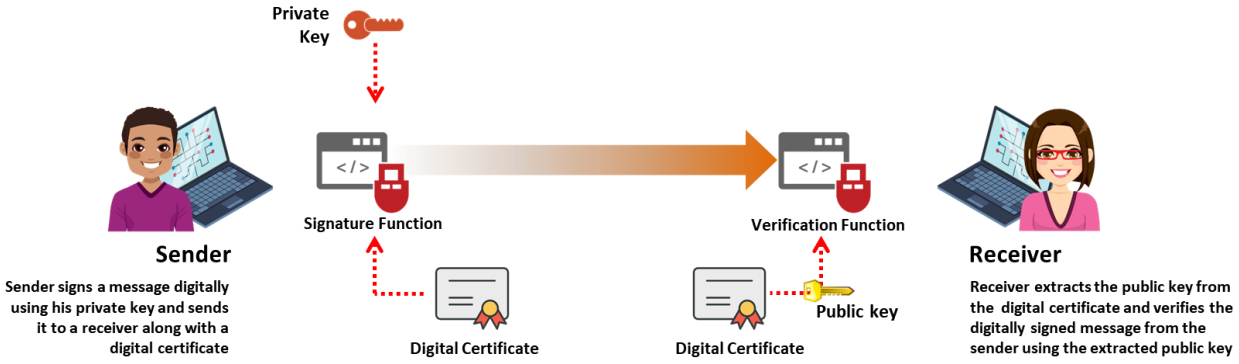


Figure 10.18: Working of digital certificates

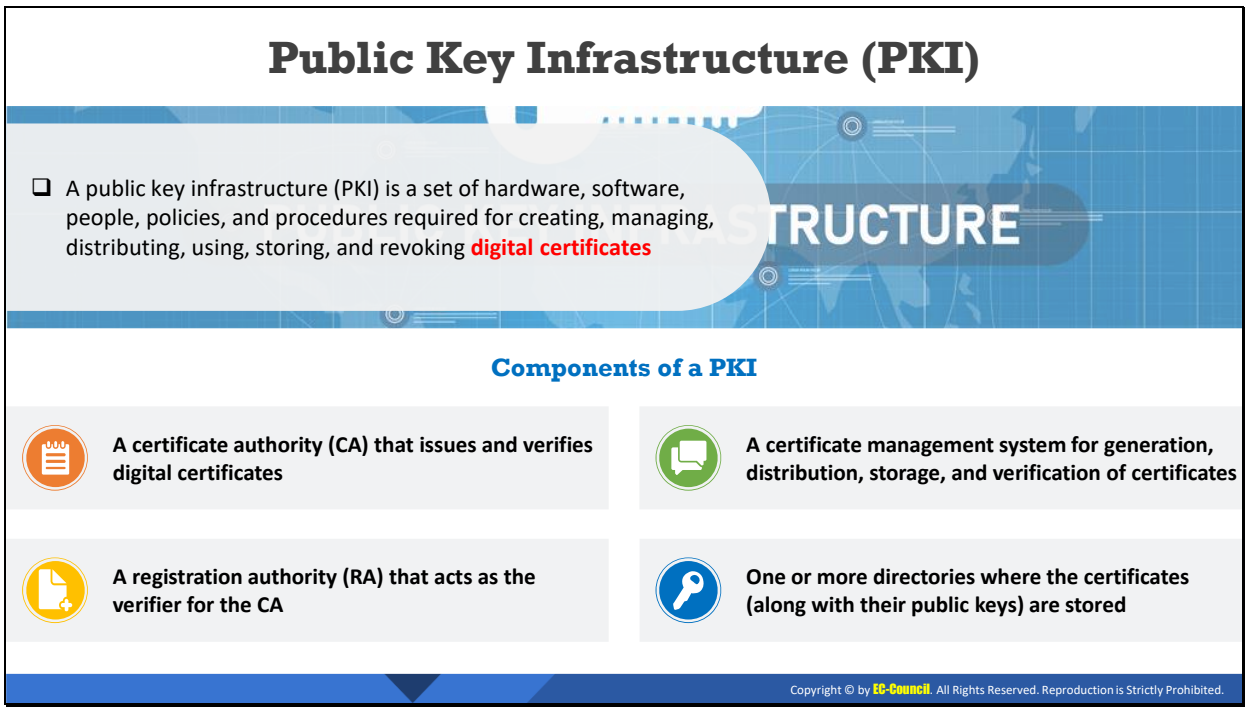
A digital certificate can hold information such as the name of the sender who applied for the certificate, expiration date, and a copy of the sender's public key digital signature of the CA. The receivers who receive the digital certificate can check the validity of the certificate using the signature attached from the approved authorities using the private key of the authority. Each OS and web browser carries authorized certificates from the CA which enables easy validation. The main aim of implementing a digital certificate is to ensure nonrepudiation.

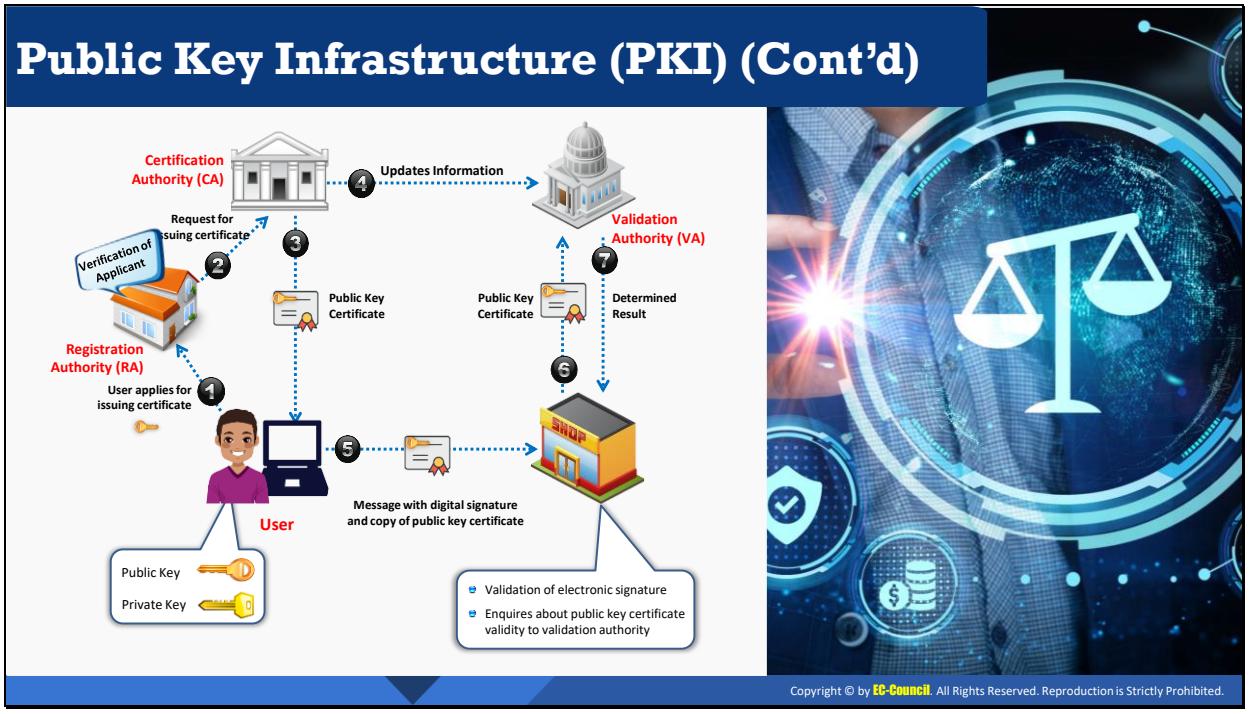
Most of the secure sockets layer (SSL)/ transport layer security (TLS) protocols use certificates in order to prevent attackers from changing or modifying the data. Digital certificates are used in email servers and code signing.

Digital Certificate Attributes

- **Serial number**: Represents the unique certificate identity.
- **Subject**: Represents the owner of the certificate which may be a person or an organization.
- **Signature algorithm**: States the name of the algorithm used for creating the signature.
- **Key-usage**: Specifies the purpose of the public key, whether it should be used for encryption, signature verification, or both.
- **Public key**: Used for encrypting a message or verifying the signature of the owner.
- **Issuer**: Provides the identity of the intermediary who issued the certificate.
- **Valid from**: Denotes the date from which the certificate is valid.
- **Valid to**: Denotes the date till which the certificate is valid.
- **Thumbprint algorithm**: Specifies the hashing algorithm used for digital signatures.
- **Thumbprint**: Specifies the hash value for the certificate, which is used for verifying the certificate's integrity.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets





Public Key Infrastructure (PKI)

A public key infrastructure (PKI) is a security architecture developed for increasing the confidentiality of the information exchanged over the Internet. It includes hardware, software, people, policies, and procedures required for creating, managing, distributing, using, storing, and revoking digital certificates. In cryptography, a PKI helps to bind the public keys with the corresponding user identities by means of a CA.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

PKI is a comprehensive system that allows the use of public-key encryption and digital signature services across a wide variety of applications. PKI authentication depends on digital certificates (also known as public-key certificates) that CAs sign and provide. A digital certificate is a digitally signed statement with a public key and the subject's (i.e., a user, company, or system) name on it.

The components of a PKI include,

- A certificate authority (CA) that issues and verifies digital certificates
- A registration authority (RA) that acts as the verifier for the CA.
- A certificate management system for generation, distribution, storage, and verification of certificates.
- One or more directories where the certificates (along with their public keys) are stored.

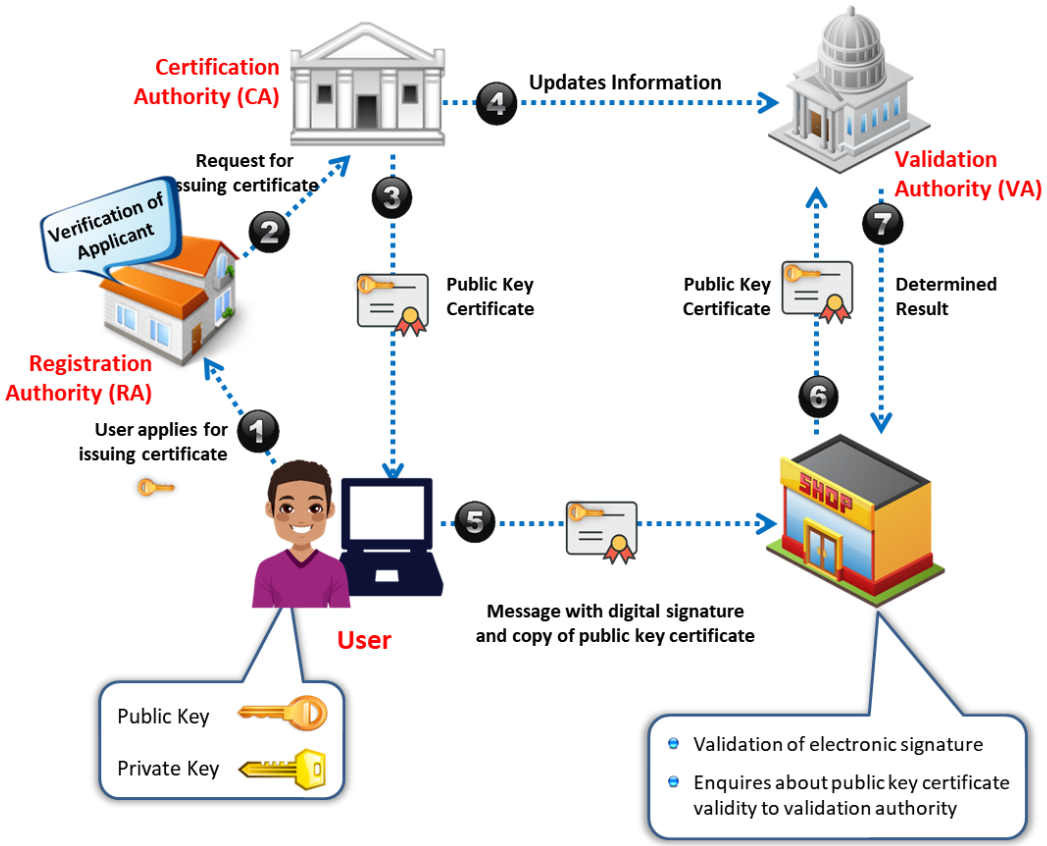


Figure 10.19: PKI Components

PKI is widely recognized as a best practice for ensuring digital verification for electronic transactions. These are the most effective methods for providing verification during electronic transactions. The digital signatures supported by PKI include the following:

- With whom you are dealing (identification)
- Who is authorized to access what information (entitlements)
- A verifiable record of the transaction (verification)

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Uses of PKI

PKI does not serve only as a business function; it provides the foundation for other security services. The primary use of PKI is to allow the distribution and use of public keys and certificates with security. The security mechanisms that are based on PKI include email, chip card application, value exchange with e-commerce, home banking, and electronic postal systems. PKI enables basic security services for a variety of systems as listed below:

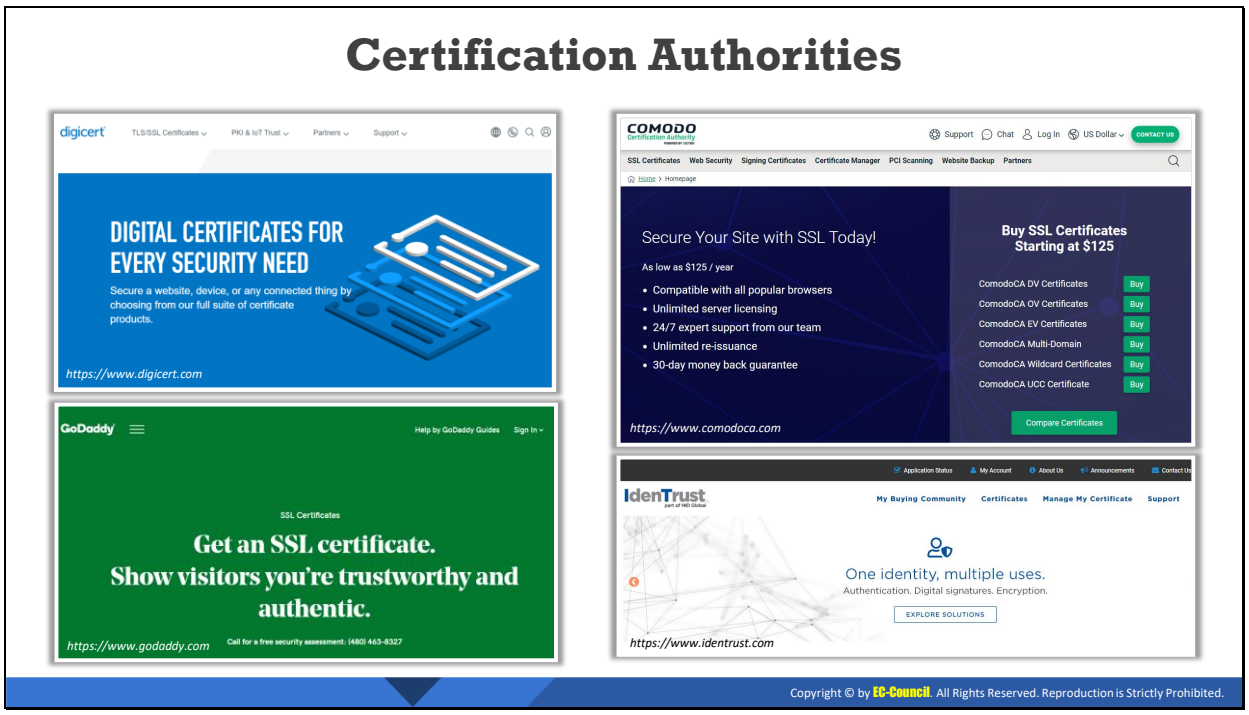
- It uses the SSL, internet protocol security (IPsec), and the hypertext transfer protocol secure (HTTPS) protocols for communication security.
- It uses the secure/multipurpose internet mail extensions (S/MIME) and pretty good privacy (PGP) protocols for email security.
- It uses the secure electronic transaction (SET) protocol for value exchange.

The following are the key benefits of PKI:

- It reduces the transactional processing expenses.
- It reduces risk.
- It improves the efficiency and performance of systems and networks.
- It reduces the difficulty of security systems with binary symmetrical methods.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Certification Authorities

Certification authorities (CAs) are trusted entities that issue digital certificates. The digital certificate certifies the possession of the public key by the subject (user, company, or system) specified in the certificate. This aids others to trust signatures or statements made by the private key that is associated with the certified public key.

Some popular CAs are discussed below:

- **Comodo**

  Source: *https://www.comodoca.com*

  Comodo offers a range of PKI digital certificates with strong SSL encryption (128/256 available) with Server-Gated Cryptography (SGC). It ensures standards of confidentiality, system reliability, and pertinent business practices as judged via qualified independent audits. It offers PKI management solutions such as Comodo Certificate Manager and Comodo EPKI Manager.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

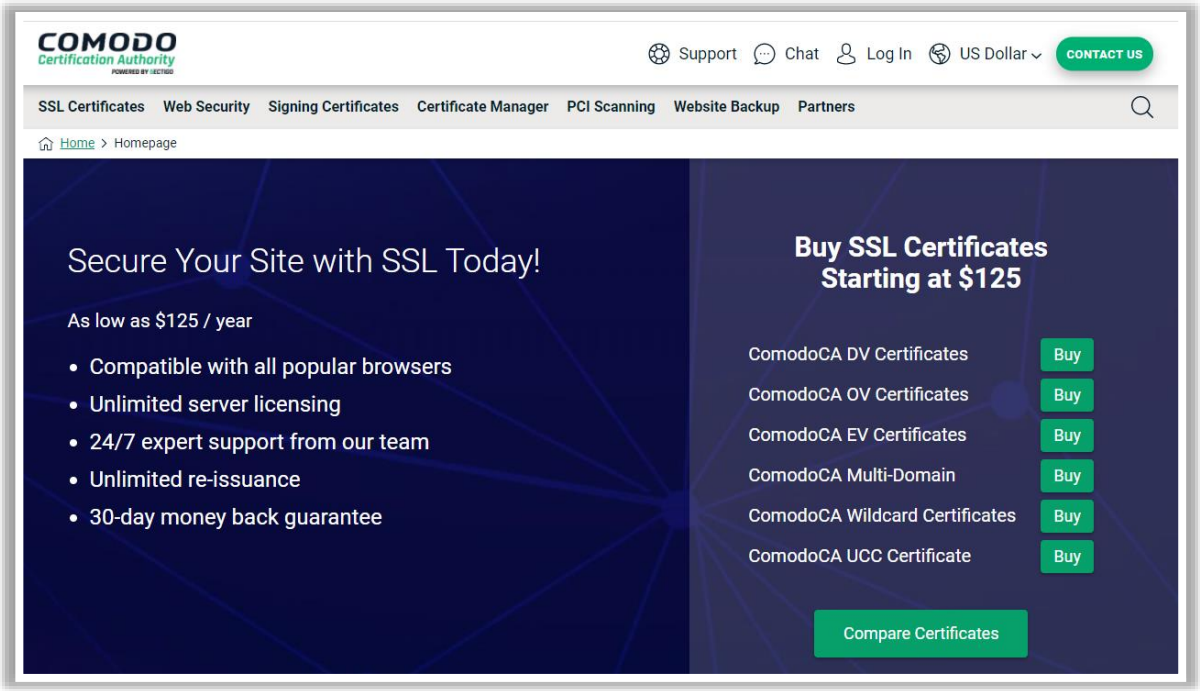


Figure 10.20: Screenshot of Comodo Website

- **IdenTrust**

  Source: *https://www.identrust.com*

  IdenTrust is a trusted third party that provides CA services for many sectors such as banks, corporates, governments, and healthcare. It provides solutions such as digital signing and sealing, compliance with NIST SP 800-171, global identity networks, and managed PKI hosting services.

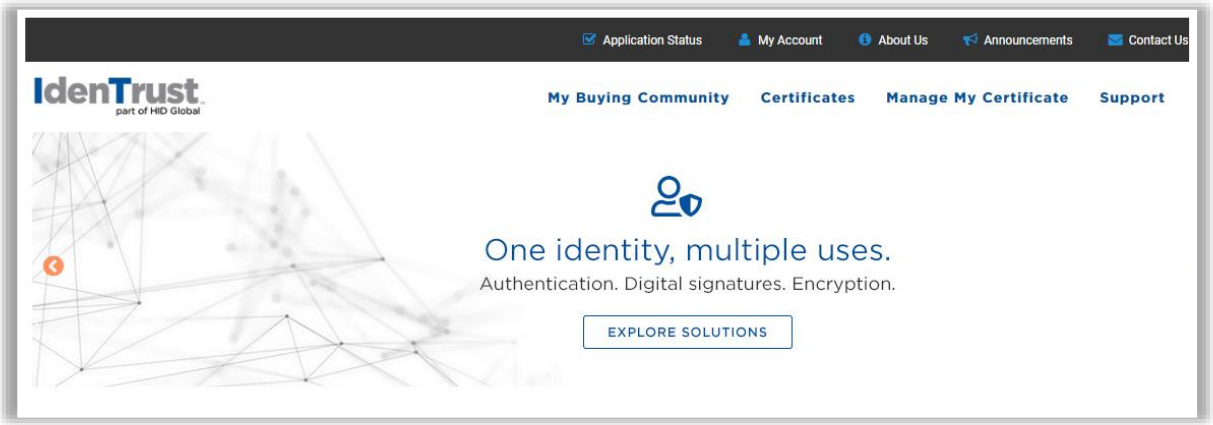


Figure 10.21: Screenshot of IdenTrust Website

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **DigiCert CertCentral**

  Source: *https://www.digicert.com*

  CertCentral simplifies the entire lifecycle by consolidating tasks for issuing, installing, inspecting, remediating, and renewing TLS/SSL certificates. It manages high-volume TLS/SSL certificate issuance for multiple individuals and teams.

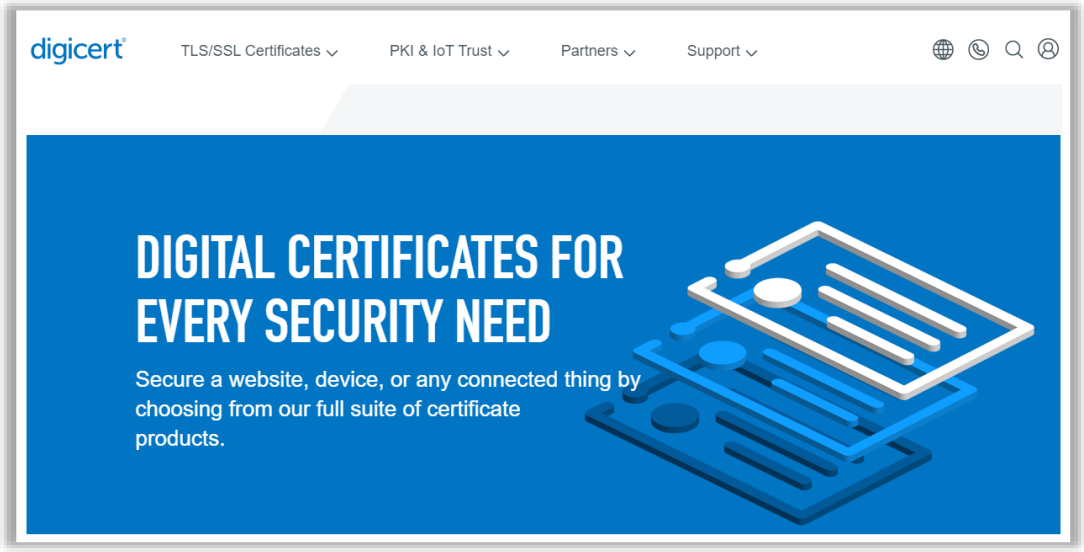


Figure 10.22: Screenshot of DigiCert Website

- **GoDaddy**

  Source: *https://www.godaddy.com*

  GoDaddy SSL Certificates offer a complete range of certificates that comply with CA/Browser Forum guidelines. They provide the SHA-2 hash algorithm and 2048-bit encryption, protection of unlimited servers, etc.

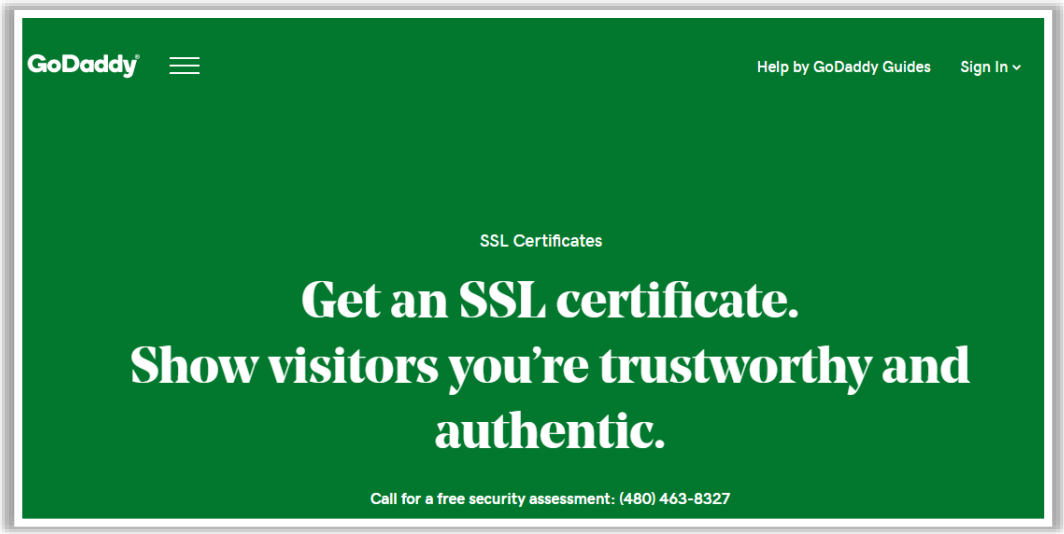
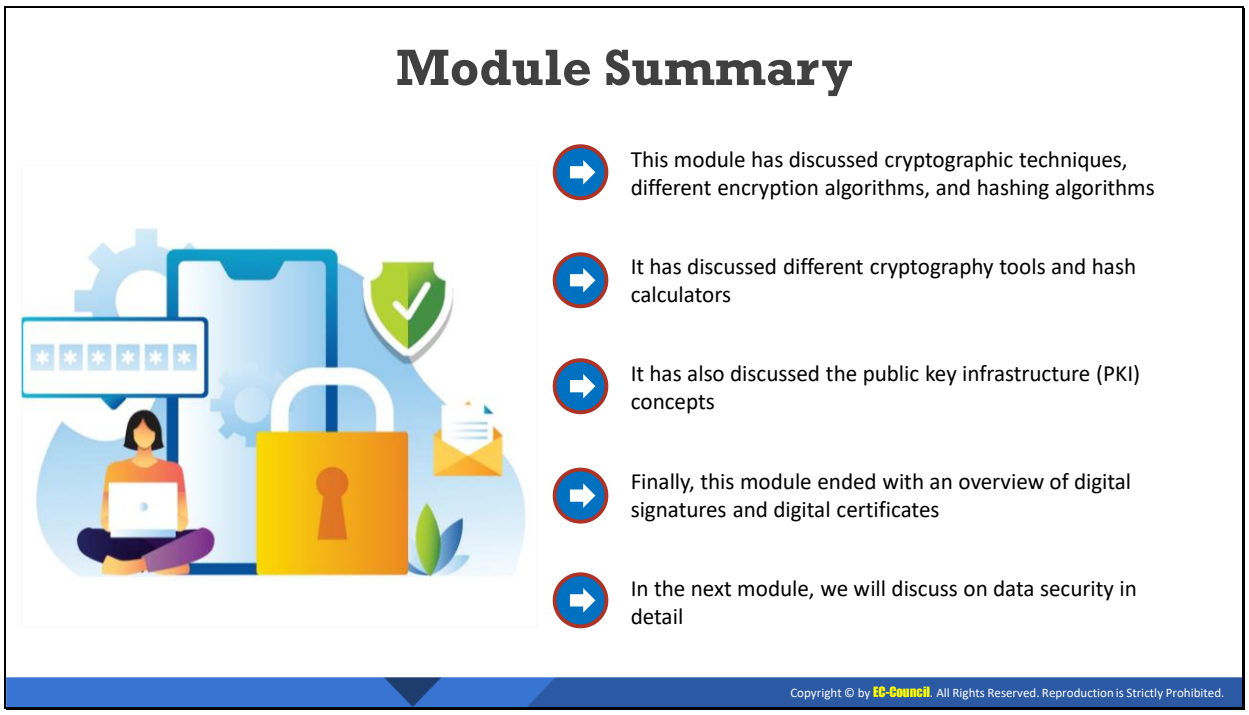


Figure 10.23: Screenshot of GoDaddy Website

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Module Summary

This module discussed cryptographic techniques, different encryption algorithms, and hashing algorithms. It discussed different cryptography tools and hash calculators. Furthermore, it explained concepts related to public key infrastructure (PKI). Finally, this module presented an overview of digital signatures and digital certificates.

In the next module, we will discuss data security in detail.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

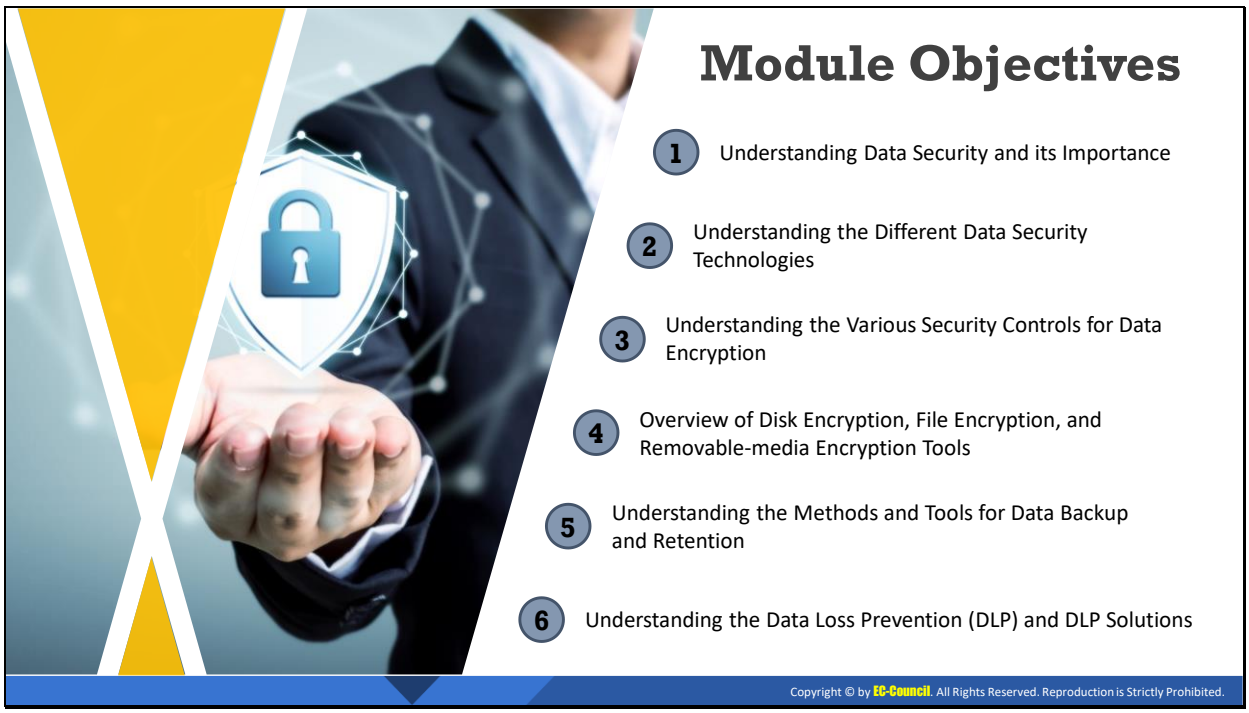
EC-Council

N|DE
Network Defense Essentials

Module 11

Data Security

https://t.me/learningnets



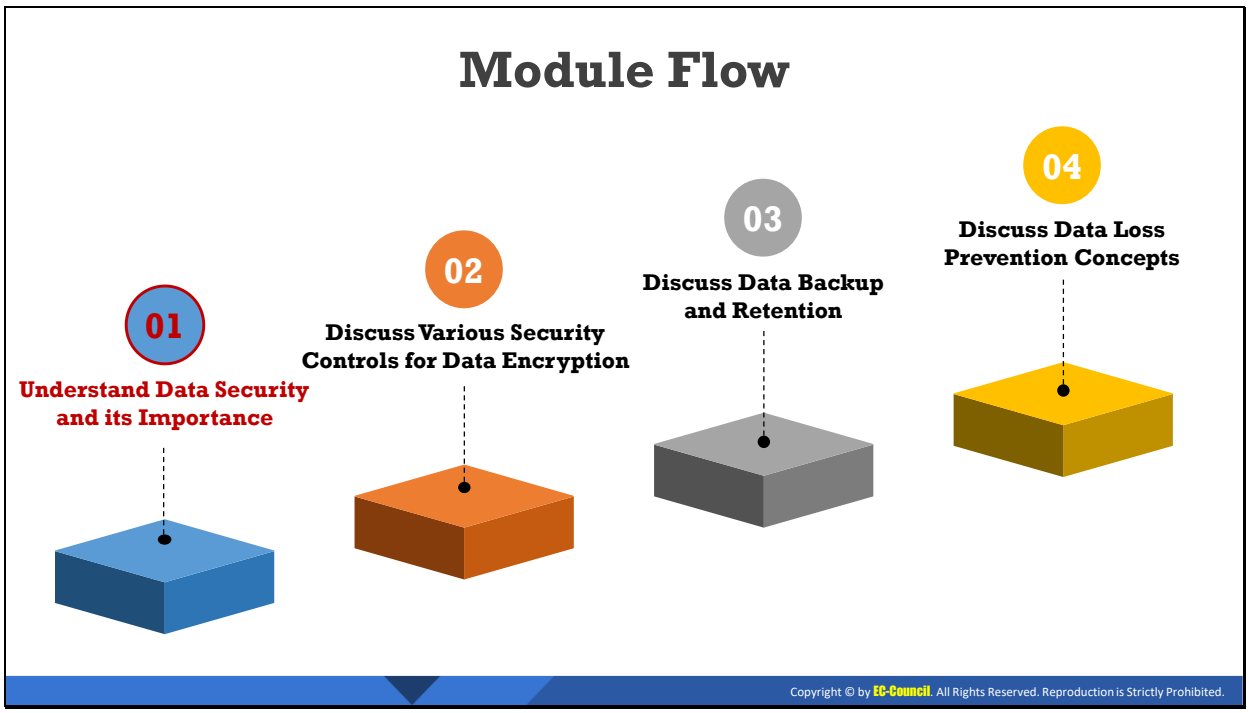
Module Objectives

Data breaches can be costly for organizations. Therefore, it is important to keep organization data safe from prying eyes. This module explains the importance of data, and various techniques to protect data.

At the end of this module, you will be able to do the following:

- Understand data security and its importance
- Understand the different data security technologies
- Explain the various security controls for data encryption
- Use different disk encryption, file encryption, and removable-media encryption tools
- Explain methods and tools for data backup and retention
- Understand data loss prevention (DLP) and DLP solutions

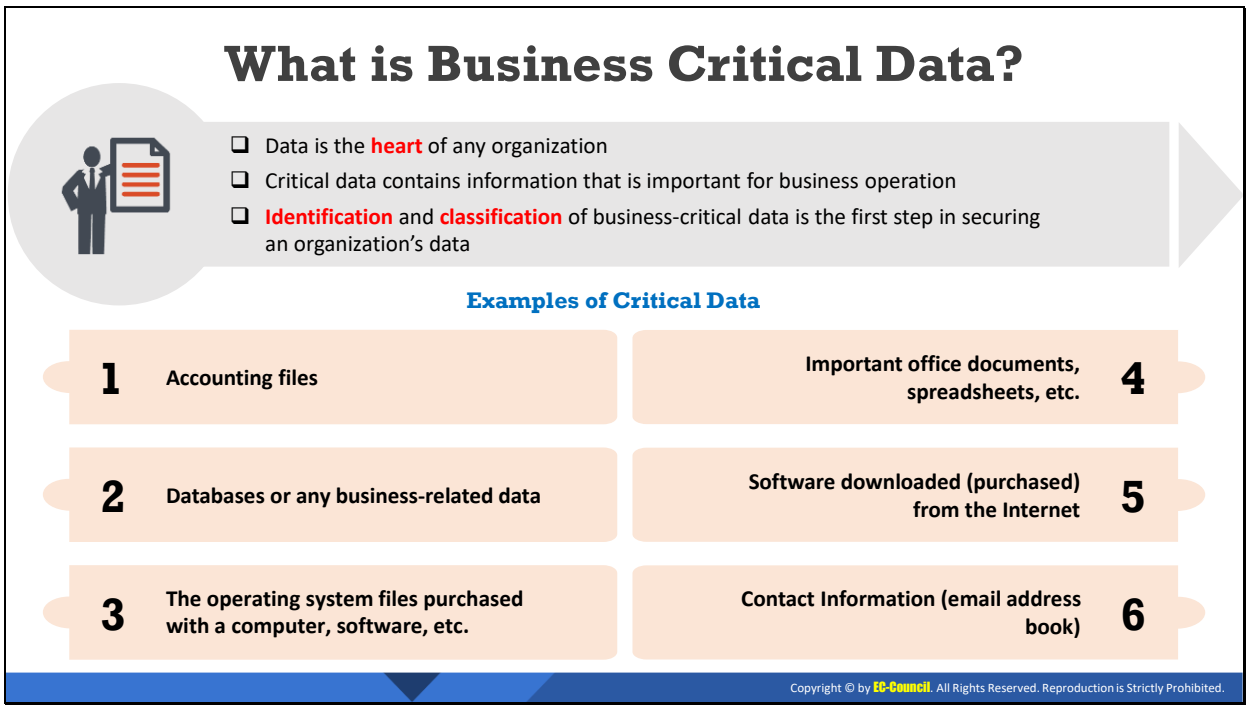
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Understand Data Security and its Importance

The objective of this section is to explain the importance of data security. The module also explains the three states of data, i.e., data at rest, data in use, and data in transit, and introduces various data security technologies.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



What is Business Critical Data?

Data is the heart of any organization. Critical data contains information that is important for business operation. Identification and classification of business-critical data is the first step in securing an organization's data. Every organization has an abundance of data. An organization should identify their critical data or files. The criticality of data is based on its importance to the organization. This requires analyzing and deciding which information is more important for the organization to function properly. Critical data may consist of revenue, emerging trends, market plans, database, files including documents, spreadsheet, emails, etc. Loss of such critical data can significantly affect the organization.

How Can Critical Data Be Identified?

- Conduct a business impact analysis to determine the critical functions and data in an organization. Identify processes and functions that depend on and co-exist with the critical data.
- Evaluate the impact of data damage on the business.

Examples of Critical Data:

- Accounting files
- Databases or any business-related data
- The operating system files purchased with a computer, software, etc.
- Important office documents, spreadsheets, etc.
- Software downloaded (purchased) from the Internet
- Contact Information (email address book)
- Personal photos, music, and videos
- Any other critical file(s)

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Need for Data Security

Data is an important asset for an organization, and it is essential to safeguard it from cybercriminals. If an organization's data is exposed or lost by any means, it can damage the organization's business and reputation to a great extent.

Effect of data loss:

- Brand damage and reputation loss
- Competitive advantage loss
- Loss of customers
- Market share loss
- Shareholder value erosion
- Fines and civil penalties
- Litigation/legal actions
- Regulatory fines/sanctions
- Significant cost and effort to notify affected parties and recover from breach

There are numerous causes for data loss, including

- Loss/theft of laptops and mobile devices
- Unauthorized data transfer to USB devices
- Improper sensitive data categorization

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- Data theft by employees/external parties
- Printing and copying of sensitive data by employees
- Insufficient response to intrusions
- Unintentional sensitive data transmission

The resulting data loss leads to loss of brand loyalty and trust, decreases the number of customers, and affects market share and shareholder value, regulatory fines, legal proceedings, etc. Data breaches and cyberattacks have increased because of the expansion of computer networks; hence, data security is necessary to protect the data in an organization.

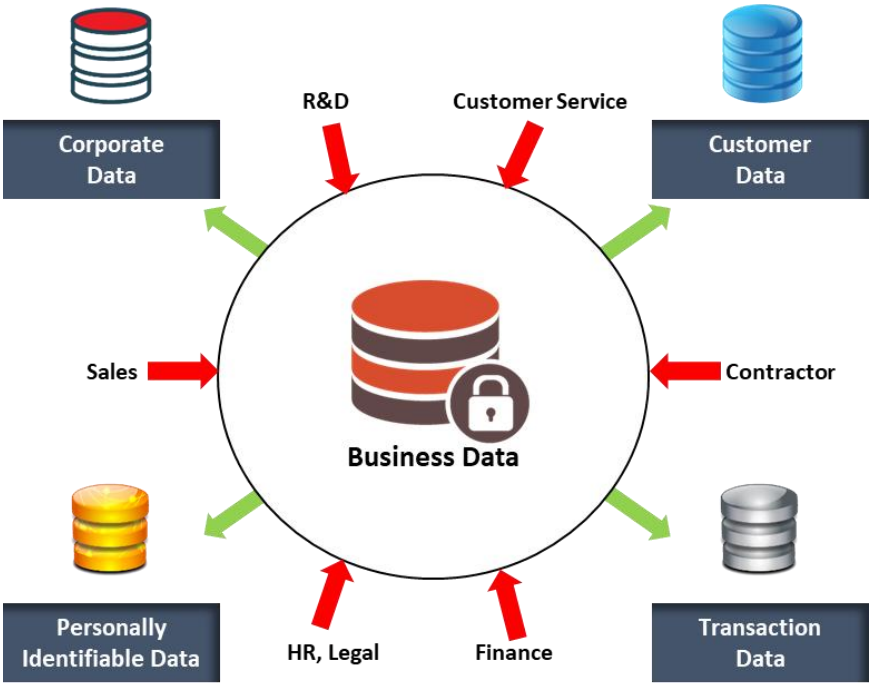
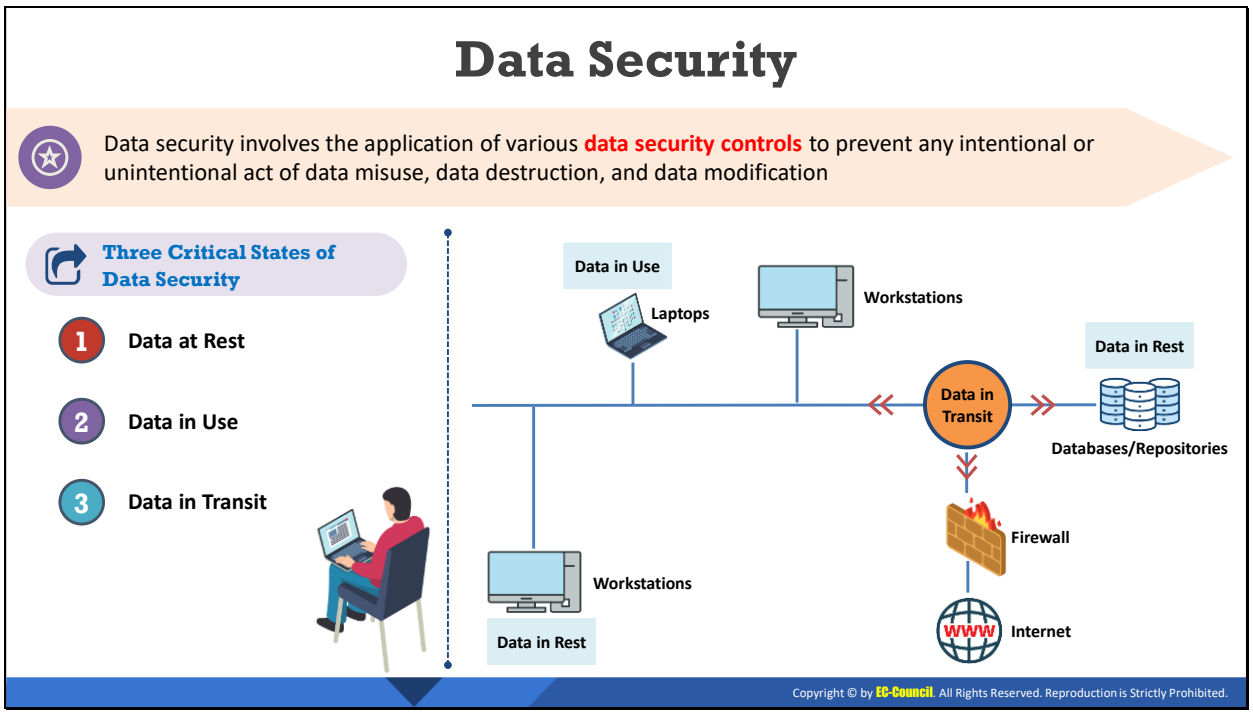


Figure 11.1: Business environment

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Data Security

Data security involves the application of various data security controls to prevent any intentional or unintentional act of data misuse, data destruction, and data modification.

An organization's data is considered to be secured when they have sufficient provisions for:

- Restricting data from intentional or accidental destruction, modification, or disclosure
- Recovering lost or modified data following incidents
- appropriate data retention and destruction policies

Three Basic States of Data

- **Data at rest:** This data is inactive and is stored on a device or a backup medium such as hard drives, laptops, backup tapes, mobile devices, or at the offsite cloud backup. Data at rest remains in a stable state. The data at rest will not move actively in a system or network and cannot be accessed by an application or program.
- **Data in use:** This data is stored or processed by RAM, CPUs, or databases. It is not passively stored on the system, but actively moves across IT infrastructure. It is updated, erased, processed, accessed, and/or read by the system.
- **Data in transit:** This data actively moves from one location to another across the network, or is encrypted before moving and/or being transmitted through encrypted connections such as HTTPS, SSL, transport layer security (TLS), FTPS, etc.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

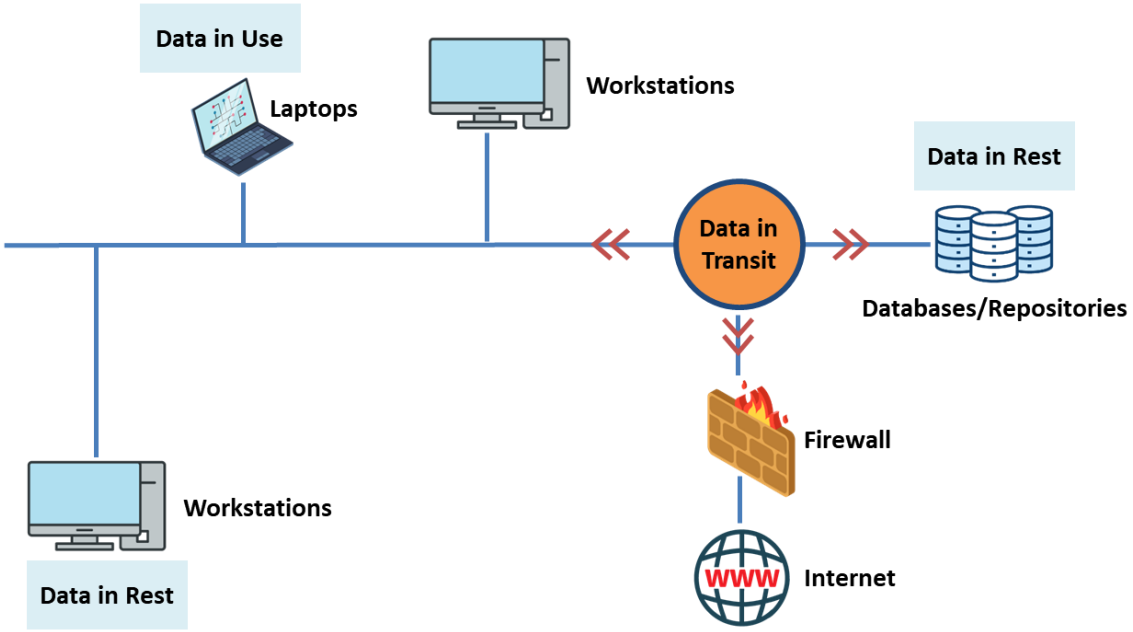
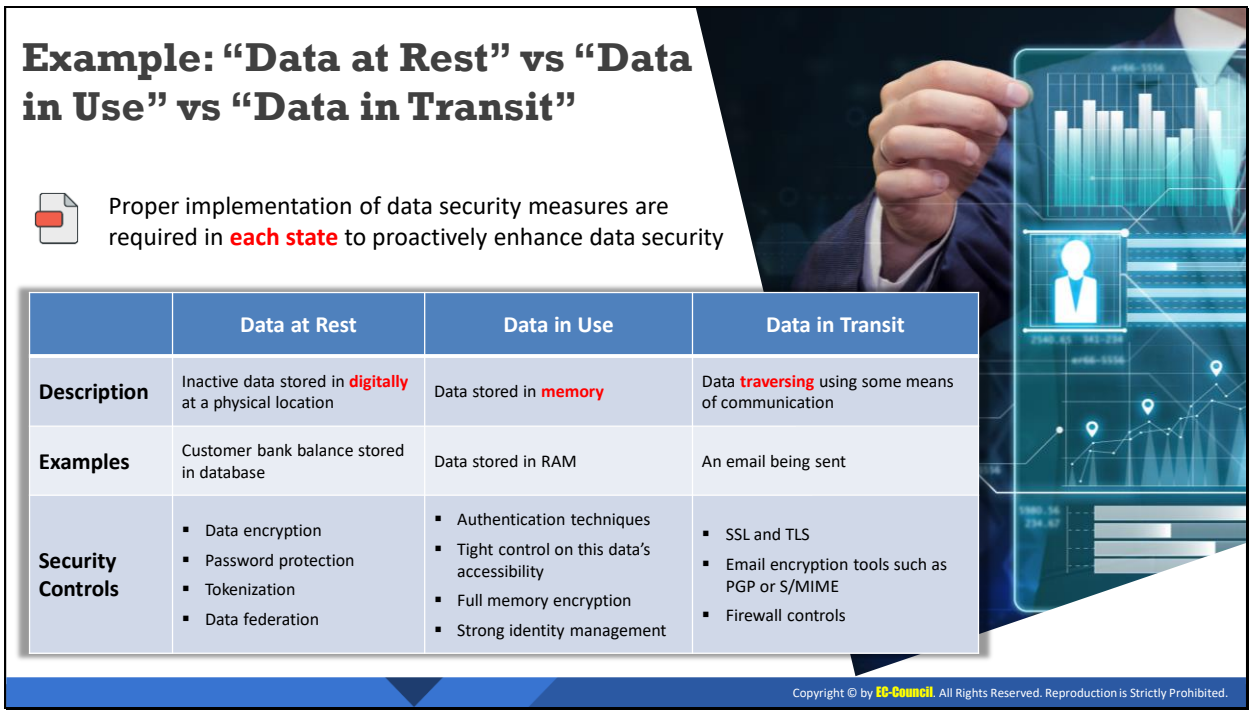


Figure 11.2: Three Basic States of Data

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



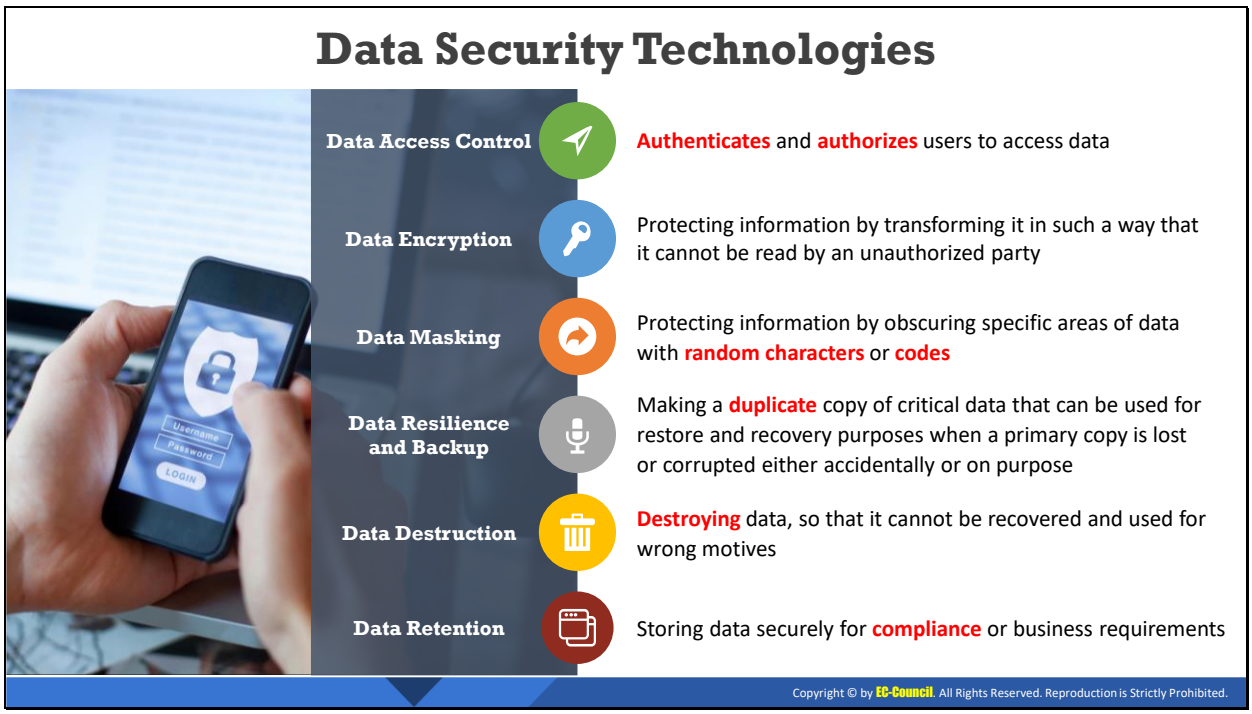
Example: "Data at Rest" vs "Data in Use" vs "Data in Transit"

A proper implementation of security measures is required in each state to proactively enhance data security. The following table describes the various states of data, their specific examples, and security controls to protect against attacks.

	Data at Rest	Data in Use	Data in Transit
Description	Inactive data stored in digitally at a physical location	Data stored in memory	Data traversing using some means of communication
Examples	Customer bank balance stored in database	Data stored in RAM	An email being sent
Security Controls	▪ Data encryption ▪ Password protection ▪ Tokenization ▪ Data federation	▪ Authentication techniques ▪ Tight control on this data's accessibility ▪ Full memory encryption ▪ Strong identity management	▪ SSL and TLS ▪ Email encryption tools such as PGP or S/MIME ▪ Firewall controls

Table 11.1: Data at rest vs Data in use vs Data in transit

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Data Security Technologies

- **Data Access Control**

  Data access controls enable authentication and authorization of users to access the data. It is an important component of security compliance programs that protect unauthorized access to confidential information.

- **Data Encryption**

  Protecting information by transforming it so that it becomes unreadable for an unauthorized party. It safeguards corporate secrets, classified information, and personal information. The encrypted data cannot be read by any unauthorized persons or entities.

- **Data Masking**

  Protecting information by obscuring specific areas of data with random characters or codes. Data masking protects sensitive data such as personally identifiable information, protected health information, payment card information, intellectual property, etc. Apart from this, data masking also protects against an insider threat. Implementing data masking will bolster the security strategies of an organization.

- **Data Resilience and Backup**

  Making a duplicate copy of critical data to be used for restoring and recovery purposes when the primary copy is lost or corrupted, either accidentally or on purpose. Data resilience allows the data to remain available to the applications if there is any failure in the hosted data. Retaining multiple copies of a data backup help in restoring the data with ease and mitigate the risks of data corruption or malicious attacks.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **Data Destruction**

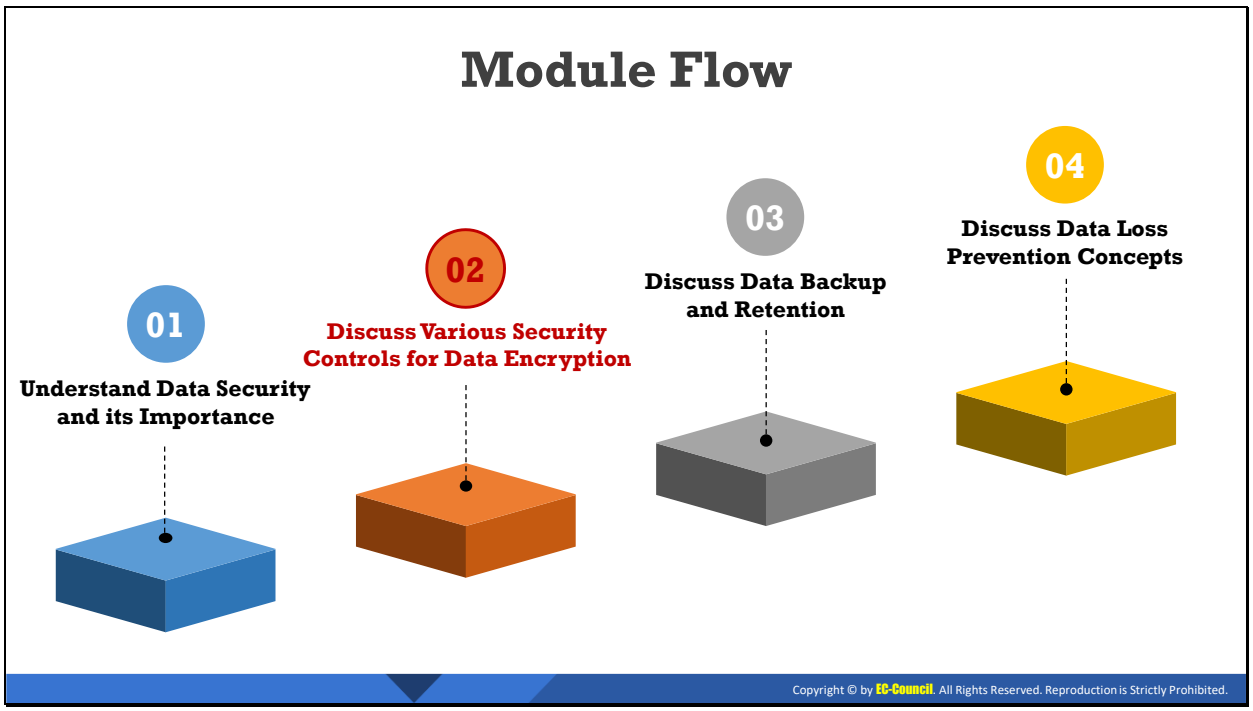
  It involves destroying the data so that it cannot be recovered and used for a wrong motive. The destruction of old hard drives or electronic devices should be done securely and safely. Data destruction helps in physically destroying the old information of customers and employees.

- **Data Retention**

  Storing data securely for compliance or business requirements. An organization should have policies and processes for retention and removal of data. Data retention programs have a tremendous impact on data security and can meet the expectations of customers and governments in safeguarding privacy.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Discuss Various Security Controls for Data Encryption

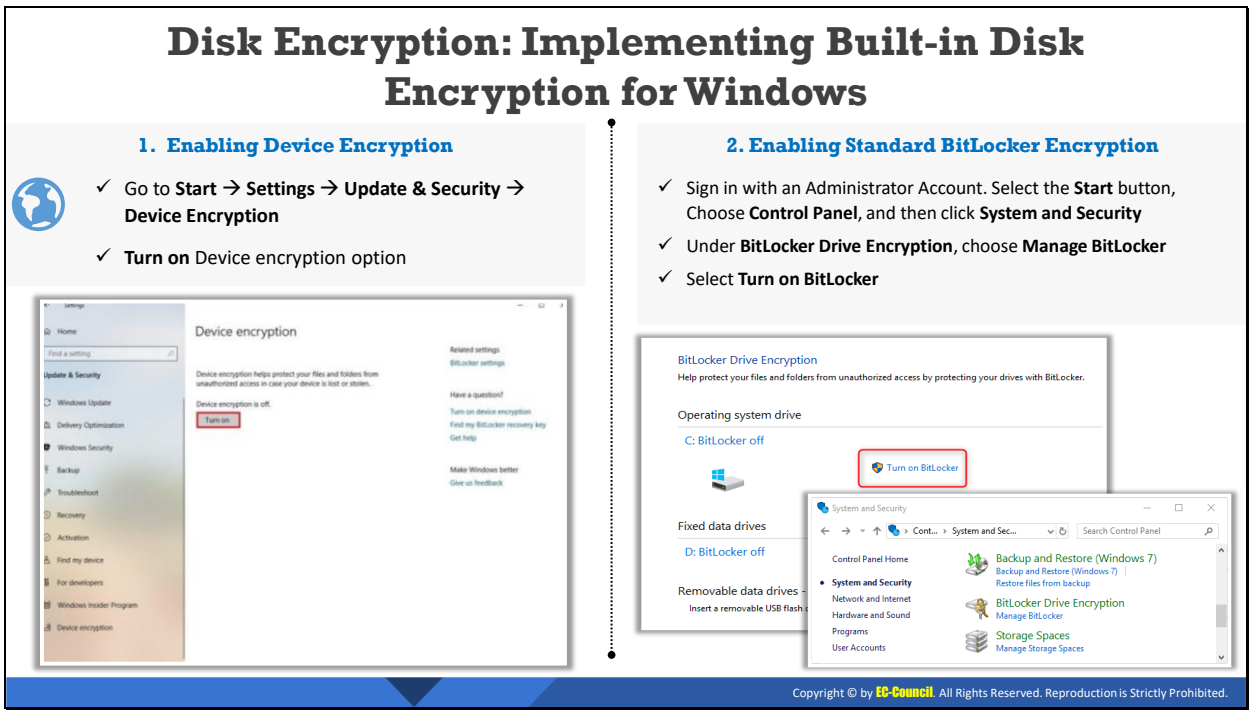
The objective of this section is to explain the use of encryption technology to secure the data.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Data Encryption Techniques

- **Disk encryption**: Encryption of data stored in a physical or logical disk. Full disk encryption is the encryption of all data in a disk except the master boot record (MBR). The data is automatically converted into a form which cannot be easily deciphered by an unauthorized user. In full disk encryption, the data is encrypted while being written on the disk, and decrypted when the user reads the data from the disk. The benefits of full disk encryption are
  - It is a simple encryption method.
  - The encryption method is clear and coherent to users, applications, and databases.
  - It is a hardware-based encryption with high performance.
- **File-level encryption**: Encryption of data stored in files/folders. In this type of encryption, the encryption occurs at a filesystem level, and in combination with a cryptographic algorithm, the encrypted data will be extremely secure. File-level encryption regulates the access of unauthorized users to files or folders on networks or shared computers. The advantages of file-level encryption are as follows:
  - Each file is encrypted with a discrete encryption key.
  - Access control is enforced using public key cryptography.
  - Both structured and unstructured data are supported.
- **Removable media encryption**: Removable media encryption prevents removable media devices such USB flash drives, portable hard disks, digital cameras, smartphones, tablets, etc. from unauthorized access.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Disk Encryption: Implementing Built-in Disk Encryption for Windows

Windows 10 has built-in disk encryption methods to encrypt hard drives and safeguard user data. By default, disk encryption is enabled in all devices using Windows 10. There are two methods of disk encryption in Windows 10: device encryption and BitLocker. If the users do not have device encryption, they can enable standard BitLocker encryption; however, BitLocker is not available on Windows 10 Home edition.

Device encryption

It is the simplest encryption method and is available in all editions of Windows 10. If a user loses the device, device encryption can protect the data from unauthorized access. This feature scrambles the entire system drive and secondary drives connected to the device and allows only the user to access the device.

Prerequisites for Device Encryption:

1. Trusted platform module (TPM).
2. Unified extensible firmware interface (UEFI).
3. Checking whether the device meets the device encryption requirements**.**

Steps to check whether the device meets the device encryption requirements:

- Click the **Start** button.
- Search for **System Information**, right-click on the top result, and choose **Run as administrator**.
- Click **System Summary** on the left pane.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- Search **Device Encryption Support**; the user device support device encryption if it reads **Meets prerequisites**.

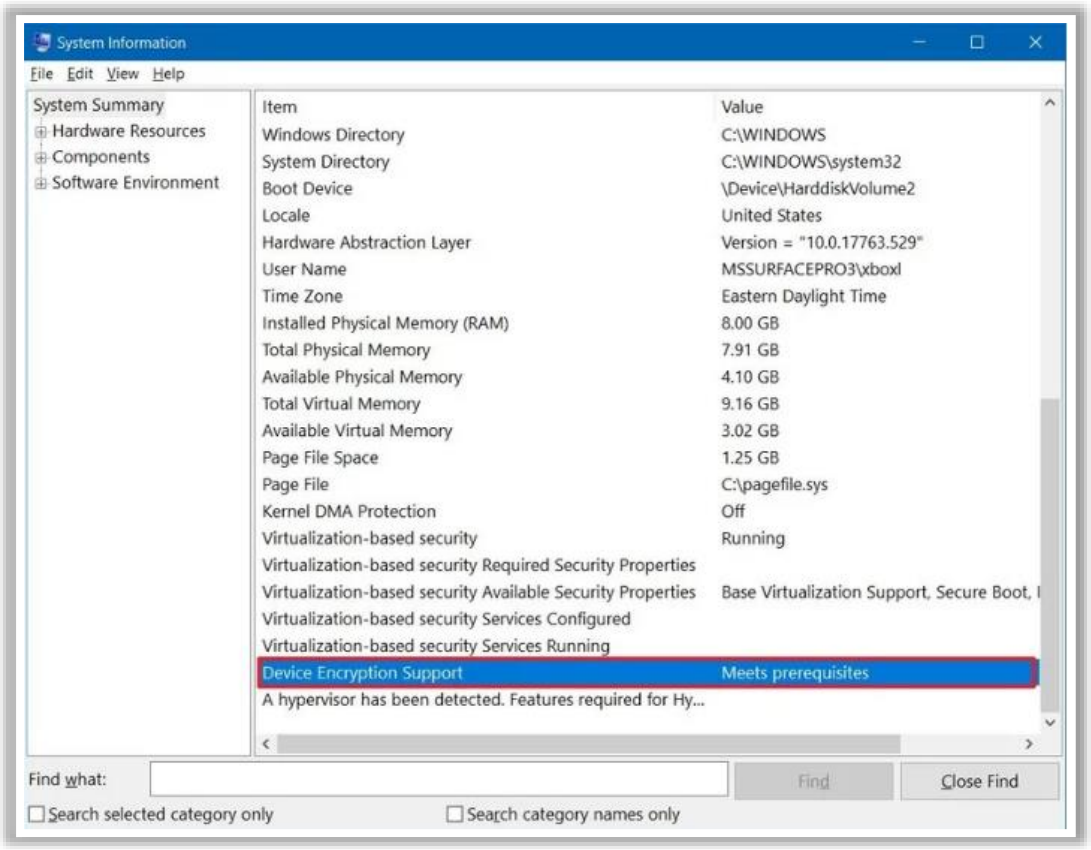


Figure 11.3: Checking whether the device is meeting the device encryption requirements

To enable TPM on UEFI

Follow these steps to enable the TPM chip in the user device if it is in a disabled state.

- Open **Settings**.
- Select **Update & Security**.
- Select **Recovery**.
- Browse to **Advanced start up** section and click **Restart now** button.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

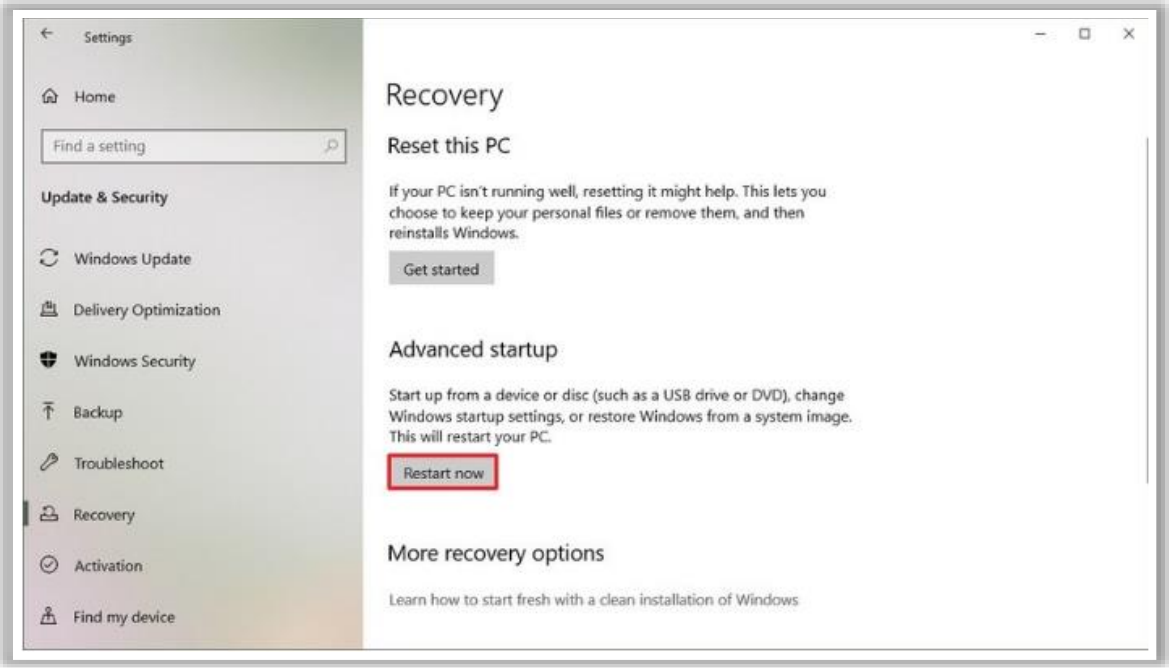


Figure 11.4: Enabling TPM on UEFI

- Click on **Troubleshoot**.

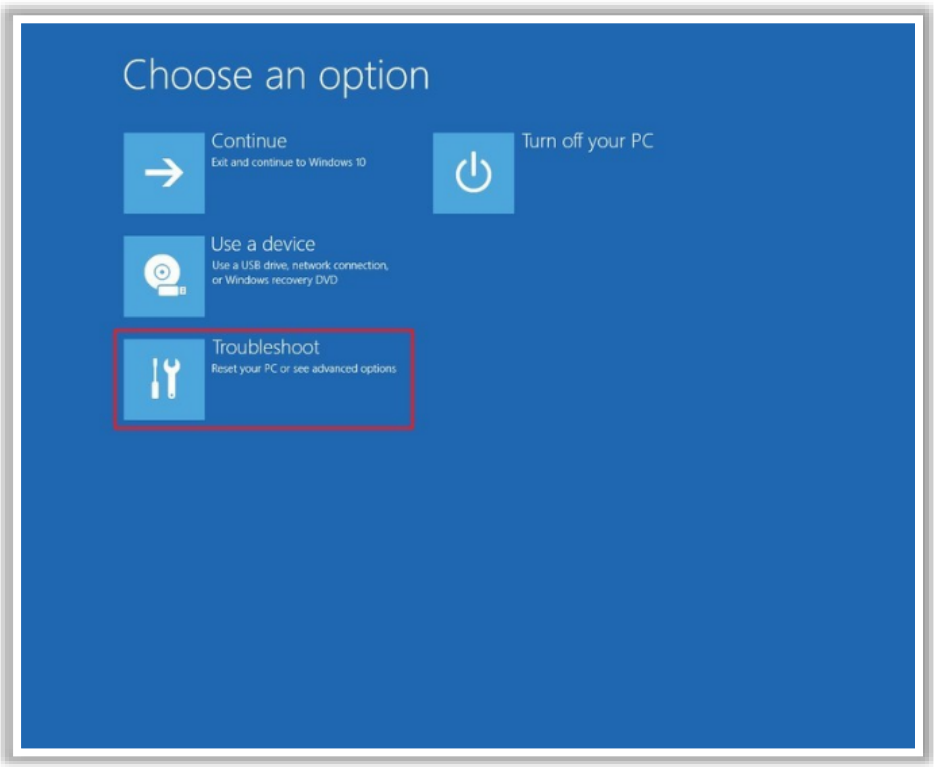


Figure 11.5: Choosing Troubleshoot Option

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- Click on **Advanced Options**.

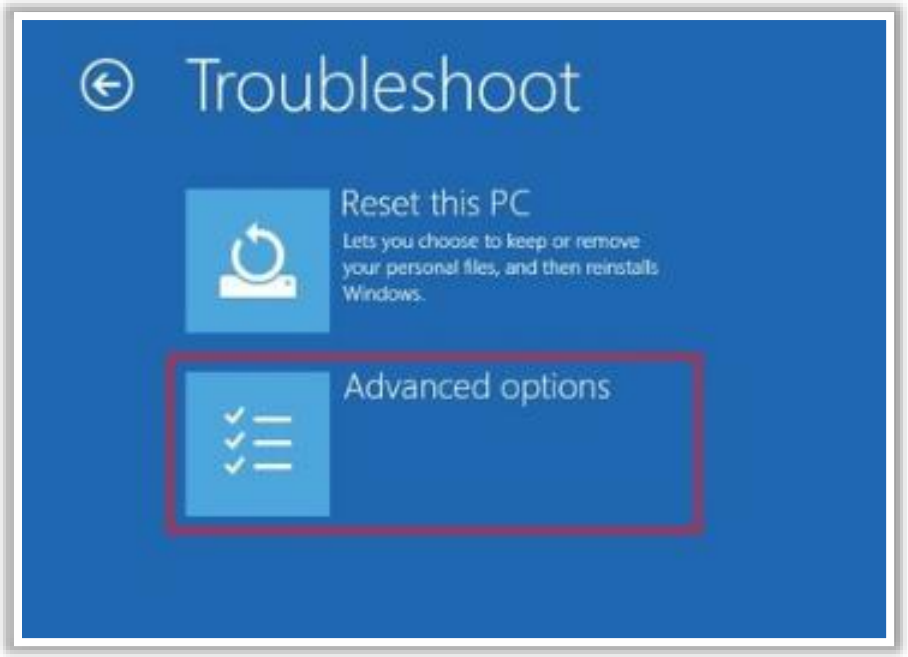


Figure 11.6: Clicking on Advanced Options

- Click on **UEFI Firmware Settings**.

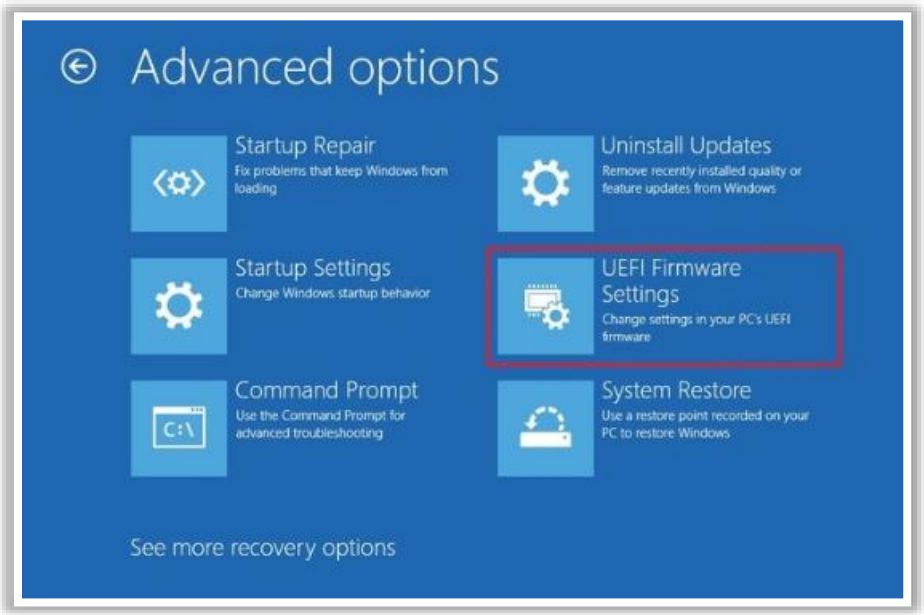


Figure 11.7: Selecting UEFI Firmware Settings

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- Click **Restart.**

Figure 11.8: Restarting the System to change the UEFI Firmware Settings

- Navigate to security settings.
- Enable the TPM feature.

To Enable Device Encryption

- Go to **Start → Settings → Update & Security → Device Encryption**.
- **Turn on** the Device encryption option.

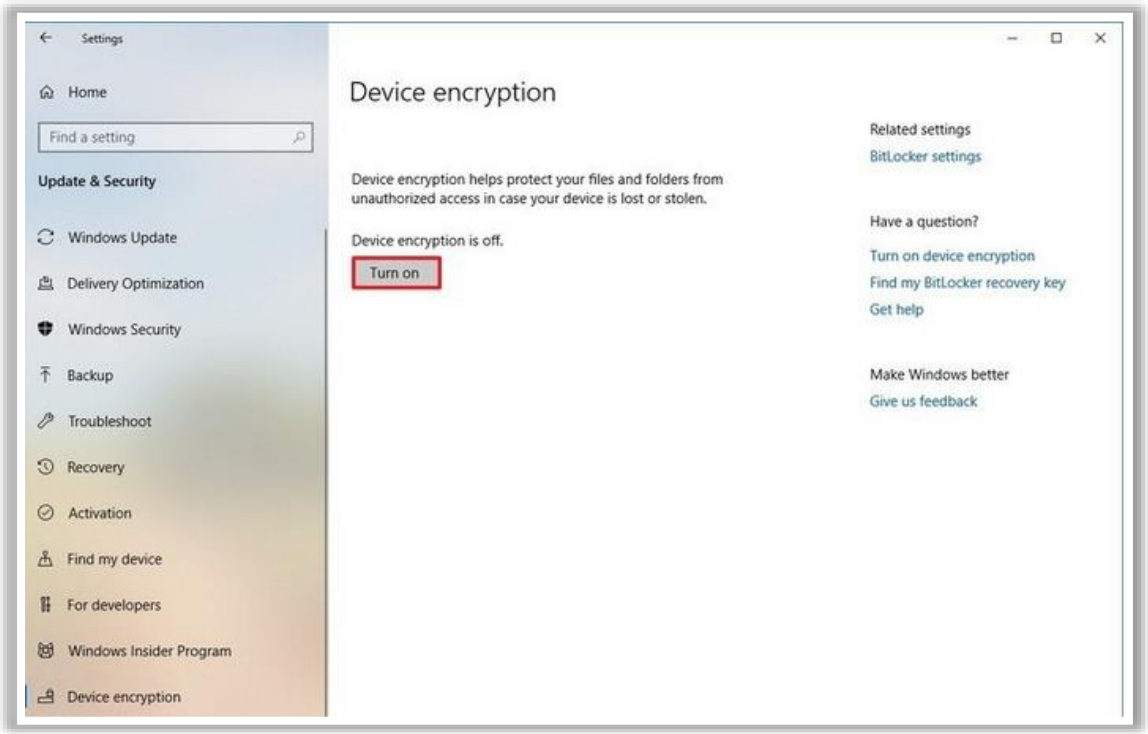


Figure 11.9: Enabling Device Encryption

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

BitLocker encryption

This protects the data by encrypting the entire volume of data using advanced encryption standard (AES) encryption algorithm in cipher block chaining (CBC) or XTS mode with a 128-bit or 256-bit key. BitLocker is available in Windows 10 Pro, Enterprise, or Education editions.

To Enable Standard BitLocker Encryption

- Sign in with an administrator account.
- Select the **Start** button.
- Choose **Control Panel**, then click on **System and Security**.
- Under **BitLocker Drive Encryption,** choose **Manage BitLocker**.
- Select **Turn on BitLocker**.

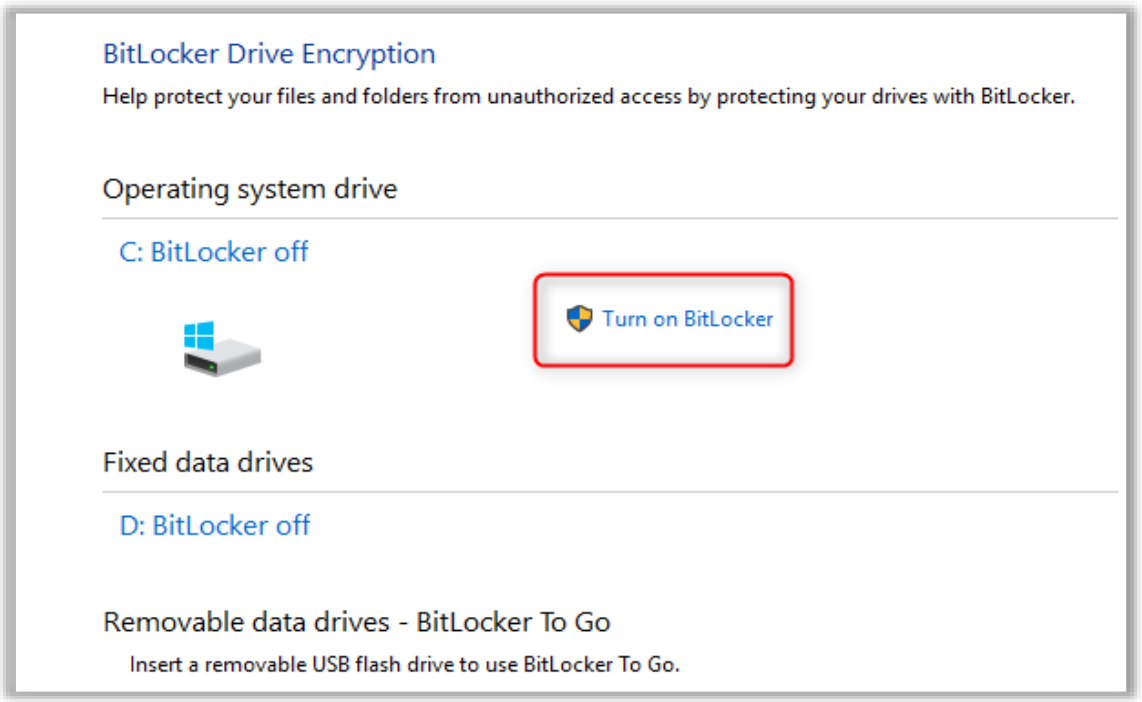


Figure 11.10: Enabling Standard BitLocker Encryption

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Disk Encryption Tools

The common goal of disk encryption tools is to encrypt a disk partition to provide confidentiality to the information stored on it. Some disk encryption tools are discussed below.

- **VeraCrypt**

  Source: *https://www.veracrypt.fr*

  VeraCrypt is a software for establishing and maintaining an on-the-fly-encrypted volume (data storage device). On-the-fly encryption means that data is automatically encrypted just before it is saved and decrypted just after it is loaded without any user intervention. No data stored on an encrypted volume can be read (decrypted) without using the correct password/keyfile(s) or correct encryption keys. The entire file system is encrypted (e.g., file names, folder names, free space, metadata, etc.).

  Files can be copied to and from a mounted VeraCrypt volume just like they are copied to/from any normal disk (e.g., by simple drag-and-drop operations). Files are automatically decrypted on the fly (in memory/RAM) while they are read or copied from an encrypted VeraCrypt volume. Similarly, files that are written or copied to the VeraCrypt volume are automatically encrypted on the fly (just before they are written to the disk) in RAM.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

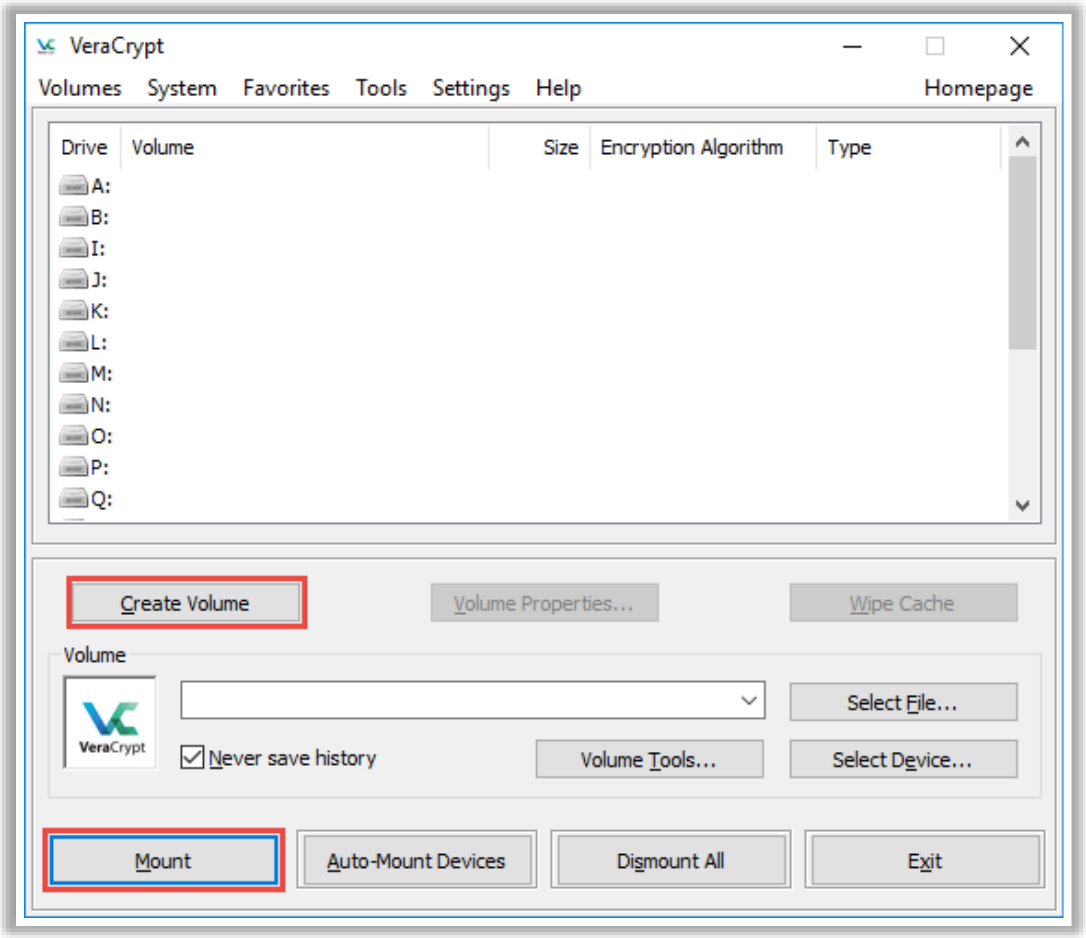
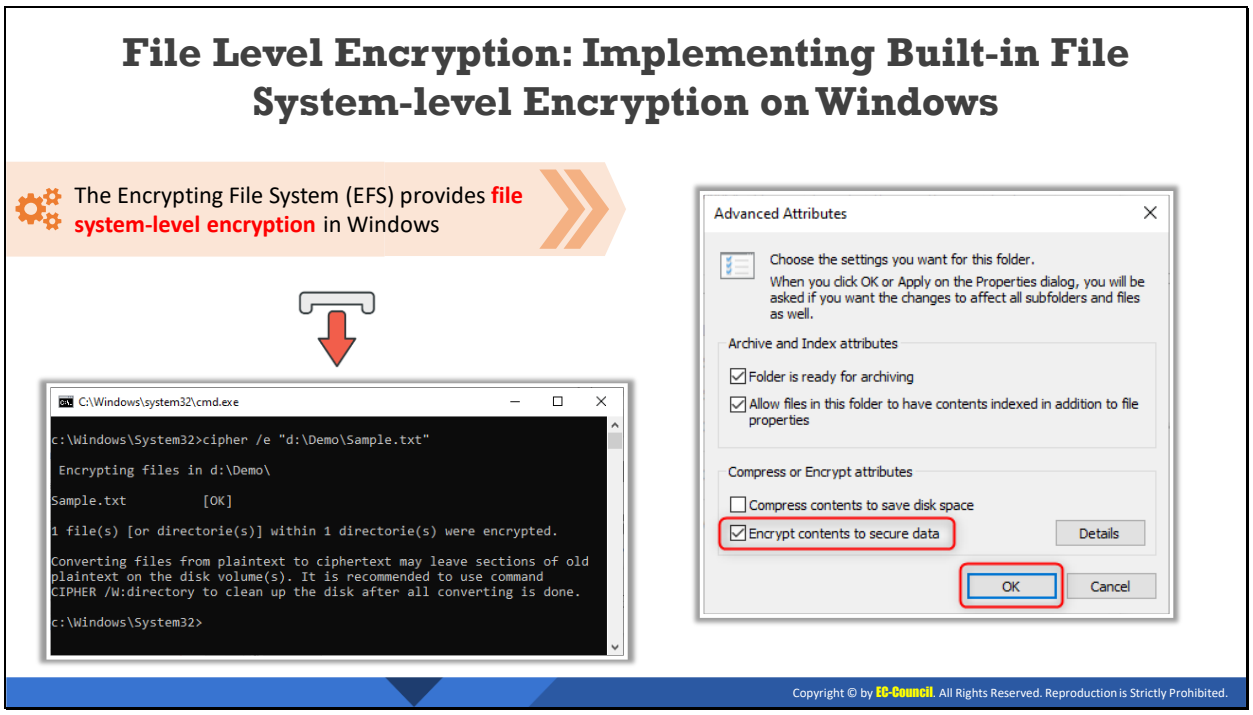


Figure 11.11: Screenshot of VeraCrypt

Some additional disk encryption tools are as follows:

- BitLocker Drive Encryption (*https://docs.microsoft.com*)
- FinalCrypt (*https://www.finalcrypt.org*)
- Seqrite Encryption Manager (*https://www.seqrite.com*)
- FileVault (*https://support.apple.com*)
- Gilisoft Full Disk Encryption (*http://www.gilisoft.com*)

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



File Level Encryption: Implementing Built-in File System-level Encryption on Windows

The Encrypting File System (EFS) provides file system-level encryption in Windows (starting from Windows 2000), except the home version. The user needs to enable this feature on a specific file, directory, or drive. EFS protects the confidential information from unauthorized users who have physical access to a computer.

File Encryption with EPS Using Command Prompt

- Right-click on the Start button and select **Command Prompt (Admin)**.
- Type the following command:

  cipher /e “<PATH>”
- Enter the file path with extension and hit **Enter**.

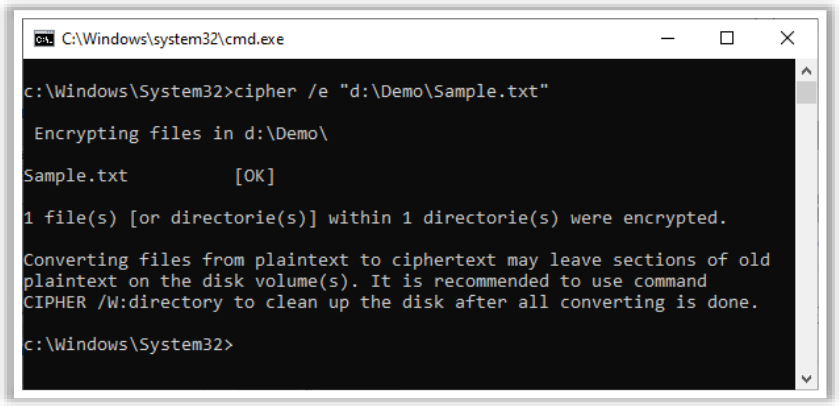


Figure 11.12: File encryption with EPS

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

To enable EPS Using Advanced Attributes in a Selected File/Folder

- Select the file for encryption using EFS.
- Right-click on the file and select **Properties.**

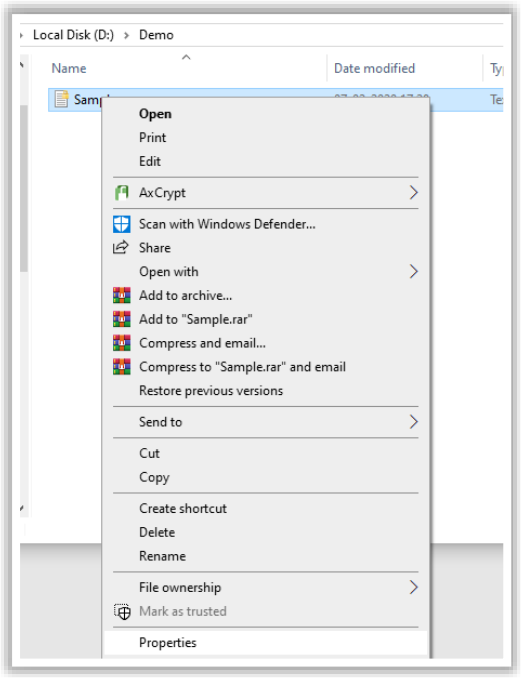


Figure 11.13: Screenshot of Selecting Properties

- Click **Advanced**

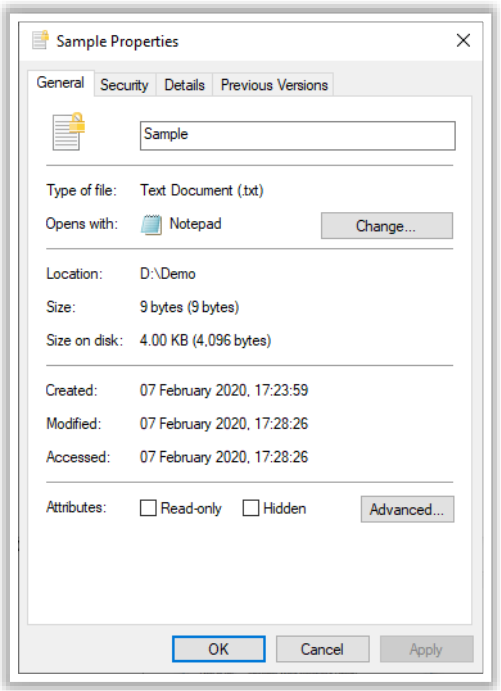


Figure 11.14: Choosing Advanced Option

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- Check the box **Encrypt content to secure data** and click **OK**

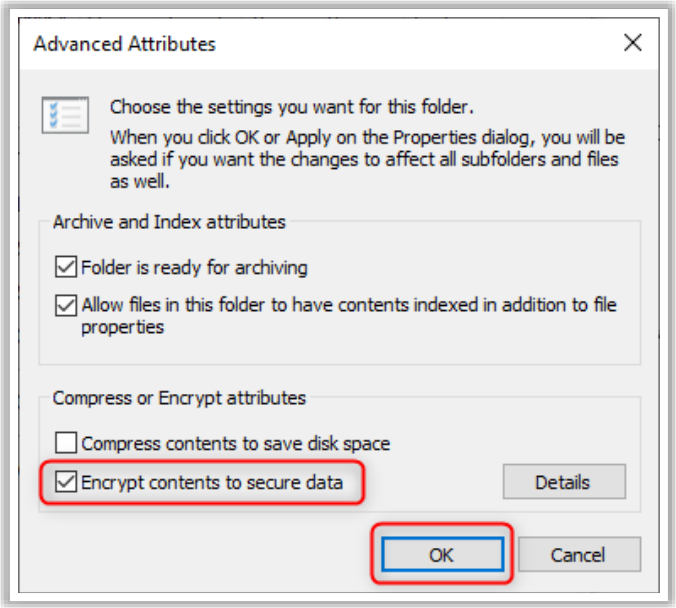


Figure 11.15: Selecting Encrypt Content to Secure Data

- Click **Apply**. A box will appear with the option to encrypt the file only or encrypt the file and its parent folder. Select as per requirements, and click **OK**

Figure 11.16: Encryption Warning

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

File Encryption Tools

- **Advanced Encryption Package**

  Source: *http://www.aeppro.com*

  Advanced Encryption Package is a file encryption software for Windows 10, 8, and 7. It uses strong and proven algorithms to protect sensitive documents. It supports both file and text encryption and uses both symmetric and asymmetric algorithms.

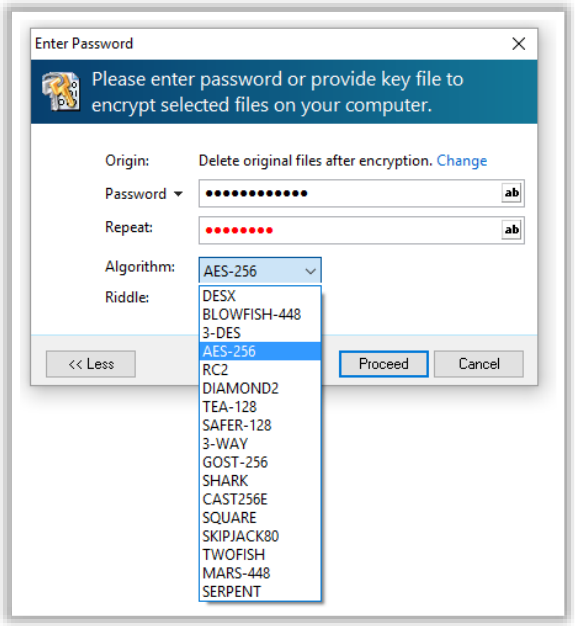


Figure 11.17: Screenshot of Advanced Encryption Package

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

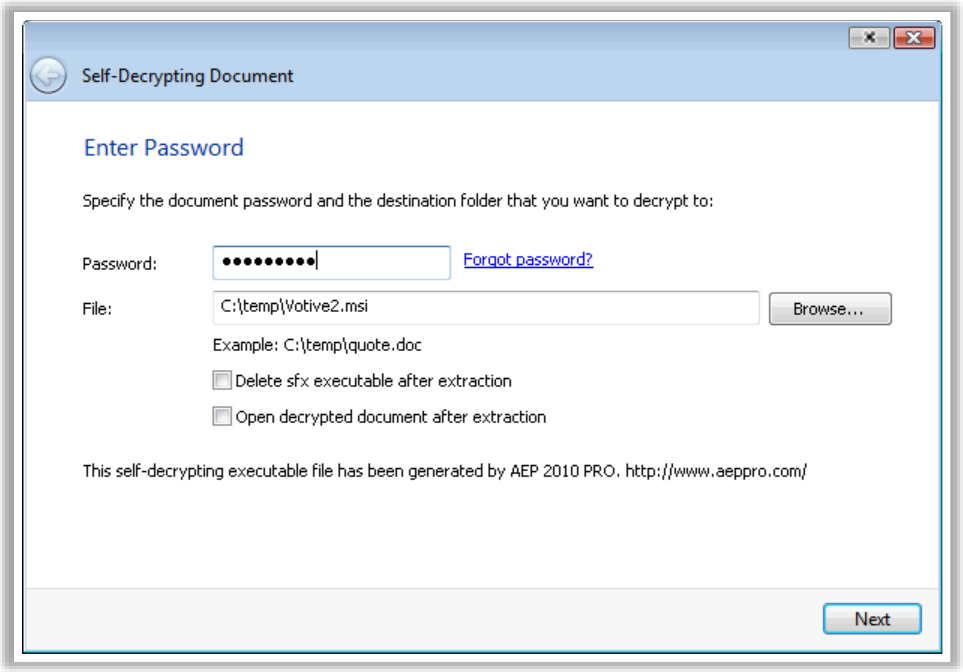
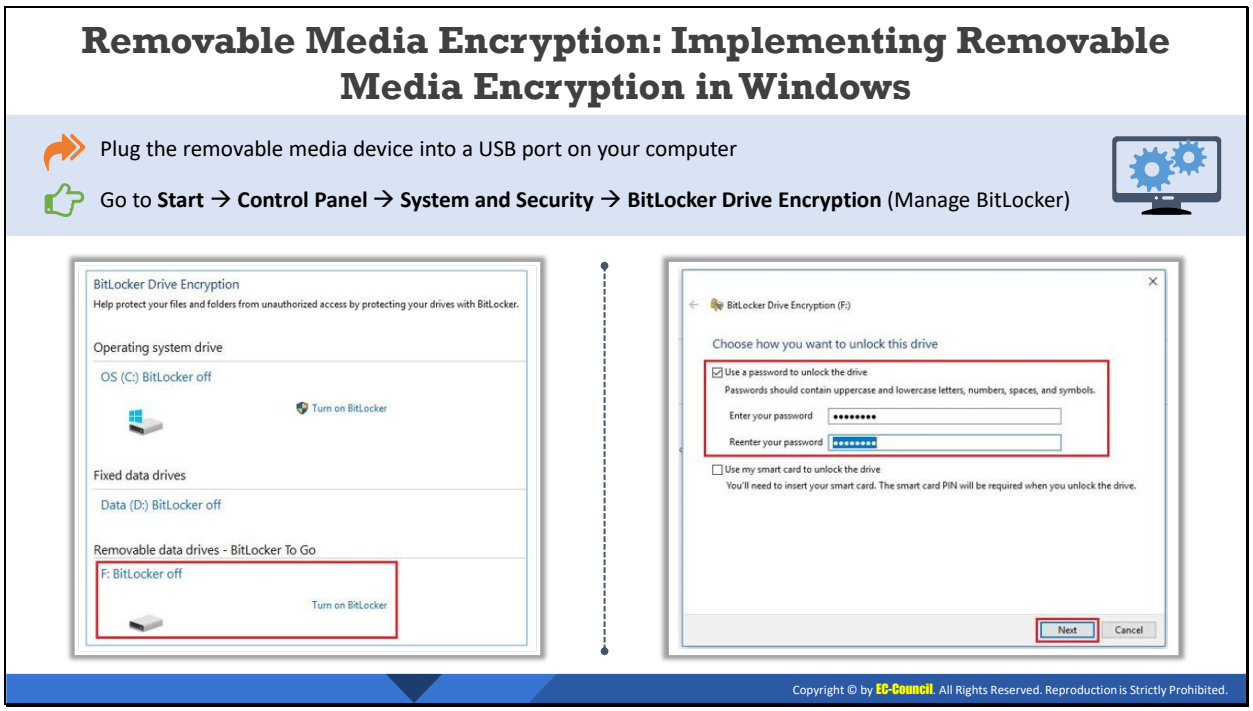


Figure 11.18: Screenshot of Advanced Encryption Package

Some additional file encryption tools are as follows:

- AxCrypt (*https://www.axcrypt.net*)
- idoo File Encryption (*https://www.idooencryption.com*)
- Cryptomator (*https://cryptomator.org*)
- Encrypto (*https://macpaw.com*)
- AES Crypt (*https://www.aescrypt.com*)

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Removable Media Encryption: Implementing Removable Media Encryption in Windows

Removable media such as USB flash drives, iPods, smartphones, tablets, digital cameras, portable hard disks, etc. are prevalent in a workplace and pose a real threat to an organization. With these devices, the attackers can easily introduce a malicious code in a network or carry sensitive data out of an organization. Hence, encryption is the best way to protect sensitive data from being taken out of an organization.

Encryption can be applied to removable media to prevent it from unauthorized access in case of loss or theft. This will add an extra layer of security to confidential information. Various encryption solutions are available in the market with different features. Some encryption solutions encrypt the data stored on a local drive, but not on USB devices, whereas some encryption solutions automatically encrypt the data stored on removable media. While selecting a removable media encryption solution, it is important to verify how it is configured to restrict access to devices using an authorized list, personal devices, an authorized file copy, and encryption keys.

Operating systems such as Windows, Linux, and Mac use a couple of methods to encrypt removable media such as USB drives. They use either built-in features or third-party encryption solutions to encrypt removable media.

Implementing Removable Media Encryption in Windows: BitLocker

To Enable Removable Media Encryption in Windows 10

- Plug the removable media device into a USB port on the computer.
- Go to **Start → Control Panel → BitLocker Drive Encryption.**

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

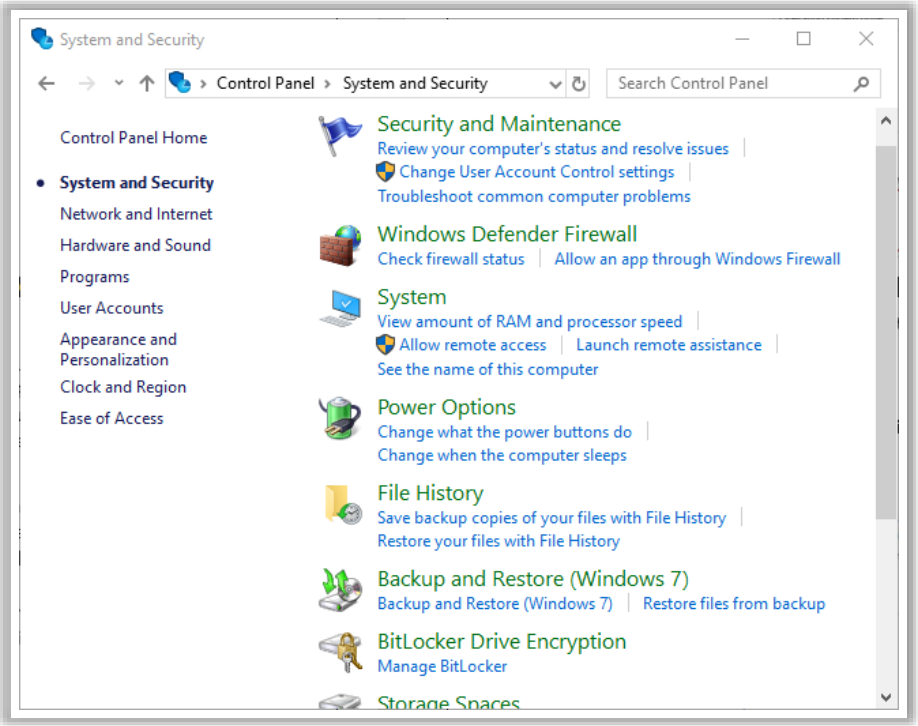


Figure 11.19: Choosing BitLocker Drive Encryption Option

- Select the removable media device to encrypt and click **Turn on BitLocker**.

Figure 11.20: Turning on BitLocker

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- BitLocker initialization process will start. Wait for some time to finish the initialization process.

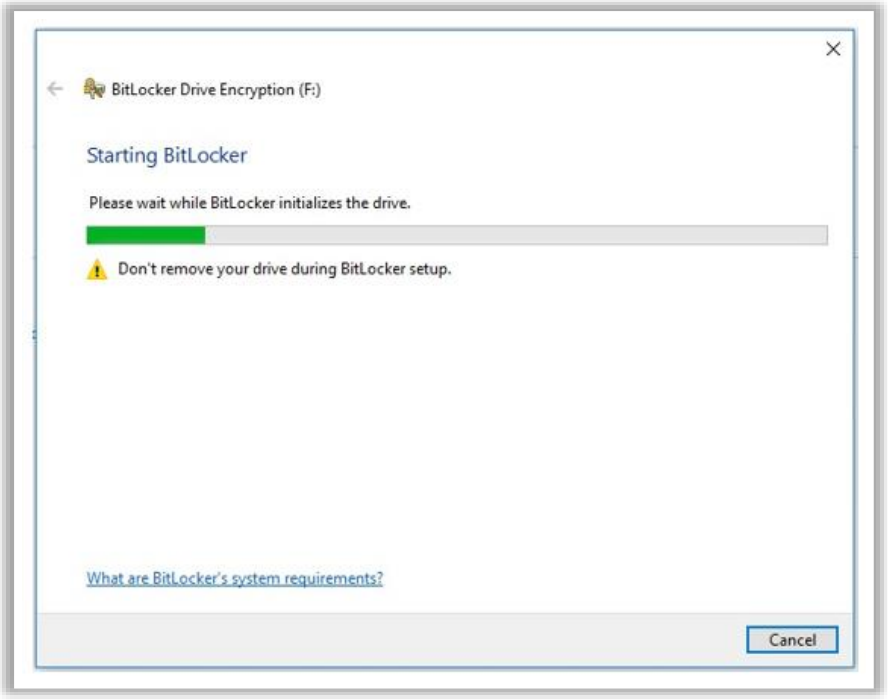


Figure 11.21: BitLocker Initiating the Drive

- In the **Choose how you want to unlock this drive** window**,** tick the **Use a password to unlock the drive** checkbox and enter a strong password, then click **Next**.

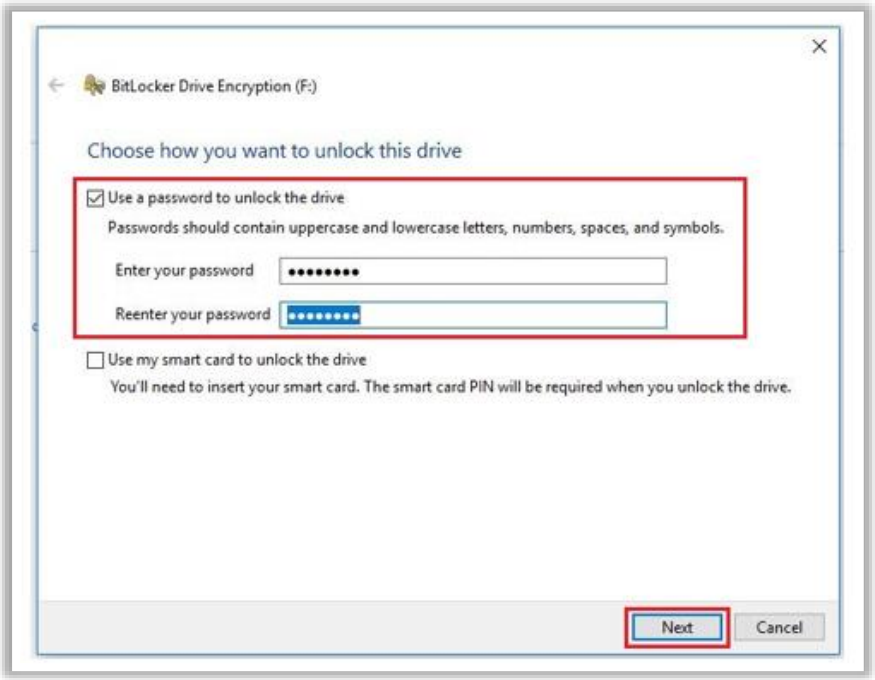


Figure 11.22: Unlocking the Drive

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- In **How do you want to back up your recovery key?** window, either choose **Save to a file** or **Print the recovery key**, then click **Next**.

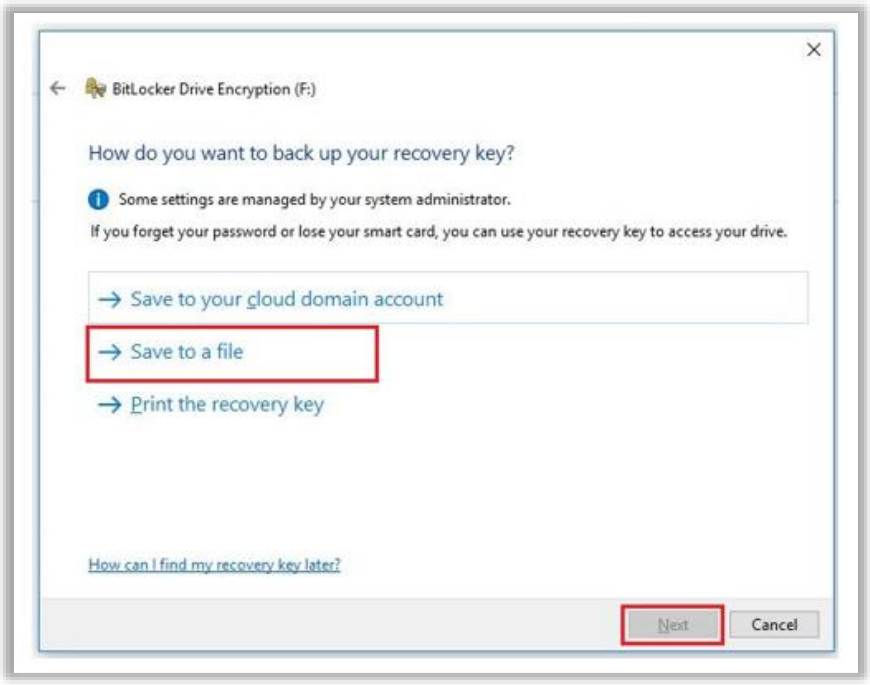


Figure 11.23: Saving to a File

- In the **Choose how much of your drive to encrypt** window, Select **Encrypt used disk space only** if the drive is new or select **Encrypt entire drive** if the drive contains data**,** then click **Next.**

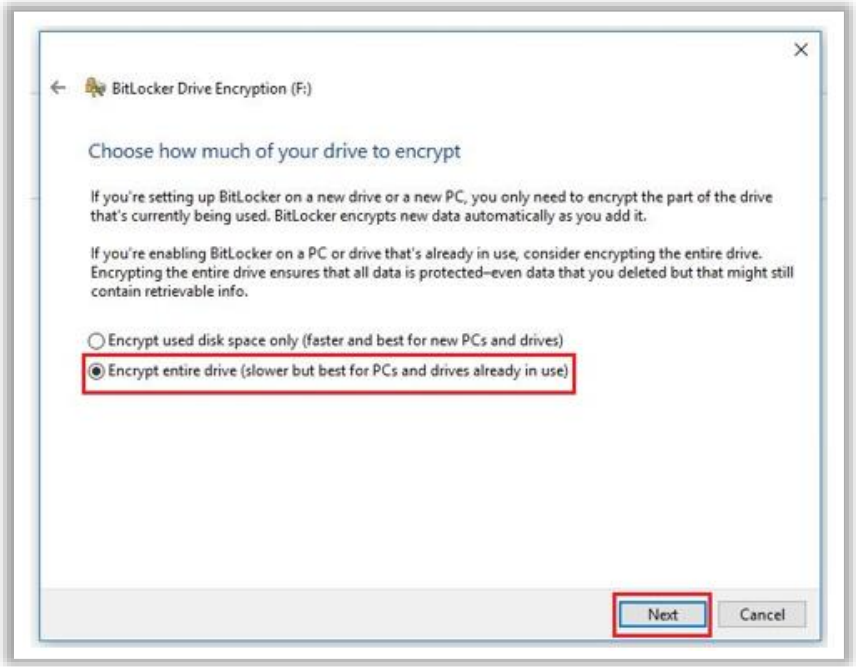


Figure 11.24: Choosing Encrypt Entire Drive Option

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- In the **Choose which encryption mode to use** window, select **Compatible mode** if the user wants to use the encrypted drive on older versions of Windows, or select **New encryption mode** if the user wants to use the encrypted drive on Windows 10 only. Then click **Next**.

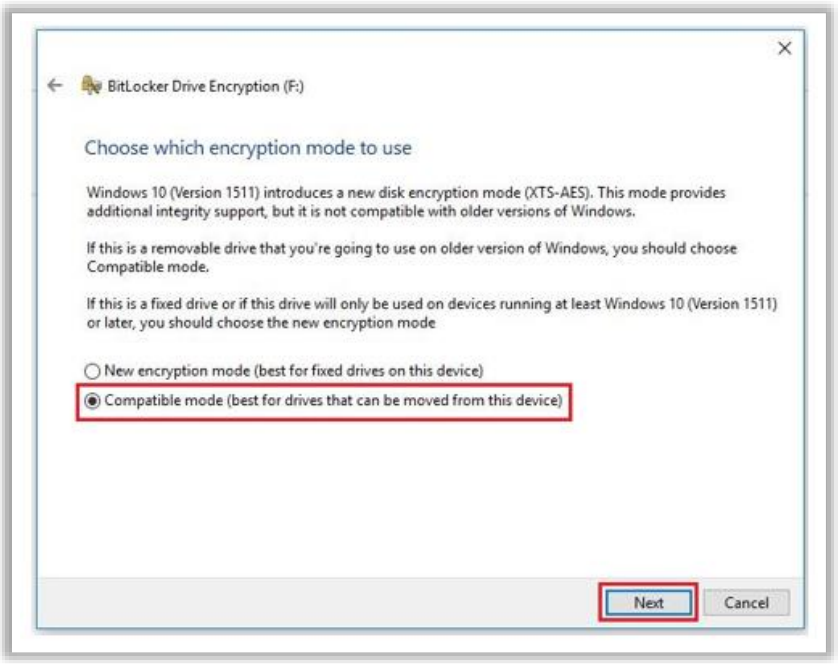


Figure 11.25: Choosing Compatible Mode

- Click **Start encrypting**.

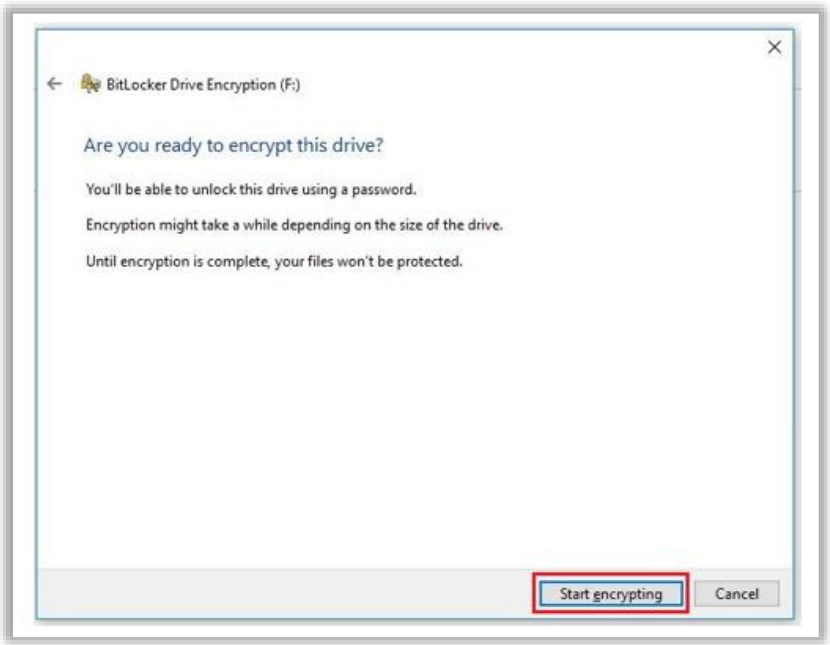


Figure 11.26: Starting the Encryption

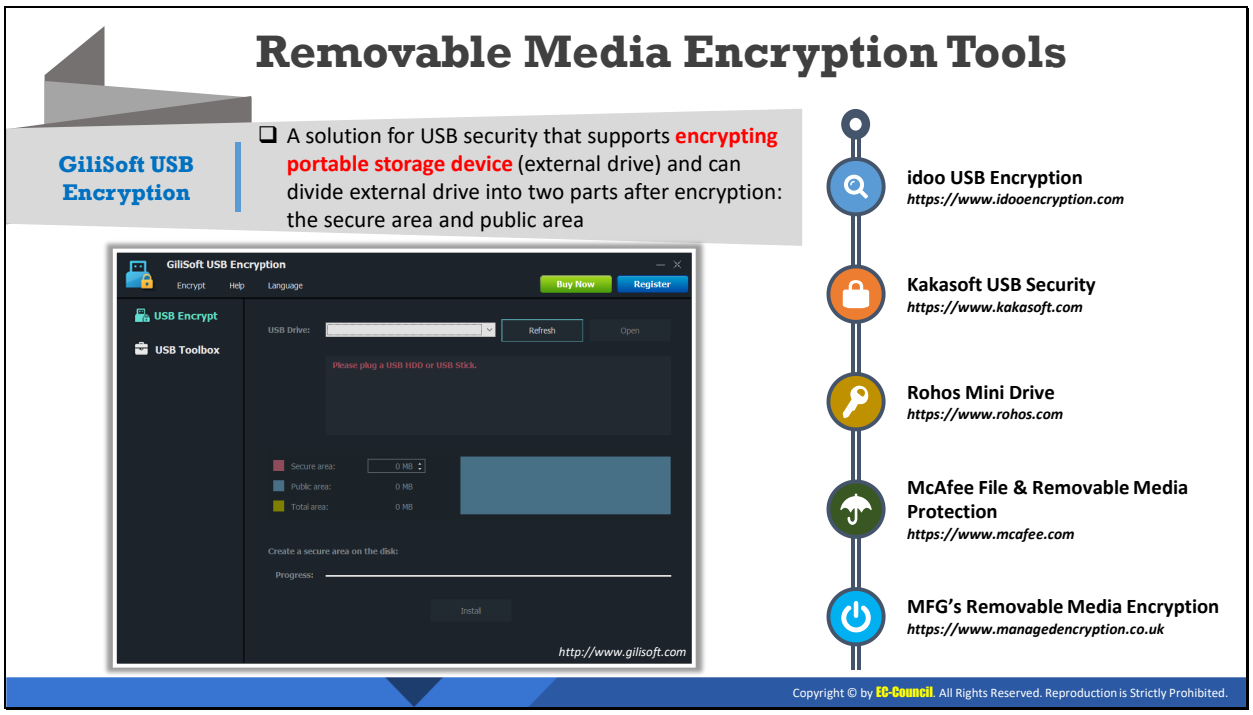
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- Click **Close** when the encryption process is completed.

Figure 11.27: Completion of Encryption

Note: Whenever the user tries to connect the encrypted drive, they have to provide the password to unlock it.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Removable Media Encryption Tools

- **GiliSoft USB Encryption**

  Source*: http://www.gilisoft.com*

  GiliSoft USB Encryption is a solution for USB security that supports the encryption of portable storage devices (external drives) and can divide an external drive into two parts after encryption: a secure area and a public area. It converts a regular USB flash drive into a secured one in less than a minute, and data on the protected area (secure area) is encrypted by a 256-bit AES on-the-fly encryption.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

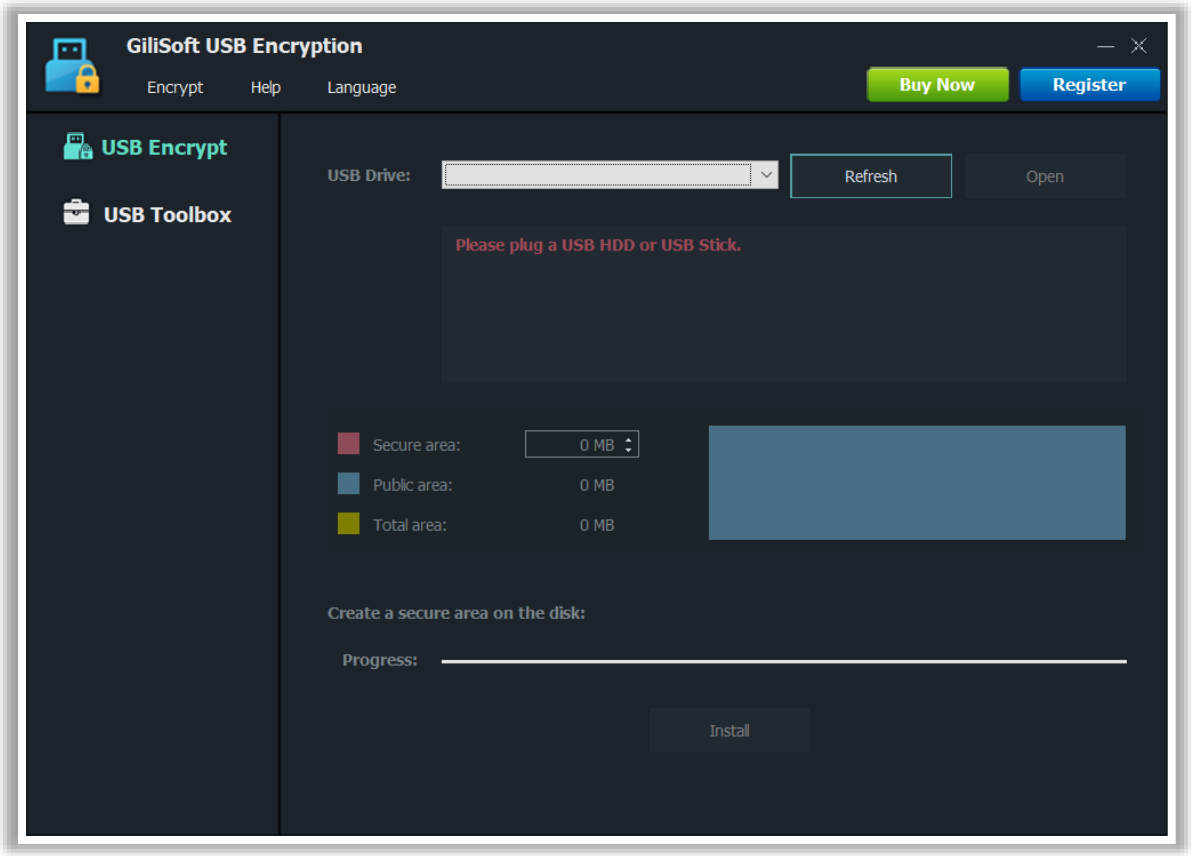
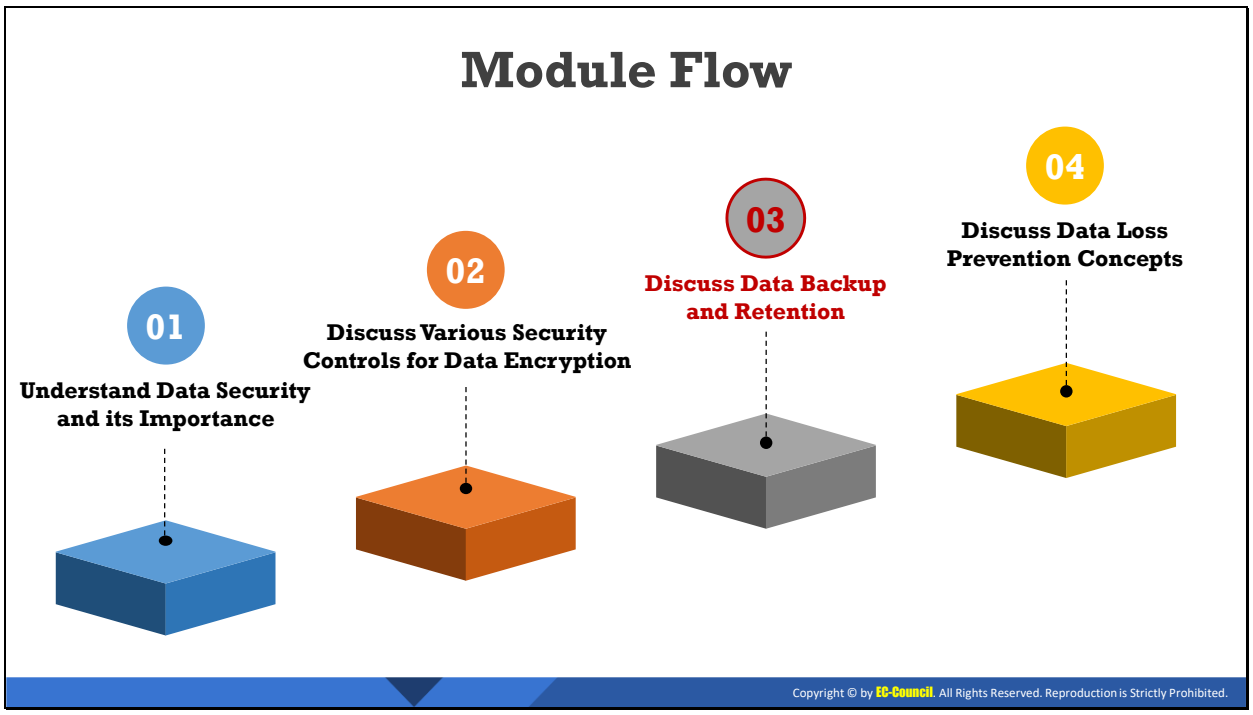


Figure 11.28: Screenshot of GiliSoft USB Encryption

Some additional removable media encryption tools are as follows:

- idoo USB Encryption (*https://www.idooencryption.com*)
- Kakasoft USB Security (*https://www.kakasoft.com*)
- Rohos Mini Drive (*https://www.rohos.com*)
- McAfee File & Removable Media Protection (*https://www.mcafee.com*)
- MFG's Removable Media Encryption (*https://www.managedencryption.co.uk*)

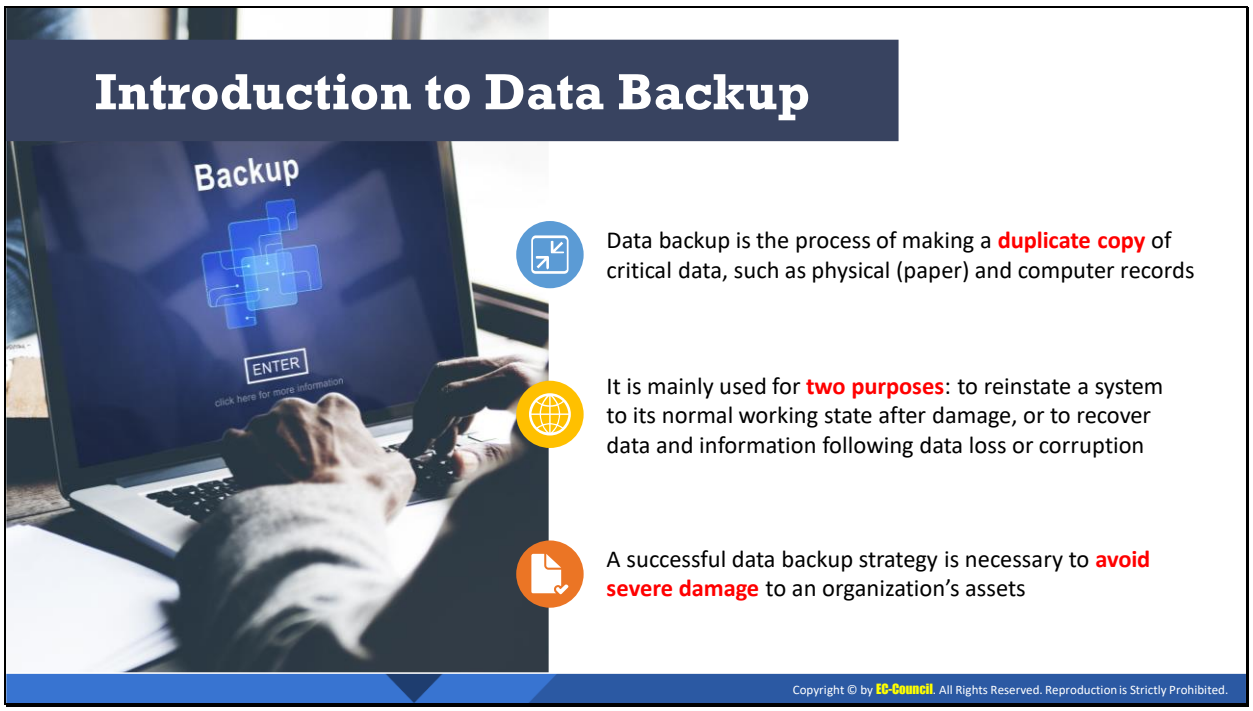
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Discuss Data Backup and Retention

Data loss is a major risk that organizations are facing today. Loss of critical data can result in a lot of damage to the organization. Any organization that encounters a critical data loss has a higher probability of facing serious issues later. Therefore, you should have a strong data backup and retention plan in place to deal with such incidents. The objective of this section is to explain the concept of data backup and retention.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Introduction to Data Backup

Data backup is the process of copying or storing important data. A backup copy will help you restore the original data when data is lost or corrupted. Backup is a mandatory process for all organizations. The process of retrieving lost files from a backup is known as restoring or recovery of files.

The main idea behind data backup is to protect data and information and recover the same after data loss. Data backup is mainly used for two purposes: to reinstate a system to its normal working state after damage, or to recover data and information following data loss or corruption.

Data loss in an organization affects its finances, customer relationship, and company data. Data loss in personal computers may lead to the loss of personal files, images, and other important documents saved in the system.

Reasons for Data Loss

- **Human error**: Deletion of data purposefully or accidently, misplacement of data storage devices, and errors in administering databases.
- **Crimes**: Stealing or making modifications to critical data in an organization.
- **Natural causes**: Power failures, sudden software changes, or hardware damages.
- **Natural disaster**: Floods, earthquakes, fire, etc.

Benefits of Performing a Data Backup

- It offers access to critical data even in the event of a disaster, ensuring peace of mind in a workplace.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

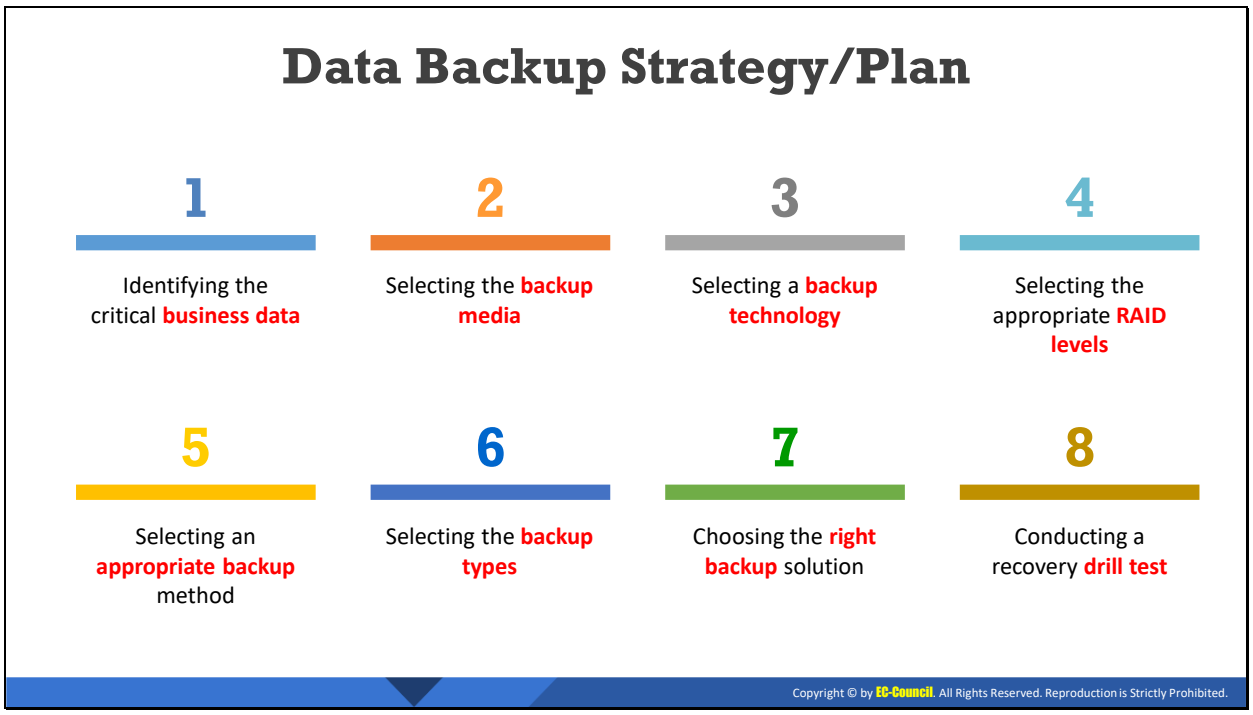
- Backup of critical data prevents an organization from losing its business. It also helps them retrieve data anytime.
- Data recovery helps organizations recover lost data and ensure business continuity.

It is recommended that every organization performs a data backup on a regular schedule to run their business successfully and efficiently.

To avoid severe damage to an organization's assets, it is important to design a strategy for a successful data backup process. Going forward, this data backup strategy can act as a blueprint while working on the data backup process for the entire organization. Certain companies also create a data backup policy that is required while implementing a backup strategy.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Data Backup Strategy/Plan

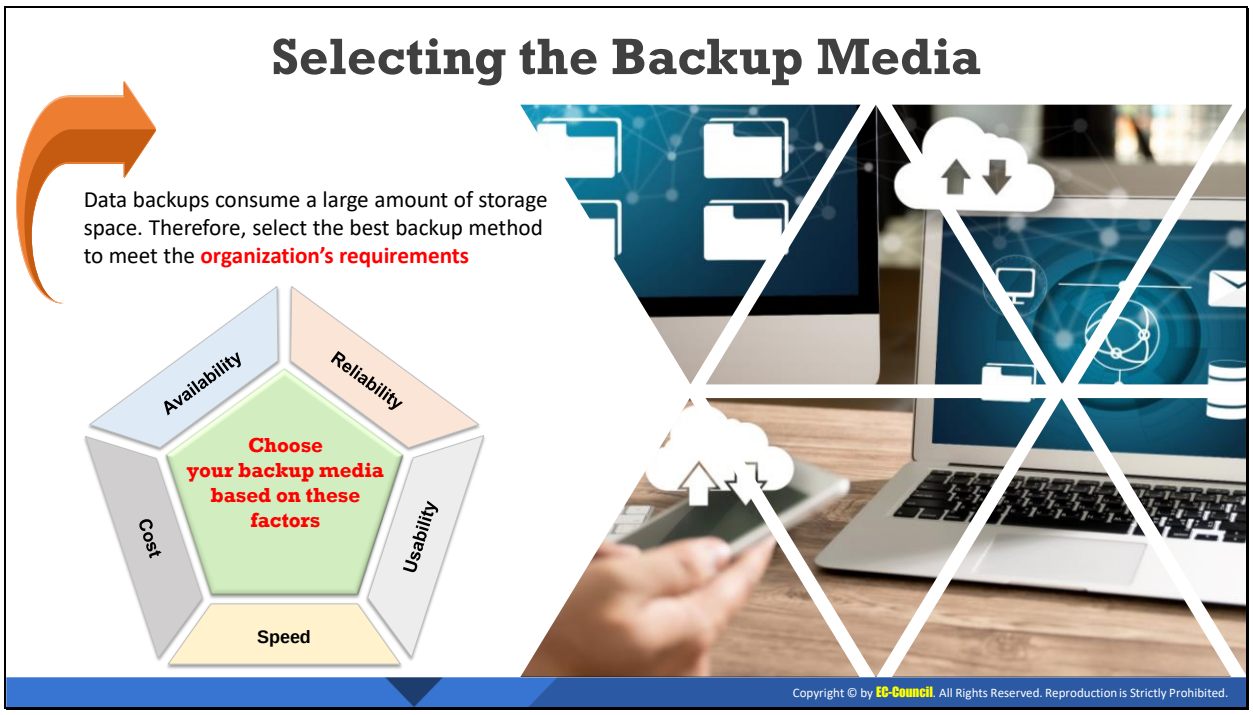
An ideal backup strategy includes steps ranging from selecting the right data to conducting a test data restoration drill. Although the backup strategy might differ among organizations, it is important to consider the following features before drafting a backup strategy:

- The backup strategy should have a data recovery feature from any external device. These devices may include servers, host machines, laptops, etc.
- If the data loss is because of a natural disaster, the backup strategy should not be restricted to only a certain number of incidents. The strategy should also cover the methods for recovering the data after a natural disaster.
- The strategy should include the steps to recover data at the earliest.
- The lower the cost for data recovery, the more the financial benefit to the organization.
- Auto recovery options should be included in the backup strategy as well, as they reduce the chances of human error during the recovery process.

Steps involved in data backup strategy/plan:

1. Identifying the critical business data
2. Selecting the backup media
3. Selecting a backup technology
4. Selecting the appropriate RAID levels
5. Selecting an appropriate backup method
6. Selecting the backup types
7. Choosing the right backup solution
8. Conducting a recovery drill test

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Selecting the Backup Media

Choosing the best backup media is a common concern within most organizations. The selection of a wrong media device can lead to a segregation of data across different media devices. With a carefully considered plan, selecting an appropriate media will enable a better level of data backup.

Once the data is identified, it is important to choose an appropriate backup media to store the data. Backup media selection depends on the type and amount of data in the backup. At times, data backup consumes a large amount of space; consequently, an increased attention is necessary to select the best backup media for a situation, and to fulfill the organizational needs.

Choosing the best backup media is based on the following factors:

- **Cost**: Organization should have backup storage mediums that best fit their budget. The backup media should have more storage space than the data it will contain.
- **Reliability**: Organizations must be able to rely on the data stored on the backup media without fail. Organizations must select a media that is reliable and not susceptible to damage or loss.
- **Speed**: Organizations should select backup mediums which require reduced number of human interactions during the backup process. Speed becomes a concern if the backup process cannot be completed when a machine is idle.
- **Availability**: The unavailability of the backup medium could be an issue following data loss or data corruption. Organizations should decide on a medium that is always available.
- **Usability**: Organizations should select a media that is easy to use. An easy media type has a greater flexibility during the backup process.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Examples of Data Backup Media Devices

Media	Capacity	Advantages	Disadvantages	Illustrations
Optical disks (DVD)	~200 GB	▪ Affordable, easy to store and transport	▪ Several manual disk swaps may be required because of the limited data capacity ▪ Recording and verifying a backup is slow	
Portable hard drives/USB flash drives	No limit	▪ Relatively higher storage capacity than optical disks ▪ Ideal for the home or small offices ▪ Faster recording of backups	▪ More expensive than DVD backups ▪ Less recommended for small backups	
Tape drives	No limit	▪ Media for enterprise-level backups ▪ Easy to store and transport	▪ Expensive	

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Examples of Data Backup Media Devices

- **Optical Disks (DVD)**

  DVD recordable disks can store up to ~200 GB of data and are readily available. DVDs store more data and are available at affordable rates, in bulk if need be. However, they are not used as much as in the past, as external hard drives are available at reasonable prices and can store more data than DVDs.

  - **Advantage:**
    - Less expensive , easy to store, and transport
  - **Disadvantage:**
    - Several manual disk swaps may be required because of the limited data capacity
    - Recording and verifying a backup is slow

- **Portable Hard Drives/USB Flash Drives**

  Portable hard drives are considered a better medium for data backup than a DVD. They are available in high capacities and can also be used for smaller backups. Flash drives are available in different sizes and have the ability to store large backup files.

  RAID is another available hard drive option. It contains two or more hard drives. The second drive may be used to copy data stored in the first drive. This process allows important data to be preserved. Any change in the data will be automatically reflected in all other drives as well.

  - **Advantages:**
    - Relatively higher storage capacity than optical disks

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- Ideal for the home or small offices
- Faster recording of backups

- **Disadvantages:**
  - Expensive than DVD
  - Less recommended for small backups

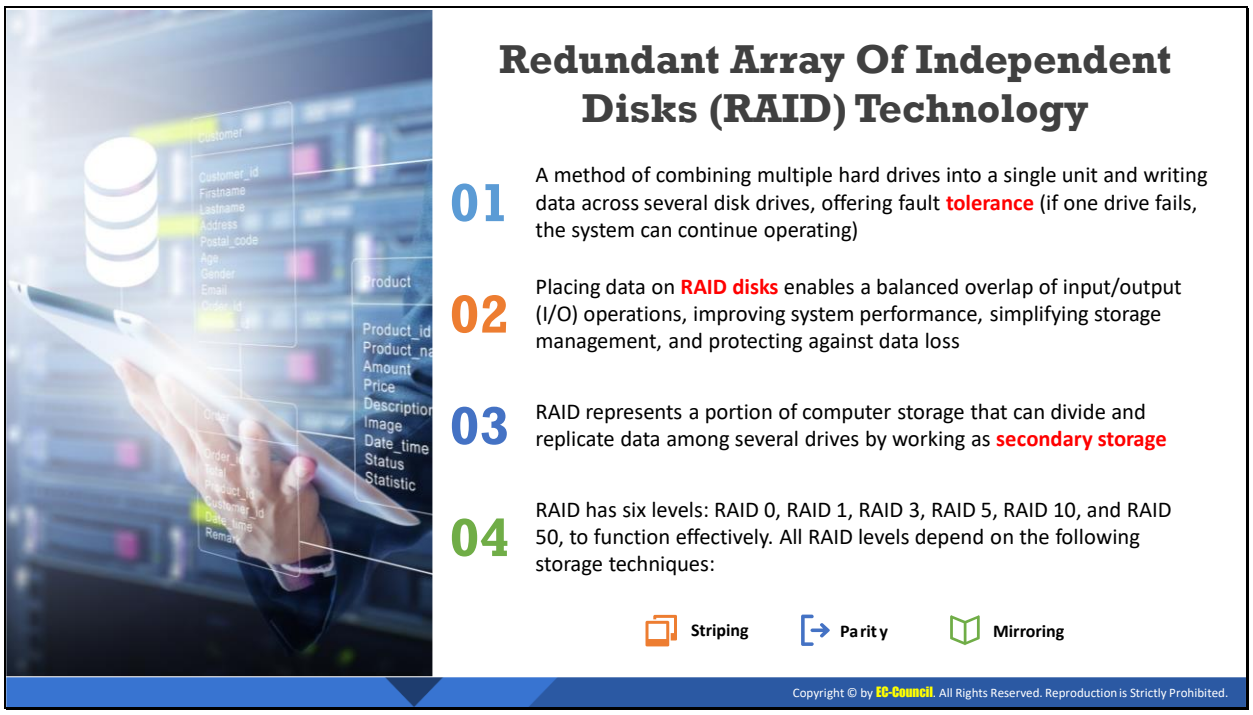
- **Tape Drives**

  A Tape drive is considered as the best media for data backup. It facilitates data backup at an enterprise level. Tape drives are used for storing programs and data. There is no limit in storage capacity and can be used to store large amounts of data.

  - **Advantages:**
    - Media for enterprise-level backups
    - Easy to store and transport
    - Requires no user intervention
    - Tape backup is completely automatic
  - **Disadvantages:**
    - Expensive for home users
    - Home computers require additional hardware and software updates

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Redundant Array Of Independent Disks (RAID) Technology

Many organizations depend on RAID technology for handling their critical backup needs, especially with the increase in data flow and data volume. Organizations are expanding their networks to improve their productivity. However, this additional increase can cause network bottlenecks. The probability of losing data because of disaster, threats, mistakes, and hardware failures hamper an organization's ability to grow. RAID technology overcomes these situations providing an option for data availability, high performance, efficient and accessible recovery options without a loss of data.

Understanding RAID Technology

RAID technology is used to store data in different places on several disks. Storing the data on multiple disks improves the performance of I/O operations. RAID technology functions by implementing multiple hard disks as a single logical disk. It allows a more balanced storage of the same data across an array of disks. An effective implementation of this technology helps address the complex issues in fault tolerance. The data organized in RAID levels depends on the RAID storage techniques and installation methods. Usually, the implementation of RAID is done on a server. Although personal computers do not necessarily need this technology, they can still setup and utilize it in a smaller environment than an enterprise.

RAID has six levels for functioning effectively: RAID 0, RAID 1, RAID 3, RAID 5, RAID 10, and RAID 50. Each level has the following features:

- **Fault tolerance:** Even if a disk fails to work, other disks will continue to function normally.
- **Performance:** RAID achieves high performance during read and write processes across multiple disks.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

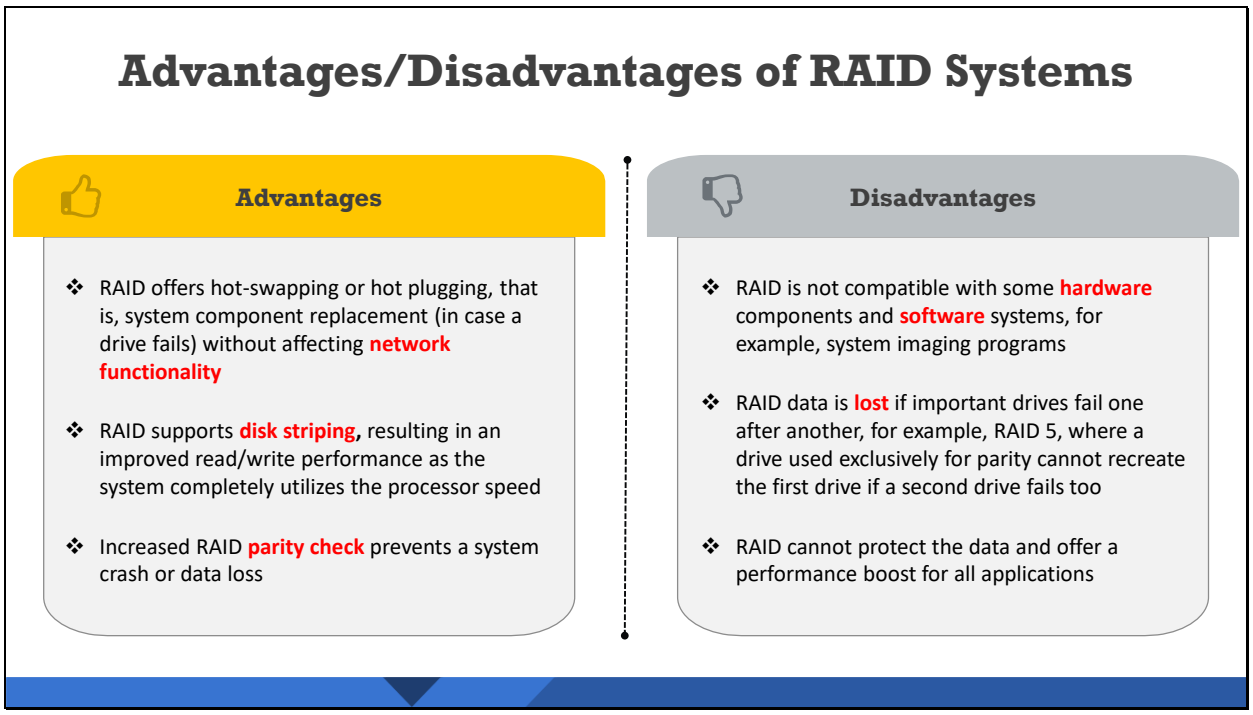
- **Competence:** This is defined by the amount of data stored. The storage capacity of disks depends on the chosen RAID level. The storage capacity need not be equal the size of the individual RAID disks.

All the RAID levels depend on the storage techniques listed below:

- **Striping:** Striping divides the data into multiple blocks. These blocks are further written across the RAID system. Striping improves the data storage performance.
- **Mirroring:** Data mirroring makes image copies of the data and simultaneously stores this data across the RAID. This affects fault tolerance and data performance.
- **Parity:** Parity uses a striping method to calculate the parity function of a data block. During a drive failure, the parity recalculates the function using a checksum method.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Advantages/Disadvantages of RAID Systems

Before RAID technology was introduced, many organizations used a single drive to store data. RAID technology is now found across all storage devices in an organization. Advantages and disadvantages RAID depend on the implemented level.

Advantages of RAID Systems

- **Performance and reliability:** RAID technology increases the read/write performance of the data on disks. The speed is much faster than when using a single drive as storage. It improves the performance by distributing the I/O. A RAID controller distributes data over several physical drives, ensuring that a single drive in the RAID system is not overburdened. RAID sustains the reliability of data even if a disk fails. Failed components can be replaced in a RAID system without shutting the system down. This feature is called hot swapping or hot plugging . The replacement process does not affect the network or how the other disks function.
- **Parity check:** Parity check is a process where the RAID system compares the data stored in a crashed system with the data stored in other disks. This check process is accomplished on all drives. The parity check is performed after mirroring the data. Regular parity checks detect the probability of a system crash, thereby preventing data loss.
- **Data redundancy:** A disk can fail anytime. Therefore, data redundancy is important for an organization. RAID provides enhanced data redundancy in case of a hardware failure.
- **Disk striping:** Disk striping improves the read/write performance of data. The data is divided into small chunks and spread over multiple disks. Depending on the

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

implemented RAID level, the data is divided into bytes, bits, or blocks. Data reading and writing can be done simultaneously on a RAID system.

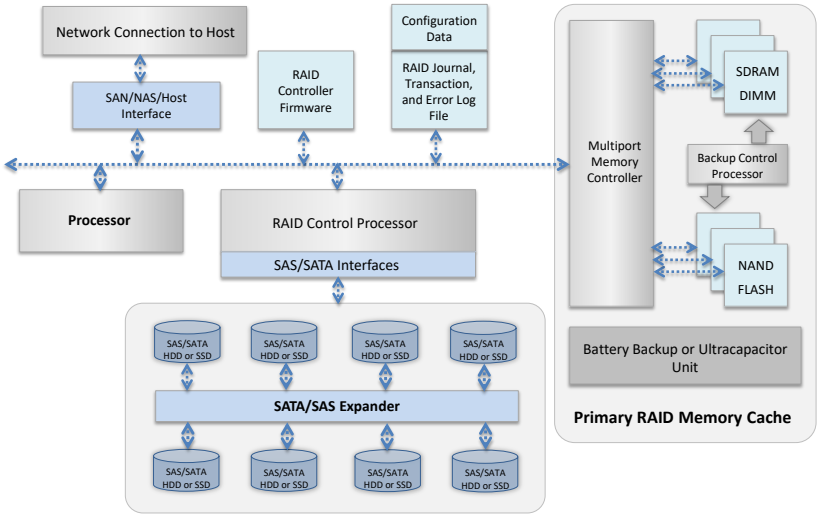
- **System uptime:** This metric detects the reliability and stability of a computer. System uptime defines the time till which a system can be left unattended without any assistance. Configuring RAID on a system helps enhance system uptime. A high system uptime in an organization signifies a high productivity.

Disadvantages of RAID Systems

- **Writing network drivers:** RAID technology is designed to be widely used on servers. A major disadvantage of RAID technology is the writing of all network drivers. RAID technology is complex, and this process can be time consuming.
- **Non compatibility:** Different systems support different types of RAID drives. Certain hardware or software components may not be compatible with the RAID drive configured on a server. This non compatibility may lead to the RAID not functioning properly. The compatibility between RAID drives, hardware, and software must be checked prior to configuring a system. RAID can protect data for all applications available on the network. For example, RAID is not compatible with system imaging programs.
- **Loss of data:** All RAID drives function in the same environment. They can become nonfunctional because of mechanical issues. Thus, the potential data loss increases if the disks fail one after another. When two drives fail at the same time, recovering the data from the disk becomes difficult. For example, RAID 5, where a drive used exclusively for parity cannot recreate the first drive if a second drive fails too.
- **Time consumed in rebuilding:** The increase in drive capacity has been much more than the increase in transfer speed. Recovering data from drives with a large storage capacity can be time consuming. In such scenarios, rebuilding a failed disk can also be time consuming. Increasing the number of drives does not help increase the data transfer speed.
- **Cost:** Implementation of RAID technology can be costly. Organizations need to hire consultants to sustain its performance. It also requires external RAID controllers and hard drives to function correctly, and this adds to the overall cost.
- RAID cannot protect the data and offer a performance boost for all applications.
- RAID should be maintained by commercial consultants.
- RAID configuration is difficult.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

RAID Storage Architecture



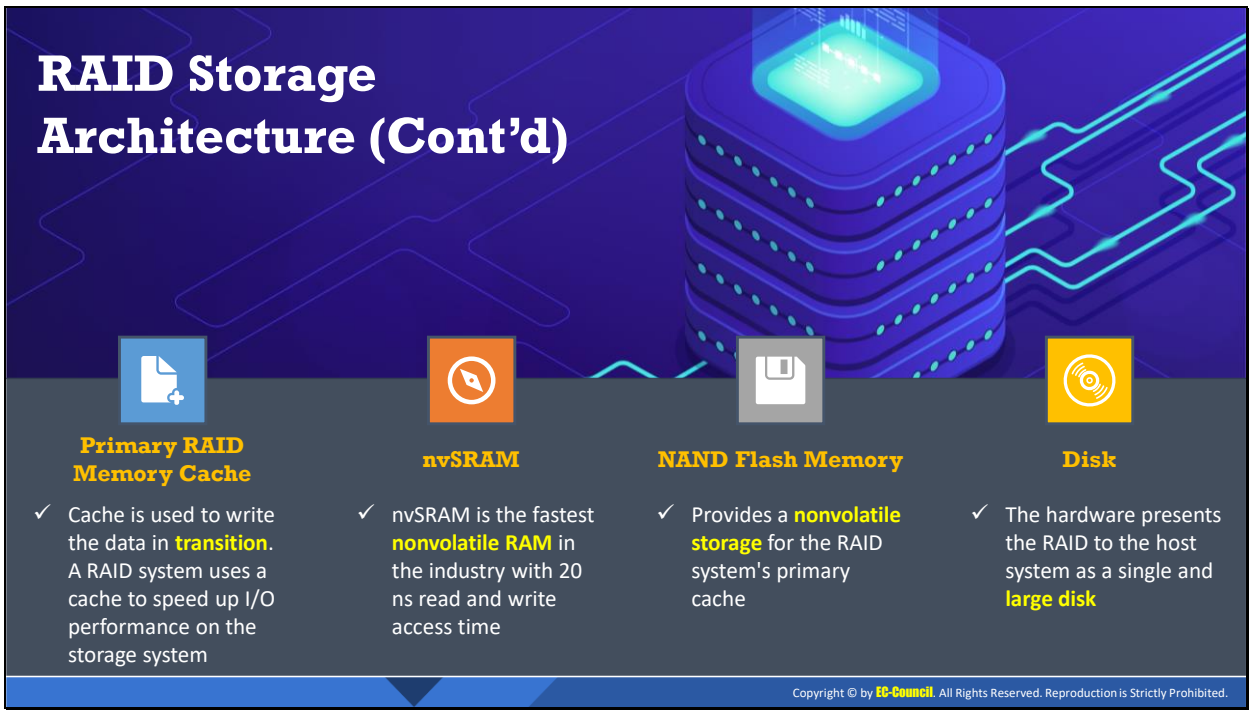
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

RAID Storage Architecture (Cont'd)

1. **RAID Controller**
   Manages an array of **physical disk drives** and presents them to the computer as logical units
2. **IDE, SATA, or SCSI Interface**
   Internal drives are connected using these **interfaces**; Connection to the server is also through one of these interfaces
3. **Multiport Memory Controller**
   Provides access to a memory bank, and helps achieve a **high efficiency** with random address accesses
4. **SDRAM**
   Dynamic random access memory (DRAM) that is **synchronized** with the CPU clock speed

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



RAID Storage Architecture

The RAID architecture depends on two principles: redundancy and parallelism, providing a wide range of storage options with better performance and freedom from disk failures. The Internet's increasing footprint has led to an increase in the use of RAID systems because of their high data storage capabilities and management systems. Many available RAID implementations depend on the following factors: parallelism, duplication, and redundancy.

In a RAID architecture, a switch receives the data from servers connected to the network. The switch then sends the data to the processor at a later stage. The processor transfers the received data to a RAID controller. The RAID controller may be implemented either as a hardware using a RAID-on-Chip (ROC) or in a software. The ROC can contain the I/O interfaces, a processor, a host interface, and a memory controller. The ROC is installed directly in a motherboard using an expansion card, or in an external drive enclosure.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

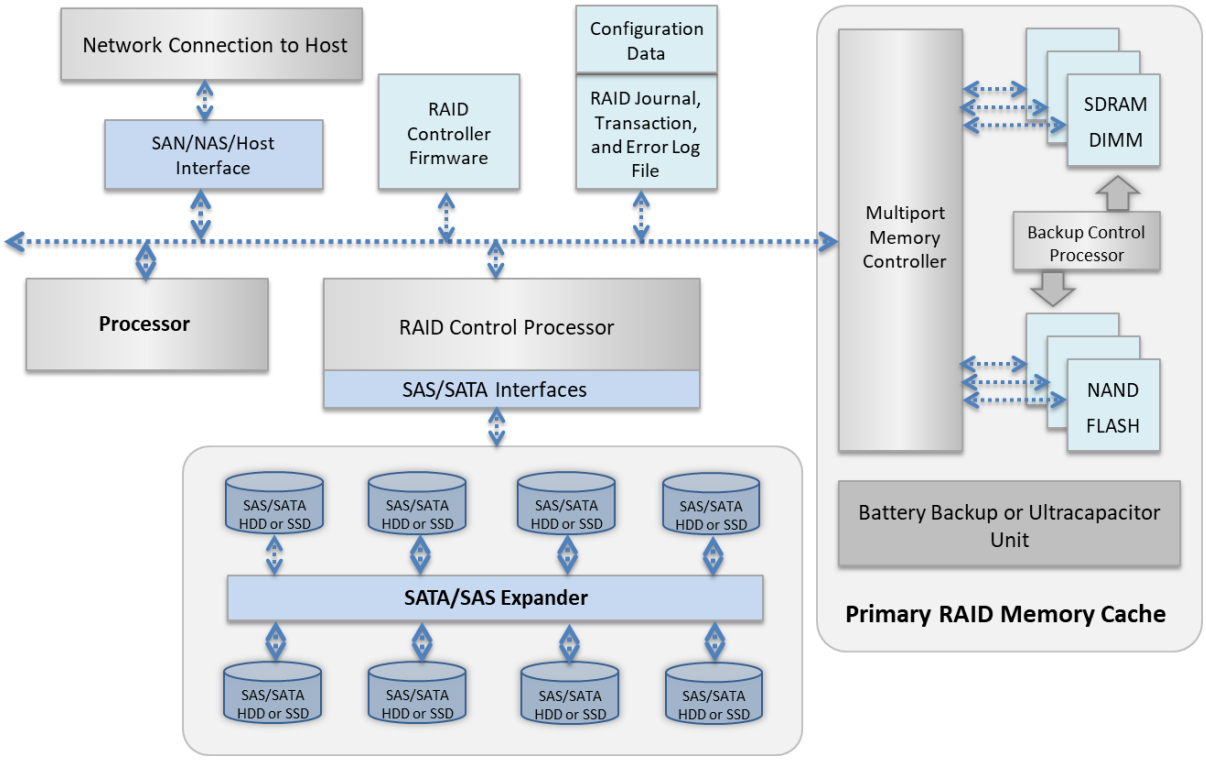


Figure 11.29: RAID storage architecture

The RAID storage architecture outlines how the RAID server functions. The processor controls the entire functioning of the drive arrays and interfaces. It provides flexible and high-performance functions. The architecture in the figure above shows a RAID system can depend on hard disk drives (HDDs) as well as SSDs. The processor requires DRAM and NAND flash memory. The NAND flash memory provides a nonvolatile storage to the primary RAID memory cache.

A battery backup or an ultra-capacitor unit in the primary RAID memory cache is helpful when the RAID control processor suffers from a power failure. In this scenario, the battery backup independently copies the DRAM contents to the NAND flash memory. A battery backup is an inexpensive alternative during a power loss. The architecture shows the requirement of a nonvolatile memory in the RAID controller firmware, RAID journal, and transaction and error log files.

Major Components of a RAID Architecture

- **RAID controller**: This is either hardware- or software-based and contains the HDDs or solid state drives as a single logical unit. A RAID controller has the permission to access multiple copies of files present on multiple disks, thereby preventing damage and increasing the system performance. In a hardware RAID, a physical controller manages the RAID array with a controller in the form of a PCI card that supports SATA or SCSI. A software RAID works similarly to a hardware RAID, except that their performance is lower than the former.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **Primary RAID memory cache**: The RAID controller has a direct access to the cache memory, enabling faster read and write access to the storage system. The cache is used to store the changing data. The cache memory is bigger in size and uses high-speed SDRAMs. A normal cache memory has a write cache and a separate read cache. The read cache decreases the latency of the read process. There are two types of write cache memories:
  - **Write-through mode**: This bypasses the cache memory and writes the data directly to the disk after the host sends it. The host sends the next data item after receiving a confirmation that the writing process has been completed.
  - **Write-back mode**: Data sent from the host is written to the cache memory. The host may perform other actions while the RAID controller transfers data from the cache to the disk drive. The RAID controller acknowledges the write process to the host soon after writing the data to the cache. Issues may arise if a RAID controller sends an acknowledgment before the data has been completely written on the disk.
- **IDE, SATA, or SCSI interfaces**: IDE, SATA, or SCSI are device cables that transmit read/write signals to and from the drive. These are mostly used for internally connecting the drives. Moreover, servers are connected using these interfaces.
  - **IDE**: Integrated drive electronics (IDE) allows the connection of two devices per channel. It is normally used for internal devices as the cables are large and flat.
  - **SATA**: Serial ATA deals with hot plugging and serial connectivity. The hot plugging technique may be used to replace computer components without shutting down the system. SATA enables only one connection per connector and is not flexible for industrial purposes.
  - **SCSI**: Small computer system interface (SCSI) allows multiple devices to be connected to a single port at the same time. SCSI uses a parallel cable for attaching internal and external devices.
- **nvSRAM**: Nonvolatile SRAM, or nvSRAM, has a faster read and write process (20 ns read and write access time) because of the presence of a standard asynchronous SRAM interface. nvSRAM ensures adequate data storage capabilities without the need for a battery during a shut down. nvSRAM is best used in applications that require high speed and nonvolatile storage at a low cost, such as in the medical industry. nvSRAM backups the data even in the event of a power failure.
- **Multiport memory controller**: An MPMC provides access to memory for up to eight ports. A memory controller can be present as a separate chip or as an integrated memory. It provides access to a memory bank, and helps achieve a high efficiency with random address accesses.
- **NAND flash memory:** Flash memory is a storage medium designed from electrically erasable programmable read-only memory (EEPROM). NAND and NOR are two types of flash memories. It provides a nonvolatile storage for the RAID system's primary cache.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

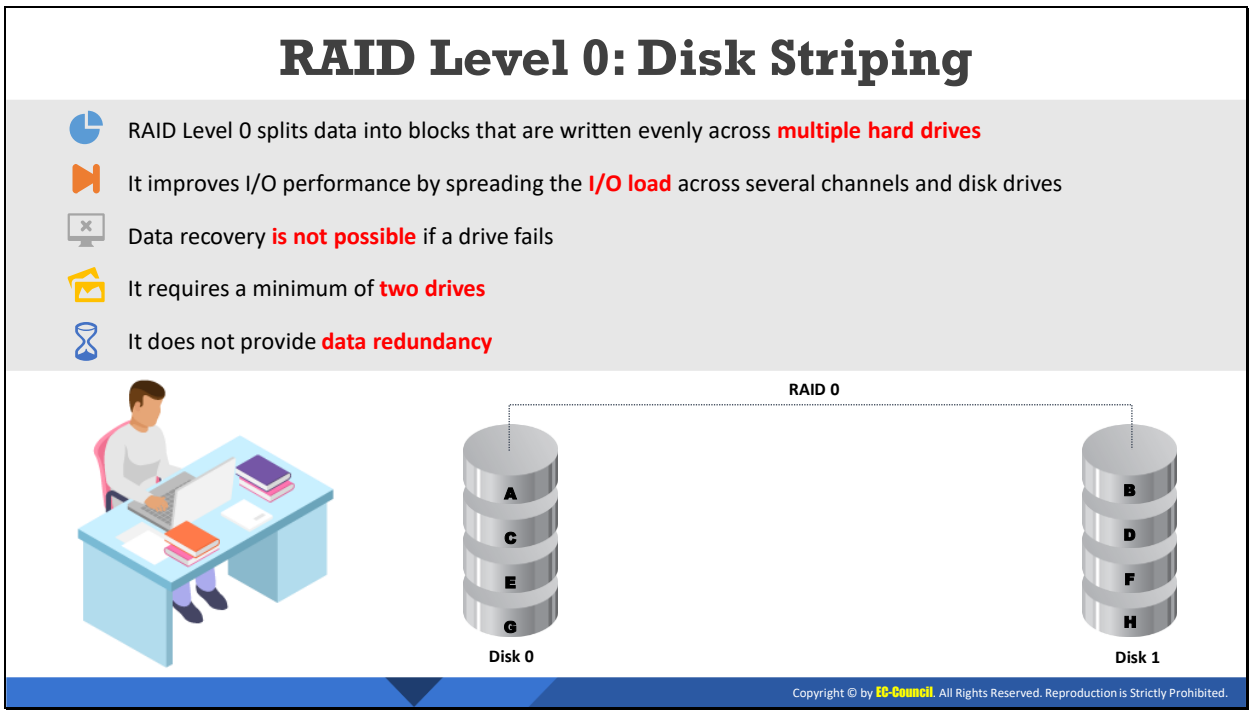
https://t.me/learningnets

Its primary aim is to reduce cost and increase capacity. It does not require power to retain the data. It can improve its read-write cycles with reduced voltage demands.

- **SDRAM:** Synchronous dynamic random access memory or synchronous DRAM (sDRAM) is a memory that is synchronized with the processor's clock speed. This increases the number of instructions the processor can process. SDRAM speed is measured in Mega Hertz (MHz). It is divided into several sections called banks that allow the device to operate on several memory access commands simultaneously.
- **Disk:** The hardware presents the RAID to the host system as a single and large disk.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



RAID Level 0: Disk Striping

Depending on the requirement of your organization, you can choose any RAID level. RAID levels are based on performance, fault tolerance, or both.

RAID 0 deals with data performance. In this level, data is broken into sections and written across multiple drives. The storage capacity of RAID 0 is equal to the sum of the disks' capacities in the set. RAID 0 does not provide fault tolerance. It requires a minimum of two drives. It does not provide data redundancy. A failure of one disk can lead to the failure of all disks in a level 0 volume. The probability of recovering data from a RAID level 0 is minimal.

The data distribution in a RAID level 0 is equal among all the disk sets, resulting in high performance. With concurrent high performance, the throughput of the read and write operations on multiple disks is equal to the throughput of the array of disks. Increased throughput is an advantage of RAID 0, considering that data recovery is not available. Software and hardware RAID controllers support RAID 0, helping boost server performance.

Example: Assume that the IT infrastructure has a hard disk with high performance. The data in the hard disk is transferred at a remarkably high speed. All the large and critical files are stored in this disk. However, if this disk fails, the entire contents of the files will be affected, leading to the unavailability of the data. It is advisable not to store any critical data in a RAID level 0.

Advantages of RAID Level 0

- **Read and write performance:** RAID level 0 has a good read and write performance. The performance is even better when the controller supports independent reads and writes to different disks in the array.
- **Cost:** RAID level 0 is more cost effective than the other RAID levels.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **Implementation:** Is easy to implement as the data is divided in a sequential set of blocks. There is no storage loss as the maximum capacity is utilized.

Disadvantages of RAID Level 0

- **No redundancy:** With no data redundancy, data loss is greater.
- **Noncritical data:** Data that is not critical to the organization can be stored on RAID level 0. This level does not use mirroring. Recovery is not possible if critical data is lost on RAID level 0.
- **Unreliable:** If one disk fails, the entire network will be affected.

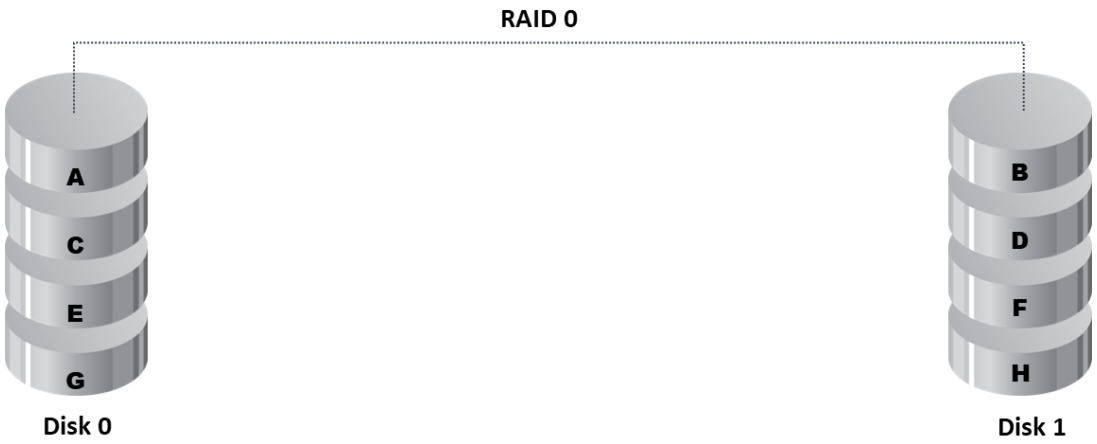
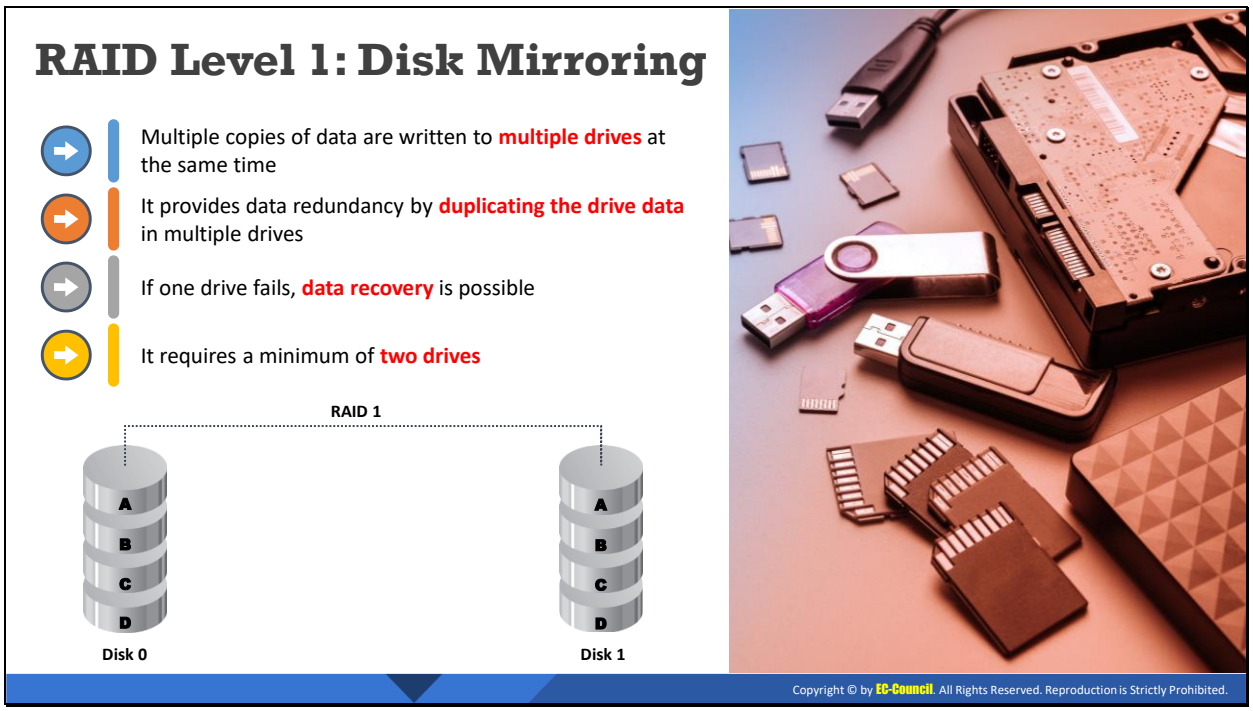


Figure 11.30: RAID level 0

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



RAID Level 1: Disk Mirroring

A typical RAID 1 contains an exact copy of the data on two or more disks. RAID 1 writes data on multiple drives and multiple mirror drives at the same time. The failure of one drive does not affect the data on other drives. This allows data retrieval from the mirror drive. Similar to RAID 0, RAID 1 provides no parity, stripping, or spanning of disk space across multiple disks. RAID 1 can be used in accounting, payroll, and other financial applications.

RAID 1 is suitable in environments where read performance matters more than write performance. RAID 1 has improved read performance because the data in a disk can be read at the same time simultaneously.

RAID level 1 provides data reliability in case of a disk failure as it can still provide access to the same data mirrored on other disks. In a RAID 1 hardware implementation, a minimum of two disks are required. In a software RAID 1, data can be copied to a disk volume. RAID 1 reduces the total disk capacity by half.

Example: If a RAID 1 server is configured with two 4 TB drives, the storage capacity will be 4 TB and not 8 TB.

The drive that accesses the data first will service the request. The write throughput in RAID 1 is always slower because every drive needs to be updated. Thus, its performance is limited by the slowest drive. It is only as fast as its slowest drive. RAID 1 will continue to function as long as there is at least one working drive.

Advantages of RAID Level 1

- **High read performance:** Because there are two disks, the read performance is higher in a RAID level 1 system. Data can be read simultaneously while being written on the other disk. Thus, the redundancy is excellent.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

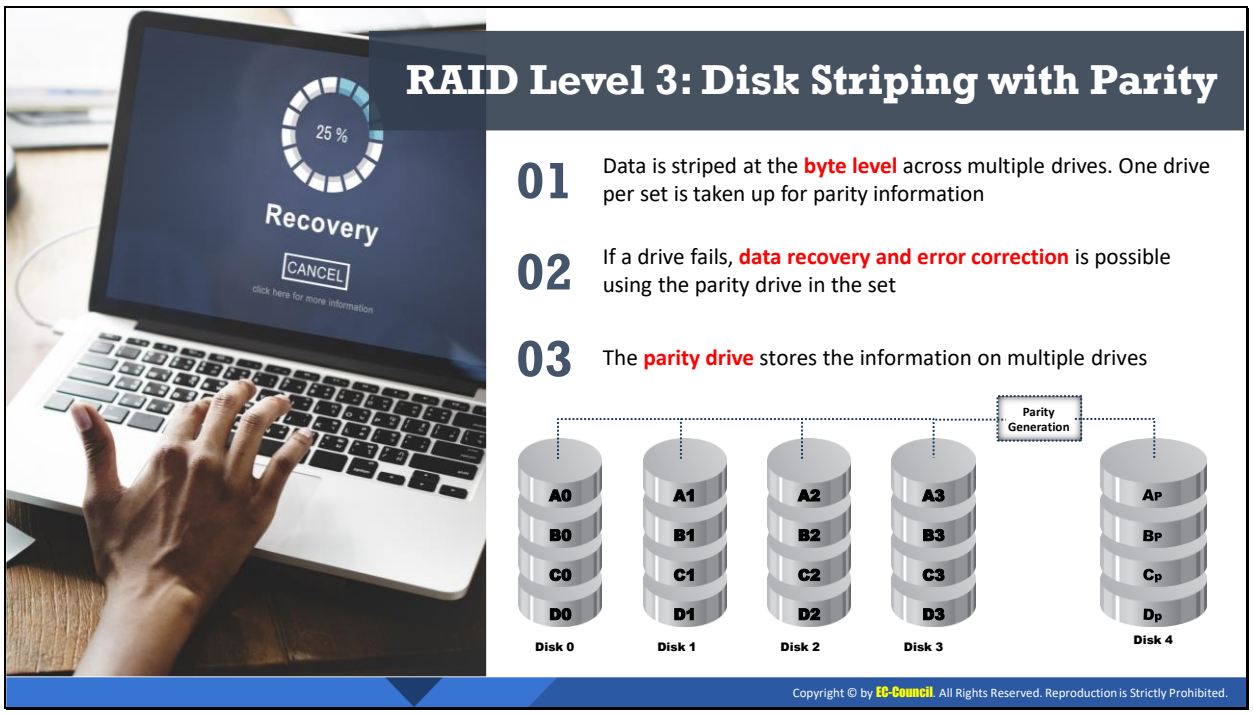
- **Compatibility:** RAID 1 is compatible with hardware and software RAID systems, including controllers.
- **Reliability:** The mirroring feature in a RAID 1 ensures the data will be available, making it more reliable than a RAID level 0.

Disadvantages of RAID Level 1

- **Capacity:** RAID level 1 undergoes duplexing, which needs twice the amount of disk space for storage.
- **Hot swapping unavailable:** If a disk fails to run, it cannot be replaced while the server is still in operation. This is called hot swapping. RAID level 1 does not support hot swapping.

Figure 11.31: RAID level 1

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



RAID Level 3: Disk Striping with Parity

RAID level 3 is disk striping with parity. It uses striping and parity as its main features to store data. To implement a RAID level 3 system, a minimum of three disks are required. The data is stored on multiple drives at the byte level. This RAID level dedicates one drive to store the parity information. The byte level division allows the drives to work simultaneously. At any point in time, either a read operation or a write operation can take place. RAID 3 is a good choice for specialized databases or single-user systems.

The RAID level 3 has a high transfer data rate along with data security. It can perform data recovery and error correction by calculating an exclusive OR (XOR) of the information recorded on the parity drive.

Advantages of RAID Level 3

- **High throughput:** RAID level 3 provides a high throughput for read and write operations for large data transfers.
- **Resistant:** This RAID level is resistant to disk failures and breakdowns.

Disadvantages of RAID Level 3

- **Complexity:** Installation and configuration of a RAID level 3 system is complex. Its implementation necessitates a larger number of resources.
- **Slow performance:** Random operations affect its performance, thereby reducing its speed.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

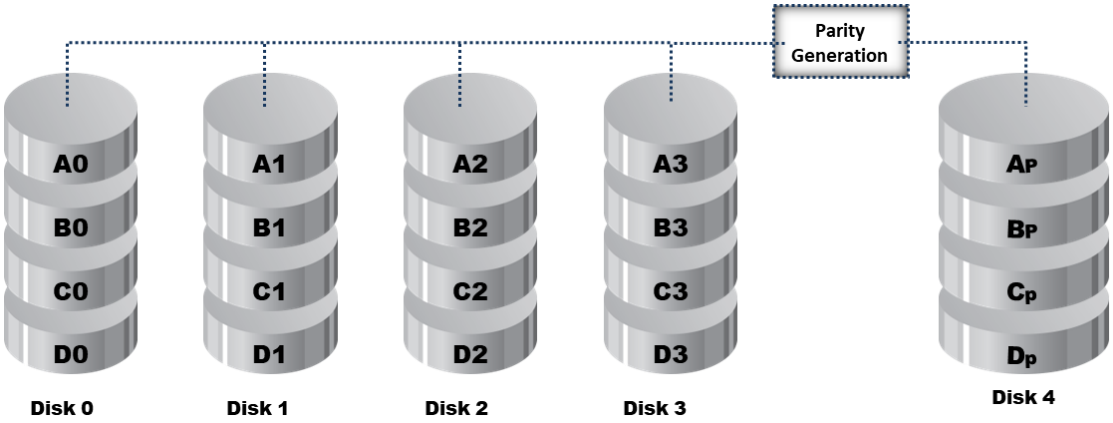
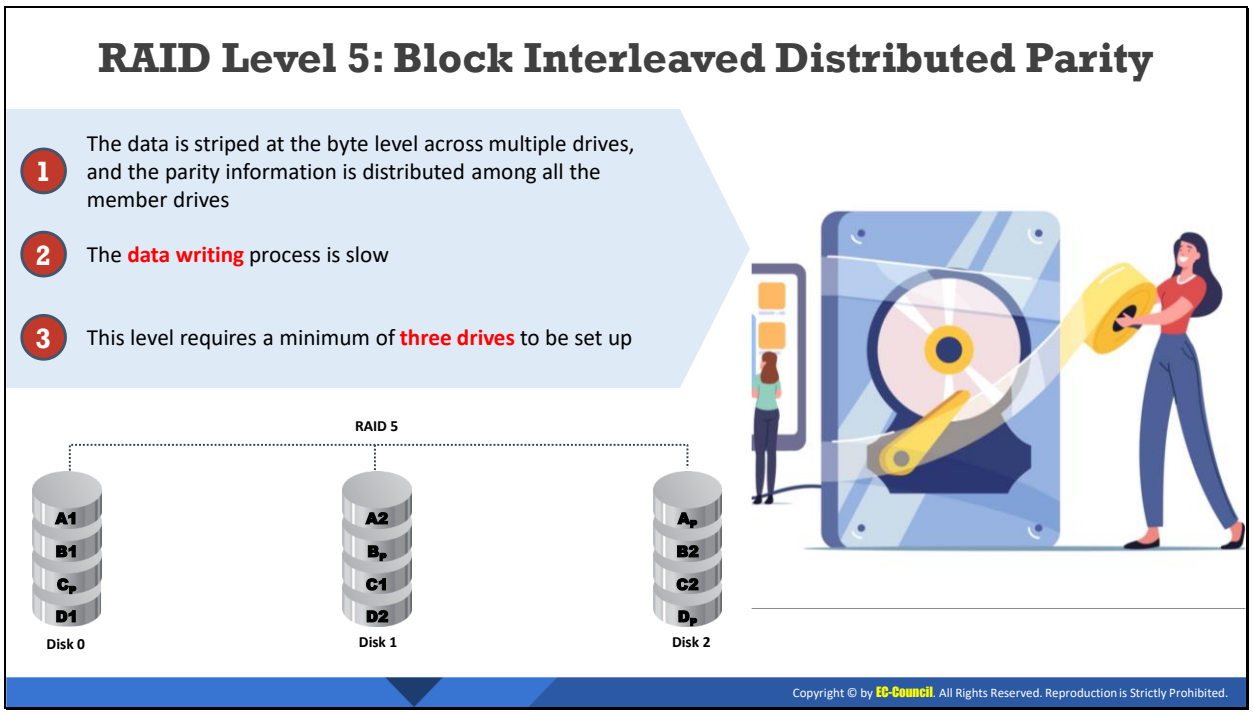


Figure 11.32: RAID level 3

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



RAID Level 5: Block Interleaved Distributed Parity

RAID level 5 involves a block-interleaved distributed parity; it includes a block-level striping with a distributed parity. The parity information is distributed among all drives except one. The data chunks in a RAID level 5 system are larger than the regular I/O size, but they can be resized. To prevent data loss following a drive failure, data can be calculated from the distributed parity.

The RAID 5 needs at least three disks; however, more than three disks can be used for a better performance. RAID 5 is not a good choice for write operations on the system. Rebuilding the RAID 5 array following a disk failure takes a long time. The performance can be degraded when the array is being rebuilt, making it vulnerable to additional disk failures. This level offers significantly better read performance as the disks independently process the data requests.

RAID 5 is most often found in file and application servers, database servers, along with web, email, and news servers.

Advantages of RAID Level 5

- **Read data:** Among all RAID levels, level 5 has the highest read data transaction rates.
- **Withstand failure:** RAID 5 can withstand the failure of a single drive and is not affected by the loss of data.
- **Hot swapping:** In case of a disk failure, the failed disk can be replaced with a new one, without a server shutdown.

Disadvantages of RAID Level 5

- **Slow write operation:** Servers built using RAID 5 suffer from performance issues with write operations, and these can eventually result in reduced speeds.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Example: Employees accessing a database on a RAID 5 server will reduce the server's production time.

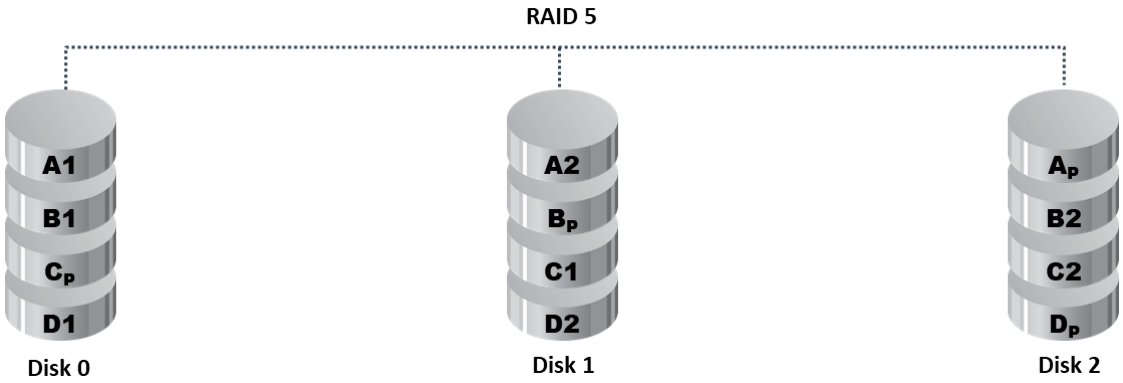
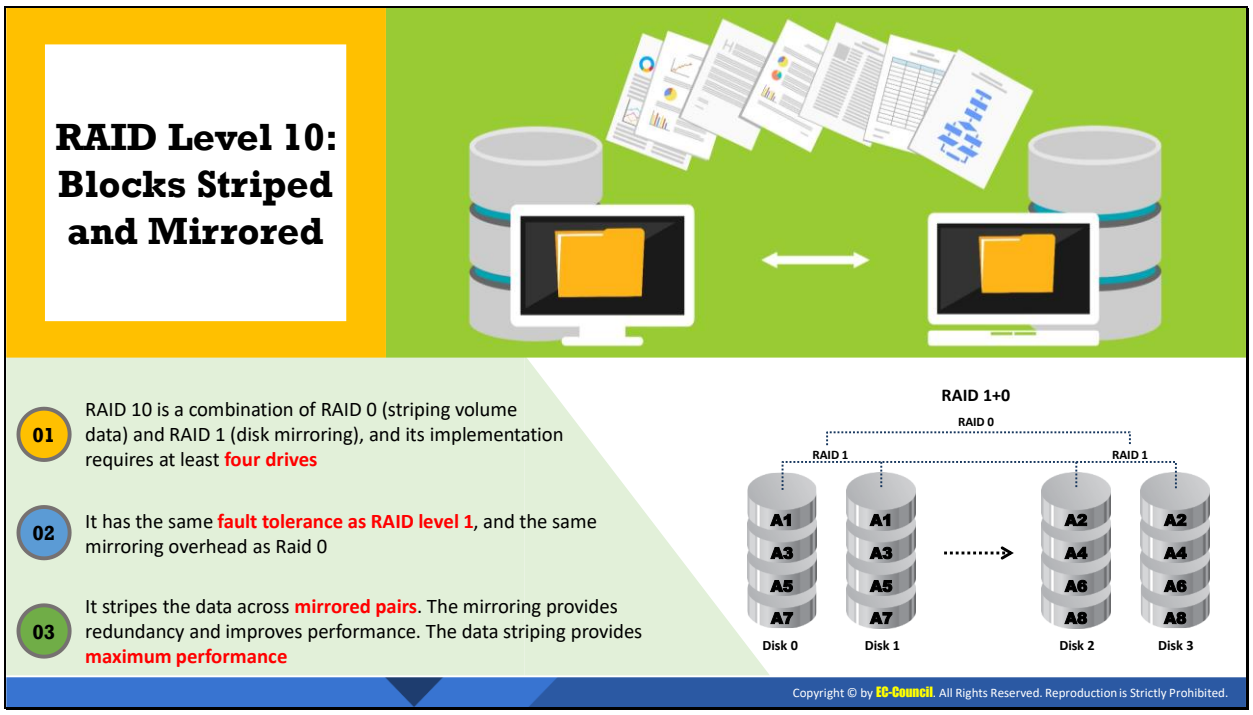


Figure 11.33: RAID level 5

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



RAID Level 10: Blocks Striped and Mirrored

RAID level 10 includes disk striping and mirroring in a nested hybrid RAID level. It is a combination of RAID level 1 and RAID level 0. It is also called as a "stripe of mirrors." This level can symbolically be represented as RAID 1+0 or RAID 10. RAID 10 includes the mirroring of RAID 1 without parity and the striping of RAID 0. The performance of RAID 10 is higher than a RAID 1. RAID level 10 has the same fault tolerance as RAID level 1. It requires a minimum of four drives for its operation. RAID 10 is a great choice for database servers, web servers, email servers, etc., and can be implemented on hardware or software. The mirroring provides redundancy and improves performance. The data striping provides maximum performance.

Advantages of RAID Level 10

- **Improved I/O operations:** With a combination of RAID levels 1 and 0, it provides improved I/O operations.
- **Better throughput:** Compared with other RAID levels, RAID 10 provides better throughput and higher latency.
- **Efficient write operations:** The write operations are efficient in this level. Therefore, RAID 10 is often implemented on database servers and other servers that perform write operations.

Disadvantages of RAID Level 10

- **Expensive:** RAID 10 is expensive than other RAID levels as it requires twice as many disks.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

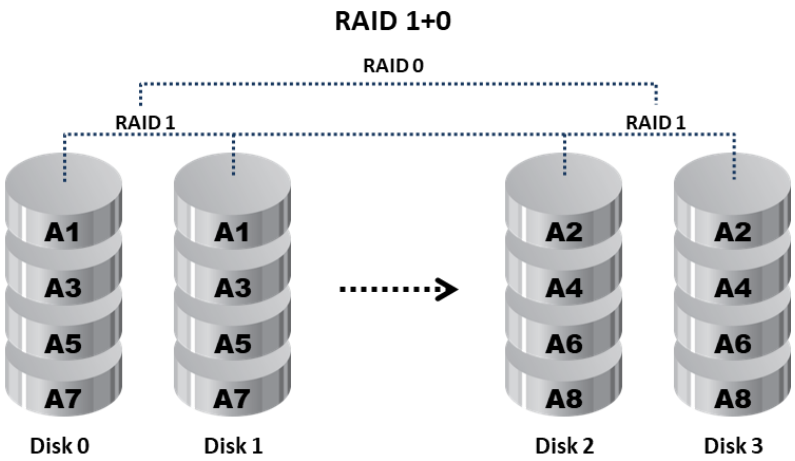
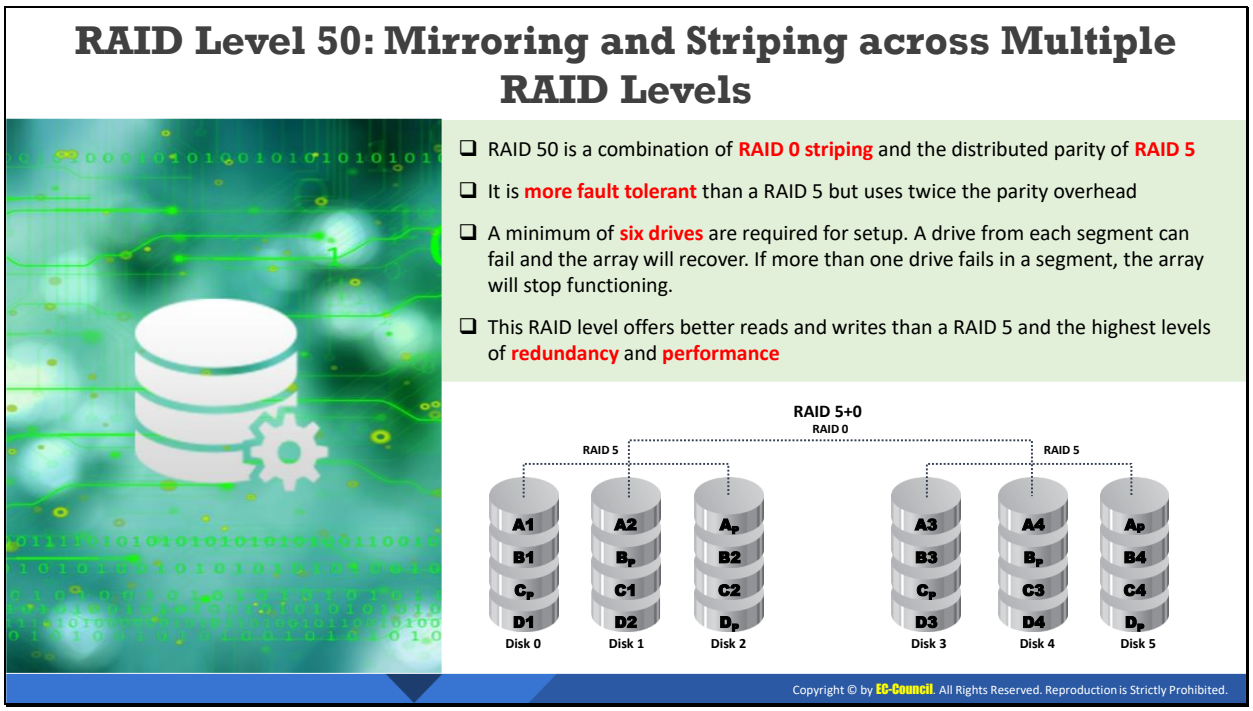


Figure 11.34: RAID level 10

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



RAID Level 50: Mirroring and Striping across Multiple RAID Levels

RAID level 50 includes mirroring and striping across multiple RAID levels. This level is a combination of a level 0 block-level striping and a level 5 distributed parity. The configuration of RAID level 50 requires a minimum of six drives. This level undergoes a hot swapping process when a disk fails. A drive from each segment can fail and the array will recover. If more than one drive fails in a segment, the array will stop functioning.

RAID 50 is an improvement over RAID 5, specifically for its write operation and fault tolerance. RAID level 50 can be implemented on servers that run applications requiring higher fault tolerance, capacity, and random access performance. This level offers data protection and faster rebuilds than a RAID 5 system. A failed disk in a segment only affects that segment and not the entire array. Only that segment is then rebuilt. The rest of the array functions normally.

Advantages

- **Security:** The data stored in a RAID 50 is more secured than in a RAID 5. With a larger storage capacity, this level offers better security than RAID 5.
- **Nondegradable:** With the use of a minimum of six drives in the configuration, failure of one disk does not impact the server function on this level.
- **Read and write performance:** The read and write performance of RAID level 50 is far better than RAID level 5.

Disadvantages

- **Controller:** Only a sophisticated controller can handle RAID level 50.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

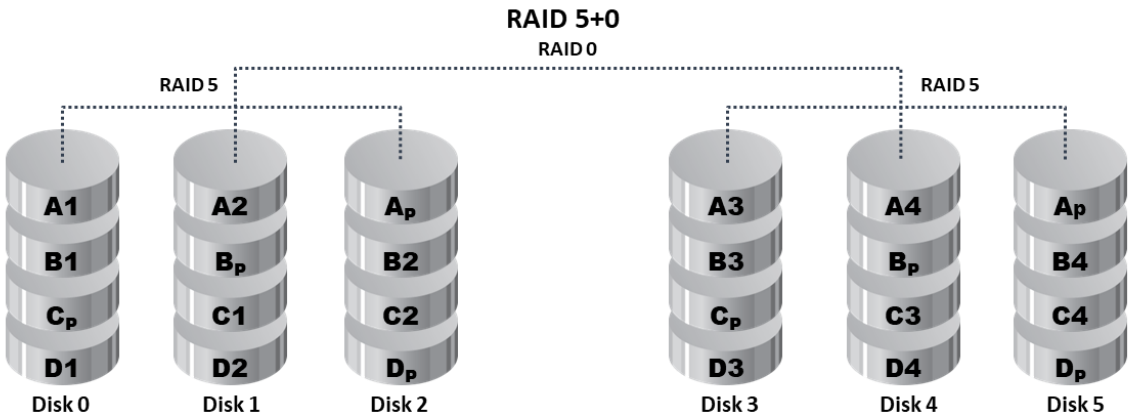
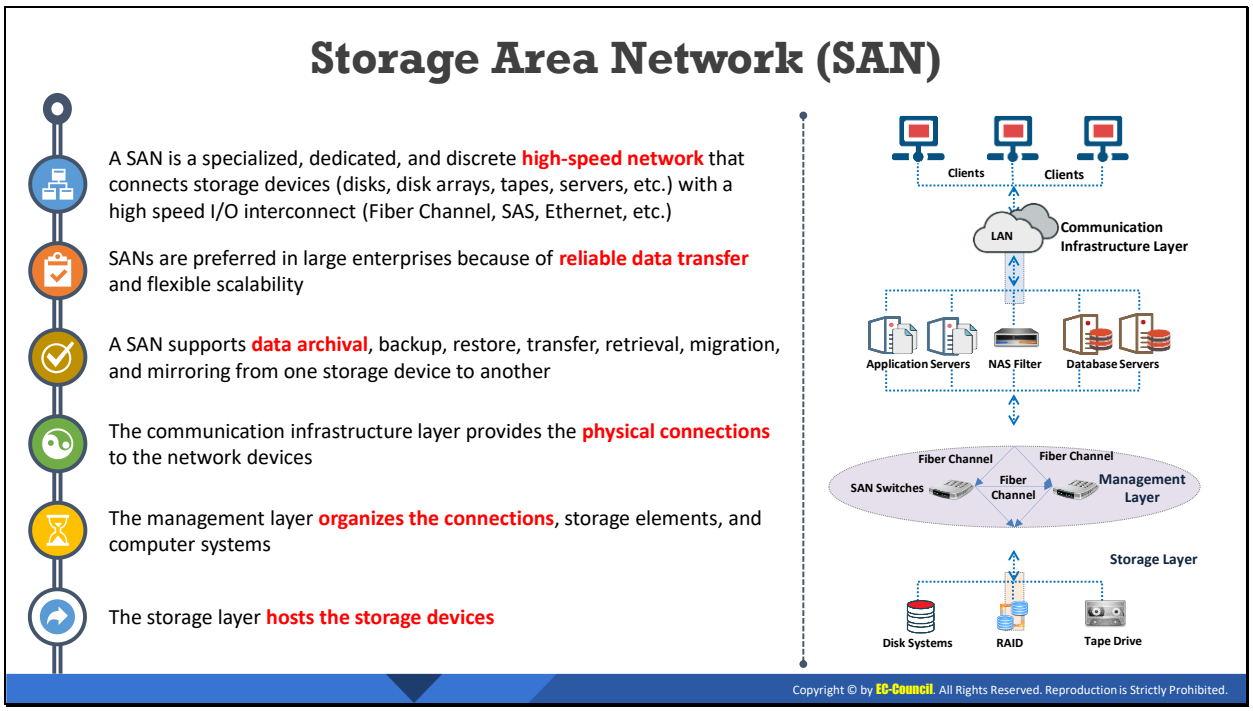


Figure 11.35: RAID level 50

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Storage Area Network (SAN)

A storage area network (SAN) is a high performance network that interconnects storage devices with multiple servers. The role of a SAN is to transfer stored resources available on the common network and reorganize them on an independent and high-performance network. This helps the servers to share their storage across the network. Primarily, a SAN enhances storage devices such as tape drives, disk drives, file servers, RAID, etc. A SAN implementation makes disk maintenance controllable and easier. The implementation needs a cable, a switch, and host bus adapters. Each storage system on the SAN must be interconnected, and in case of a physical interconnection, the bandwidth should support extreme data activities.

We know that systems in a network connect to storage devices. However, a SAN implementation is necessary to ensure that all systems in a network are connected to each available storage device on the network. SAN allows these systems to take the ownership of storage devices; systems can exchange the ownership of storage devices among themselves.

Understanding Storage Sharing

The working of a SAN depends on client-server communication. Every organization has multiple servers that are connected to the systems.

Example: If computer A needs some data from computer B, it will need a copy of the data from the server to which computer B is connected. This can be done through file transfer, inter-process communication, and backup. Although the data is transferred from computer B to computer A, it is possible that computer A may encounter untimely data errors, an expensive transfer between the two servers, or other operational processes. SAN architecture is the perfect solution for this issue. In SAN architecture, all servers are connected to storage devices such as tape drives, RAIDs, disk systems, etc. through a fiber channel. Thus, instead of

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

communicating with computer B for the data, computer A can directly get a copy of the data from the storage devices connected to the servers. For this process to be successful, data storage devices act as a common access point for all the servers.

SAN storage sharing eliminates the scheduling of data transfers among servers. It reduces the cost of data transfer among servers. Storage devices help in timely transfer of data. SAN storage offers only block-level operations that do not provide file abstraction.

However, if the file systems are structured on top of SAN, file access is provided which is known as a SAN file system.

Now-a-days, in large organizations, SAN is a storage pool for servers that are connected via a network. The fiber channel is now replaced by iSCSI, which has become the choice of many mainstream organizations. Whatever be the size of the organization, SAN has become a consolidation of workloads in the network.

A SAN supports data archival, backup, restore, transfer, retrieval, migration, and mirroring from one storage device to another. The communication infrastructure layer provides the physical connections to the network devices. The management layer organizes the connections, storage elements, and computer systems. The storage layer hosts the storage devices.

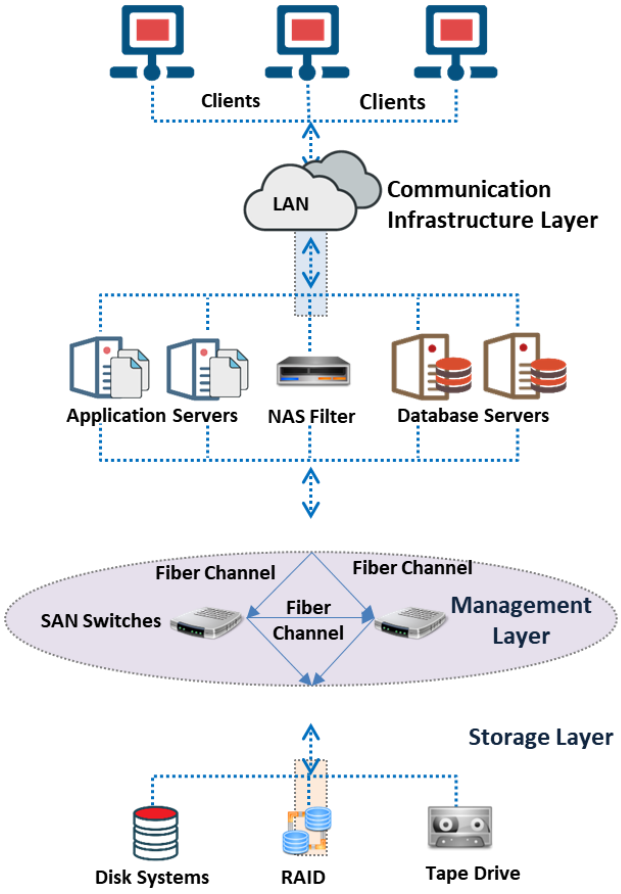
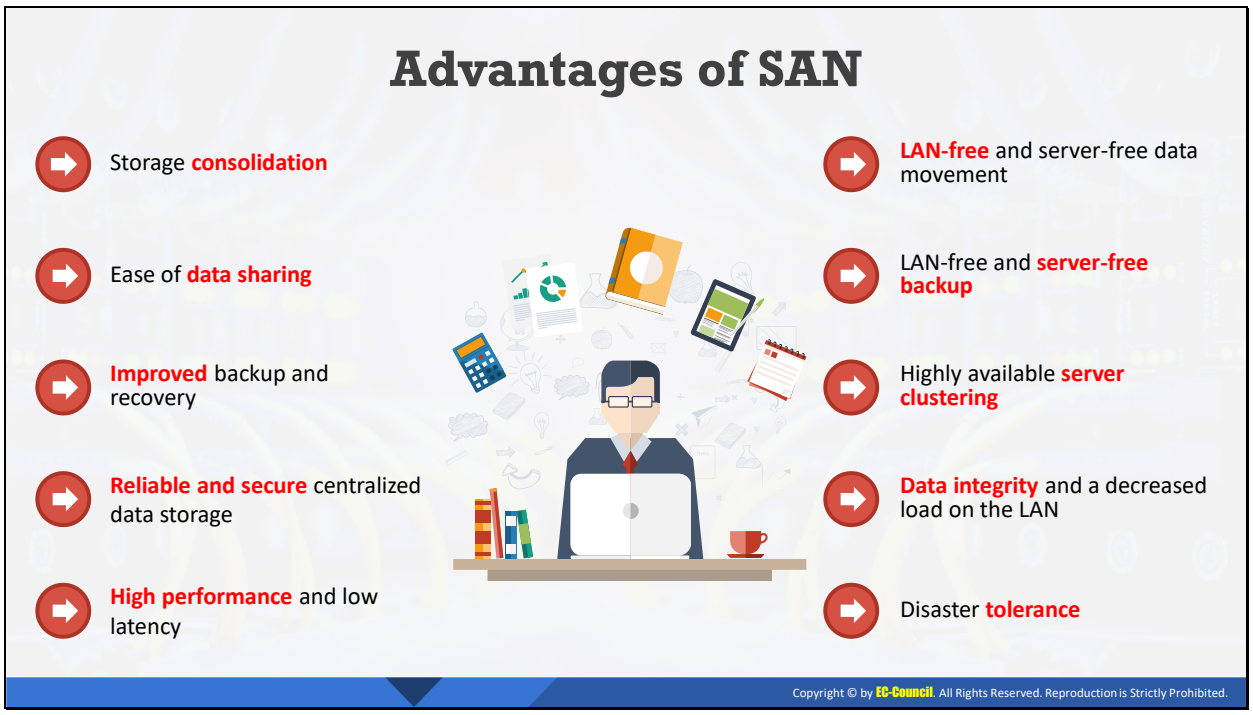


Figure 11.36: SAN

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Advantages of SAN

With rapidly developing technologies and increasing data volumes, organizations need a storage device that can fulfill and handle their needs. The below-mentioned advantages of SAN help in its deployment in an IT infrastructure.

Advantages

- **Capacity:** SAN performance is directly proportional to the network type. A SAN allows unlimited sharing of data, regardless of the storage capacity. Its capacity can be extended limitlessly to thousands of terabytes.
- **Easy sharing:** SAN data is easily shared between systems as it maintains an isolated traffic. The traffic does not interfere with the normal user traffic, thereby increasing data transfer performance.
- **Fast backup:** A data mirror copy can be created instantly. These mirror images can be used as a backup whenever required.
- **Reliability and Security:** If a SAN is configured correctly, the data is secured. Chances of device intrusion is minimal. Reliable and secure centralized data storage.
- **Productive:** A SAN is scalable; adding a new disk to the network does not stop the SAN's productivity. When adding a new hard disk, a reboot or shut down is not required.
- **Availability of applications:** The algorithms in a SAN storage array offer data protection. This results in the availability of applications at all times.
- **Bootable:** A SAN can run a server without a physical disk, and it can be booted by the SAN. This feature permits access to all page files and applications.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **Distance connectivity:** For better security, storage devices can be kept at an isolated location. One of the features of a SAN is that it can connect with devices up to a distance of ten kilometers.
- **Recovery:** A SAN is the most reliable data recovery option. Even when the servers are offline a SAN remains available.
- **Effective utilization:** A SAN is an appropriate option for storage space than local disks. If a system requires more storage, a SAN dynamically allocates the required space. This process is similar to virtual machines.
- **Integrity:** Increased data integrity and a decreased load on the LAN.
- LAN-free and server-free data movement and backup
- Effective disaster tolerance

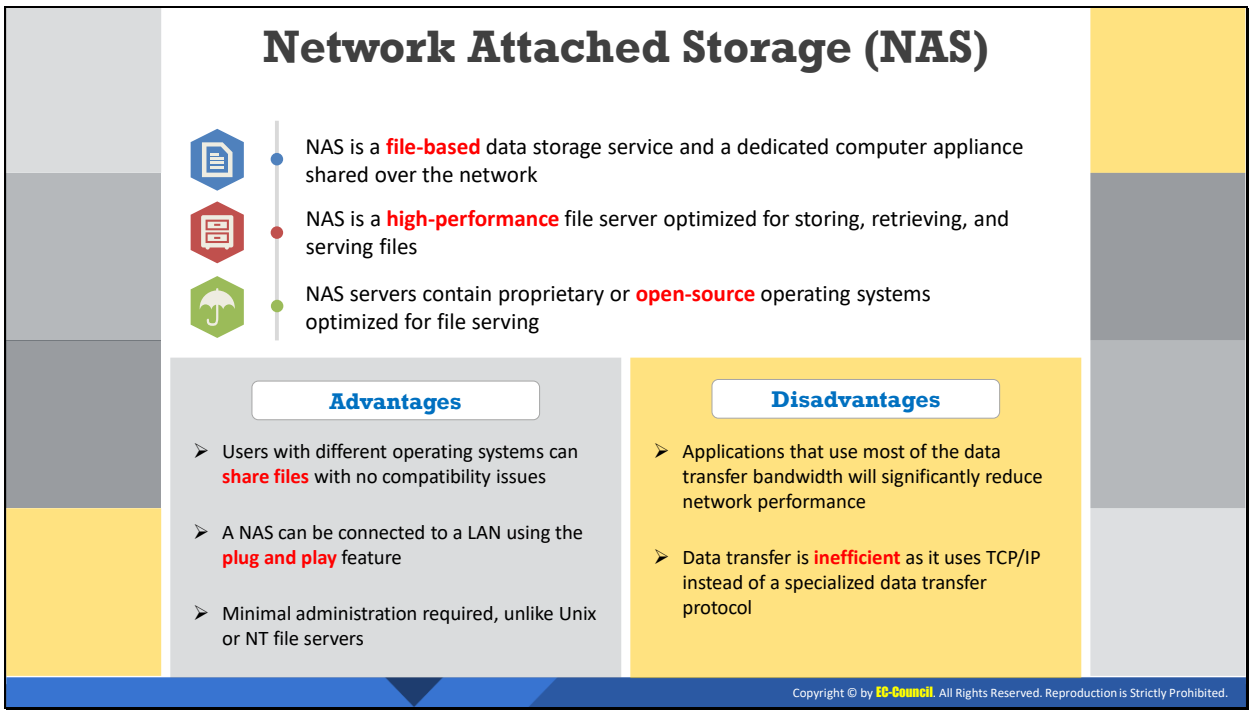
The implementation of a SAN is beneficial to an organization, especially when considering budget constraints, availability, and employee expertise.

Disadvantage

- **Very costly:** The implementation cost of a SAN can significantly exceed the available budget. A SAN is an investment and should only be implemented if it meets the goals of the organization.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Network Attached Storage (NAS)

NAS is a storage device connected to a network. It stores and retrieves data from a centralized location. NAS provides a dedicated shared storage space for a local area network. Implementing a NAS eradicates the server file sharing process on the network. The NAS contains one or more logically arranged storage devices. NAS offers file storage through a standard Ethernet connection.

NAS devices do not use an external device management, and they are operated through a web-based utility. Since it resides on every node on the LAN, it has its own IP address. NAS is similar to a file server. NAS devices are scalable, vertically as well as horizontally. A NAS implementation is accomplished using large and clustered disks.

NAS has evolved from supporting virtualization to data replication and multiprotocol access. A clustered NAS is one such example of the NAS evolution. In a clustered NAS infrastructure, access is provided to all files, irrespective of their physical location. It does not require a closed-source operating system such as Windows. Certain devices run on a stripped down OS such as FreeNAS, or any other open-source solutions.

NAS devices are in high demand in small enterprises because of their effectiveness, low cost, and scalable storage capacity. They are classified into three types based on the number of drives, drive capacity, and scalability.

Advantages

- **Accessibility:** A NAS system stores data as files and is compatible with CIFS and NFS protocols. Multiple users can access the files simultaneously using an Ethernet network. Computers in a shared network can access the data either through a wireless or a wired connection.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

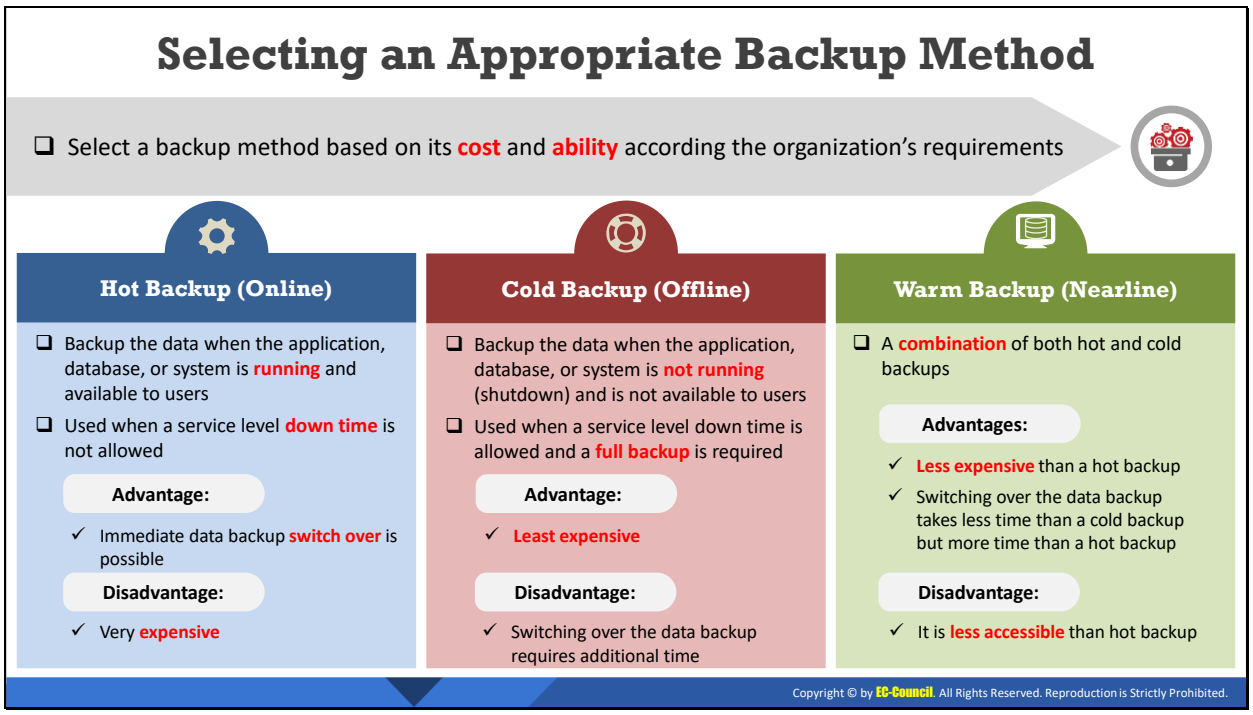
- **Storage:** NAS deployment in a network increases the amount of storage available to the other systems. A NAS system can store up to 8 TB data. A NAS is most appropriate for storing large applications or video files.
- **Efficient and Reliable:** NAS assures an efficient transfer of data and reliable network access. If a system in a network fails, the functioning of other systems is not affected. A NAS server can also be created to give users the ability to access large files or applications.
- **Automatic backup:** Certain NAS devices are configured with an automatic backup feature. The data is available on the user system as well as on the server hard drive. Changes made on the user system are reflected on the server hard drive as well. Automatic backup is not time consuming and assures the security of data.
- **Compatibility:** Users with different operating systems can share files with no compatibility issues.
- A NAS can be connected to a LAN using the plug and play feature.
- Minimal administration required, unlike Unix or NT file servers.
- Centralized usage, and reduced cost of backup and maintenance than a SAN.
- Faster response than direct attached storage (DAS).

Disadvantages

- **Consumption:** NAS shares the network with other host machines, and this tends to consume a larger amount of network bandwidth. For remote NAS systems, the data transfer performance will depend on the available bandwidth. It is advisable to avoid storing databases on a NAS, as the server response time fluctuates depending on the bandwidth. Applications that use most of the data transfer bandwidth will significantly reduce network performance.
- **Network congestion:** A large backup process can affect the function of an IP network and may lead to network congestion.
- Data transfer is inefficient as it uses TCP/IP instead of a specialized data transfer protocol.
- The storage service cannot be trusted for mission-critical operations.
- Administrators must set user quotas for storage space.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Selecting an Appropriate Backup Method

Organizations can choose any backup method depending on their budget and IT infrastructure. The different types of data backup methods are:

- **Hot Backup**

  A hot backup is a popular backup method. It is also called as dynamic backup or active backup. In a hot backup, the system continues to perform the backup even when the user is accessing the system. Implementation of a hot backup in an organization avoids downtime. However, changes made to the data during the backup process is not reflected in the final backup file. In addition, while the backup is in process, the users may find the system to be slow. A hot backup is an expensive process. It is used when a service level down time is not allowed.

  Advantage:

  - Immediate data backup switch over is possible

  Disadvantage:

  - Very expensive

- **Cold Backup**

  A cold backup is also called an offline backup. A cold backup can take place when the system is not working or is not accessible by users. A cold backup is the safest backup method as it avoids the risk of copying the data. A cold backup involves downtime as the users cannot use the machine until the process is back online. A cold backup is not as expensive as a hot backup. It is used when a service level down time is allowed and a full backup is required.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Advantage:

- Least expensive

Disadvantage:

- Switching over the data backup requires additional time

- **Warm Backup**

  A warm backup is also called a nearline backup. It will have a connectivity to the network. In a warm backup, the system updates are turned on to receive periodic updates. It is beneficial when mirroring or duplicating the data. The warm backup process can take a long time and can be conducted in intervals that can last from days to weeks. It is a combination of both hot and cold backups.

  Advantage:

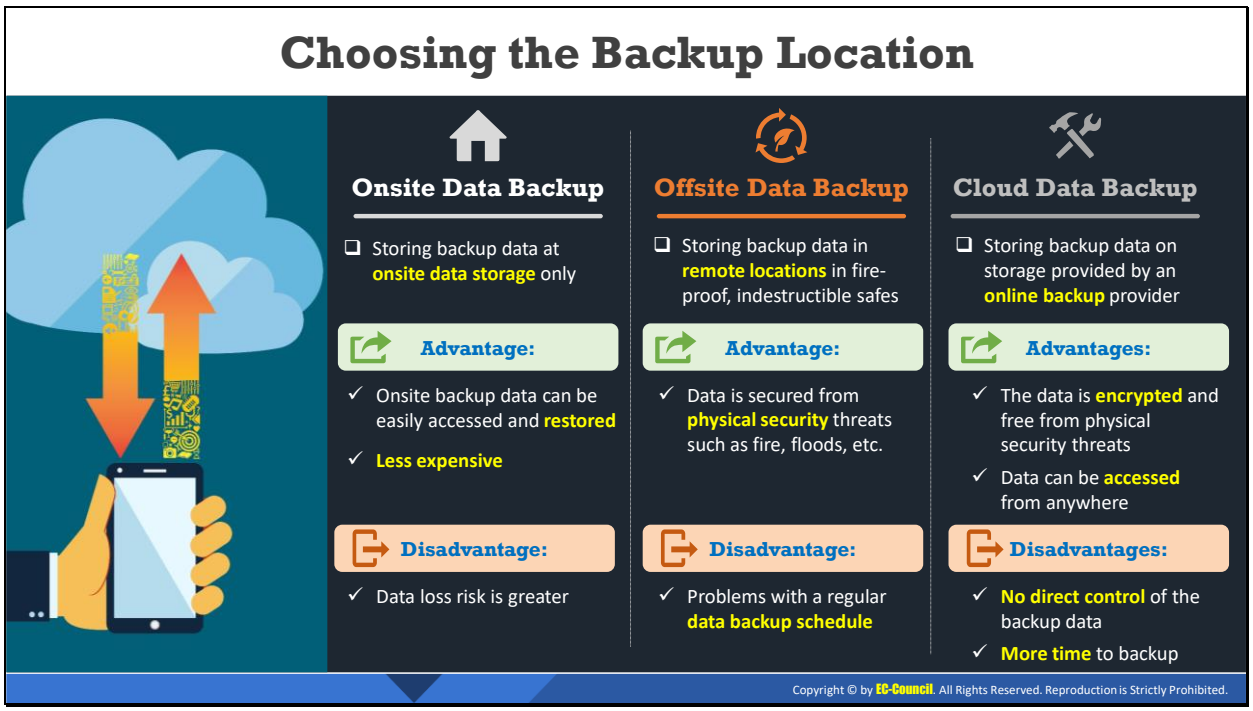
  - Less expensive than a hot backup
  - Switching over the data backup takes less time than a cold backup but more time than a hot backup

  Disadvantage:

  - It is less accessible than hot backup

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Choosing the Backup Location

Onsite Data Backup

This type of backup is performed within an organization. Onsite backup uses external devices such as a tape drive, DVD, hard disk, etc. The choice of external storage will depend on the amount of data to be backed up.

- **Advantages:**
  - Provides immediate access to data.
  - Less expensive.
  - Media used for onsite backup is readily available and costs less.
  - Faster recovery.
  - Enhanced scalability.
  - Internet access is not required.
- **Disadvantages:**
  - Requires direct human interaction to perform the backup.
  - Susceptible to theft or natural disasters.
  - Data loss risk is greater.

Offsite Data Backup

In an offsite backup, the backup is done at a remote location in fire-proof, indestructible safes. It either stores the data on physical drives, online, or a third-party backup service. Storing the data online helps in having an updated data backup available.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

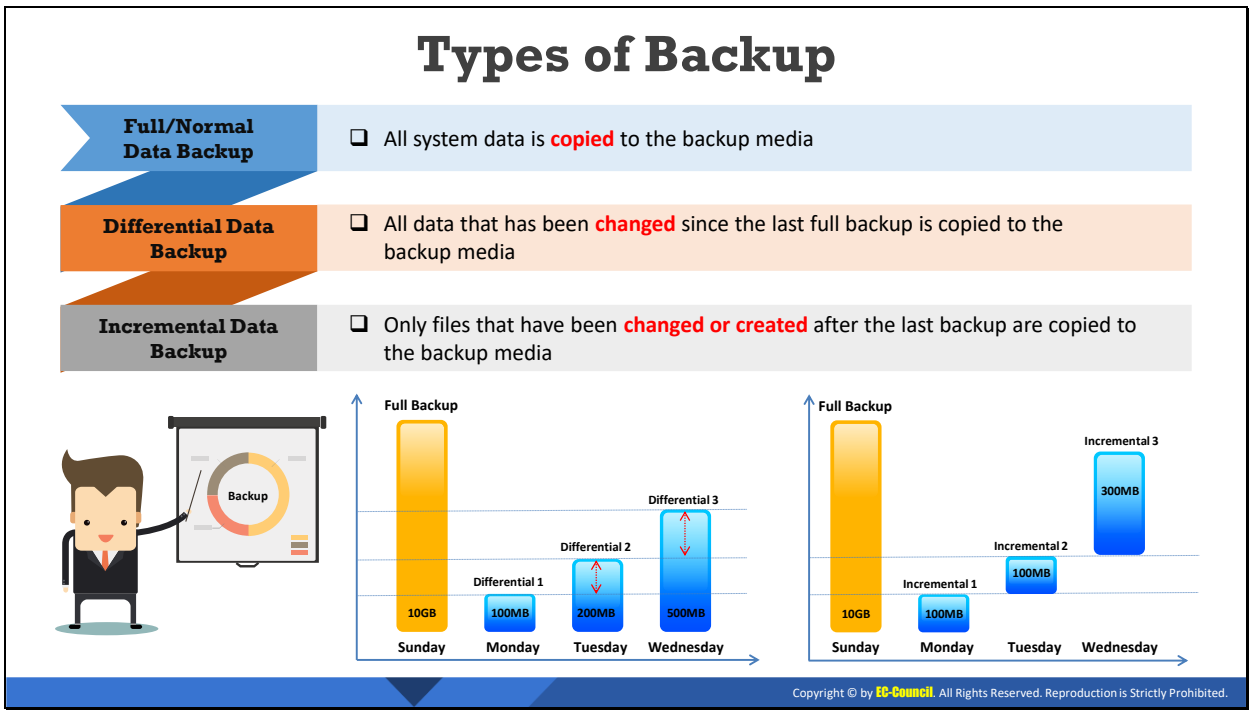
- **Advantages:**
  - Implementing offsite backup creates multiple copies that can be stored in multiple locations.
  - Human error is minimal as the backup process is automated.
  - Data retention is unlimited.
  - Data is secured from physical security threats such as fire, floods, etc.
- **Disadvantages:**
  - Problems with a regular data backup schedule.
  - It is expensive, requiring a third-party service.
  - Requires an Internet connection, and the bandwidth consumption will be higher.
  - The process is lengthy and time consuming.

Cloud Data Backup

A Cloud backup is also known as online backup. It involves storing the backup on a public network or on a proprietary server. Usually, a third-party service provider hosts the proprietary server. The cloud data backup process works according to the requirements of the organization. If the organization needs a daily backup, the proprietary server will run a daily backup. Usually, any noncritical data is archived using a cloud data backup.

- **Advantages:**
  - Cloud data backup is efficient as it uses technologies such as disk-based backup, virtualization, encryption, etc.
  - Many proprietors provide data monitoring and create reports for the organization.
  - The data in a cloud backup is easily accessed through the Internet.
  - The data is encrypted and free from physical security threats.
- **Disadvantages:**
  - Data recovery can be time consuming.
  - Cloud data backup proprietors do not give any assurances or guarantees on the completion of a backup. The organization is responsible for checking whether the backup process was successful.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Types of Backup

An appropriate backup type is one that does not have a major impact on bandwidth, cost, time required, and the organization's resources. The three most common backup types are full, differential, and incremental.

- **Full backup:** This is also called a normal backup. A full backup occurs automatically according to a set schedule. It copies all files and compresses them to save space. A full backup provides efficient data protection for the copied data.
- **Differential backup:** Differential backup is the combination of a full backup and an incremental backup. A differential backup backs up all the changes made since the last full backup.

  Example: Considering the above example, assume a full backup is scheduled for Sunday, and then a differential backup is scheduled to run until Saturday. Once the full backup is completed on Sunday, the differential backup will occur on Monday and the data that was changed will be backed up. On Tuesday, the backup will be for the changes made on Sunday and Monday. Then, on Wednesday, it will include the changes from Sunday, Monday, and Tuesday.
- **Incremental backup:** Backups only files that have been changed or created after the last backup are copied to the backup media. The last backup can be of any type. Before an incremental backup is performed, the system should be backed up using a full or normal backup.

  Example: Assume a full backup of the system is scheduled for Sunday, and an incremental backup is scheduled from Tuesday to Saturday. Once the full backup is

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

performed on Sunday, the incremental backup on Monday will only backup the changes that occurred on Sunday. This process will continue until Saturday.

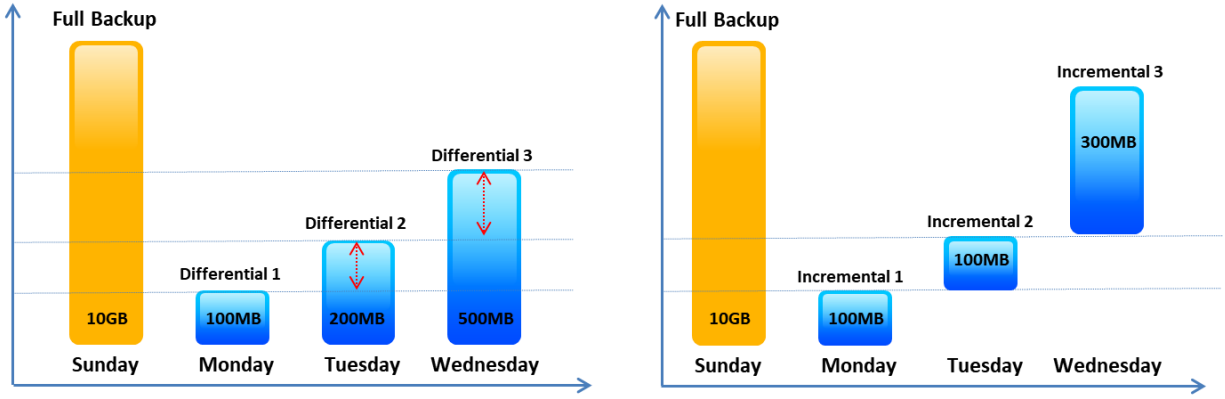
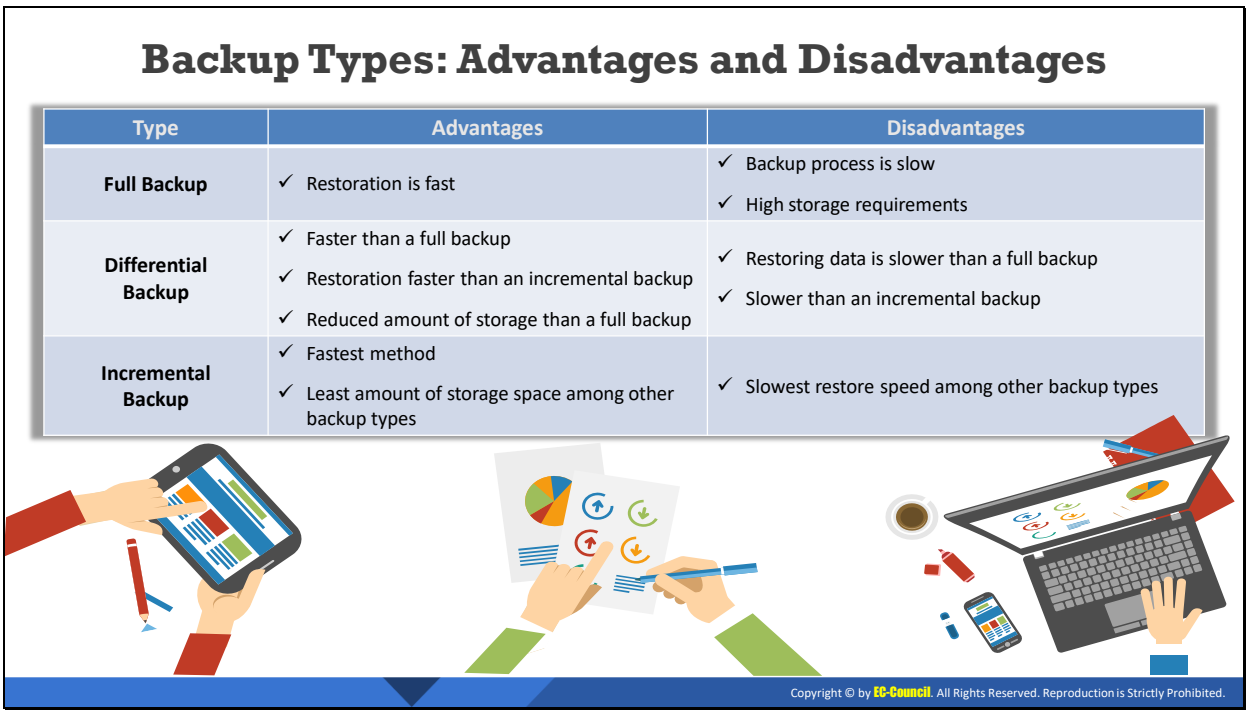


Figure 11.37: Backup types

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Backup Types: Advantages and Disadvantages

Compare the advantages and disadvantages of each backup type, and then select one that is best suited for the organization.

Full Backup

- **Advantages:**
  - It is easy to restore; the process requires a file name and location.
  - Maintains different versions of the data.
- **Disadvantages:**
  - A time-consuming process because each file is backed up every time a full backup is performed.
  - Large storage requirements.

Incremental Backup

- **Advantages:**
  - Faster than a full backup.
  - Uses storage space efficiently, and there is no data duplication.
  - Least amount of storage space among other backup types.
- **Disadvantages:**
  - Data restoration is time consuming and a complex process; first, a full backup is done, which is followed by an incremental backup.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Differential Backup

- **Advantages:**
  - Faster than a full backup.
  - Uses storage space more efficiently than a full backup; the backup only contains the changes made at regular intervals.
  - Data restoration is faster than an incremental backup.
  - Reduced amount of storage than a full backup.
- **Disadvantages:**
  - Slower than an incremental backup.
  - Restoration process is slower than a full backup.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

Data Backup Tools

File History Tool

Use **File History** to backup and restore in Windows. By default, it backs up the system drive. Other drives can be selected for backup if needed. Regular data and settings back up is recommended to prevent data loss.

Steps to Backup your PC with File History

- Select **Start** → **Settings** → **Update & Security** → **Backup** → **Add a drive** +, and then select an external drive or network location for backups.

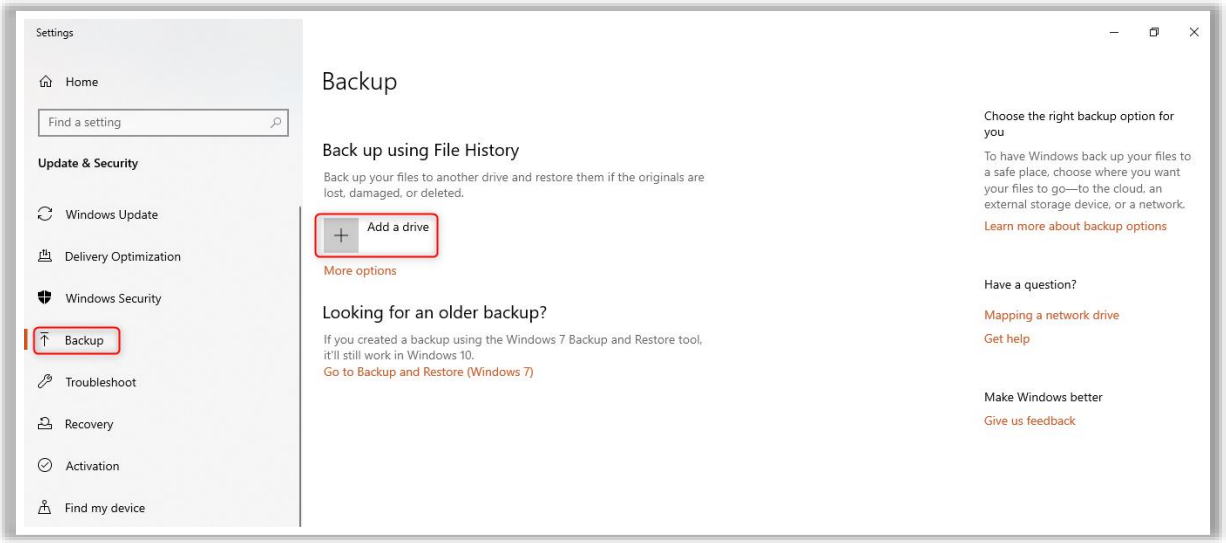


Figure 11.38: Backup PC with File History

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

File History before it is activated in Windows 10

- Select an external drive. File History is now archiving data. An on/off slider appears under a new heading **Automatically back up my files**.

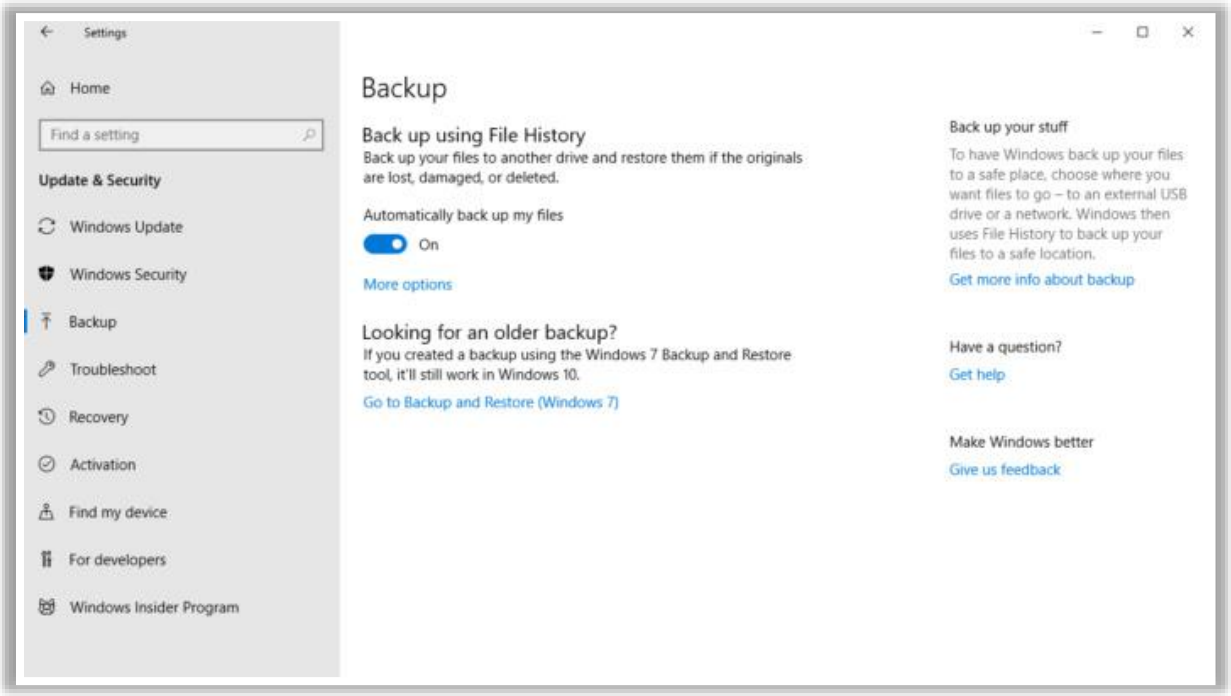


Figure 11.39: Back Up Using File History

- Click **More options** to change the File History defaults.
- By default, Windows 10 File History will back up all folders in the User folder, back up files every hour as long as the backup drive is available and keep previous copies of the files forever. To change any of these settings, click **More options** under the on/off slider.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

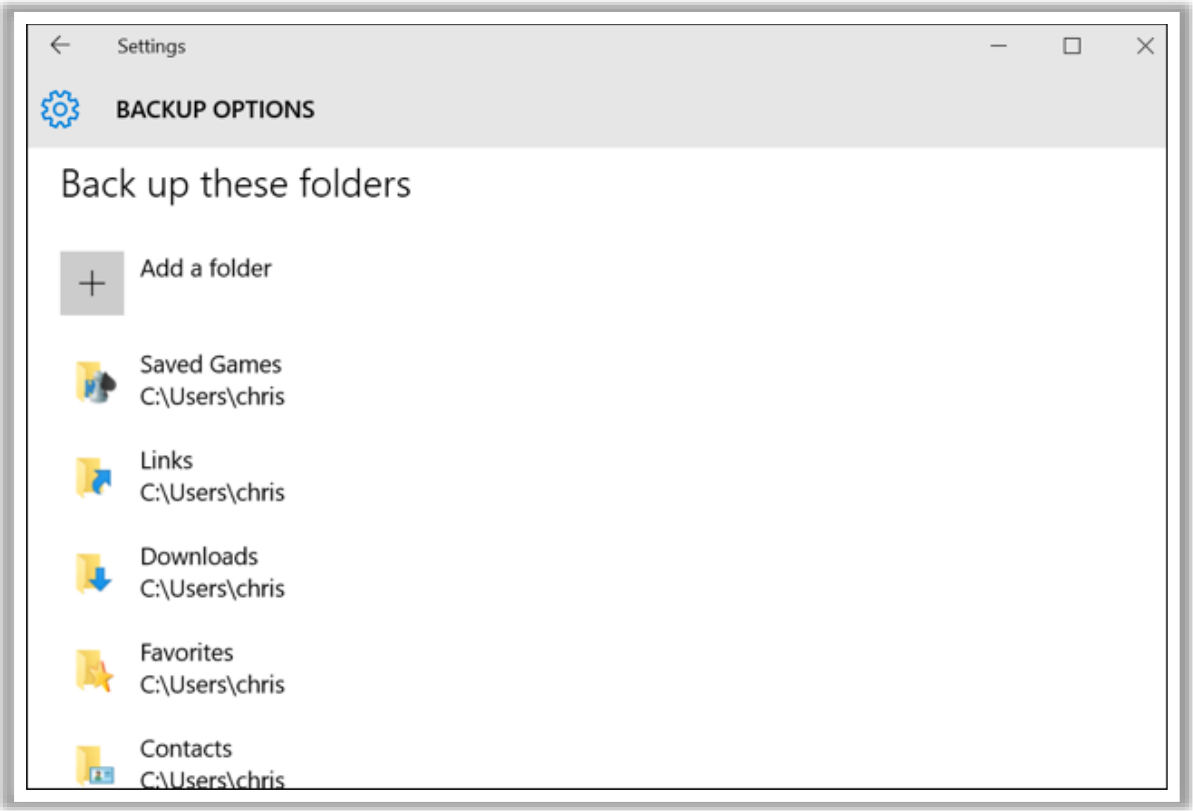
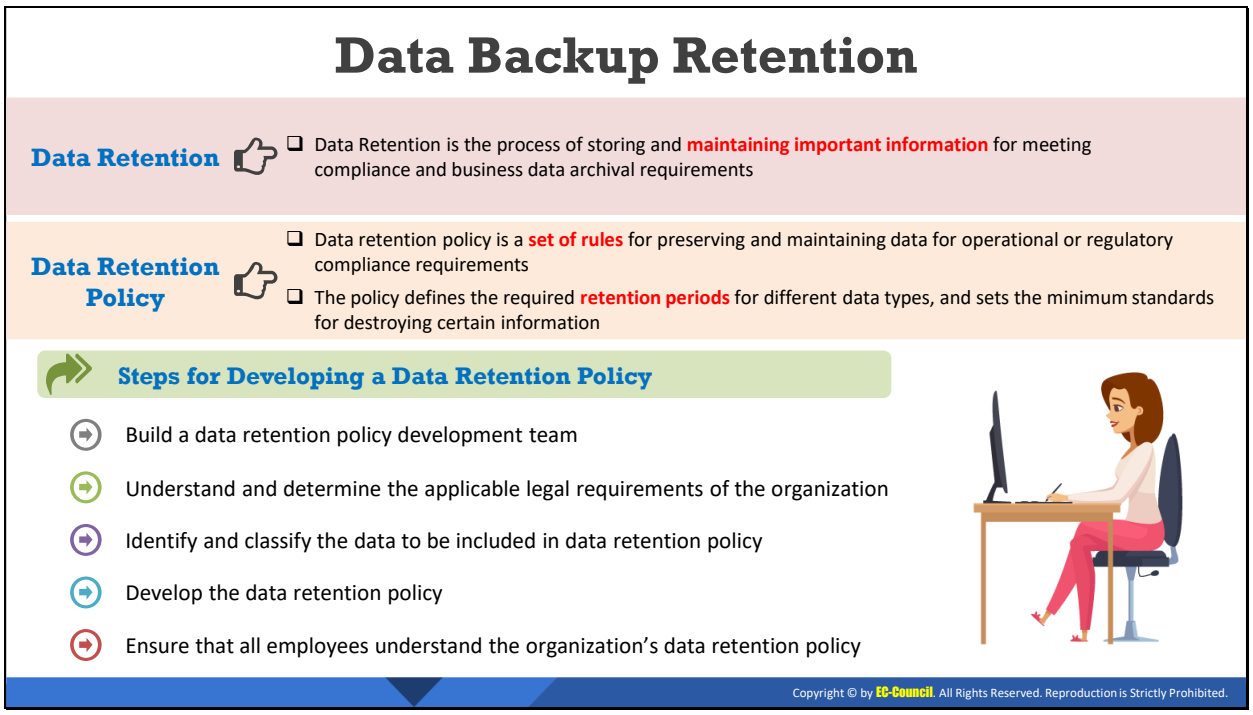


Figure 11.40: Folder Back Up

Some additional data backup tools are as follows:

- Genie Backup Manager Pro (*https://www.zoolz.com*)
- BullGuard Backup (*https://www.bullguard.com*)
- NTI Backup Now EZ (*https://www.nticorp.com*)
- Power2Go 13 (*https://www.cyberlink.com*)
- Backup4all (*https://www.backup4all.com*)

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Data Backup Retention

Data retention is the process of storing and maintaining important information for meeting compliance and business data archival requirements. It helps organizations in recovering business-critical data in case of data loss.

Every organization should develop a data retention policy to ensure that all important data is satisfactorily stored. The data retention policy is a set of rules for preserving and maintaining data for operational or regulatory compliance requirements. The policy defines the required retention periods for different data types, and also sets the minimum standards for destroying certain information.

A data retention policy is applied to all business units, processes, and systems in all countries where an organization operates. It is applied to an organization's officers, directors, employees, agents, affiliates, contractors, consultants, advisors, or service providers who can collect, process, or have access to different data types. Moreover, it is applied to all documents such as emails, hard copy documents, soft copy documents, audio, and video files, etc.

Steps to Create Data a Retention Policy

The following steps are used to create a data retention policy:

1. **Build a data retention policy development team**

   You should build a data retention policy development team that includes the members such as:

   - In-house legal counsels
   - Departmental managers and supervisors

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- Those who receive and manage financial reports
- Those who develop financial reports
- Staff members for managing data retention settings

2. Identify the types of regulatory compliances applicable to your business

Different regulatory compliances specify different data retention durations and data removal conditions. Some of them are listed below:

- The Health Insurance Portability and Accountability Act (HIPAA)
- The Sarbanes-Oxley Act (SOX)
- The Internal Revenue Service (IRS)
- The Children's Online Privacy Protection Act (COPPA)
- The EU's GDPR

3. Specify the types of data to be included in your data retention policy

The following types of data should be included in the data retention policy:

- Documents
- Emails and other electronic documents
- Customer records
- Transactional information
- Spreadsheets
- Contracts
- Correspondence between staff and clients, agents, vendors, shareholders, and the public
- Supplier and partner data
- Employee records
- Customer records
- Sales, invoice, and billing information
- Tax and accounting documentation
- Financial reports
- Healthcare and patient data
- Student and educational data
- Other information produced, collected, and maintained for satisfying regular business activities

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

4. **Develop a data retention policy**

   Develop a data retention policy considering the following points:

   - Purpose
   - Applicable laws, regulations, policies, rules, and acts
   - Record retention and deletion schedule
   - Litigation plan
   - Review and update schedule

5. **Inform all employees about the data retention policy**

   All employees should be aware of and comprehensively understand the different aspects of the data retention policy. Provide each employee a copy of the data retention policy and also design training and review sessions to keep them updated.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

Data Retention Policy Best Practices

The following data retention best practices for an organization can help establish and enforce a more compliant and useful data retention policy suited to their needs:

- Create a data retention policy that fulfills legal and business requirements
- Justify the reasons behind the policy details
- Start creating a policy with minimal requirements, and add new requirements as and when required
- Create a simple policy which is easy for the employees to implement
- Create different data retention policies for different data types, as per their legal and business impacts
- Retain customer, subscriber, and user information only till they are necessary
- Implement software to manage the data retention tasks
- Classify data and decide if it should be archived or deleted
- Files which are not accessed frequently should be moved to a lower-level archive
- Organize and store archived data such that it is easily accessible

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Data Recovery Tools

- **EaseUS Data Recovery Wizard**

  Source: *https://www.easeus.com*

  EaseUS data recovery software can quickly retrieve lost files after deletion or emptying the recycle bin. It scans for all recoverable files from any inaccessible storage device and completes file recovery safely and efficiently. It is used not only for the recovery of deleted files and formatted drives, but also for overcoming other data-loss issues such as virus attacks, human errors, power failures, system crashes, OS re-installation/upgrade, hard-drive crashes, and software crashes.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

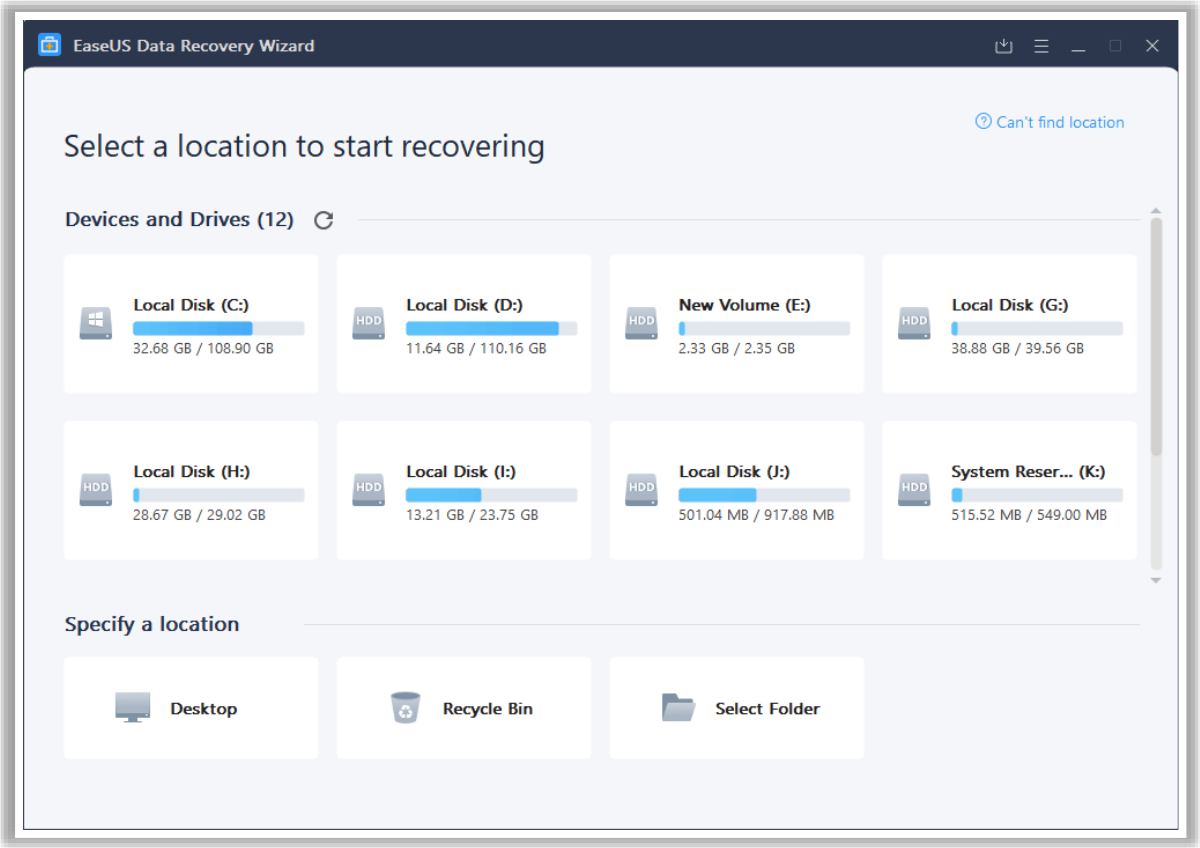
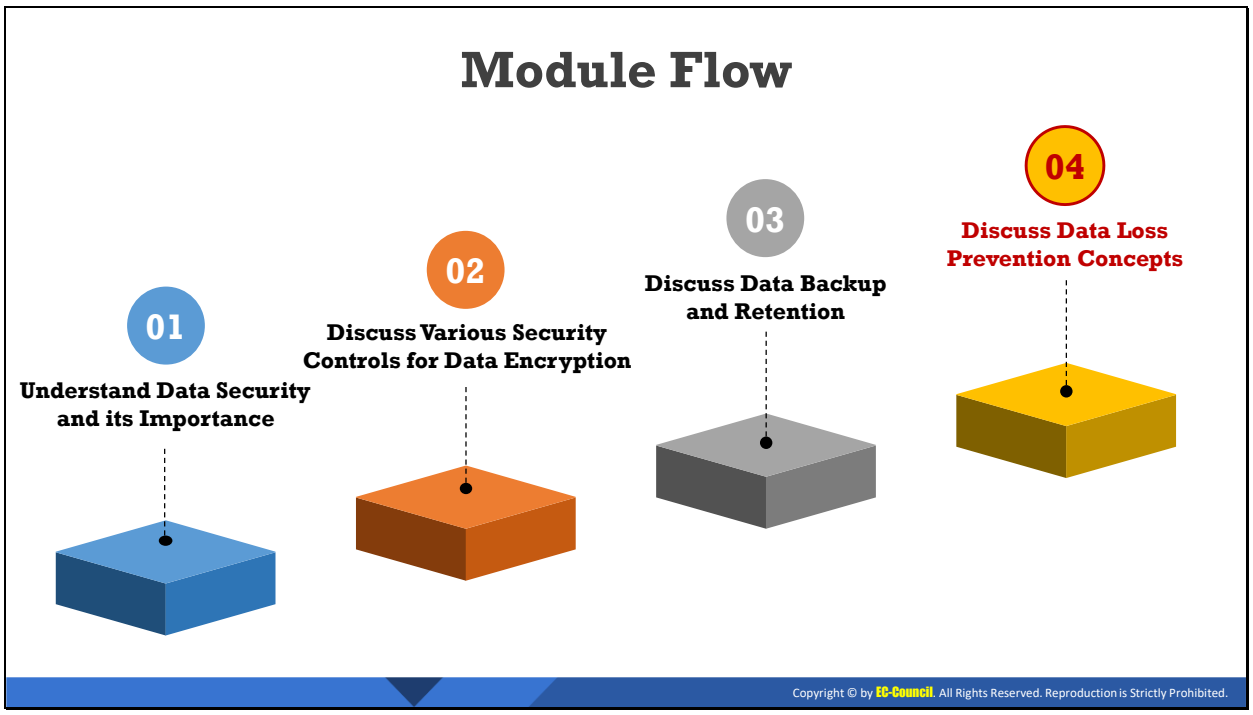


Figure 11.41: Screenshot of EaseUS Data Recovery Wizard

Some additional data recovery tools are as follows:

- Recuva® (*https://www.ccleaner.com*)
- Puran File Recovery (*http://www.puransoftware.com*)
- Glary Undelete (*https://www.glarysoft.com*)
- SoftPerfect File Recovery (*https://www.softperfect.com*)
- Wise Data Recovery (*https://www.wisecleaner.com*)

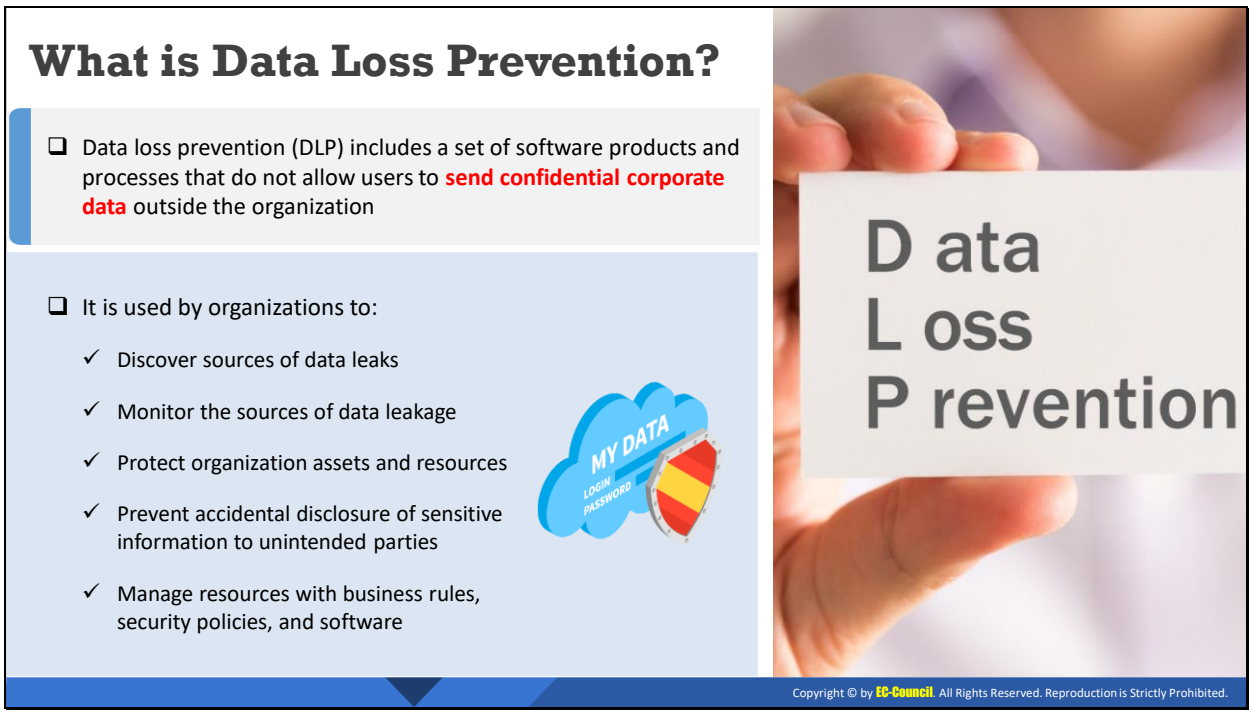
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Discuss Data Loss Prevention Concepts

The objective of this section is to explain the importance of data loss prevention (DLP) in data security.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



What is Data Loss Prevention?

Data loss prevention (DLP) includes a set of software products and processes that do not allow users to send confidential corporate data outside the organization. These software products help security professionals in controlling what data end users can transfer. DLP rules block the transfer of any confidential information across external networks. They control any unauthorized access to company information and prevent anyone from sending malicious programs to the organization.

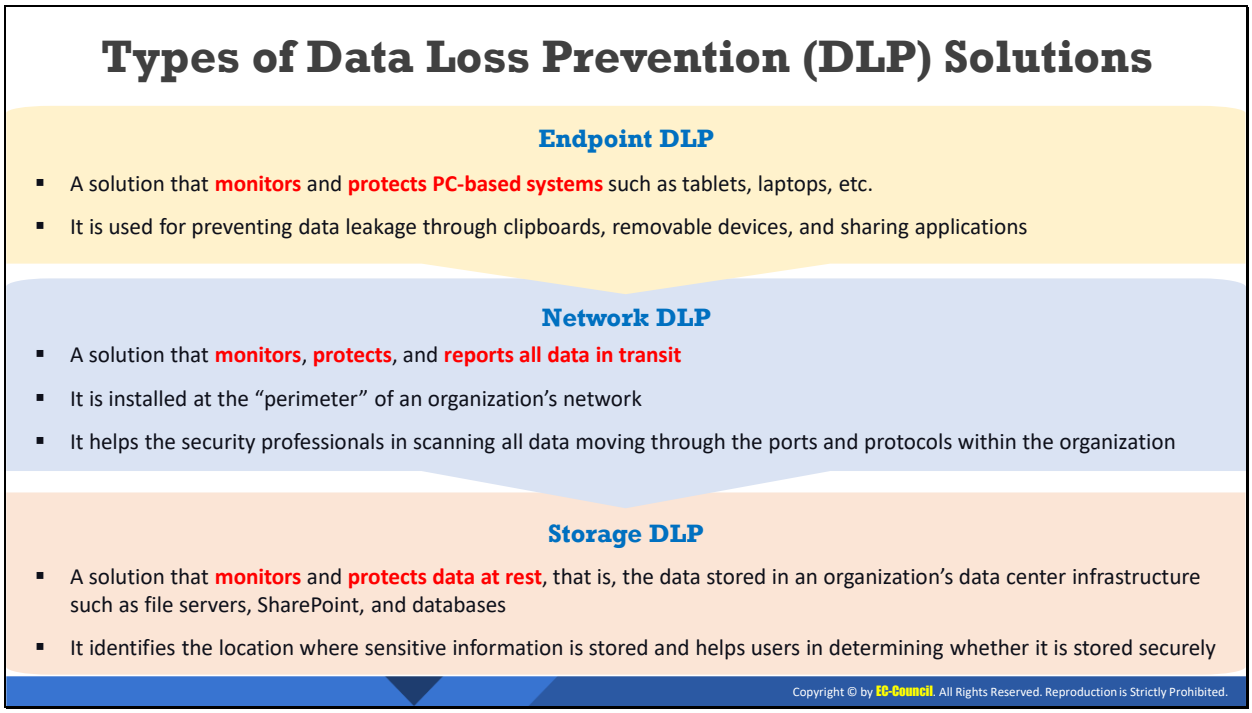
DLP software are implemented according to the organizational rules set by the management. This prevents accidental/malicious data leaks and losses. If an employee tries to forward or even upload company data on cloud storage or on a blog, the access will be denied by the system. A DLP policy is adopted by the management when internal threats to a company are detected. A DLP policy ensures that none of its employees send sensitive information outside the organization. New emerging DLP tools not only prevent the loss of data but also monitor and control irregular activities from occurring on the system.

Different DLP products are available to help security professionals determine what data users can transfer. DLP products are also known as data leak prevention, information loss prevention, or extrusion prevention products.

DLP is used by organizations to:

- Discover sources of data leaks
- Monitor the sources of data leakage
- Protect organization assets and resources
- Prevent accidental disclosure of sensitive information to unintended parties
- Manage resources with business rules, security policies, and software

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Types of Data Loss Prevention (DLP) Solutions

There are various types of DLP solutions that function differently with the same objective, that is, to prevent data leakage.

- **Endpoint DLP:** Endpoint DLP is a solution that monitors and protects PC-based systems such as tablets, laptops, etc. It is used for preventing data leakage through clipboards, removable devices, and sharing applications. The solution includes an agent that monitors specific user operations such as sending an email, copying a file to removable media devices, printing a file, etc. Endpoint DLP protects data in use.
- **Network DLP:** Network DLP is a solution that monitors, protects, and reports all data in transit. It is installed at the "perimeter" of an organization's network. It helps the security professional in scanning all data moving through the ports and protocols within the organization. It may analyze email traffic, social media interactions, SSL traffic, instant messaging, etc. The solution maintains reports containing information such what data is used, who is using the data, and where the data is sent. Thus, it helps in controlling the flow of data over the organization's network and meets regulatory compliance. Data collected by a Network DLP is stored in a database for retrieval later.
- **Storage DLP:** Storage DLP is a solution that monitors and protects data at rest, that is, the data stored in an organization's data center infrastructure such as file servers, SharePoint, and databases. It identifies the location where sensitive information is stored and helps users in determining whether it is stored securely. It allows authorized users to view and share sensitive files in the organization's network.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

DLP Solution: Windows Information Protection (WIP)

Windows Information Protection (WIP) has an endpoint DLP capability that can be helpful for protecting local data at rest on endpoint devices. WIP can be configured to store business data only on approved devices/within approved applications.

If the user creates a file on a Windows 10 device, the Windows Defender ATP evaluates its content for sensitive or customized information. In case of file matches, Windows Defender ATP applies DLP at its endpoints. For data discovery, Windows Defender ATP integrates with Azure Information Protection (AIP) and reports the detected sensitive data. Files with sensitive information and sensitivity labels are aggregated by AIP.

Advantages of WIP:

- As WIP separates corporate and personal data, there is no need for an employee to switch the applications or environments.
- It reinforces the data protection for existing line-of-business applications.
- WIP can remove the corporate data from Intune MDM enrolled devices.
- For configuration, deployment, and management, WIP integrates with Microsoft Intune, System Center Configuration Manager, or the current mobile device management.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

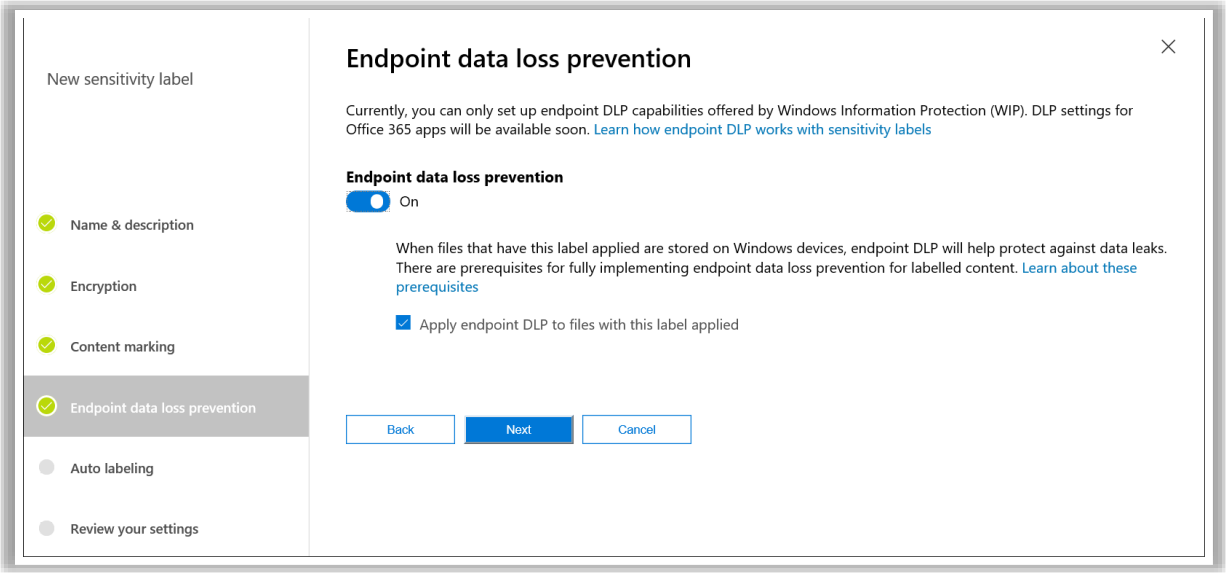
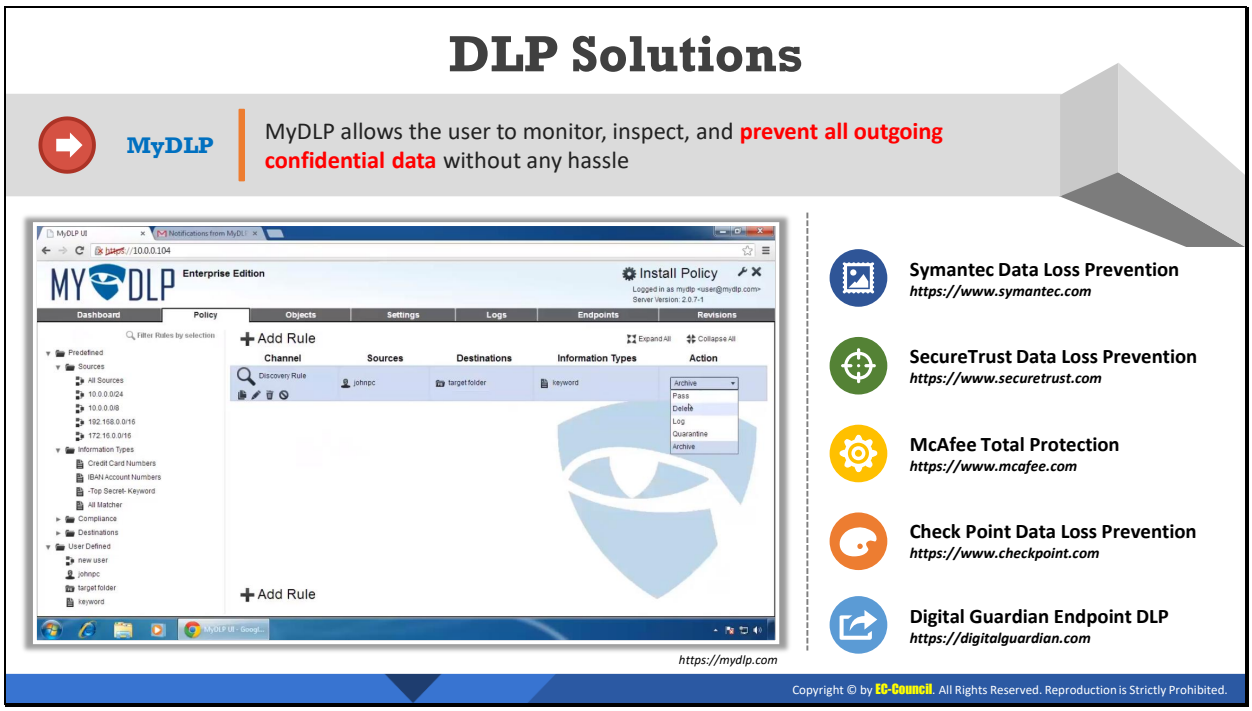


Figure 11.42: Screenshot of WIP

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



DLP Solutions

- **MyDLP**

  Source: *https://mydlp.com*

  MyDLP is a free and open-source solution that allows organizations to secure confidential data. The supported data inspection channels include web, email, instant messaging, printers, removable storage devices, screenshots, etc. MyDLP allows the user to monitor, inspect, and prevent all outgoing confidential data without any hassle. With its painless deployment and configuration, an easy-to-use policy interface, and great performance, IT administrators and security officers are able to effectively combat data leakage.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

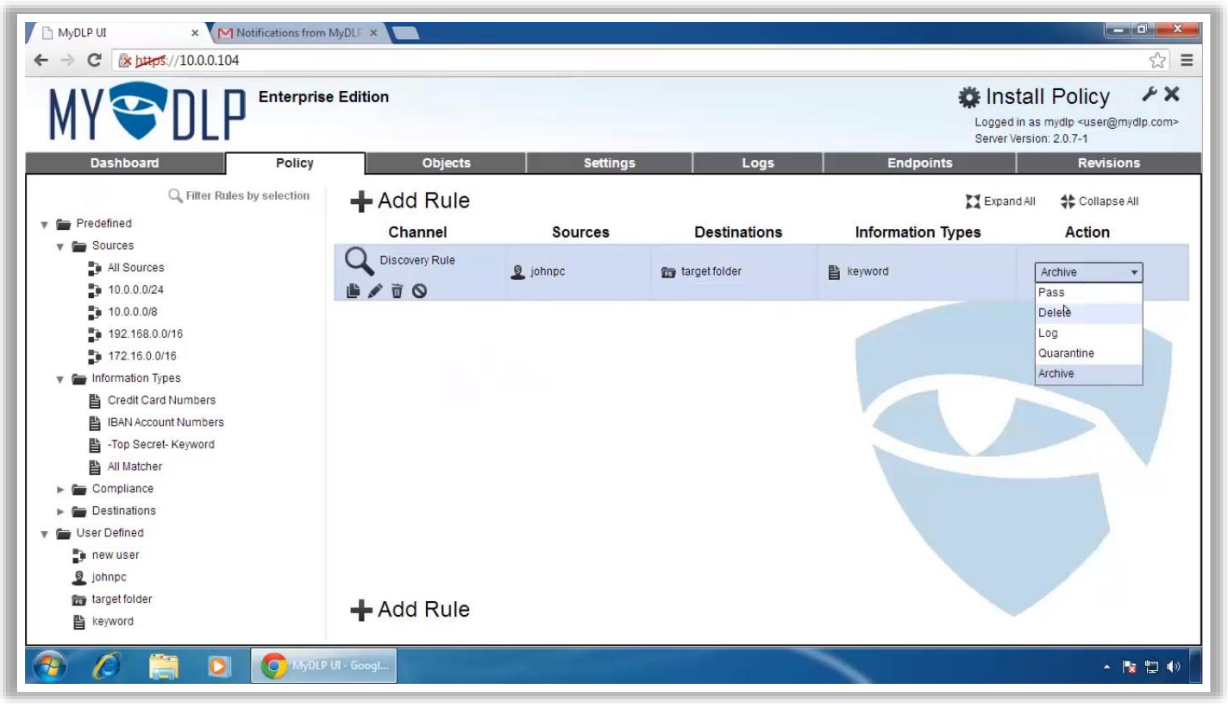


Figure 11.43: Screenshot of MyDLP

Some additional DLP solutions are as follows:

- Symantec Data Loss Prevention (*https://www.symantec.com*)
- SecureTrust Data Loss Prevention (*https://www.securetrust.com*)
- McAfee Total Protection (*https://www.mcafee.com*)
- Check Point Data Loss Prevention (*https://www.checkpoint.com*)
- Digital Guardian Endpoint DLP (*https://digitalguardian.com*)

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

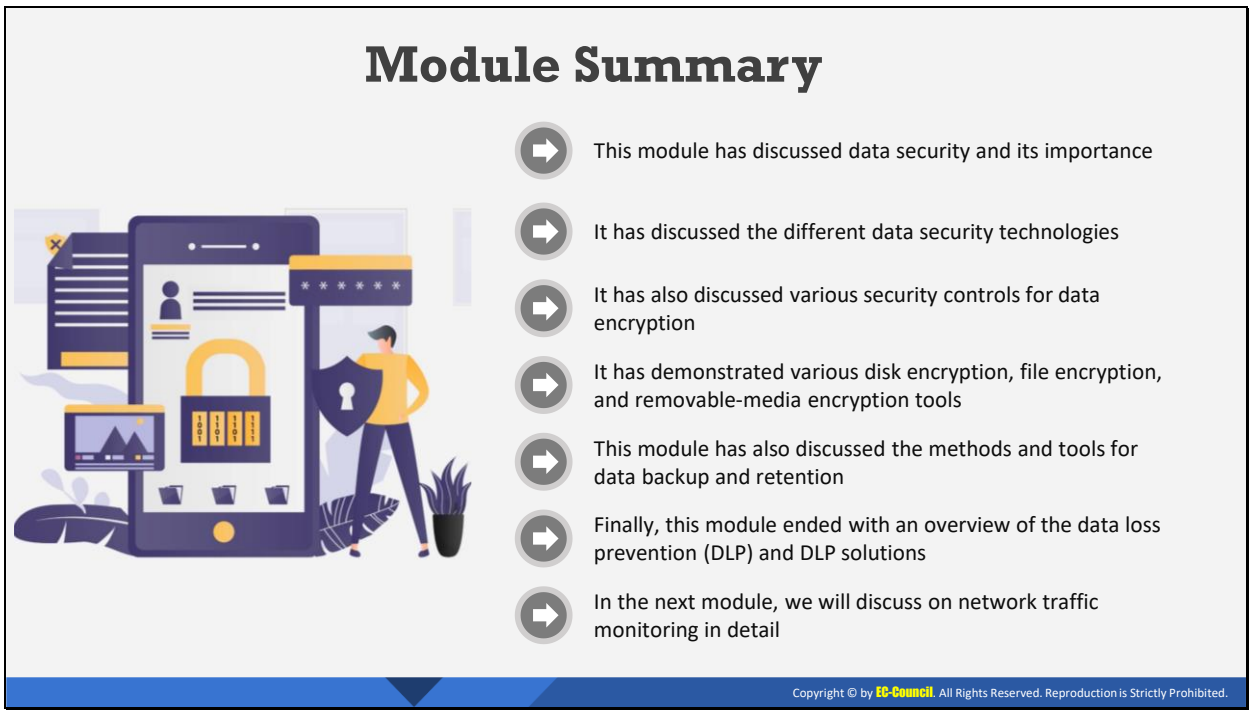
Best Practices for a Successful DLP Implementation

DLP safeguards sensitive information in an organization. Implementation of DLP not only prevents the leakage of sensitive data, but also allows the security professional to monitor and control the data accessed and shared by an end user.

Some best practices for a successful DLP implementation are as follows:

- Identify the main objective of DLP.
- Identify sensitive data for protection.
- Evaluate the available DLP vendors.
- Ensure that the selected DLP product is compatible and supports the required data types and data stores of the organization.
- Identify the roles and responsibilities of individuals for the implementation of DLP solution.
- Implement DLP with a minimal base to reduce false positives and enhance the base gradually by identifying sensitive data.
- Enhance the DLP policies to support effective DLP operations and eliminate false positives.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Module Summary

This module discussed data security and its importance. It discussed the different data security technologies as well as various security controls for data encryption. Furthermore, it demonstrated various disk encryption, file encryption, and removable-media encryption tools. This module also discussed methods and tools for data backup and retention. Finally, this module presented an overview of data loss prevention (DLP) and DLP solutions.

In the next module, we will discuss network traffic monitoring in detail.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

EC-Council

N|DE
Network Defense Essentials

Module 12

Network Traffic Monitoring

https://t.me/learningnets

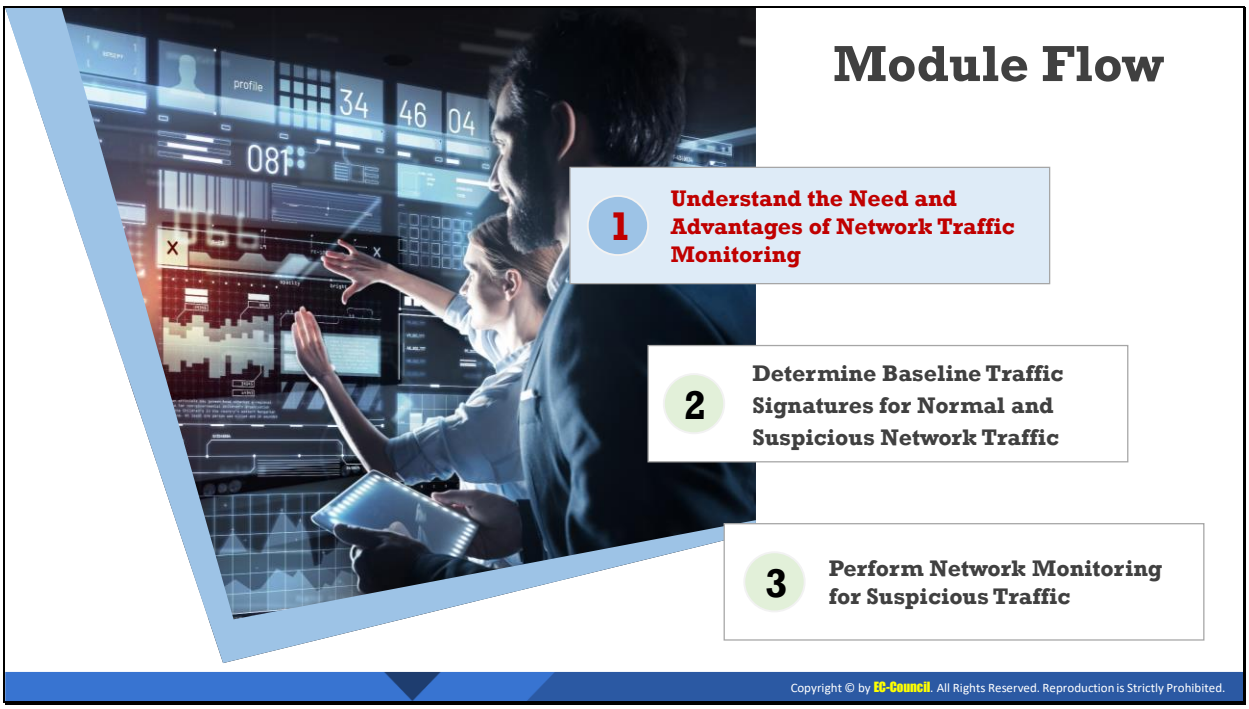
Module Objectives

Organizations need to perform network monitoring and analyze network traffic to identify suspicious activities across their networks. This module covers the concept of network traffic monitoring.

At the end of this module, you will be able to do the following:

- Understand the need for and advantages of network traffic monitoring
- Understand the network traffic signatures
- Describe the categories of suspicious traffic signatures
- Explain the attack signature analysis techniques
- Understand network monitoring for suspicious traffic
- Understand the various network monitoring tools

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Understand the Need and Advantages of Network Traffic Monitoring

The objective of this section is to explain in detail the need for and advantages of network traffic monitoring.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

Network Traffic Monitoring

Network traffic monitoring is the process of capturing network traffic and inspecting it closely to determine what is happening on the network. Network monitoring is a retrospective security approach that involves monitoring a network for abnormal activities, performance issues, bandwidth issues, etc. It is an integral part of network security and is a demanding task within the network security operations of organizations. Continuous network traffic monitoring and analysis are required for effective threat detection. Security Professional should constantly strive to maintain smooth network operation. If a network goes down even for a small period, productivity within a company may decline. To be proactive rather than reactive, the traffic movement and performance must be monitored to ensure that no security breach occurs within the network.

The network monitoring process involves sniffing the traffic flowing through the network. For this purpose, network packets must be captured, and a signature analysis must be conducted to identify any malicious activity.

Network operators use network traffic analysis tools to identify malicious or suspicious packets hiding within traffic. They monitor download/upload speeds, throughput, content, traffic behaviors, etc. to understand the status of the network operations.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

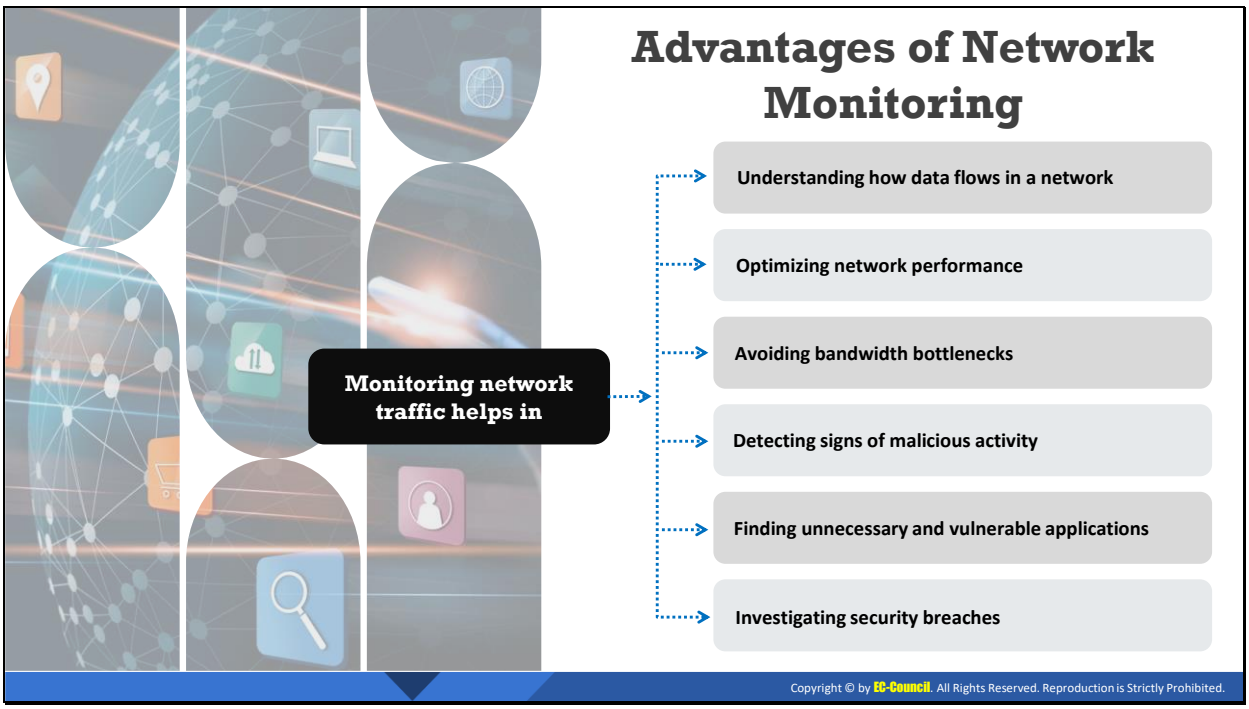
Need for Network Monitoring

Networking monitoring helps security professionals identify possible issues before they affect business continuity. If an issue occurs in the network, the root cause can be determined easily with network monitoring, and with network automation tools, the problem can be fixed automatically. Networking monitoring not only prevents outages but also gives visibility to potential issues. Continuous network monitoring minimizes downtime and increases the performance of the network.

Even when security tools are in place, attackers can find ways to bypass such security mechanisms to enter the network. Security tools generally use signature-based detection techniques, and it is difficult to identify continuously changing attack signatures/patterns. These tools are not designed to identify behavioral anomalies and are unable to detect attackers' activities that are initiated before and during attacks.

Network monitoring tools provide the first level of security and help identify anomalous conditions in the network, which indicate attacker activity.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Advantages of Network Monitoring

Network traffic analysis is performed to gain in-depth insight into the types of network packets or data flowing through a network. Typically, it is performed through network monitoring or network bandwidth monitoring utilities. The traffic statistics from network traffic analysis helps in the following:

- Understanding how data flows in a network
- Optimizing network performance
- Avoiding bandwidth bottlenecks
- Detecting signs of malicious activity
- Finding unnecessary and vulnerable applications
- Investigating security breaches
- Understanding and evaluating network utilization
- Determining download/upload speeds
- Determining the type, size, origin, destination, and content/data of packets

The typical advantages of network monitoring are as follows.

- **Proactive:** Network monitoring proactively detects applications that consume the maximum bandwidth and reduces the bandwidth. It manages server bottleneck situations and other systems connected to the network. Moreover, network monitoring delivers an efficient quality of service to users. It creates a record of all the irregularities occurring in the network that network defender can handle later.

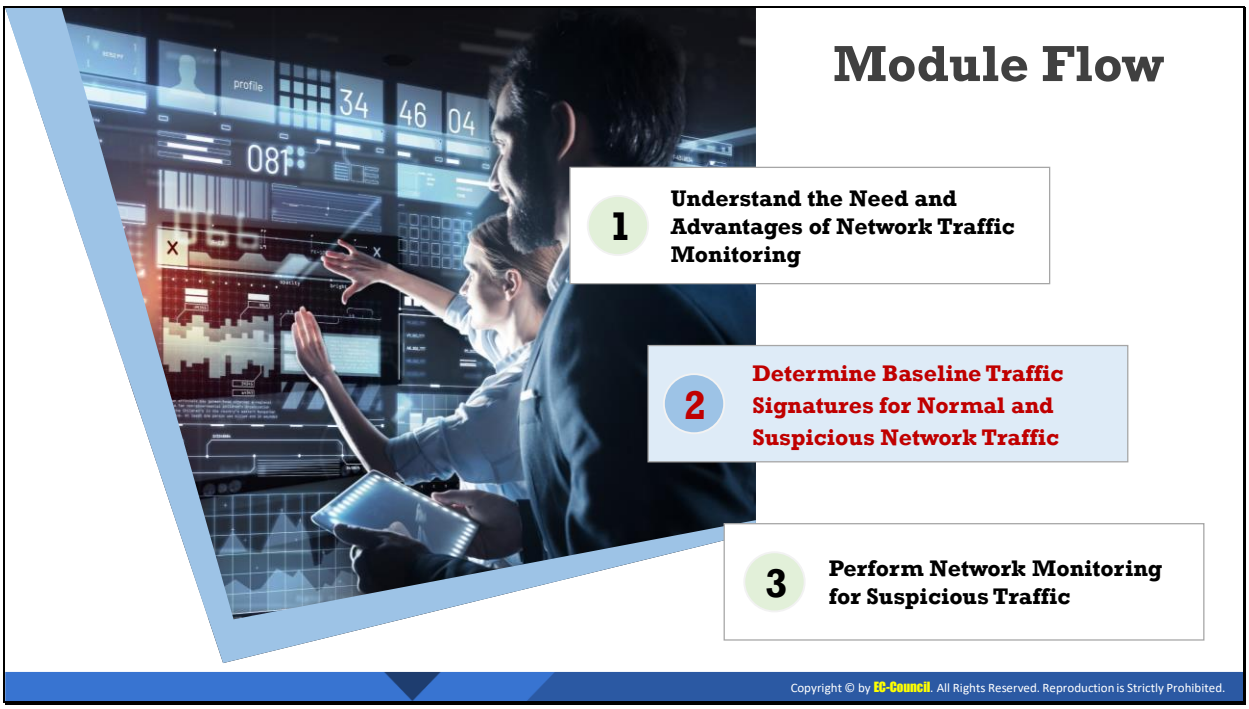
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **Utilization:** It is important to understand the need for network utilization, especially with all the new and evolving technology. Network monitoring provides complete details on the infrastructure. It provides an idea about the amount of load a network can handle during periods of heavy traffic, enabling the efficient utilization of the space in the network.
- **Optimization:** Network monitoring techniques gather network infrastructure information in a timely manner and save it for the security professionals. Security professional can then take the required actions before the situation worsens. These techniques identify applications that prove vulnerable to the network.
- **Minimizing risk:** Network monitoring techniques are necessary for establishing service-level agreements (SLAs) and compliance applicable to users or consumers. Complete infrastructure information is required when drafting SLAs. The real-time monitoring of network topologies and channels helps in creating the SLAs.

Network monitoring techniques are beneficial for security professionals. They are very easy to setup and implement, considering the complexity of networks.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

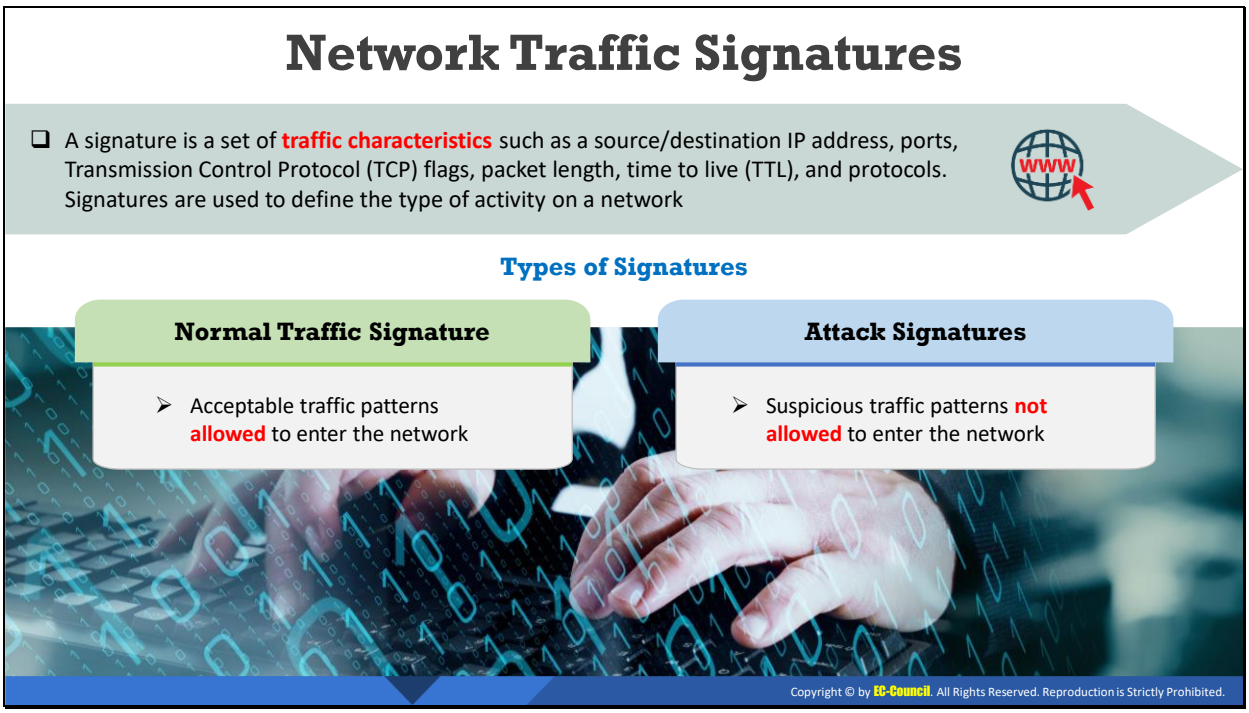
https://t.me/learningnets



Determine Baseline Traffic Signatures for Normal and Suspicious Network Traffic

The objective of this section is to explain the various types of network traffic signatures and the concept of baselining normal traffic signatures. It describes the categories of suspicious network traffic signatures and attack signature analysis techniques.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Network Traffic Signatures

A signature is a set of characters that define network activity, including IP addresses, Transmission Control Protocol (TCP) flags, and port numbers. It includes a set of rules used to detect malicious traffic entering a network. Signatures are used to perform the following:

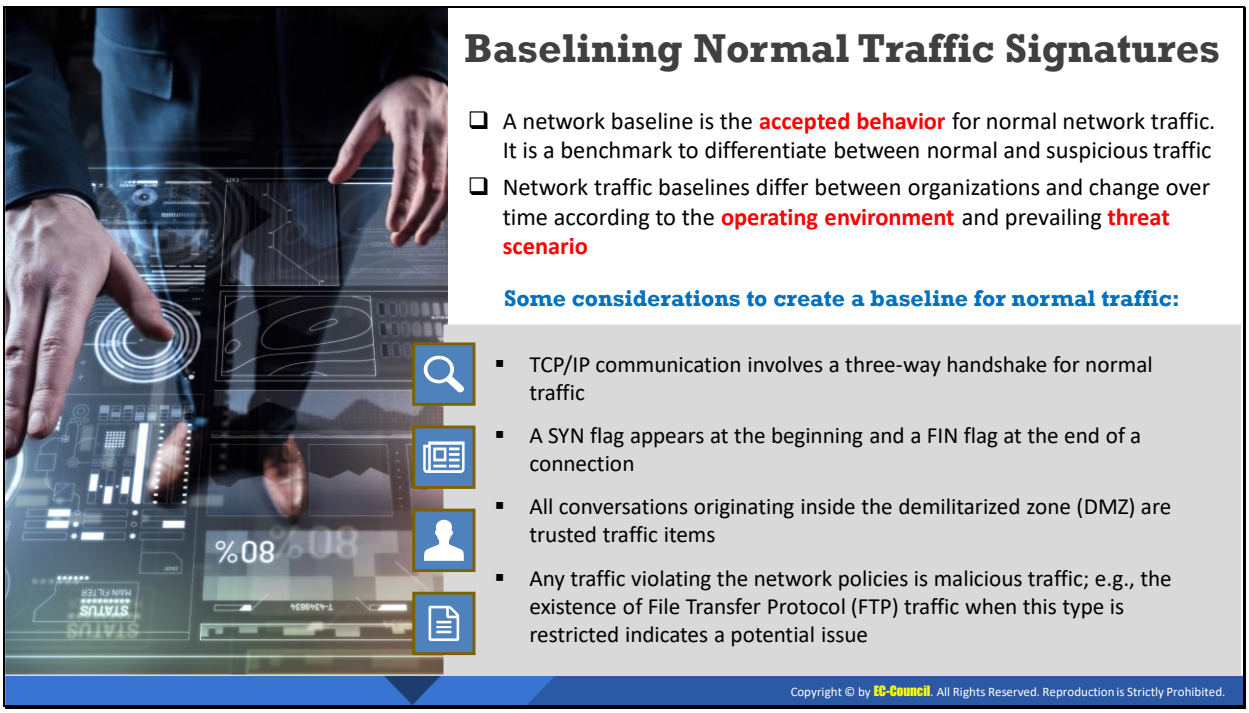
- Raise alerts in the case of unusual traffic on the network.
- Identify suspicious header characteristics in a packet.
- Configure an intrusion detection system to identify attacks or probes.
- Acquire knowledge on a specific attack that occurred or a vulnerability that can be exploited.
- Match patterns in a packet analysis.

Type of Signatures

Signatures are classified into two main categories depending on their behavior, as described below.

- **Normal traffic signatures**: These include the normal network traffic in the network and are defined based on a normal traffic baseline for the organization. These signatures do not contain any malicious patterns and can be allowed to enter the network.
- **Attack Signatures**: Traffic patterns that appear suspicious are generally treated as attack signatures. These signatures should not be allowed to enter the network. If allowed, they often cause a network security breach. These signatures deviate from the normal signature behavior and should be analyzed.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Baselining Normal Traffic Signatures

A network traffic baseline helps understand the behavioral patterns of a network. It is a benchmark to differentiate between normal and suspicious traffic. Baselining allows a set of metrics to monitor network performance. These metrics define the normal working condition of an enterprise's network traffic. The network traffic is compared with metrics to detect any changes in the traffic that could indicate a security issue in the network. A network traffic baseline establishes the accepted packets that are safe for the organization. Baselining the traffic facilitates the detection of suspicious activities on the network. Any deviation from the normal traffic baseline can be considered a suspicious traffic signature. The security professional should define a network baseline for their organization and validate the traffic against it. Baselining is more effective if it works in parallel with the organization's policy. With the help of normal traffic baselining, security professional can judge the requirements to secure the network. Network traffic baselines differ between organizations and change over time according to the operating environment and prevailing threat scenario.

Although, there is no industry standard to measure network traffic performance baselines, there are network monitoring tools that provide estimates of what type of traffic is normal. A network traffic baseline should be defined for all incoming, and outgoing Internet traffic and wide area network (WAN) links. The network traffic baseline should also contain the traffic for critical business data and backup systems.

- According to a network traffic baseline, normal traffic signatures for TCP packets should have the following characteristics:
    - To establish a three-way handshake, TCP uses SYN, SYN ACK, and ACK bits in every session.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- The ACK bit should be set in every packet, except for the initial packet, in which the SYN bit is set.
- FIN ACK and ACK are used in terminating a connection. PSH FIN and ACK may also be used initially in the same process.
- RST and RST ACK are used to quickly end an on-going connection.
- During a conversation (after a handshake and before termination), packets only contain an ACK bit by default. Occasionally, they may also have a PSH or URG bit set.

- A suspicious TCP packet has one or more of the following characteristics:
  - If both SYN and FIN bits are set, the TCP packet is illegal.
  - SYN FIN PSH, SYN FIN RST, and SIN FIN PSH RST are all variants of SIN FIN. An attacker sets these additional bits to avoid detection.
  - A packet having only a FIN flag is illegal as FIN can be used in network mapping, port scanning, and other stealth activities.
  - Some packets have all six flags unset; these are known as NULL flags and are illegal.
  - The source or destination port is zero.
  - If the ACK flag is set, then the acknowledgement number should not be zero.
  - If a packet has only the SYN bit, which is set at the beginning to establish a connection, and any other data are present, then it is an illegal packet.
  - If the destination address is a broadcast address (ending with 0 or 255), it is an illegal packet.
  - Every TCP packet has two bits reserved for future use. If either or both are set, then the packet is illegal.
- All conversations originating inside the demilitarized zone (DMZ) are trusted traffic items.
- Any traffic violating the network policies is malicious traffic, e.g., the existence of File Transfer Protocol (FTP) traffic when this type is restricted indicates a potential issue.
- Any Dynamic Host Configuration Protocol (DHCP) traffic from unknown DHCP servers indicates a rogue DHCP server.
- Mail traffic originating in the network but not sent to a mail server is suspect.
- Any DNS traffic not sent to the DNS server is suspect.
- Any outgoing traffic with internal addresses not matching the organization's address space may be malicious.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Categories of Suspicious Traffic Signatures

Network traffic deviating from normal behavior is categorized as a suspicious traffic signature. It is classified into four categories as follows.

- **Informational:** The informational traffic signature detects normal network activity. Although it may not appear suspicious, the data gathered through the informational signature can be used for suspicious activities. For example, informational traffic signatures may include the following:
  - Internet Control Message Protocol (ICMP) echo requests
  - TCP connection requests
  - User Datagram Protocol (UDP) connections
- **Reconnaissance**: Reconnaissance traffic consists of signatures that indicate an attempt to scan the network for possible weaknesses. Reconnaissance is an unauthorized discovery of vulnerabilities, which maps of systems and services. Reconnaissance is also known as information gathering, and it precedes a network attack in most cases. For example, reconnaissance traffic signatures may include the following:
  - Ping sweep attempts
  - Port scan attempts
  - Domain Name System (DNS) query attempts
- **Unauthorized access:** Traffic may contain signs of someone attempting to gain unauthorized access, unauthorized data retrieval, system access or privilege escalation, etc. An attacker who does not have privileges to access an organization's network

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

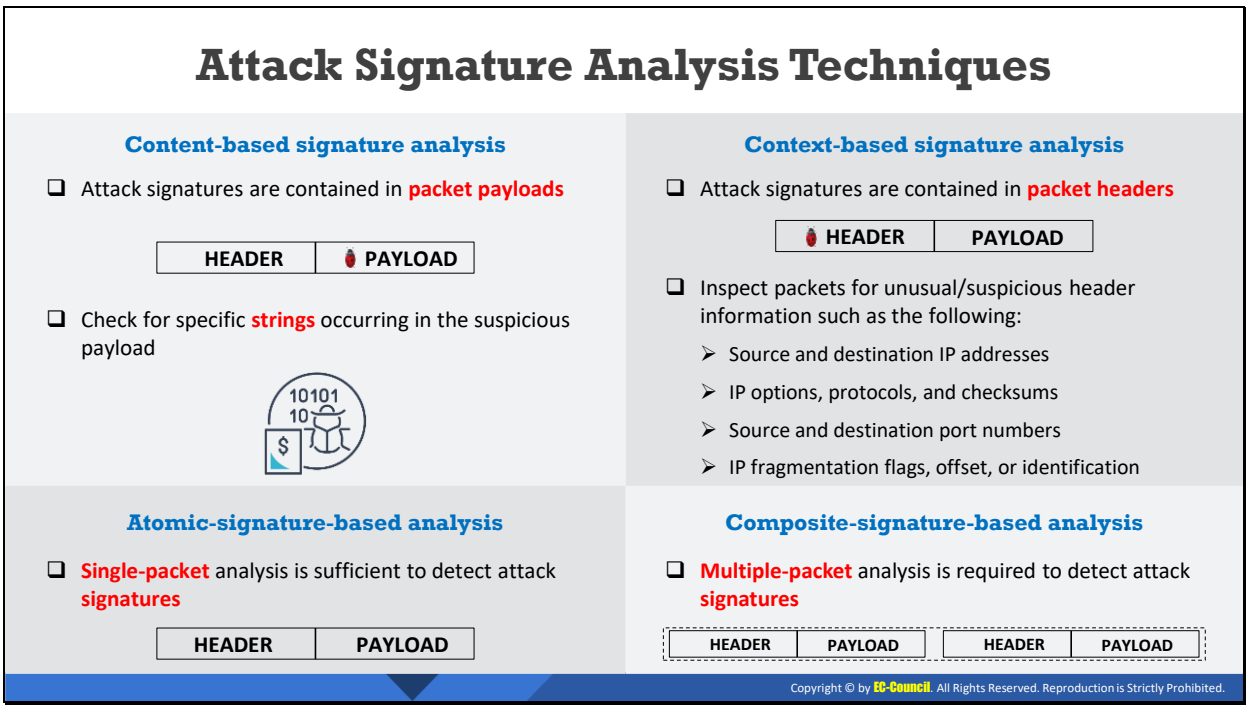
usually generates this type of traffic with the intention of capturing sensitive data. For example**,** unauthorized access traffic signatures may include the following:

- Password cracking attempts
- Sniffing attempts
- Brute-force attempts

- **Denial of service (DoS):** This type of traffic may contain a large number of requests from a single source or multiple sources, which are sent as an attempt to perform a DoS attack. This type of attack is performed to disrupt the service of the target organization. For example, DoS traffic signatures may include the following:
  - Ping of death attempts
  - SYN flood attempts

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Attack Signature Analysis Techniques

Attack signature analysis techniques are classified into four different categories as follows.

- **Content-based signature analysis:** Content-based signatures are detected by analyzing the data in the payload and matching a text string to a specific set of characters. If undetected, these signatures can open backdoors in a system, providing administrative controls to an outsider.
- **Context-based signature analysis:** Packets are usually altered using the header information. Suspicious signatures in the header can include malicious data that can affect the following:
  - Source and destination IP addresses
  - Source and destination port numbers
  - IP options
  - IP protocols
  - IP, TCP, and UDP checksums
  - IP fragmentation flags, offset, or identification
- **Atomic-signature-based analysis:** To detect an atomic signature, security professionals need to analyze a single packet to determine whether the signature includes malicious patterns. Security professionals do not require any knowledge of past or future activities to detect these signature patterns.
- **Composite-signature-based analysis:** In contrast to atomic signatures, security professionals need to analyze a series of packets over a long period of time to detect

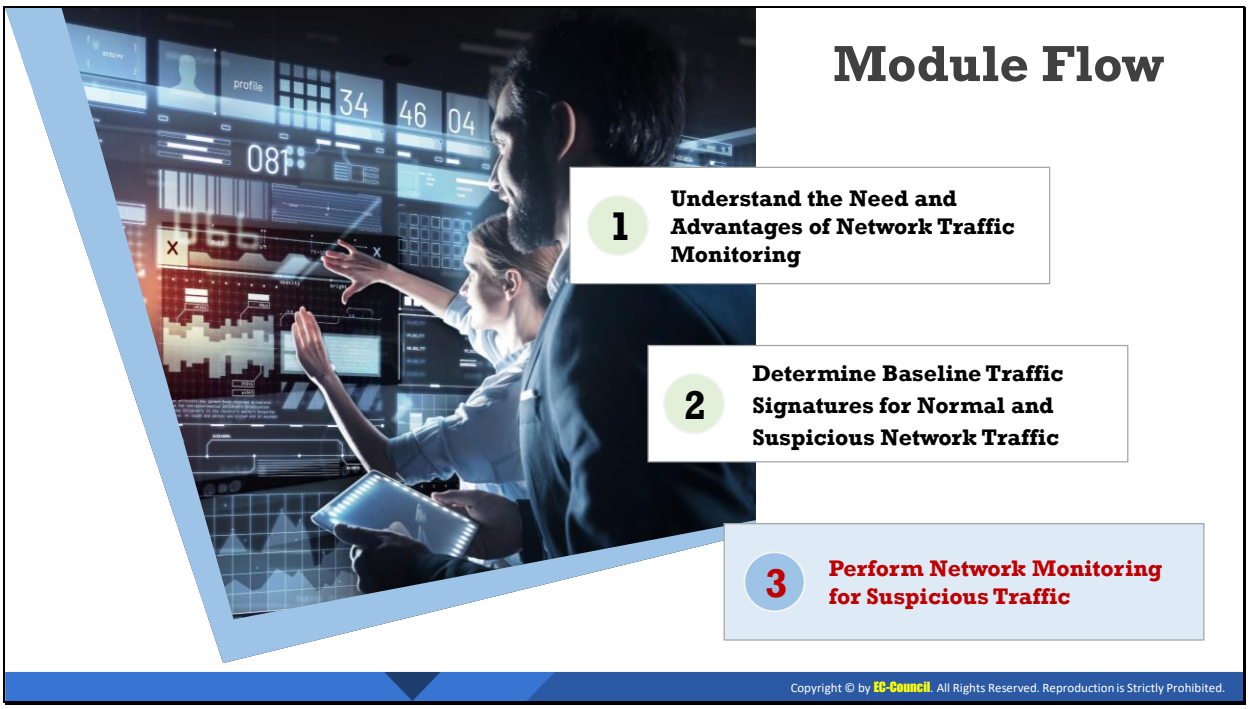
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

composite attack signatures. Detecting these attack patterns is exceedingly difficult. ICMP flooding is an example of an attack performed using composite signatures. In this attack, multiple ICMP packets are sent to a single host so that the server remains busy responding to the requests.

Attacker signatures may be located in either the header or payload of the packet.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

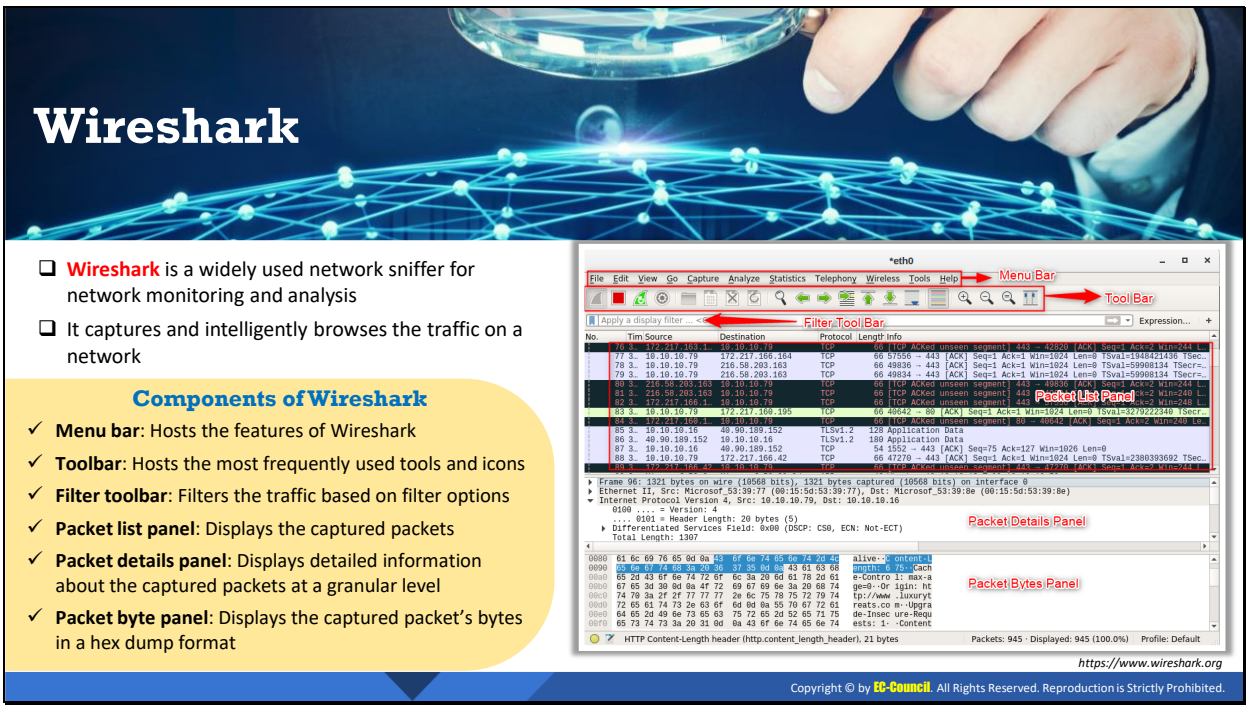
https://t.me/learningnets



Perform Network Monitoring for Suspicious Traffic

The objective of this section is to explain how to use Wireshark to perform network monitoring and analysis. It describes how to use Wireshark for monitoring and analyzing File Transfer Protocol (FTP) traffic, Telnet traffic, and Hypertext Transfer Protocol (HTTP) traffic.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Wireshark

Source: *https://www.wireshark.org*

Wireshark is a packet sniffer that can be used for network troubleshooting to investigate security issues and to analyze and understand network protocols. It can exploit information passed in plain text.

- **Features**

  Wireshark has a rich feature set that includes the following:

  - Identify poor network performance due to high path latency.
  - Locate internetwork devices that drop packets.
  - Validate the optimal configuration of network hosts.
  - Analyze application functionality and dependencies.
  - Optimize application behavior for best performance.
  - Analyze network capacity before application launch.
  - Verify application security during launch, login, and data transfer.
  - Identify unusual network traffic indicating potentially compromised hosts.

- **Prerequisites for network packet capture**

  Setting up Wireshark to capture packets for the first time can be tricky. The following are a few common problems that are encountered while capturing packets with Wireshark for the first time:

  - Special privileges are required to start a live capture.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- The correct network interface must be chosen to capture packet data from.
- Network packets should be captured at the correct location in the network to view the desired traffic.

- **Wireshark network analysis activities**

  Capturing live network data is one of the major features of Wireshark. The Wireshark capture engine enables network defenders to perform the following:

  - Capture from different types of network hardware such as Ethernet and 802.11.
  - Stop the capture based on different triggers such as the amount of captured data, elapsed time, or number of packets.
  - Simultaneously show decoded packets while capturing is in progress.
  - Filter packets to reduce the amount of data to be captured.
  - Save packets in multiple files during a long capture.
  - Simultaneously capture from multiple network interfaces.

- **First network packet capture using Wireshark**

  To capture packets using Wireshark, first install and launch the tool on the target network. Select the appropriate network interface to capture traffic from. The following are the steps to start capturing packets with Wireshark:

  1. Double-click on an interface in the main window.
  2. An overview of the available interfaces can be obtained using the Capture Interface dialog box.
  3. Start a capture from this dialog box using the Start button.
  4. A capture can be immediately started using the current settings by selecting **Capture → Start** or by clicking the first toolbar button.
  5. If the name of the capture interface is known, Wireshark can be launched from the command line through the following command: $ wireshark -i eth0 –k

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

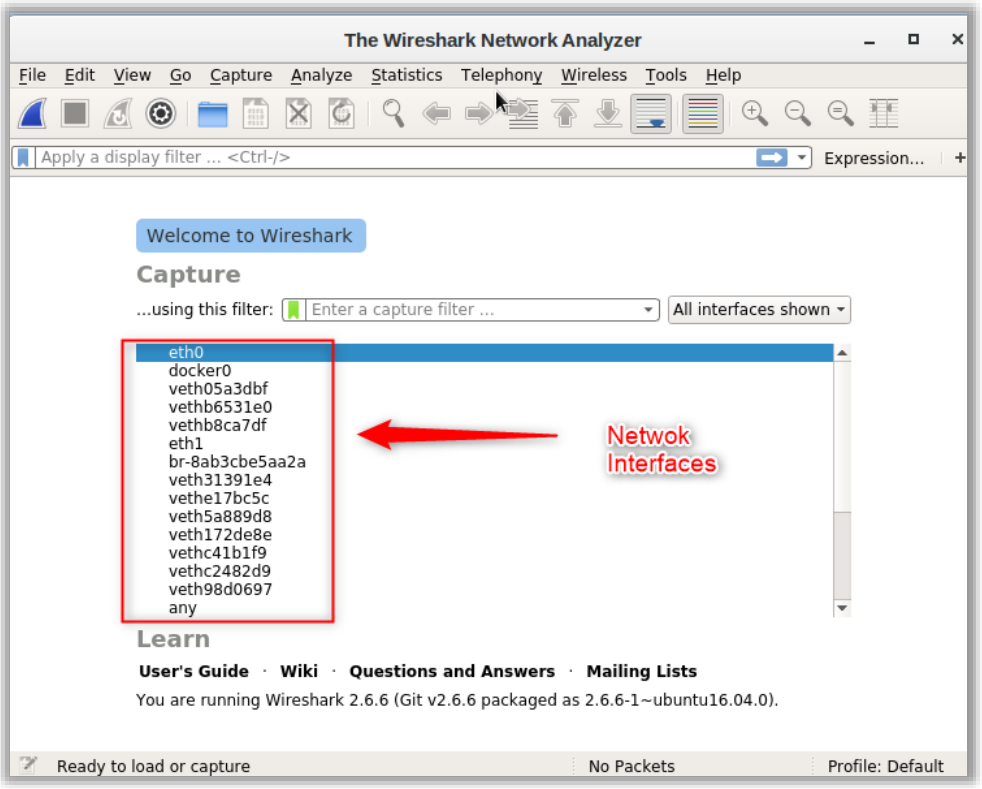


Figure 12.1: Wireshark Network Interfaces

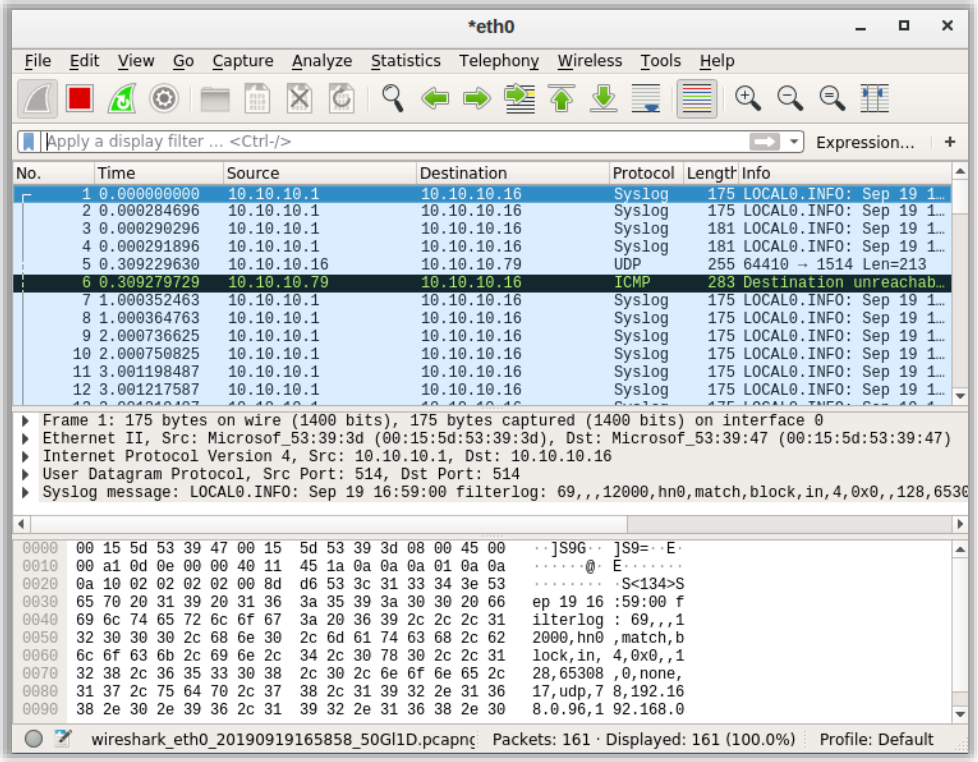


Figure 12.2: Capturing Traffic

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Wireshark components

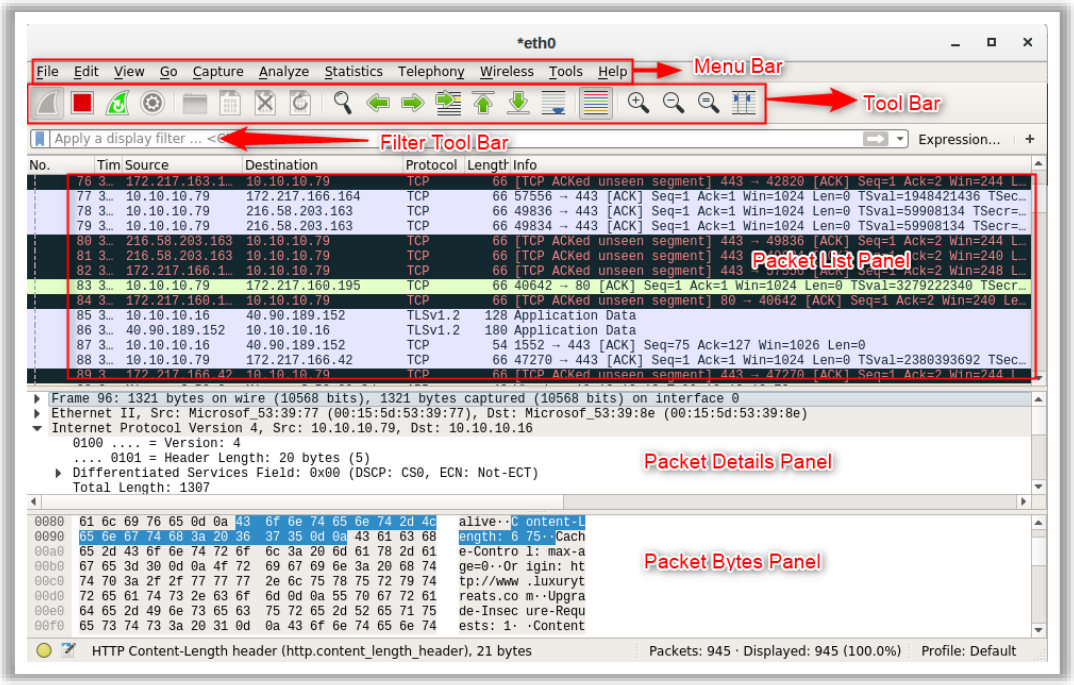


Figure 12.3: Wireshark components

The main menu of Wireshark contains the following items:

- **File:** This menu contains items to open and merge, capture files, save, print, import and export capture files in whole or in part, and quit the Wireshark application.
- **Edit:** This menu contains items to find a packet, time reference, and mark one or more packets. It handles configuration profiles and sets preferences.
- **View:** This menu controls the display of the captured data, including the colorization of packets, font zoom, display of a packet in a separate window, and expanding and collapsing of the packet tree details.
    - **Colorize packet list:** This option allows network defenders to control whether Wireshark should colorize the packet list. Enabling colorization slows down the display of new packets while capturing and loading capture files.
    - **Coloring rules:** This option allows network defenders to color packets in the packet list pane according to the filter expressions of their choice. It can be very useful for spotting certain types of packets.
    - **Colorize conversation:** This menu item brings up a submenu that allows the color of the packets to be changed in the packet list pane based on the addresses of the currently selected packet. This makes it easy to distinguish packets belonging to different conversations.
- **Go:** This menu contains options to navigate to a specific packet including a previous packet, the next packet, the corresponding packet, the first packet, and the last packet.

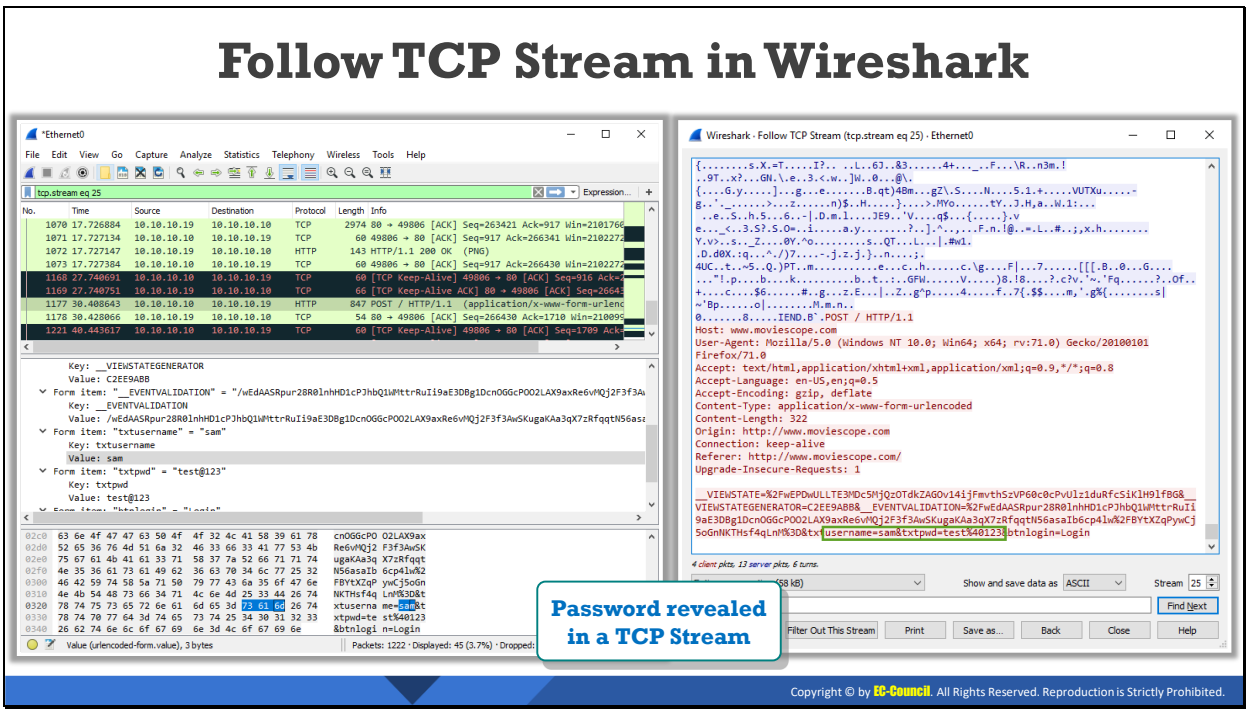
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **Capture:** This menu allows the network defenders to start, stop, and restart capture and to edit capture filters.
  - **Capture filters:** This option allows network defenders to create and edit capture filters. Filters can be named and saved for future use.
- **Analyze:** This menu contains items to manipulate, display and apply filters, enable or disable the dissection of protocols, configure user-specified decodes, and follow a different stream including TCP, UDP, and Secure Sockets Layer (SSL).
  - **Follow TCP stream:** This option displays all the captured TCP segments that are on the same TCP connection as a selected packet.
  - **Follow UDP stream:** This option displays all the captured UDP segments that are on the same UDP connection as a selected packet.
  - **Follow SSL stream:** This option displays all the captured SSL segments that are on the same SSL connection as a selected packet.
- **Statistics:** This menu contains options to display various statistic windows, including a summary of the packets that have been captured, display protocol hierarchy statistics, IO graphs, and flow graphs.
- **Telephony:** This menu contains options to display various telephony-related statistic windows including a media analysis, flow diagrams, and display protocol hierarchy statistics.
- **Wireless:** This menu shows Bluetooth and IEEE 802.11 wireless statistics.
- **Tools:** This menu contains various tools available in Wireshark including the creation of firewall access control list (ACL) rules and use of the Lua interpreter.
  - **Firewall ACL rules:** This tool can be used create command-line ACL rules for many different firewall products, including Cisco IOS, Linux Netfilter, OpenBSD and Windows Firewall. Rules for MAC addresses, IPv4 addresses, TCP and UDP ports, and IPv4+port combinations are supported. It is assumed that the rules will be applied to an outside interface.
  - **Lua:** This tool includes options that allow network defenders to work with the built-in Lua interpreter of Wireshark. Wireshark uses Lua to write protocol dissectors.
- **Help:** This menu contains items to help the user, including access to basic help manual pages for the various command-line tools, online access to some webpages, and the About Wireshark dialog.
- **Main toolbar:** The main toolbar provides quick access to frequently used items from the menu. This toolbar cannot be customized by the user. If the space on the screen is needed to show more packet data, then the toolbar can be hidden using the View menu. As in the menu, only the items that can be used in the current program state will be available. The others will be greyed out.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **Filter toolbar:** The filter toolbar allows network defenders to quickly edit and apply display filters.
- **Packet list panel:** This panel displays a list of packets in the current capture file. It colors the packets based on the protocol. Each line in the packet list corresponds to one packet in the capture file. If a line in this pane is selected, more details will be displayed in the Packet Details and Packet Bytes panes.
- The default columns show the following:
  - **No:** This column shows the number of the packets in the capture file. This number does not change, even if a display filter is used.
  - **Time**: This column shows the timestamp of the packet. The presentation format of this timestamp can be changed.
  - **Source:** This column shows the source address of the packet.
  - **Destination**: This column shows the destination address of the packet.
  - **Protocol**: This column shows the protocol name in the abbreviated form.
  - **Info**: This column shows additional information about the packet content.
- **Packet details panel:** This panel displays the details of the selected packet. It includes the different protocols making up the layers of data in this packet. The protocols and fields of the packet are displayed using a tree, which can be expanded and collapsed. Layers include the frame, Ethernet, IP, TCP, UDP, ICMP, and application protocols such as HTTP.
- **Packet bytes panel:** This panel displays the packet bytes in a hex dump and American Standard Code for Information Interchange (ASCII) encodings. For a hex dump, the left side shows the offset in the packet data, and the middle of the packet data is shown in a hexadecimal representation. On the right, the corresponding ASCII characters are displayed.
- **Status bar:** The status bar displays informational messages. In general, the left side shows context-related information, the middle part shows the current number of packets, and the right side shows the selected configuration profile. The user can drag the handles between the text areas to change the size.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Follow TCP Stream in Wireshark

Source: *https://www.wireshark.org*

Wireshark displays data from the TCP port with a feature known as "**Follow TCP stream**." The tool sees TCP data in the same way as that of the application layer. Use this tool to find passwords in a telnet session or to interpret a data stream.

To see the TCP stream, select a TCP packet in the packet list of a stream/connection and then select the **Follow TCP Stream** menu item from the Wireshark **Tools** menu. Wireshark displays all the data from the TCP stream by setting an appropriate display filter. The tool displays the streaming content in the same sequence as it appeared on the network. It displays the captured data in ASCII, EBCDIC, hex dump, C array, or raw formats.

As shown in the screenshot, you can capture network traffic and gain the credentials of a target machine. You can attempt to capture its remote interface and monitor the traffic generated from a user's browsing activities to extract confidential user information.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

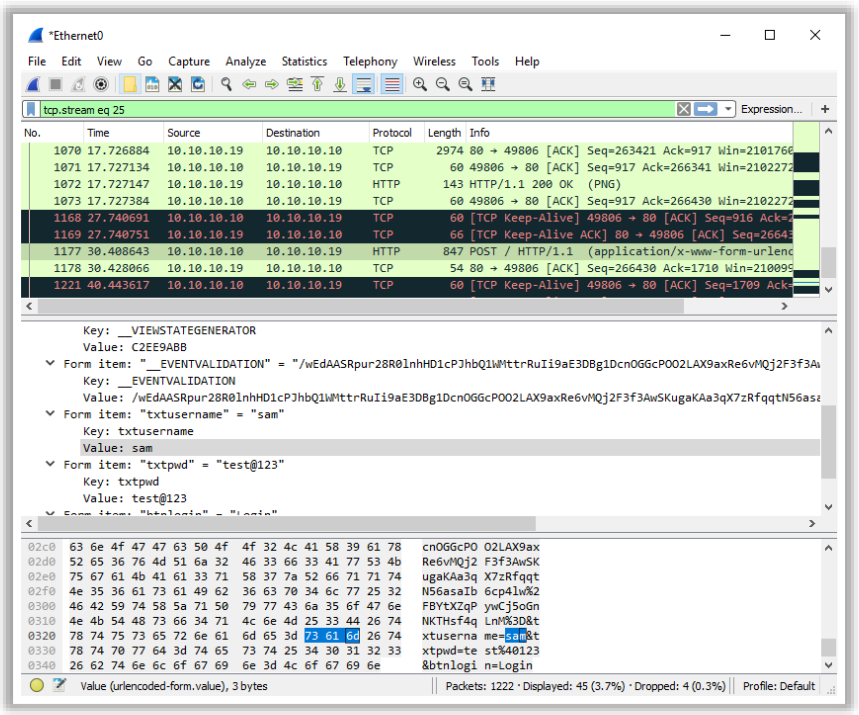


Figure 12.4: Wireshark capturing TCP Stream

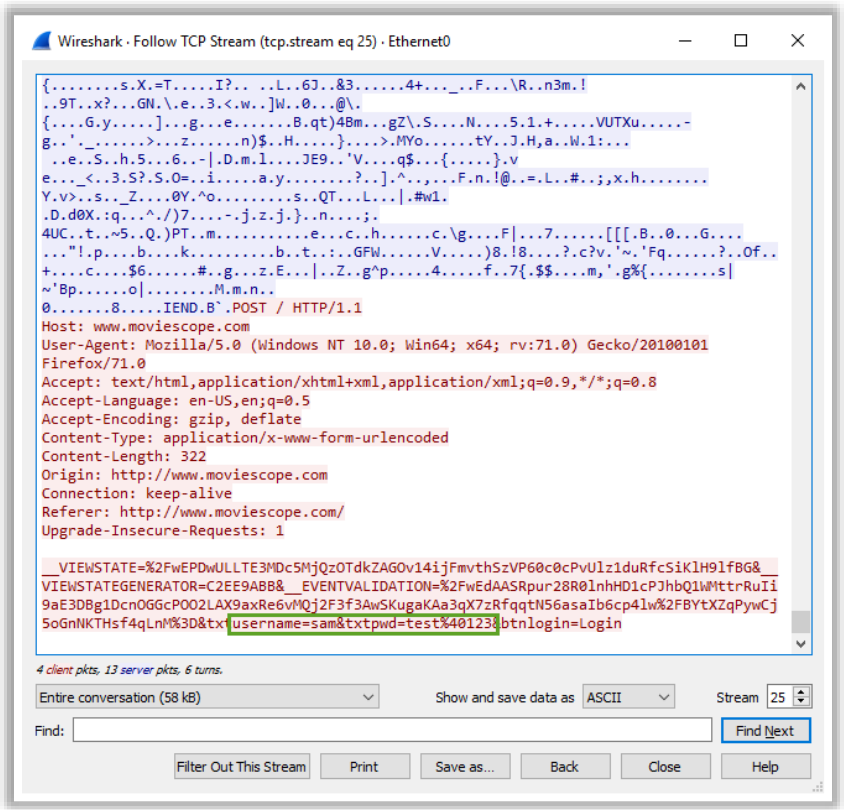
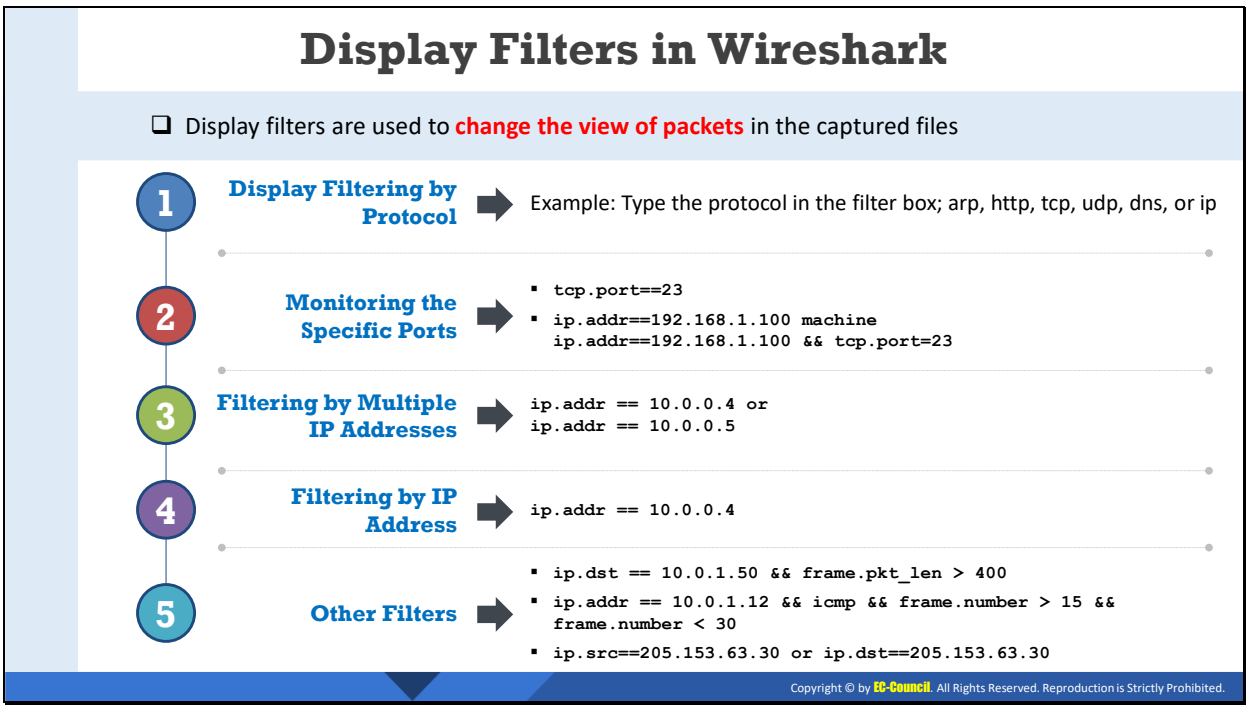


Figure 12.5: Wireshark feature Follow TCP Stream

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Display Filters in Wireshark

Source: *https://wiki.wireshark.org*

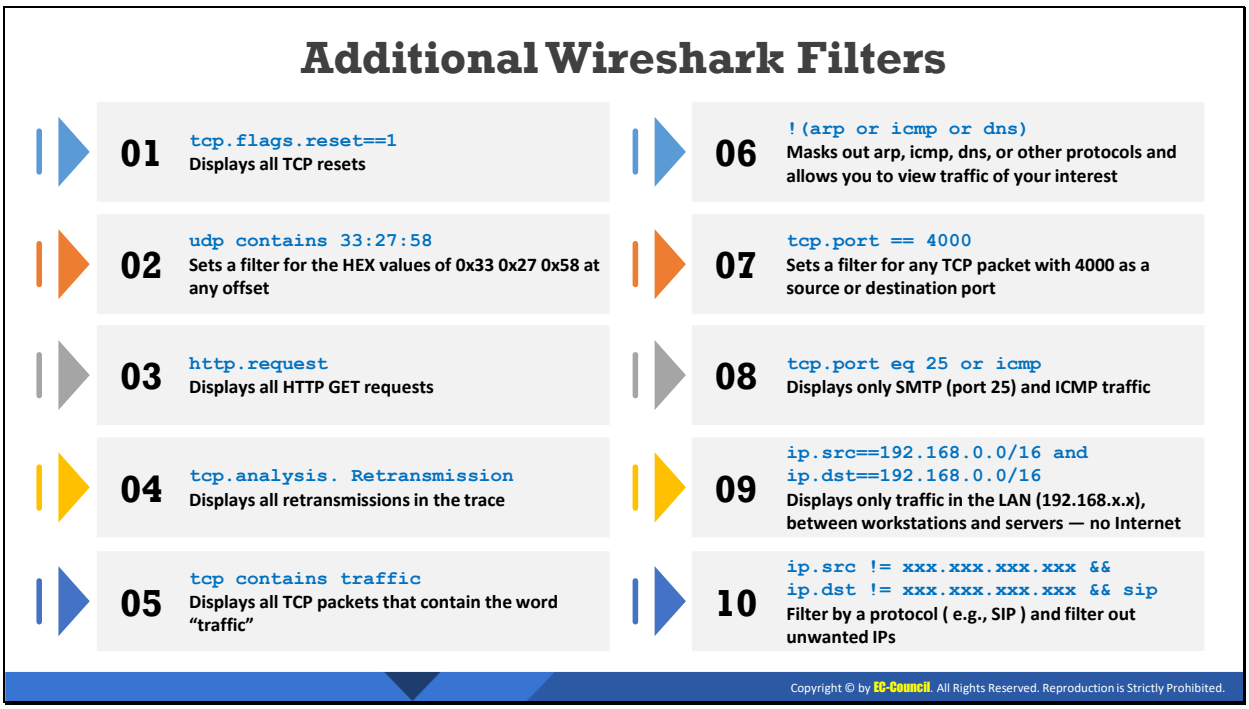
Wireshark features display filters that filter traffic on the target network by protocol type, IP address, port, etc. Display filters are used to change the view of packets in the captured files. To set up a filter, type the protocol name, such as arp, http, tcp, udp, dns, and ip, in the filter box of Wireshark. Wireshark can use multiple filters at a time.

Some of the display filters in Wireshark are listed below:

- **Display Filtering by Protocol**

  Example: Type the protocol in the filter box: arp, http, tcp, udp, dns, ip
- **Monitoring the Specific Ports**
  - `tcp.port==23`
  - `ip.addr==192.168.1.100 machine`
    `ip.addr==192.168.1.100 && tcp.port==23`
- **Filtering by Multiple IP Addresses**
  - `ip.addr == 10.0.0.4 or ip.addr == 10.0.0.5`
- **Filtering by IP Address**
  - `ip.addr == 10.0.0.4`
- **Other Filters**
  - `ip.dst == 10.0.1.50 && frame.pkt_len > 400`
  - `ip.addr == 10.0.1.12 && icmp && frame.number > 15 && frame.number < 30`
  - `ip.src==205.153.63.30 or ip.dst==205.153.63.30`

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Additional Wireshark Filters

Source: *https://wiki.wireshark.org*

Some examples of additional Wireshark filters are listed below:

- **`tcp.flags.reset==1`**

  Displays all TCP resets

- **`udp contains 33:27:58`**

  Sets a filter for the hex values of 0×33 0×27 0×58 at any offset

- **`http.request`**

  Displays all HTTP GET requests

- **`tcp.analysis.retransmission`**

  Displays all retransmissions in the trace

- **`tcp contains traffic`**

  Displays all TCP packets that contain the word "traffic"

- **`!(arp or icmp or dns)`**

  Masks out arp, icmp, dns, or other protocols and allows you to view the traffic of your interest

- **`tcp.port == 4000`**

  Sets a filter for any TCP packet with 4000 as a source or destination port

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **`tcp.port eq 25 or icmp`**

  Displays only SMTP (port 25) and ICMP traffic

- **`ip.src==192.168.0.0/16 and ip.dst==192.168.0.0/16`**

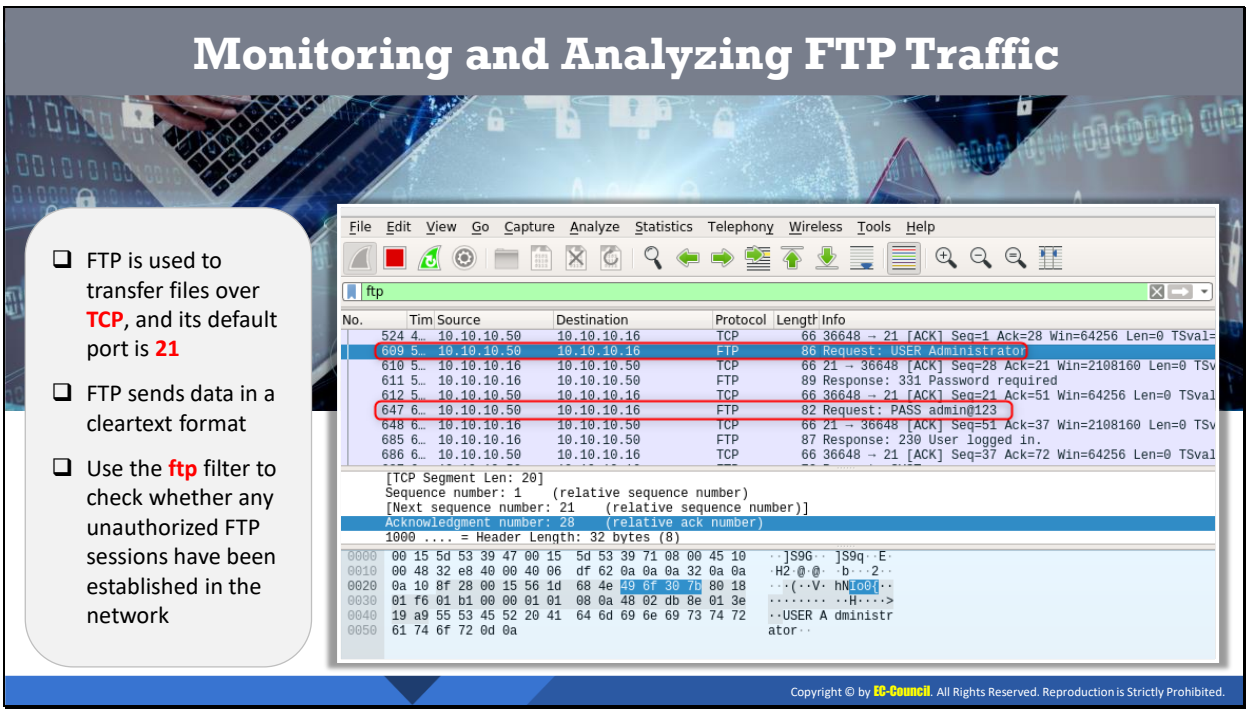
  Displays only traffic in the LAN (192.168.x.x), between workstations and servers—no Internet

- **`ip.src != xxx.xxx.xxx.xxx && ip.dst != xxx.xxx.xxx.xxx && sip`**

  Filters by a protocol (e.g., SIP) and filters out unwanted IPs

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Monitoring and Analyzing FTP Traffic

FTP offers neither a secure network environment nor secure user authentication. Individuals do not need authentication to access an FTP server in a network. This provides an easy method for attackers to enter the network and access resources. FTP does not provide encryption in the data transfer process, and the data transfer between the sender and receiver is in plain text. Consequently, critical information such as usernames and passwords are exposed to attackers. The implementation of FTP in an organization's network leaves the data accessible to external sources. Deploying FTP in a network can lead to types of attacks such as FTP bounce, FTP brute force, and packet sniffing attacks.

Wireshark provides complete information about the FTP traffic on a network for monitoring. Applying an FTP filter helps detect unauthorized sessions running on the server. Apart from monitoring the traffic on the FTP server, the existing file contents and file sizes in the server should be monitored.

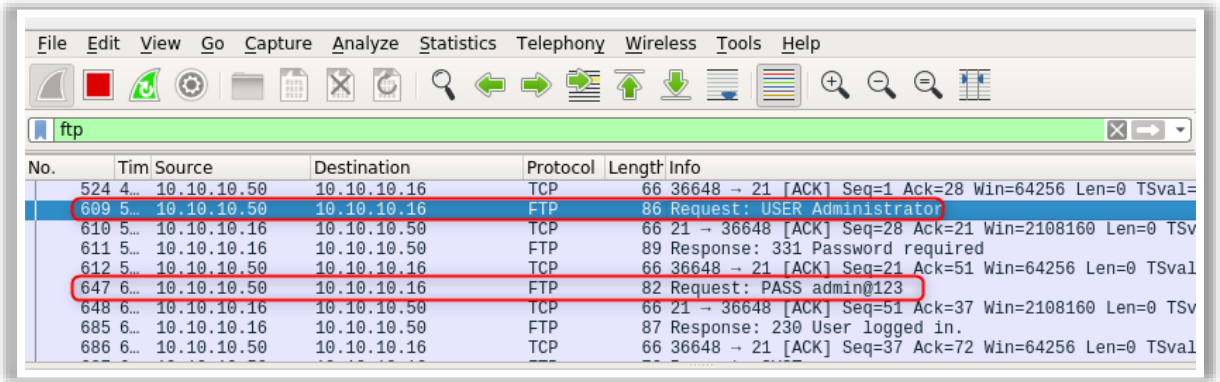
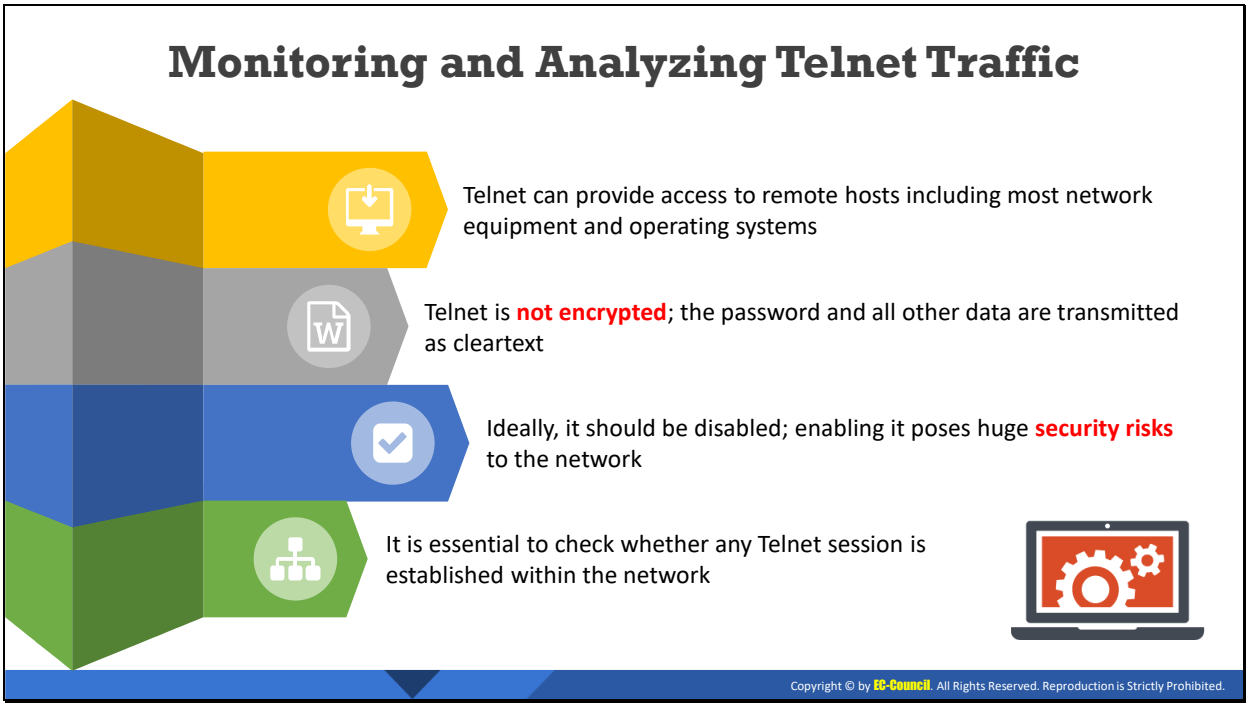
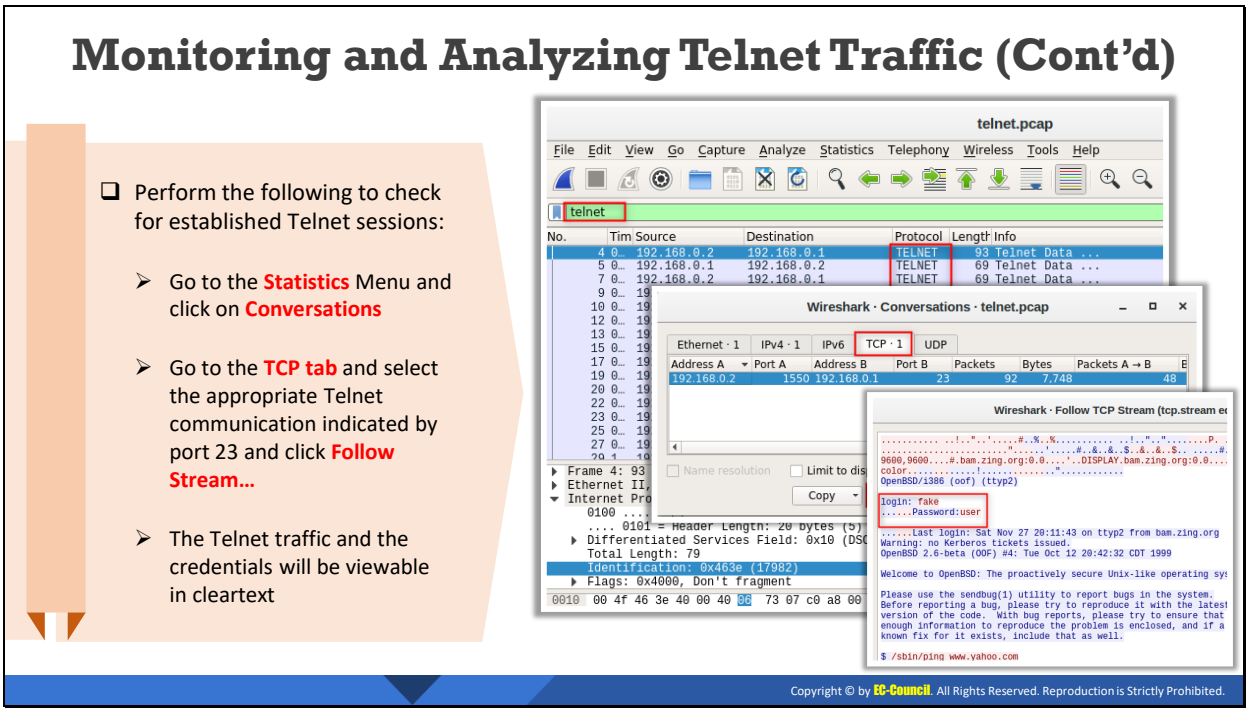


Figure 12.6: FTP traffic

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets





Monitoring and Analyzing Telnet Traffic

The Telnet protocol works on a client–server model. It provides access to remote network equipment and OSes. The data transferred through Telnet is not encrypted, making it easy for intruders to eavesdrop. If a person has access to a network device with Telnet configured, they can gain access to the network and user account information. Generally, Telnet should be disabled in an organization.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Telnet is a session-oriented protocol, which implies that the connection must be open for the entire session. Attackers can use Telnet open sessions to perform a network security breach. Therefore, security professionals should monitor Telnet sessions (if any) running on their network. Timely monitoring of Telnet sessions through Wireshark can greatly minimize the risk for network intrusion.

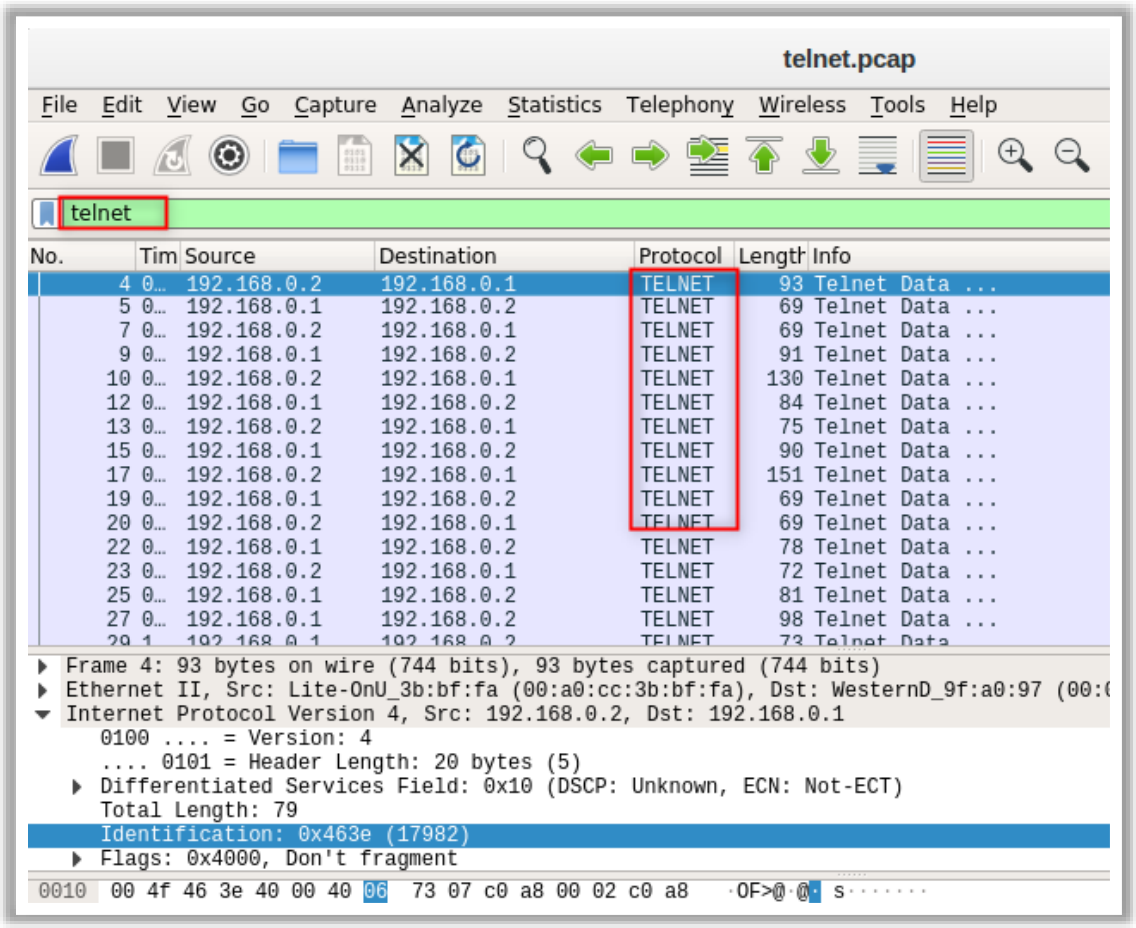


Figure 12.7: Telnet traffic

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- Perform the following to check for established Telnet sessions:
  - Go to the **Statistics** Menu and click on **Conversations.**
  - Go to the **TCP tab** and select the appropriate Telnet communication indicated by port 23 and click **Follow Stream…**

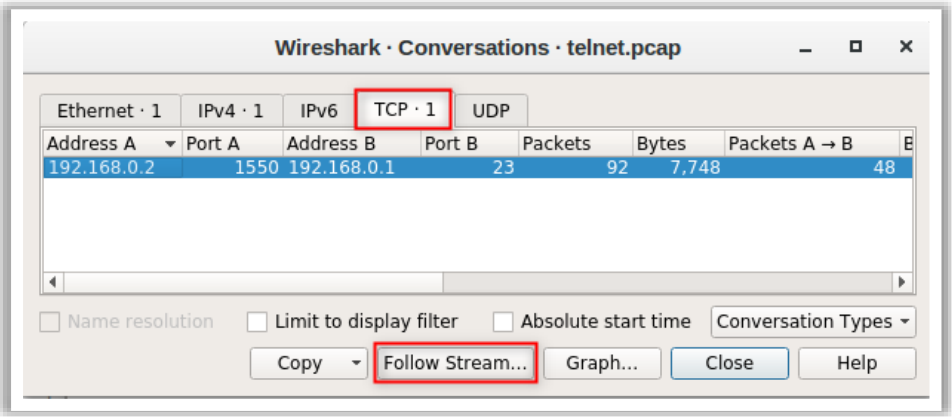
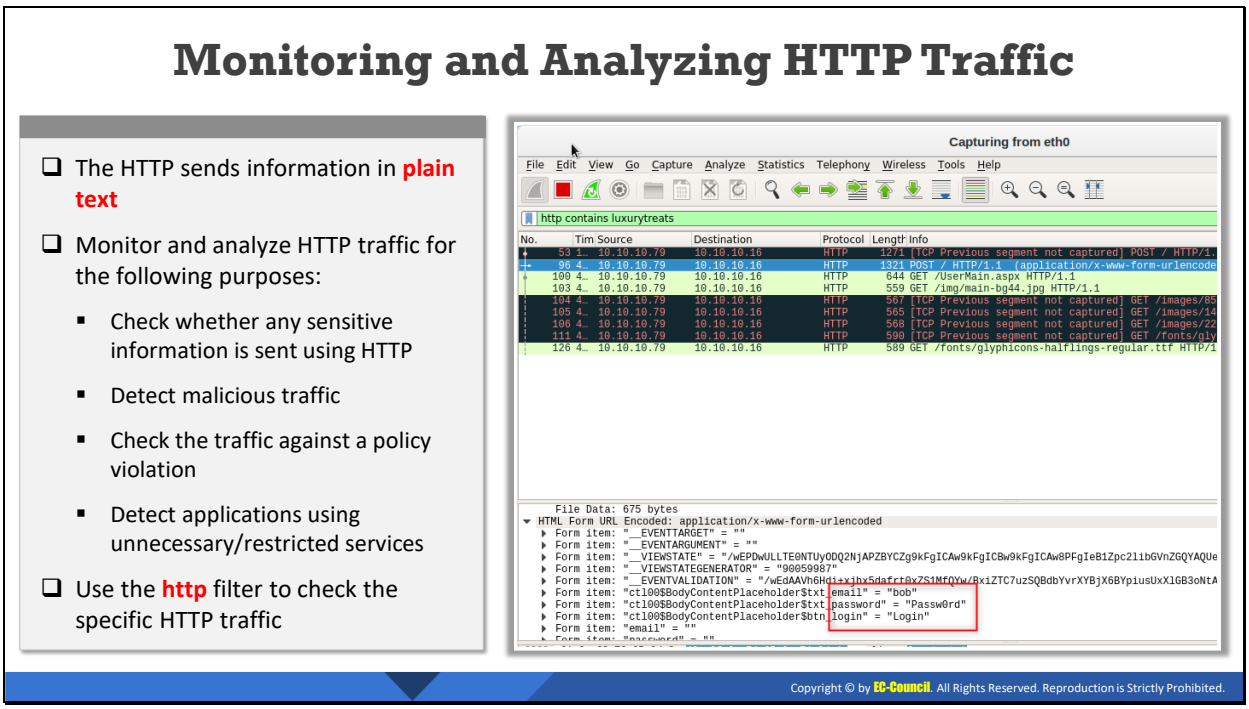


Figure 12.8: TCP tab

  - The Telnet traffic and the credentials will be viewable in cleartext.

Figure 12.9: Cleartext credential in telnet traffic

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Monitoring and Analyzing HTTP Traffic

Applications implementing HTTP send data in cleartext. Implementing HTTP can pose security risks to the organization as sensitive information such as usernames and passwords are sent over as HTTP requests. The attacker can easily sniff the traffic and steal sensitive information for malicious use. Therefore, security professionals must ensure that their HTTP traffic is sent over an encrypted protocol such as HTTP Secure (HTTPS). Simultaneously, they should monitor applications and ensure that they do not send data over HTTP. Monitoring the HTTP traffic also helps detect the volume of HTTP traffic in the network. It also helps detecting malicious traffic, policy violation attempts, applications using unnecessary/restricted services.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Use the http filter to check the specific HTTP traffic.

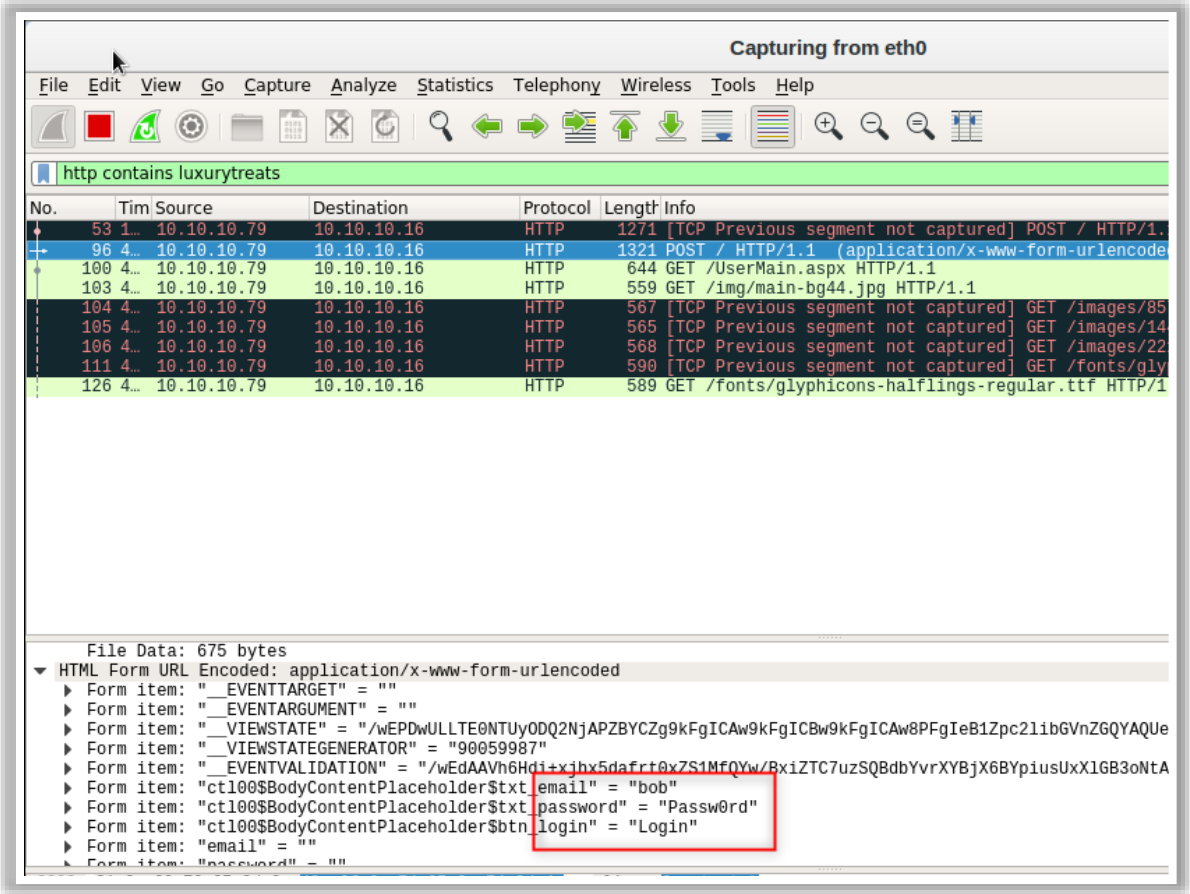
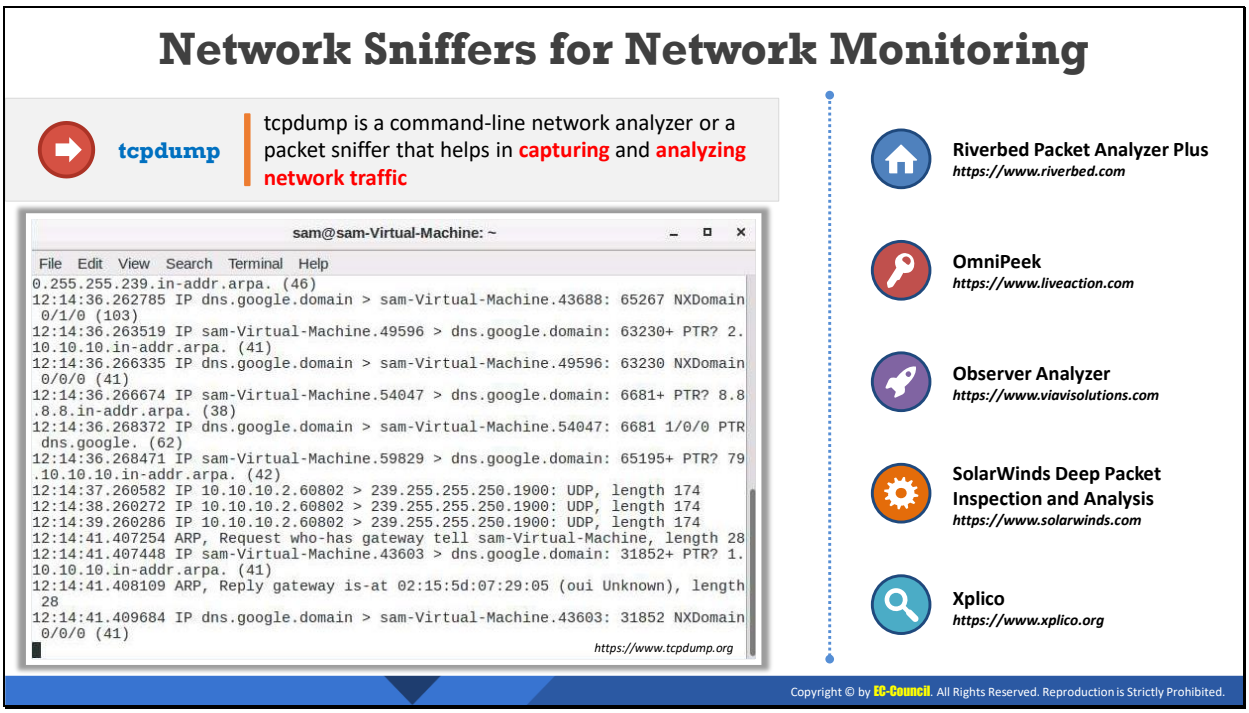


Figure 12.10: Cleartext credential in HTTP traffic

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Network Sniffers for Network Monitoring

- **tcpdump**

  Source: *https://www.tcpdump.org*

  tcpdump is a command-line network analyzer or a packet sniffer. Security professionals can use this utility for network monitoring and analysis.

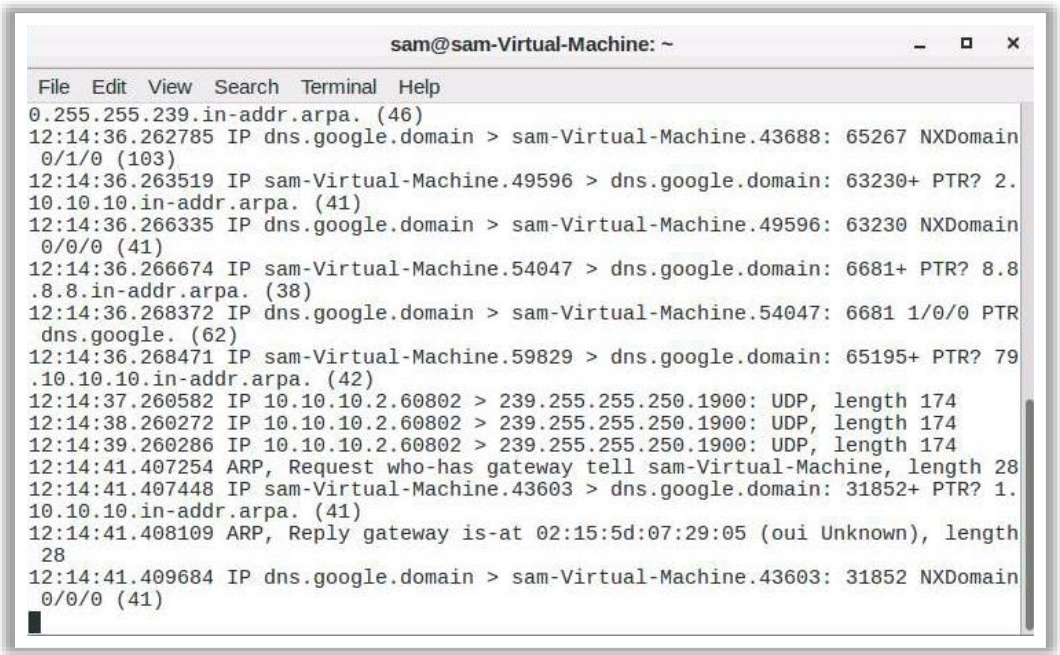


Figure 12.11: Screenshot of tcpdump

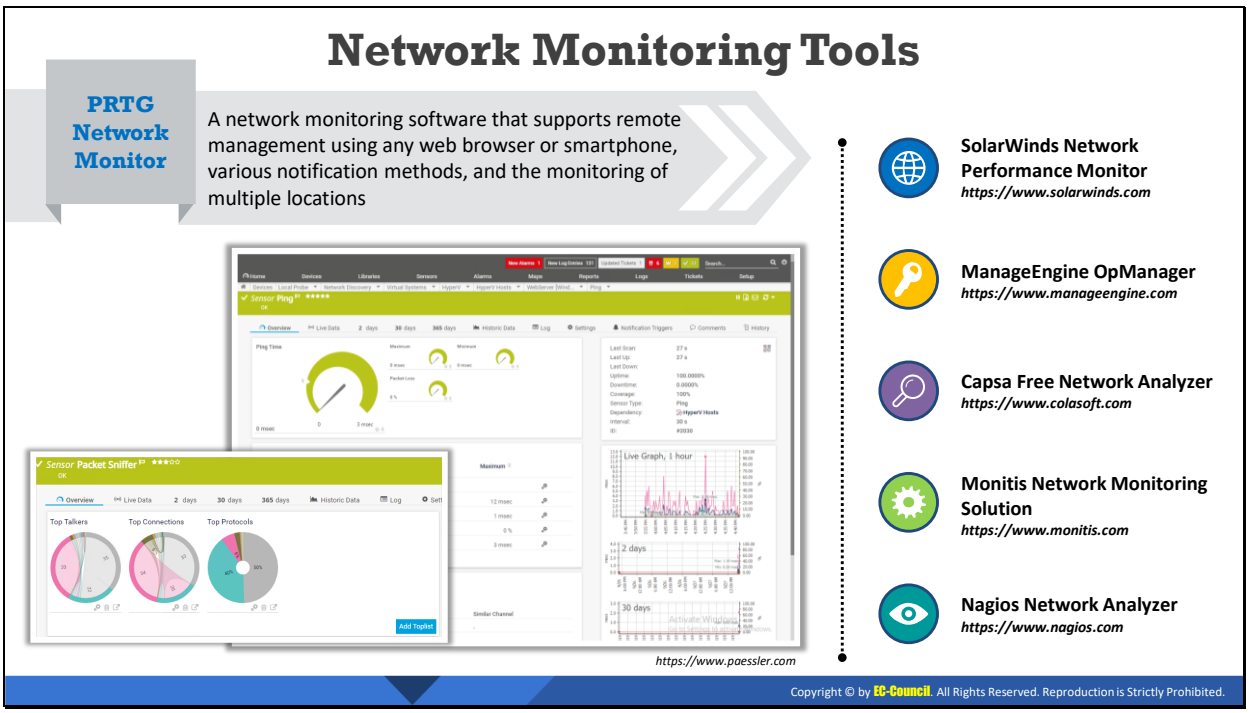
Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Some additional network sniffing tools are as follows:

- Riverbed Packet Analyzer Plus (*https://www.riverbed.com*)
- OmniPeek (*https://www.liveaction.com*)
- Observer Analyzer (*https://www.viavisolutions.com*)
- SolarWinds Deep Packet Inspection and Analysis (*https://www.solarwinds.com*)
- Xplico (*https://www.xplico.org*)

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets



Network Monitoring Tools

- **PRTG Network Monitor**

  Source: *https://www.paessler.com*

  PRTG Network Monitor is a network monitoring software that supports remote management using any web browser or smartphone, various notification methods, and the monitoring of multiple locations. Network defender can use this utility for availability, usage, and activity monitoring, and it covers the entire range from website monitoring to database performance monitoring.

  It helps in the following:

  - Avoid bandwidth and performance bottlenecks.
  - Identify applications or servers using up the available bandwidth.
  - Instantly identify sudden spikes caused by malicious code.
  - Reduce the costs of purchasing additional hardware and bandwidth.

  PRTG can collect data for almost anything of interest on the network. It supports multiple protocols for collecting data:

  - Simple Network Management Protocol (SNMP) and Windows Management Instrumentation (WMI)
  - Packet sniffing
  - NetFlow, IP Flow Information Export (IPFIX), jFlow, and sFlow

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

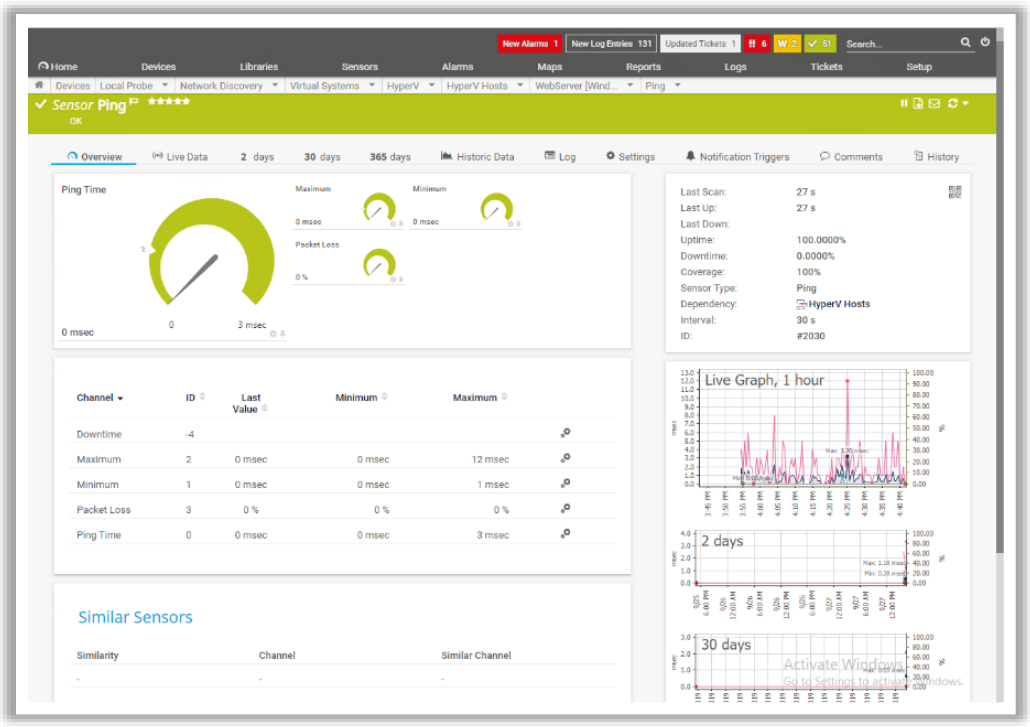


Figure 12.12: Screenshot of PRTG Network Monitor

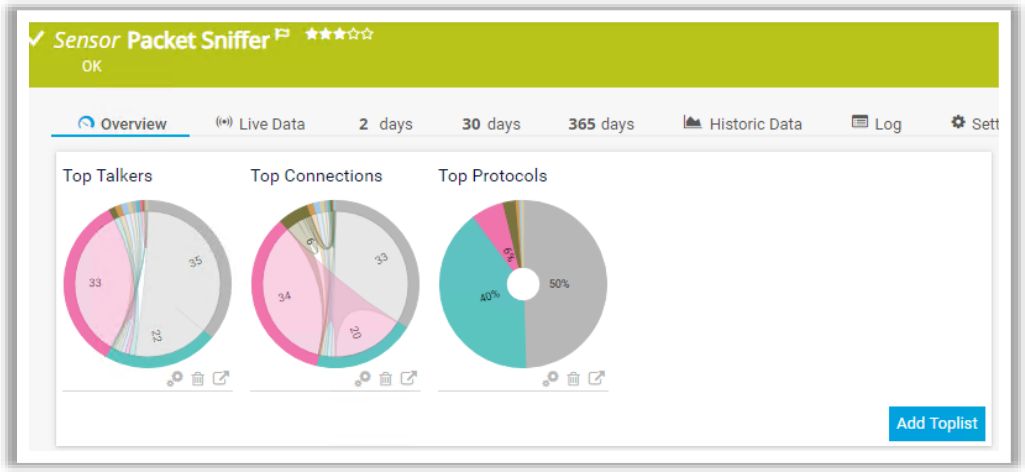
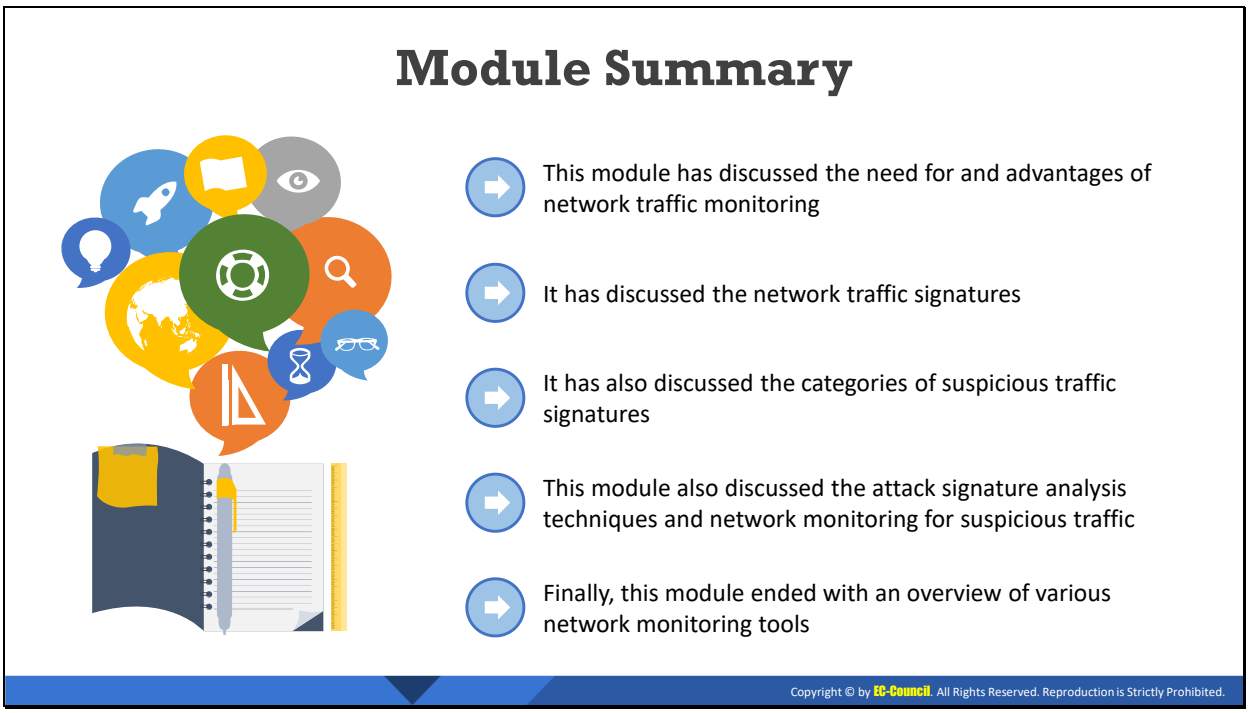


Figure 12.13: Performance monitoring using PRTG Network Monitor

Some additional network monitoring tools are as follows:

- SolarWinds Network Performance Monitor (*https://www.solarwinds.com*)
- ManageEngine OpManager (*https://www.manageengine.com*)
- Capsa Free Network Analyzer (*https://www.colasoft.com*)
- Monitis Network Monitoring Solution (*https://www.monitis.com*)
- Nagios Network Analyzer (*https://www.nagios.com*)

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets



Module Summary

This module discussed the need for and advantages of network traffic monitoring. It discussed the signatures of network traffic as well as the categories of suspicious traffic signatures. Furthermore, this module discussed attack signature analysis techniques and network monitoring for suspicious traffic. Finally, this module presented an overview of various network monitoring tools.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

Glossary

A

- **Availability:** Ensures information is available to authorized parties without any disruption.
- **Authentication:** Ensures the identity of an individual is verified by the system or service.
- **Authorization:** Authorization refers to the process of providing permission to access the resources or perform an action on the network.
- **Accounting:** Accounting is a method of keeping track of user actions on the network. It keeps track of who, when, and how the users access the network.
- **Application Level Gateways:** Application level gateways can filter packets at the application layer of the OSI model.
- **Application Proxy:** An application-level proxy works as a proxy server and filters connections for specific services.
- **Anonymous Proxy:** An anonymous proxy does not transfer information about the IP address of its user, thereby hiding information about the user and their surfing interests.
- **Anomaly Detection:** It detects the intrusion based on the fixed behavioral characteristics of the users and components in a computer system.
- **Administrative Security Controls**: Administrative security controls are management limitations, operational and accountability procedures, and other controls that ensure the security of an organization.
- **Access Control**: Access control is the selective restriction of access to an asset or a system/network resource.
- **Alert**: An alert is a graduated event that notifies that a particular event (or series of events) has reached a specified threshold and needs appropriate action by a responsible party.
- **Alert Systems:** An alert system sends an alert message when any anomaly or misuse is detected.
- **Alarm System**: Alarms are used to draw attention when there is a breach or during an attempt of breach.
- **Access point (AP)**: Used to connect wireless devices to a wireless/wired network.
- **Anomaly-based Detection**: The anomaly-based detection process depends on observing and comparing the observed events with the normal behavior and then detecting any deviation from it.
- **AAA Server:** The AAA server is used to establish secure access in a remote-access VPN environment.
- **Anything-as-a-Service (XaaS):** Anything as a service (XaaS) is a cloud-computing and remote-access service that offers anything as a service over the Internet based on the user's demand.
- **Association**: It refers to the process of connecting a wireless device to an AP.
- **Antenna:** Converts electrical impulses into radio waves and vice versa.
- **Asymmetric Encryption**: Asymmetric encryption uses two separate keys to carry out encryption and decryption.
- **Advanced Encryption Standard (AES):** The AES is a National Institute of Standards and Technology (NIST) specification for the encryption of electronic data.
- **Audit Trails**: An audit trail is a set of records that provide documentary evidence of a system's activity.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

- **Application Containers**: These are containers used to run a single service. They have layered file systems and are built on top of OS container technologies.
- **ANT**: It is a wireless sensor protocol that enables communication between sensors and their controllers.

B

- **Biometric Authentication:** Biometrics is a technology which identifies human characteristics for authenticating people.
- **Bollards:** A bollard may be defined as a short vertical post which controls and restricts motor vehicles to the parking areas, offices etc.
- **Bastion Host:** A bastion host is a computer system designed and configured to protect network resources from attacks.
- **Bandwidth**: It describes the amount of information that may be broadcast over a connection.
- **Basic Service Set Identifier (BSSID)**: It is the media access control (MAC) address of an access point (AP) or base station that has set up a basic service set (BSS).
- **Bollards**: A bollard may be defined as a short vertical post which controls and restricts motor vehicles to the parking areas, offices etc.
- **Behavior-based IDS**: Behavior-based intrusion detection techniques assume an intrusion can be detected by observing a deviation from normal or expected behavior of the system or users.
- **Bluetooth:** In the Bluetooth technology, data is transmitted between cell phones, computers, and other networking devices over short distances.
- **Biometrics:** Biometrics is an advanced and unique security technology that utilizes an individual's physical attributes such as fingerprint, iris, face, voice, and behavior for verifying their identity.
- **Bring Your Own Device (BYOD):** BYOD refers to a policy that allows employees to bring their devices such as laptops, smartphones, and tablets to the workplace.
- **Business Critical Data:** Business critical data contains information that is important for business operation.

C

- **Confidentiality:** Ensures information is not disclosed to unauthorized parties
- **Compensating Controls:** These controls are used as an alternative control when the intended controls fail or cannot be used.
- **Combination Locks:** It has a combination of numbers and letters. The user needs to provide the combination to open the lock.
- **Computer Fraud and Abuse Act**: States that, whoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer, and if the conduct involves an interstate or foreign communication, shall be punished under the Act.
- **Circuit-Level Gateway:** Circuit level gateways work at the session layer of the OSI model, or the TCP layer of TCP/IP.
- **Client-to-Site (Remote-access) VPNs:** Remote-Access VPNs allow individual hosts or clients, such as telecommuters and mobile users to establish secure connections to a company's network over the Internet.
- **Container:** Containers refer to virtualization based on an operating system, in which the kernel's operating system functionality is replicated on multiple instances of isolated user space.
- **Cloud Computing:** Cloud computing is an on-demand delivery of IT capabilities where IT infrastructure and applications are provided to subscribers as a metered service over a network.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- **Cloud Storage**: Cloud storage is a data storage medium used to store digital data in logical pools using a network.
- **Cloud-to-Cloud (Back-End Data-Sharing) Communication Model**: This type of communication model extends the device-to-cloud communication type such that the data from the IoT devices can be accessed by authorized third parties.
- **Cloud Platform**: In an IoT ecosystem, the cloud component is referred to as the central aggregation and data management point.
- **Cloud Data Backup**: Storing backup data on storage provided by an online backup provider.
- **Container-as-a-Service (CaaS):** This cloud computing model provides containers and clusters as a service to its subscribers.
- **Community Cloud:** Shared infrastructure between several organizations from a specific community with common concerns (security, compliance, jurisdiction, etc.).
- **Cloud Consumer:** A person or organization that uses cloud computing services.
- **Cloud Provider:** A person or organization providing services to interested parties via network access.
- **Cloud Carrier:** A cloud carrier acts as an intermediary that provides connectivity and transport services between CSPs and cloud consumers.
- **Cloud Auditor:** A cloud auditor is a party that performs an independent examination of cloud service controls to express an opinion thereon.
- **Cloud Broker:** An entity that manages cloud services in terms of use, performance, and delivery, and maintains the relationship between cloud providers and consumers.
- **Cellular Communication:** Cellular communication is based on a single network tower that serves devices located within a specific radius.
- **Cross-Container Attacks**: Gaining access to a container and utilizing it to attack other containers of the same host or within the local network.
- **Communication Layer**: The communication (connectivity/edge computing) layer includes the components of communication protocols and networks used for connectivity and edge computing.
- **Cloud Layer**: Servers hosted in the cloud accept, store, and process the sensor data received from IoT gateways.
- **Contraband**: Contraband includes materials that are banned from entering the environment such as explosives, bombs, weapons, etc.
- **5G Cellular (Mobile) Communication**: It is a broadband cellular network that operates at high bandwidth with low latency and provides high-speed data downloads.
- **Centralized IDS**: In a centralized system, the data is gathered from different sites to a central site.
- **Context-aware Authentication:** Context-aware authentication is a type of enhanced security technique that uses the contextual information of a user for enhancing data security decisions.
- **Containerization:** Containerization is a technique in which all personal and organizational data are segregated on an employee's mobile device.
- **Choose Your Own Device (CYOD):** CYOD refers to a policy in the employees select their device of choice from a preapproved set of devices (laptops, smartphones, and tablets) to access company data according to the access privileges of an organization.
- **Corporate Owned, Personally Enabled (COPE):** Corporate Owned, Personally Enabled (COPE) refers to a policy that allows employees to use and manage the devices purchased by the organizations.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- **Company Owned, Business Only (COBO):** Company Owned, Business Only (COBO) refers to a policy that allows employees to use and manage the devices purchased by the organization but restrict the use of the device for business use only.
- **Cryptography:** Cryptography is the practice of concealing information by converting plaintext (readable format) into ciphertext (unreadable format) using a key or encryption scheme.
- **CCMP**: An encryption protocol used in WPA2 for stronger encryption and authentication.
- **Certification Authorities**: Certification authorities (CAs) are trusted entities that issue digital certificates.
- **Centralized Authorization**: It maintains a single database for authorizing all the network resources or applications.
- **Command Console:** It provides a user interface to an administrator for the purpose of receiving and analyzing security events, alert message, and log files.
- **Ciphers:** A cipher is an algorithm for performing encryption and decryption.

D

- **Deterrence Controls:** These are used to discourage the violation of security policies.
- **Detection Controls:** These are used to detect unauthorized access attempts.
- **Discretionary Access Control (DAC):** DAC determines the access control taken by any possessor of an object in order to decide the access control of a subject on that object.
- **Detective Controls:** These controls detect security violations and record any intrusion attempts.
- **Digital Locks:** Digital locks use fingerprint, smart card or a PIN on the keypad to unlock.
- **Demilitarized Zone (DMZ):** A computer subnetwork is placed between the organization's private network such as a LAN, and an outside public network such as the Internet, and acts as an additional security layer.
- **Dual Firewall DMZ**: The dual firewall approach uses two firewalls to create a DMZ.
- **Distributed IDS**: A distributed intrusion detection system (dIDS) consists of multiple IDSs over a large network.
- **Database Honeypots:** Database honeypots employ fake databases that are vulnerable to perform database-related attacks such as SQL injection and database enumeration.
- **Docker:** Docker is an open source technology used for developing, packaging, and running applications and all its dependencies in the form of containers, to ensure that the application works in a seamless environment.
- **Docker Networking**: The Docker networking architecture is developed on a set of interfaces known as container network model (CNM). CNM provides application portability across heterogeneous infrastructures.
- **Docker Registry Attacks**: Gaining access to the docker registry.
- **Device Layer**: The device or thing layer of IoT includes the hardware that constitutes IoT devices.
- **Device-to-Device Communication**: In this type of communication, inter-connected devices interact with each other through the Internet, but they predominantly use protocols such as ZigBee, Z-Wave or Bluetooth.
- **Device-to-Cloud Communication**: In this type of communication, devices communicate with the cloud directly, rather than directly communicating with the client to send or receive data or commands.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- **Device-to-Gateway Communication**: In the device-to-gateway communication model, the IoT device communicates with an intermediate device called a gateway, which in turn communicates with the cloud service.
- **Decentralized Authorization**: A decentralized authorization maintains a separate database for each resource.
- **Data Backup Strategy**: An ideal backup strategy includes steps ranging from selecting the right data to conducting a test data restoration drill.
- **Direct-sequence Spread Spectrum (DSSS):** DSSS is a spread spectrum technique that multiplies the original data signal with a pseudo-random noise-spreading code.
- **Directional Antenna:** A directional antenna can broadcast and receive radio waves from a single direction.
- **Dipole Antenna:** A dipole antenna is a straight electrical conductor measuring half a wavelength from end to end, and it is connected at the center of the radio frequency (RF) feed line.
- **Data Encryption Standard (DES):** DES is designed to encipher and decipher blocks of data consisting of 64 bits under control of a 56-bit key.
- **Digital Signature Algorithm (DSA): The** digital signature algorithm (DSA) is a Federal Information Processing Standard (FIPS) for digital signatures.
- **Digital Signature:** Digital signatures use the asymmetric key algorithms to provide data integrity.
- **Digital Certificates:** Digital certificates allow a secure exchange of information between a sender and a receiver.
- **Data Security:** Data security involves the application of various data security controls to prevent any intentional or unintentional act of data misuse, data destruction, and data modification.
- **Data Protection Act 2018 (DPA)**: The DPA is an act to make provision for the regulation of the processing of information relating to individuals.
- **Data Access Control:** Data access controls enable authentication and authorization of users to access the data.
- **Data Encryption:** Protecting information by transforming it so that it becomes unreadable for an unauthorized party.
- **Data Masking:** Protecting information by obscuring specific areas of data with random characters or codes.
- **Data Resilience and Backup:** Making a duplicate copy of critical data to be used for restoring and recovery purposes.
- **Data Destruction:** It involves destroying the data so that it cannot be recovered and used for a wrong motive.
- **Data Retention:** Storing data securely for compliance or business requirements.
- **Disk Encryption:** Encryption of data stored in a physical or logical disk.
- **Data Backup:** Data backup is the process of making a duplicate copy of critical data, such as physical (paper) and computer records.
- **Differential Data Backup:** All data that has been changed since the last full backup is copied to the backup media.
- **Data Retention:** Data Retention is the process of storing and maintaining important information for meeting compliance and business data archival requirements.
- **Data Loss Prevention (DLP):** DLP includes a set of software products and processes that do not allow users to send confidential corporate data outside the organization.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- **Denial of Service Traffic Signatures**: Traffic containing certain signatures that indicate a DoS attempt that floods a server with a large number of requests.

E

- **Enterprise Information Security Policy (EISP):** EISP drives an organization's scope and provides direction to their security policies.
- **Electric/Electromagnetic Locks**: Electric locks or an electronic locking system operates on an electric current.
- **Electromagnetic Interference (EMI):** EMI occurs when electronic device's performance is interrupted or degraded due to electromagnetic radiation or conduction**.**
- **Email Honeypots:** Email honeypots are also called email traps. They are nothing but fake email addresses that are specifically used to attract fake and malicious emails from adversaries.
- **Encapsulation**: Encapsulation is the method in which protocols have separate functions to communicate among each other by hiding the data.
- **Endpoint**: This connects a sandbox to a network and abstracts the actual connection to the network from the application.
- **Enterprise Mobility Management (EMM):** EMM consists of tools and technologies used in an organization to secure the data in employees' personal (BYOD) and organizational devices.
- **EDGE**: The edge is the main physical device in the IoT ecosystem that interacts with its surroundings and contains various components like sensors, actuators, operating systems, hardware and network, and communication capabilities.
- **Encryption:** Encryption is the practice of concealing information by converting a plain text (readable format) into a cipher text (unreadable format) using a key or an encryption scheme.
- **Explicit Authorization**: An explicit authorization maintains separate authorization details for each resource request.
- **EAP**: The Extensible Authentication Protocol (EAP) supports multiple authentication methods, such as token cards, Kerberos, and certificates.

F

- **Firewall**: Firewall is a software or hardware, or a combination of both, which is generally used to separate a protected network from an unprotected public network.
- **Freedom of Information Act (FOIA)**: The Freedom of Information Act (FOIA) has provided the public the right to request access to records from any federal agency.
- **False Positive (No attack – Alert)**: A false positive occurs if an event triggers an alarm when no actual attack is in progress.
- **False Negative (Attack – No Alert)**: A false negative is a condition that occurs when an IDS fails to react to an actual attack event.
- **Function-as-a-Service (FaaS):** This cloud computing service provides a platform for developing, running, and managing application functionalities without the complexity of building and maintaining necessary infrastructure.
- **Frequency-Hopping Spread Spectrum (FHSS)**: FHSS, also known as frequency-hopping code-division multiple access (FH-CDMA), is a method of transmitting radio signals by rapidly switching a carrier among many frequency channels.
- **Fingerprint Scanning**: Compares two fingerprints for verification and identification on the basis of the patterns on the finger.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- **Face Recognition**: Compares and identifies a person on the basis of the facial features from an image or a video source.
- **Fences/Electric fences/Metal Rails**: Fences/metal rails/electric fences generally mark the restricted areas, controlled areas and prevents unauthorized access.
- **Full Mesh VPN Topology**: In a fully meshed VPN network, all peers can communicate with each other, making it a complex network.
- **Full Virtualization**: In this type of virtualization, the guest OS is not aware that it is running in a virtualized environment.
- **File System Virtualization**: This refers to the virtualization of data at the level of the file system.
- **Fabric Virtualization**: This level of virtualization makes the virtual devices independent of the physical computer hardware.
- **Full Data Backup**: This is also called a normal backup. It copies all files and compresses them to save space.
- **File-Level Encryption**: Encryption of data stored in files/folders.
- **Full Device Encryption:** Full disk encryption is a security feature that can encrypt all the information stored on any storage medium within a mobile device.

G

- **Gramm-Leach-Bliley Act (GLBA):** The Gramm-Leach-Bliley Act (GLB Act or GLBA) is a United States federal law that requires financial institutions to explain how they share and protect their customers' private information.
- **General Data Protection Regulation (GDPR):** The GDPR will levy harsh fines against those who violate its privacy and security standards, with penalties reaching tens of millions of euros.
- **Guest Machine:** Independent instance of an operating system created by virtual machine monitor.
- **Global System for Mobile Communications (GSM)**: It is a universal system used for mobile data transmission in wireless networks worldwide.
- **Global Positioning System (GPS)**: GPS is a radio navigation and positioning system based on satellite communication.
- **Geolocation:** Geolocation is a technology that can identify the real-world geographical location of users or devices when connected to the Internet.
- **Geofencing:** Geofencing is a technique through which mobile-application marketers utilize the location of the user to gather information.
- **Government Access to Keys (GAK):** GAK refers to the statutory obligation of individuals and organizations to disclose their cryptographic keys to government agencies.

H

- **Hypertext Transfer Protocol Secure (HTTPS):** HTTPS ensures secure communication between two computers over HTTP.
- **Health Insurance Portability and Accountability Act (HIPAA):** The HIPAA Privacy Rule provides federal protections for the individually identifiable health information held by covered entities and their business associates and gives patients an array of rights to that information.
- **Hardware Firewalls:** A hardware firewall is either a dedicated stand-alone hardware device or it comes as part of a router.
- **Host-based Firewalls:** The host-based firewall is used to filter inbound/outbound traffic of an individual computer on which it is installed.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- **Honeypot:** A honeypot is an information system resource that is expressly set up to attract and trap people who attempt to penetrate an organization's network.
- **Honeynets:** Honeynets are networks of honeypots. They are very effective in determining the entire capabilities of the adversaries.
- **Hardware VPNs:** A dedicated hardware VPN appliance is used to connect routers and gateways to ensure communication over an insecure channel.
- **Hypervisor:** An application or firmware that enables multiple guest operating systems to share a host's hardware resources.
- **Host Machine:** Real physical machine that provides computing resources to support virtual machines.
- **Hybrid Cloud:** Combination of two or more clouds (private, community, or public) that remain unique entities but are bound together, thereby offering the benefits of multiple deployment models**.**
- **Hotspot**: These are places where wireless networks are available for public use.
- **Host Intrusion Detection Systems (HIDS)**: HIDS is installed on a specific host and is used to monitor, detect, and analyze events occurring on that host.
- **Hybrid Intrusion Detection Systems (Hybrid IDS)**: A hybrid IDS is a combination of both HIDS and NIDS.
- **High-Interaction Honeypots**: High-interaction honeypots do not emulate anything; they run actual vulnerable services or software on production systems with real OS and applications
- **Hybrid VPNs**: Hybrid VPNs are those with trusted VPNs as part of the secure VPNs. They implement different network components of an organization at the same time in order to confirm security at very low costs.
- **Hub-and-Spoke VPN Topology**: In hub-and-spoke technology, the main organization is considered the hub, and its remote offices are considered the spokes.
- **Hybrid Virtualization**: In this type of virtualization, the guest OS adopts the functionality of para virtualization and uses the VMM for binary translation to different types of hardware resources.
- **Hot Backup (Online)**: It is also called as dynamic backup or active backup. In a hot backup, the system continues to perform the backup even when the user is accessing the system.
- **Hash-based Message Authentication Code (HMAC):** HMAC is a type of message authentication code (MAC) that uses a cryptographic key along with a cryptographic hash function.

I

- **Integrity:** Ensures information is not modified or tampered with by unauthorized parties.
- **Internet Protocol Security (IPsec):** IPsec is a network layer protocol that ensures a secure IP level communication.
- **Identity and Access Management (IAM):** Identity and access management (IAM) is responsible for providing the right individual with the right access at the right time.
- **Issue Specific Security Policy (ISSP):** ISSP directs the audience on the usage of technology-based systems with the help of guidelines.
- **Intrusion Detection and Prevention System (IDS/IPS):** An intrusion detection and prevention system (IDS/IPS) is a network security appliance that inspects all inbound and outbound network traffic for suspicious patterns that might indicate a network or system security breach.
- **Iris Scanning**: Analyzes the colored part of the eye suspended behind the cornea.
- **Implicit Authorization**: Implicit authorization provides access to the resources indirectly.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- **Internal Bastion Host**: It can be single-homed or multi-homed bastion hosts.
- **Interval-based IDS**: Interval-based or offline analysis refers to the storage of the intrusion-related information for further analysis.
- **IPsec Server**: The IPsec server enhances VPN security through the use of strong encryption algorithms and authentication.
- **Infrastructure-as-a-Service (IaaS):** Provides virtual machines and other abstracted hardware and operating systems which may be controlled through a service API.
- **Identity-as-a-Service (IdaaS):** This cloud computing service offers authentication services to the subscribed enterprises and is managed by a third-party vendor to provide identity and access management services.
- **Identity and Access Management (IAM):** IAM is the management of the digital identities of users and their rights to access resources.
- **Information Assurance (IA) Principles**: Information assurance (IA) principles act as enablers for an organization's security activities to protect and defend its network from security attacks.
- **ISM band**: A set of frequencies for the international industrial, scientific, and medical communities.
- **Industrial, Scientific, and Medical (ISM) band**: This band is a set of frequencies used by the international industrial, scientific, and medical communities.
- **Infrared (IR)**: IR is a wireless technology for transferring data between two devices in the digital form within a short range of up to 5 m.
- **Internet of Things (IoT):** IoT also known as the Internet of Everything (IoE), refers to computing devices that are web-enabled and have the capability of sensing, collecting, and sending data using sensors, and the communication hardware and processors.
- **Infrastructure Network Topology**: Devices in the wireless network are connected through an AP.
- **IoT User Management**: Provide control over the users who have access to an IoT system.
- **IoT Device Management**: IoT device management helps security professionals to track, monitor, and manage physical IoT devices from a remote location.
- **Incremental Data Backup:** Only files that have been changed or created after the last backup are copied to the backup media.
- **IDE**: Integrated drive electronics (IDE) allows the connection of two devices per channel. It is normally used for internal devices as the cables are large and flat.
- **Informational Traffic Signature**: Traffic containing certain signatures that may appear suspicious but might not be malicious.

K

- **Kerberos**: Kerberos is a network authentication protocol that is implemented for authenticating requests in computer networks.
- **Kubernetes:** Kubernetes, also known as K8s, is an open-source, portable, extensible, orchestration platform developed by Google for managing containerized applications and microservices.

L

- **Lighting System:** Adequate lighting should be provided inside, outside, and at the entrance of the building which helps in seeing long distances during security patrols.
- **Logical Segmentation:** Logical segmentation utilizes VLANs, which are isolated logically without considering the physical locations of devices.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- **LEAP**: Lightweight EAP (LEAP) is a proprietary version of EAP developed by Cisco.
- **Low-interaction Honeypots**: Low-interaction honeypots emulate only a limited number of services and applications of a target system or network.

M

- **Mandatory Access Control (MAC):** The MAC determines the usage and access policies for the users.
- **Mechanical Locks**: Provide an easy method to restrict unauthorized access in an organization.
- **Mantrap:** It is a security system having an entry and exit door on opposite sides, separating non-secure area from secure area.
- **Malware Honeypots:** Malware honeypots are used to trap malware campaigns or malware attempts over the network infrastructure.
- **Medium-interaction Honeypots**: Medium-interaction honeypots simulate a real OS as well as applications and services of a target network.
- **Management Server**: Virtualization platform components used to directly manage the virtual machines and to simplify the administration of resources.
- **Multi-layer Security**: Involves preventing unauthorized access to IoT things by using multi-factor authentication (MFA), Transport Layer Security (TLS), device identity management, etc.
- **Multiport Memory Controller**: An MPMC provides access to memory for up to eight ports. A memory controller can be present as a separate chip or as an integrated memory.
- **Multi Cloud:** It is a dynamic heterogeneous environment that combines workloads across multiple cloud vendors that are managed via one proprietary interface to achieve long-term business goals.
- **Management Console**: Interface used to access, configure, and manage the virtualization product.
- **Multi-homed Bastion Host**: A firewall device with at least two network interfaces.
- **Multiple Input, Multiple output Orthogonal Frequency-division Multiplexing (MIMO-OFDM):** An air interface for 4G and 5G broadband wireless communications.
- **Mobile Device Management (MDM):** MDM provides platforms for over-the-air or wired distribution of applications, data, and configuration settings for all types of mobile devices, including mobile phones, smartphones, and tablet computers.
- **Mobile Application Management (MAM):** Mobile application management (MAM) is a software or service that enables network defenders to secure, manage, and distribute enterprise applications on employee mobile devices.
- **Mobile Content Management (MCM):** Mobile content management (MCM) or mobile information management (MIM) solutions provide secure access to corporate data on smartphones, tablets, and other mobile devices.
- **Mobile Email Management (MEM):** Mobile email management (MEM) solutions ensures the security of the corporate email infrastructure and data.
- **Mobile Security Management:** Mobile security management involves actions and precautionary steps for securing the organizational data and mobile devices used by employees.
- **MD5:** The MD5 algorithm takes a message of arbitrary length as the input and then outputs a 128-bit fingerprint or message digest of the input.
- **MD6:** MD6 uses a Merkle-tree-like structure to allow for large-scale parallel computation of hashes for very long inputs.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

N

- **Non-Repudiation:** Ensures that a party in a communication cannot deny sending the message.
- **Network Segmentation:** Network segmentation is the practice of splitting a network into smaller network segments and separating groups of systems or applications from each other.
- **Network Defense Essentials (NDE)**: Network Defense Essentials (NDE) is a security program covering the fundamental concepts of network security.
- **Network Virtualization:** Network virtualization is a process of combining all the available network resources and enabling security professionals to share these resources amongst the network users using a single administrative unit.
- **Network Security Controls**: Network security controls are the security features that should be appropriately configured and implemented to ensure network security.
- **Network Security Protocols**: Network security protocols implement security related operations to ensure the security and integrity of data in transit.
- **Network Security Devices**: Network security appliances are devices that are deployed to protect computer networks from unwanted traffic and threats.
- **Network Intrusion Detection System (NIDS)**: NIDS is used to observe the traffic for any specific segment or device and recognize the occurrence of any suspicious activity in the network and application protocols.
- **Network Packets**: A network packet is a unit of data transmitted over a network for communication.
- **Network Access Server (NAS)**: It is also called a media gateway or a remote-access server (RAS). It is responsible for setting up and maintaining each tunnel in a remote-access VPN.
- **Network**: A network is a collection of endpoints that have connectivity between them.
- **Network Drivers**: These are pluggable and provide the actual implementation for the functioning of the network.
- **Network Defense:** The ultimate goal of network defense is to protect an organization's information, systems, and network infrastructure from unauthorized access, misuse, modification, service denial, or any degradation and disruptions.
- **Network Access Controls**: Network access controls offer various access control mechanisms for network devices like routers and switches.
- **Non-routing Dual-homed Hosts**: This type of the host is completely a firewall, or it might be a component of a multi-faceted firewall.
- **Network-based Firewalls:** The network-based firewall is used to filter inbound/outbound traffic from Internal LAN.
- **Network Address Translation (NAT):** Network address translation separates IP addresses into two sets and enables the LAN to use these addresses for internal and external traffic, respectively.
- **Next Generation Firewall (NGFW):** NGFW firewall technology is third-generation firewall technology that moves beyond port/protocol inspection.
- **nvSRAM**: nvSRAM is the fastest nonvolatile RAM in the industry with 20 ns read and write access time.
- **NAND Flash Memory**: Provides a non-volatile storage for the RAID system's primary cache.
- **Network Sensors:** Network sensors are hardware and software components that monitor network traffic and trigger alarms if any abnormal activity is detected.
- **Non-transparent Proxy:** Non-transparent proxies are also known as explicit proxies and require client software to be configured to use the proxy server.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- **Near-field Communication (NFC):** NFC covers very short distances. It employs electromagnetic induction to enable communication between devices connected within 10 cm.
- **Network Attached Storage (NAS):** NAS is a file-based data storage service and a dedicated computer appliance shared over the network.
- **Network Traffic Monitoring:** Network monitoring is a retrospective security approach that involves monitoring a network for abnormal activities, performance issues, bandwidth issues, etc.
- **Network Traffic Signatures:** A signature is a set of traffic characteristics such as a source/destination IP address, ports, Transmission Control Protocol (TCP) flags, packet length, time to live (TTL), and protocols. Signatures are used to define the type of activity on a network.
- **Normal Traffic Signatures**: Acceptable traffic patterns allowed to enter the network.

O

- **Object:** An object is an explicit resource on which an access restriction is imposed.
- **Operation:** An operation is an action performed by a subject on an object.
- **OS Containers**: OS containers are virtual environments sharing the kernel of the host environment that provides them isolated user space.
- **Orthogonal Frequency-Division Multiplexing (OFDM):** Method of encoding digital data on multiple carrier frequencies.
- **Omnidirectional Antenna:** Omnidirectional antennas radiate electromagnetic (EM) energy in all directions.
- **Onsite Data Backup:** Storing backup data at onsite data storage only.
- **Offsite Data Backup:** Storing backup data in remote locations in fire-proof, indestructible safes.
- **Open System Authentication**: Open system authentication is a null authentication algorithm that does not verify whether it is a user or a machine requesting network access.
- **OS Assisted Virtualization or Para Virtualization**: In this type of virtualization, the guest OS is aware of the virtual environment in which it is running and communicates with the host machine to request for resources.
- **Operating System Virtualization**: This type of virtualization enables the hardware to execute multiple operating systems simultaneously.

P

- **Preventive Approach:** Consist of methods or techniques that are used to avoid threats or attacks on the target network.
- **Proactive Approaches:** Consist of methods or techniques that are used to make informed decisions on potential attacks in the future on the target network.
- **Prevention Controls:** These are used to prevent unwanted or unauthorized access to resources.
- **Principle of Least Privilege (POLP):** The principle of least privilege (POLP) extends the need-to-know principle in providing access to a system.
- **Password Authentication:** Password Authentication uses a combination of a username and a password to authenticate the network users.
- **Policies**: Policies are high-level statements dealing with the administrative network security of an organization.
- **Promiscuous Policy**: This policy does not impose any restrictions on the usage of system resources.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- **Permissive Policy**: This policy is wide open, and only known dangerous services/attacks or behaviors are blocked.
- **Paranoid Policy**: A paranoid policy forbids everything. There is a strict restriction on all company computers, whether it is system or network usage.
- **Prudent Policy**: A prudent policy starts with all services blocked. The Network defender enables safe and necessary services individually.
- **Password Blacklist**: A password blacklist contains a list of words that are prohibited from use as passwords because of their familiarity.
- **Physical Security**: It deals with restricting unauthorized physical access to the infrastructure, office premises, workstations, and employees of the organization.
- **Physical Security Policy**: Physical security policy defines guidelines to ensure that adequate physical security measures are in place.
- **Payment Card Industry Data Security Standard (PCI-DSS):** PCI-DSS is a proprietary information security standard for organizations that handle cardholder information for major debit, credit, prepaid, e-purse, ATM, and POS cards.
- **Password Policy:** Password policy provides guidelines for using strong passwords for an organization's resources.
- **Preventive Controls:** These controls prevent security violations and enforce various access control mechanisms.
- **Physical Barriers:** Physical barriers restrict unauthorized people from entering the building; always use a combination of barriers to deter unauthorized entry.
- **Physical Segmentation:** Physical segmentation is a process of splitting a larger network into smaller physical components.
- **Packet Filtering Firewall:** Packet filtering firewalls work at the network level of the OSI model (or the IP layer of TCP/IP).
- **Protocol Anomaly Detection:** Protocol anomaly detection depends on the anomalies specific to a protocol.
- **Production Honeypots:** Production honeypots are deployed inside the production network of the organization along with other production servers.
- **Proxy Servers:** A proxy server is an application that can serve as an intermediary when connecting with other computers.
- **Platform-as-a-Service (PaaS):** This cloud computing service offers development tools, configuration management, and deployment platforms on-demand that can be used by subscribers to develop custom applications.
- **Public Cloud:** The provider makes services such as applications, servers, and data storage available to the public over the Internet.
- **Private Cloud:** A private cloud is a cloud infrastructure operated by a single organization and implemented within a corporate firewall.
- **Parabolic Grid Antenna:** A parabolic grid antenna uses the same principle as a satellite dish, but it does not have a solid dish. It consists of a semi-dish in the form of a grid consisting of aluminum wires.
- **PEAP**: It is a protocol that encapsulates the EAP within an encrypted and authenticated Transport Layer Security (TLS) tunnel.
- **Point-to-point (P2P) Connection:** A P2P connection enables secure communication between two mobile devices without data encryption.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- **Pure Honeypots**: Pure honeypots emulate the real production network of a target organization.
- **Packet Filters**: Packet filters examine the routing information of the packet.
- **Point-to-Point VPN Topology**: In a point-to-point topology, any two endpoints are considered as peer devices which can communicate with each other. Any of the devices can be used to initiate the connection.
- **Process Layer**: The process layer gathers information and processes the received information.
- **Point-to-multipoint Connection:** A point-to-multipoint (P2MP, PTMP, and PMP) connection allows one-to-many connections by providing multiple paths from a single location to several other locations.
- **Passwords and PINs:** Passwords and PINs are basic security features used in all mobile devices.
- **Push Notification Services:** It is a messaging feature that originates from a server and enables the delivery of data or a message from an application to a mobile device without any explicit request from the user.
- **Public Key Infrastructure (PKI):** A public key infrastructure (PKI) is a security architecture developed for increasing the confidentiality of the information exchanged over the Internet.
- **Physical Security Controls:** Physical security controls provide physical protection of the information, buildings, and all other physical assets of an organization.
- **Pretty Good Privacy (PGP)**: Pretty good privacy (PGP) is an application layer protocol which provides cryptographic privacy and authentication for network communication.
- **Primary RAID Memory Cache**: Cache is used to write the data in transition. A RAID system uses a cache to speed up I/O performance on the storage system.

R

- **Reactive Approach:** Consist of methods or techniques that are used to detect attacks on the target network.
- **Retrospective Approaches:** Consist of methods or techniques that examine the causes for attacks, and contain, remediate, eradicate, and recover from damage caused by the attack on the target network.
- **Reference Monitor:** A reference monitor monitors the restrictions imposed on the basis of certain access control rules.
- **Role-Based Access Control (RBAC):** In a role-based access control, the access permissions are available based on the access policies determined by the system.
- **Rule-based Access Control (RB-RBAC):** Permissions are assigned to a user role dynamically based on a set of rules defined by the administrator.
- **Recovery Controls:** These controls are used in a more serious condition to recover from security violation and restore information and systems to a persistent state.
- **Research Honeypots:** Research honeypots are high-interaction honeypots primarily deployed by research institutes, governments, or military organizations to gain detailed knowledge about the actions of intruders.
- **Reverse Proxy:** A reverse proxy is usually situated closer to the server(s) and will only return a configured set of resources.
- **RFID:** The radio-frequency identification (RFID) technology uses radio frequency (RF) electromagnetic waves to transfer data for automatic identification and for tracking tags attached to objects.
- **Reflector Antennas:** Reflector antennas are used for concentrating electromagnetic energy that is radiated or received at a focal point.
- **RADIUS**: Remote authentication dial-in user service (RADIUS) is an authentication protocol which provides centralized authentication, authorization, and accounting (AAA) for remote access servers to communicate with a central server.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- **Retinal Scanning**: Analyzes the layer of blood vessels at the back of their eyes to identify a person.
- **Regulatory Frameworks**: IT security regulatory frameworks contain a set of guidelines and best practices.
- **Real-time–based IDS**: Real-time–based IDS gathers and monitors information from network traffic streams regularly.
- **Response System**: The response system issues countermeasures against any intrusion that is detected.
- **Registry**: A registry contains all images that an organization deploys.
- **Real-time Monitoring**: Real-time monitoring involves monitoring IoT assets, processing products, maintaining a flow, helping detect issues, and taking actions immediately.
- **Real-time Analytics**: Real-time analytics involves analyzing IoT things and taking steps accordingly.
- **Redundant Array of Independent Disks (RAID) Technology:** A method of combining multiple hard drives into a single unit and writing data across several disk drives, offering fault tolerance.
- **RAID Controller**: Manages an array of physical disk drives and presents them to the computer as logical units.
- **RAID Level 0: Disk Striping**: RAID 0 deals with data performance. In this level, data is broken into sections and written across multiple drives.
- **RAID Level 1: Disk Mirroring**: Multiple copies of data are written to multiple drives at the same time.
- **RAID Level 3: Disk Striping with Parity**: Data is striped at the byte level across multiple drives. One drive per set is taken up for parity information.
- **RAID Level 5: Block Interleaved Distributed Parity**: The data is striped at the byte level across multiple drives, and the parity information is distributed among all the member drives.
- **RAID Level 10: Blocks Striped and Mirrored**: RAID 10 is a combination of RAID 0 (striping volume data) and RAID 1 (disk mirroring), and its implementation requires at least four drives.
- **RAID Level 50: Mirroring and Striping across Multiple RAID Levels**: RAID level 50 includes mirroring and striping across multiple RAID levels.
- **Remote Wipe:** Remote wipe is a technique used for securing and protecting data from miscreants if a mobile device used by an employee was stolen or lost.
- **RC4**: RC4 is a variable key-size symmetric-key stream cipher with byte-oriented operations, and it is based on the use of a random permutation.
- **RC5**: It is a parameterized algorithm with a variable block size, variable key size, and variable number of rounds. The key size is 128 bits.
- **RC6**: It is a parameterized algorithm with a variable block size, key size, and number of rounds.
- **Rivest-Shamir-Adleman (RSA)**: RSA is an Internet encryption and authentication system that uses an algorithm developed by Ron Rivest, Adi Shamir, and Leonard Adleman.
- **Removable Media Encryption**: Removable media encryption prevents removable media devices from unauthorized access.
- **Reconnaissance Traffic Signatures**: Reconnaissance traffic consists of signatures that indicate an attempt to scan the network for possible weaknesses.

S

- **Secure/Multipurpose Internet Mail Extensions (S/MIME):** S/MIME is an application layer protocol which is used for sending digitally signed and encrypted email messages.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- **Secure Sockets Layer (SSL):** The secure sockets layer (SSL) is a protocol used for providing a secure authentication mechanism between two communicating applications such as a client and a server.
- **Subject:** A subject can be defined as a user or a process that attempts to access the objects.
- **Separation of Duties (SoD):** This involves a breakdown of the authorization process into various steps.
- **Smart Card Authentication:** A smart card consists of a small computer chip that stores personal information of the user for identification.
- **Single Sign-on (SSO) Authentication:** It allows the users to access multiple applications using a single username and password.
- **Sarbanes Oxley Act (SOX):** The Sarbanes-Oxley Act is designed to protect investors and the public by increasing the accuracy and reliability of corporate disclosures:
- **Security Policy:** A security policy is a well-documented set of plans, processes, procedures, standards, and guidelines required to establish an ideal information security status of an organization.
- **System Specific Security Policy (SSSP):** SSSP directs users while configuring or maintaining a system.
- **Software Firewalls:** A software firewall is a software program installed on a computer, just like normal software.
- **Stateful Multilayer Inspection Firewall:** A stateful multilayer inspection firewall combines the aspects of the other three types.
- **Signature Recognition:** Signature recognition, also known as misuse detection, tries to identify events that indicate an abuse of a system or network resource.
- **Secure Hypertext Transfer Protocol (S-HTTP)**: Secure hypertext transfer protocol (S-HTTP) is an application layer protocol that is used to encrypt web communications carried over HTTP.
- **Standards**: Standards comprise specific low-level mandatory controls or controls related to the implementation of a specific technology.
- **Single-homed Bastion Host**: A firewall device with only one network interface.
- **Single Firewall DMZ**: In this model, the network architecture containing the DMZ consists of three network interfaces.
- **Spam Honeypots:** Spam honeypots specifically target spammers who abuse vulnerable resources such as open mail relays and open proxies.
- **Spider Honeypots:** Spider honeypots are also called spider traps. These honeypots are specifically designed to trap web crawlers and spiders.
- **SOCKS Proxy:** SOCKS, an Internet Engineering Task Force (IETF) standard, is a proxy server that does not have the special caching abilities of a caching HTTP proxy server.
- **Site-to-Site VPNs:** Site-to-site VPN extends the company's network, allows access of an organization's network resources from different locations.
- **Software VPNs:** VPN software is installed and configured on routers, servers and firewalls or as a gateway that functions as a VPN.
- **Star Topology**: Each device on the network is connected to a central hub that manages the traffic through the network.
- **Storage Device Virtualization**: This is the virtualization of storage devices using techniques such as data striping and data mirroring.
- **Server Virtualization:** This involves the logical partitioning of the server's hard drive.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- **Sandbox**: This contains the configuration of a container's network stack such as routing table, management of container's interfaces, and DNS settings.
- **Security Incident and Event Management (SIEM):** SIEM performs real-time SOC (Security Operations Center) functions like identifying, monitoring, recording, auditing, and analyzing security incidents.
- **Software-as-a-Service (SaaS):** This cloud computing service offers software to subscribers on-demand over the Internet.
- **Security-as-a-Service (SECaaS):** This cloud computing model integrates security services into corporate infrastructure in a cost-effective way.
- **Service Set identifier (SSID)**: An SSID is a 32-alphanumeric-character unique identifier given to a WLAN that acts as a wireless identifier of the network.
- **Shared Responsibility**: Security is a shared responsibility in cloud systems, wherein the cloud consumers and cloud service providers have varying levels of control over the available computing resources.
- **Shared Key Authentication**: In this process, each wireless station receives a shared secret key over a secure channel that is distinct from the 802.11 wireless network communication channels.
- **Simple Network Management Protocol (SNMP) Polling**: Simple network management protocol (SNMP) polling is used for identifying the IP devices attached to a wired network.
- **SDRAM:** Dynamic Random Access memory (DRAM) that is synchronized with the CPU clock speed.
- **Storage Area Network (SAN):** A SAN is a specialized, dedicated, and discrete high-speed network that connects storage devices with a high speed I/O interconnect.
- **System Access Controls**: System access controls are used for the restriction of access to data according to sensitivity of data, clearance level of users, user rights, and permissions.
- **Secure VPNs**: Secure VPNs are networks constructed using encryption.
- **Security Monitoring**: To address security breaches at early stages and to prevent malicious attacks on an IoT system.
- **SATA**: Serial ATA deals with hot plugging and serial connectivity. The hot plugging technique may be used to replace computer components without shutting down the system.
- **SCSI**: Small computer system interface (SCSI) allows multiple devices to be connected to a single port at the same time.
- **Satellite Communication (Satcom):** Satcom is an artificial geostationary satellite that provides services across the globe, but it is much slower.
- **Screen Lock:** Screen lock is a feature in mobile devices that is used to secure data and prevent illegal access by perpetrators.
- **Symmetric Encryption:** Symmetric encryption requires that both the sender and the receiver of the message possess the same encryption key.
- **Secure Hashing Algorithm (SHA):** This algorithm generates a cryptographically secure one-way hash; it was published by the National Institute of Standards and Technology as a US Federal Information Processing Standard.
- **SHA-1**: It produces a 160-bit digest from a message with a maximum length of (264 − 1) bits, and it resembles the MD5 algorithm.
- **SHA-2**: It is a family of two similar hash functions with different block sizes, namely, SHA-256, which uses 32-bit words, and SHA-512, which uses 64-bit words.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- **SHA-3**: SHA-3 uses the sponge construction, in which message blocks are XORed into the initial bits of the state, which is then invertibly permuted.

T

- **Transport Layer Security (TLS):** TLS ensures a secure communication between client-server applications over the internet.
- **Two-factor Authentication:** Two-factor authentication is a process where a system confirms the user identification in two steps.
- **The Digital Millennium Copyright Act (DMCA):** The DMCA is a United States copyright law that implements two 1996 treaties of the World Intellectual Property Organization (WIPO).
- **The Federal Information Security Management Act (FISMA):** The FISMA provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets.
- **The Electronic Communications Privacy Act**: The Electronic Communications Privacy Act and the Stored Wire Electronic Communications Act are commonly referred together as the Electronic Communications Privacy Act (ECPA) of 1986.
- **The Human Rights Act 1998**: This Act buttresses the rights and freedoms guaranteed under the European Convention on Human Rights.
- **The Freedom of Information Act 2000**: This Act makes provision for the disclosure of information held by public authorities or by persons providing services for them and to amend the Data Protection Act 1998 and the Public Records Act 1958.
- **TACACS+**: TACACS+ provides authentication, authorization, and accounting (AAA) services for network communication.
- **True Positive (Attack - Alert)**: A true positive is a condition that occurs when an event triggers an alarm and causes the IDS to react as if a real attack is in progress.
- **True Negative (No attack - No Alert)**: A true negative is a condition that occurs when an IDS identifies an activity as acceptable behavior, and the activity is acceptable.
- **Transparent Proxy:** A transparent proxy is a proxy through which a client system connects to a server without its knowledge.
- **Technical Security Controls**: Technical security controls are used for restricting access to devices in an organization to protect the integrity of sensitive data.
- **Turnstiles**: This type of physical barrier allows entry to only one person at a time.
- **TKIP**: It is a security protocol used in WPA as a replacement for WEP.

U

- **User Identity Management (IDM):** Deals with confirming the identity of a user, process, or device accessing the network.
- **User Behavior Analytics (UBA):** UBA is the process of tracking user behavior to detect malicious attacks, potential threats, and financial fraud.
- **Universal Serial Bus (USB):** USB enables wired communication for devices. It can be used for power supply and serial data transmission between devices.
- **USA Patriot Act 2001**: The purpose of the USA PATRIOT Act is to deter and punish terrorist acts in the U.S. and around the world and enhance law enforcement investigatory tools.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- **Unauthorized Access Traffic Signatures**: Traffic containing certain signatures that indicate an attempt to gain unauthorized access.

V

- **Video Surveillance:** Video surveillance refers to monitoring activities in and around the premises using CCTV (Close Circuit Television) systems.
- **Vein Structure Recognition**: Analyzes thickness and location of veins to identify a person.
- **Voice Recognition**: Compares and identifies a person on the basis of the voice patterns or speech patterns.
- **Virtual Private Network:** A VPN is a private network constructed using public networks, such as the Internet.
- **VPN Topologies:** A VPN topology specifies how the peers and networks within a VPN are connected.
- **Virtualization:** Virtualization refers to a software-based virtual representation of an IT infrastructure that includes network, devices, applications, storage, etc.
- **VPN Concentrators**: A VPN Concentrator is a network device used to create secure VPN connections.

W

- **Warning Signs:** Warning signs are used to ensure someone does not inadvertently intrude in any restricted areas.
- **Wi-Fi:** It uses radio waves or microwaves to allow electronic devices to exchange data or connect to the Internet.
- **WiMAX:** The worldwide interoperability for microwave access (WiMAX) technology uses long distance wireless networking and high-speed Internet.
- **WLAN:** It connects users in a local area with a network. The area may range from a single room to an entire campus.
- **WWAN:** WWAN covers an area larger than the WLAN. It can cover a particular region, nation, or even the entire globe.
- **WPAN:** It interconnects devices positioned around an individual, in which the connections are wireless. It has a very short range.
- **WMAN:** It accesses broadband area networks by using an exterior antenna. It is a good alternative for a fixed-line network.
- **Wireless Networks**: Wireless networks use radio frequency (RF) signals to connect wireless-enabled devices in a network.
- **Wired Network Scanning**: Wired network scanners such as Nmap are used for identifying a large number of devices on a network by sending specially crafted TCP packets to the device (Nmap-TCP fingerprinting).
- **Wireless Network Cards (NIC): W**ireless network interface cards (NICs) are cards that locate and communicate to an AP with a powerful signal, giving network access to the users.
- **Wireless Modem:** A wireless modem is a device that allows PCs to connect to a wireless network and access the Internet connection directly with the help of an ISP.
- **Wireless Bridge:** A wireless bridge connects multiple LANs at the medium access control (MAC) layer.
- **Wireless Repeater (range expanders):** This device retransmits the existing signal captured from the wireless router or an AP to create a new network.
- **Wireless Router:** A wireless router is a device in a WLAN which interconnects two types of networks using radio waves to the wireless enabled devices such as computers, laptops, and tablets.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- **Wireless Gateways:** A wireless gateway is a key component of a wireless network. It is a device that allows Internet-enabled devices to access the network.
- **Wireless Scanning**: It performs an active wireless network scanning to detect the presence of wireless APs in the vicinity.
- **Wireless USB Adapter:** A wireless USB adapter connects different devices to a wireless network in order to access the Internet without a computer, router, or any other network device.
- **Wired Equivalent Privacy (WEP)**: WEP is a security protocol defined by the 802.11b standard; it was designed to provide a wireless LAN with a level of security and privacy comparable to that of a wired LAN.
- **Wi-Fi Protected Access (WPA)**: It is an advanced wireless encryption protocol using TKIP and Message Integrity Check (MIC) to provide strong encryption and authentication.
- **WPA2**: WPA2 is an upgrade to WPA, and it includes mandatory support for counter mode with cipher block chaining message authentication code protocol (CCMP), an AES-based encryption mode with strong security.
- **WPA2 Enterprise**: Integrates EAP standards with WPA2 encryption.
- **WPA3**: WPA3 is an advanced implementation of WPA2 providing trailblazing protocols and uses the AES-GCMP 256 encryption algorithm.
- **Windows Information Protection (WIP):** WIP has an endpoint data loss prevention (DLP) capability that can be helpful in protecting local data at rest on endpoint devices.
- **Warm Backup (Nearline)**: A warm backup is also called a nearline backup. In a warm backup, the system updates are turned on to receive periodic updates.

Y

- **Yagi antenna:** Yagi antenna, also called as the Yagi-Uda antenna, is a unidirectional antenna commonly used in communications using the frequency band from 10 MHz to very high frequency (VHF) and ultra-high frequency (UHF).

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

References

Module 01: Network Security Fundamentals

1. Network Security, from www.njcpu.net/security.htm.
2. Ms. Mousami Pawar, (2014), Network Security, from https://www.slideshare.net/mousmip/network-security-fundamental.
3. Department of Defense, (2001), Support to Computer Network Defense (CND), from https://info.publicintelligence.net/DoD-SupportCND.pdf.
4. Computer Network Defense, from https://www.oreilly.com/library/view/cyber-warfare-2nd/9780124166721/xhtml/CHP011.html.
5. Computer Network Defense (CND), from https://www.techopedia.com/definition/27906/computer-network-defense-cnd.
6. (2011), 5 Core Principles of Information Assurance, from https://onlinebusinesscertificates.wordpress.com/2011/05/23/5-core-principles-of-information-assurance/.
7. Physical Security , from https://searchsecurity.techtarget.com/definition/physical-security.
8. Margaret Rouse, Pretty good privacy (PGP), from https://searchsecurity.techtarget.com/definition/Pretty-Good-Privacy.
9. Pretty good privacy, from https://en.wikipedia.org/wiki/Pretty_Good_Privacy.
10. S/MIME, from https://en.wikipedia.org/wiki/S/MIME.
11. De Clerq, Secure mail using SMIME, from https://flylib.com/books/en/2.244.1.106/1/.
12. Margaret Rouse, S-HTTP, from https://searchsoftwarequality.techtarget.com/definition/S-HTTP.
13. Secure Hypertext transfer protocol, from https://en.wikipedia.org/wiki/Secure_Hypertext_Transfer_Protocol.
14. HTTPS, from https://en.wikipedia.org/wiki/HTTPS.
15. GH Admin, (2017), What is Secure Sockets Layer (SSL) and How it Works, from https://www.gohacking.com/secure-sockets-layer-ssl/.
16. What Is An SSL Certificate And How Does It Work?, from https://www.digicert.com/what-is-an-ssl-certificate.
17. Michael Cobb, Peter Loshin, Secure Socket layer, from https://searchsecurity.techtarget.com/definition/Secure-Sockets-Layer-SSL.
18. Transport Layer Security (TLS), from http://etutorials.org/Networking/802.11+security.+wi-fi+protected+access+and+802.11i/Part+II+The+Design+of+Wi-Fi+Security/Chapter+9.+Upper-Layer+Authentication/Transport+Layer+Security+TLS/.
19. Andrew Froehlich, Kevin Beaver, Michael Cobb, Transport layer security (TLS), from https://searchsecurity.techtarget.com/definition/Transport-Layer-Security-TLS.
20. Transport Layer Security, from https://en.wikipedia.org/wiki/Transport_Layer_Security#TLS_record.
21. Zeus Kerravala, (2018), What is Transport Layer Security (TLS)?, from https://www.networkworld.com/article/2303073/lan-wan-what-is-transport-layer-security-protocol.html.
22. IPsec, from https://en.wikipedia.org/wiki/IPsec.
23. IPsec (Internet Protocol Security), from https://searchsecurity.techtarget.com/definition/IPsec-Internet-Protocol-Security.

Module 02: Identification, Authentication, and Authorization

24. Ravi S. Sandhu and Pierangela Samarati, (1994), Access Control: Principles and Practice, from https://www.profsandhu.com/journals/commun/i94ac(org).pdf.
25. Access Control Categories, from https://en.wikibooks.org/wiki/Fundamentals_of_Information_Systems_Security/Access_Control_Systems#Access_Control_Categories.
26. Computer Access Control, from https://en.wikipedia.org/wiki/Computer_access_control#Access_control_models.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
https://t.me/learningnets

27. Access Control Types, from https://en.wikibooks.org/wiki/Fundamentals_of_Information_Systems_Security/Access_Control_Systems#Access_Control_Types .
28. Access Control List, from https://en.wikipedia.org/wiki/Access_control_list.
29. Access Control Lists, from https://docs.microsoft.com/en-us/windows/win32/secauthz/access-control-lists?redirectedfrom=MSDN.
30. Linda Rosencrance, Role-based Access control, from https://searchsecurity.techtarget.com/definition/role-based-access-control-RBAC.
31. Attribute-based Access Control, from https://en.wikipedia.org/wiki/Attribute-based_access_control.
32. (2016), Attribute based Access control (ABAC)- Overview, from https://csrc.nist.gov/projects/attribute-based-access-control.
33. Choosing a secure and memorable password, from https://en.wikipedia.org/wiki/Password#Choosing_a_secure_and_memorable_password.
34. Memory card, from https://en.wikipedia.org/wiki/Memory_card.
35. Smart card, from https://en.wikipedia.org/wiki/Smart_card.
36. Biometrics, from https://en.wikipedia.org/wiki/Biometrics.
37. Stephen J. Bigelow , (2008), Implement access control systems successfully in your organization, from https://searchitchannel.techtarget.com/feature/The-importance-of-access-control.
38. (2016), Access Control Policy and Implementation Guides, from https://csrc.nist.gov/projects/access-control-policy-and-implementation-guides.
39. Vincent C. Hu, David F. Ferraiolo, D. Rick Kuhn, (2006), Assessment of Access Control Systems, from http://csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf.
40. Network Access Control (NAC), from https://searchnetworking.techtarget.com/definition/network-access-control.
41. Network Access Control, from https://en.wikipedia.org/wiki/Network_Access_Control#Controversy.
42. Andrew Plato, Implementing network access control products: How to prep your clients, from https://searchitchannel.techtarget.com/tip/Implementing-network-access-control-products-How-to-prep-your-clients.
43. Deb Shinder, (2001), Understanding and selecting authentication methods, from https://www.techrepublic.com/article/understanding-and-selecting-authentication-methods/.
44. Linda Rosencrance, Peter Loshin, and Michael Cobb, Two-factor authentication (2FA), from https://searchsecurity.techtarget.com/definition/two-factor-authentication.
45. Multi-factor authentication, from https://en.wikipedia.org/wiki/Multi-factor_authentication.
46. Fingerprint, from https://en.wikipedia.org/wiki/Fingerprint_recognition.
47. Retinal Scan, from https://en.wikipedia.org/wiki/Retinal_scan.
48. Iris Recognition, from https://en.wikipedia.org/wiki/Iris_recognition.
49. Vein Recognition, from https://findbiometrics.com/solutions/vein-recognition/.
50. Facial recognition system, from https://en.wikipedia.org/wiki/Facial_recognition_system.
51. Jesse Scardina, Voice recognition (speaker recognition), from https://searchcustomerexperience.techtarget.com/definition/voice-recognition-speaker-recognition.
52. Deb Shinder, (2001), Understanding and selecting authentication methods, from https://www.techrepublic.com/article/understanding-and-selecting-authentication-methods/.
53. Joseph Migga Kizza, Guide to Computer Network Security, from https://books.google.co.in/books?id=d2CYBgAAQBAJ&pg=PA199&lpg=PA199&dq=centralized+authorization&source=bl&ots=xOR_IzZaBh&sig=uGAw_WpDELsvHSf1PLbFZ8-avvQ&hl=en&sa=X&ved=0ahUKEwjqh5jGzbzKAhUSI44KHYDrAc04ChDoAQgnMAI#v=onepage&q=centralized%20authorization&f=false.
54. User Account Control, from https://en.wikipedia.org/wiki/User_Account_Control.
55. (2017), User Account Control, from https://docs.microsoft.com/en-us/windows/security/identity-protection/user-account-control/user-account-control-overview.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

56. Wolfgang Sommergut, (2019), Windows Admin Center: Role-based access control, from https://4sysops.com/archives/windows-admin-center-role-based-access-control/.

57. (2019), User access options with Windows Admin Center, from https://docs.microsoft.com/en-us/windows-server/manage/windows-admin-center/plan/user-access-options.

58. Sandra Gittlen, What is identity and access management? Guide to IAM, from https://searchsecurity.techtarget.com/definition/identity-access-management-IAM-system.

59. (2021), David Strom, What is IAM? Identity and access management explained, from https://www.csoonline.com/article/2120384/what-is-iam-identity-and-access-management-explained.html.

60. Jagdeep Bhambra, (2014), Identity and Access Management, from https://governmenttechnology.blog.gov.uk/2014/06/24/identity-and-access-management/.

61. (2021), Enterprise Identity and Access Management, from https://docs.evolveum.com/iam/enterprise-iam/.

Module 03: Network Security Controls - Administrative Controls

62. Andy Scott, (2013), How to create a good information security policy, from https://www.computerweekly.com/feature/How-to-create-a-good-information-security-policy.

63. Types of Security Policies, from https://www.helpwithassignment.com/blog/it_security_assignment_help/.

64. Scott Hebert, Security Policies, from http://slaptijack.com/information-systems/security-policies/.

65. (2009), Configuring Password Policies, from https://docs.microsoft.com/en-us/previous-versions/tn-archive/dd277399(v=technet.10)?redirectedfrom=MSDN.

66. ISO/IEC 27033:2010+ Information technology — Security techniques — Network security, from https://www.iso27001security.com/html/27033.html.

67. Information technology — Security techniques — Network security —, from https://webstore.iec.ch/preview/info_isoiec27033-1%7Bed2.0%7Den.pdf.

68. The IT Security Policy Guide, from http://www.instantsecuritypolicy.com/Introduction_To_Security_policies.pdf.

69. Network security policy, from https://en.wikipedia.org/wiki/Network_security_policy.

70. Security policy, from https://searchsecurity.techtarget.com/definition/security-policy.

71. Catherine Paquet, (2013), Network Security Concepts and Policies, from https://www.ciscopress.com/articles/article.asp?p=1998559&seqNum=3.

72. (2012), Information Security Management System ISO/IEC 27001 :205 Introduction and Requirements, from https://www.slideshare.net/ControlCase/isms-presentation-oct-202012?qid=b5f12936-0a7d-4dad-9e6e-2b68c654397b&v=&b=&from_search=9.

73. ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems, from https://www.iso27001security.com/html/27001.html.

74. IT Policies Every Small Business Should Have , from http://www.corpcomputerservices.com/articles/it-policies-small-business.

75. Muhanned Wajahat Rajab, (2013), Physical Security, from https://www.slideshare.net/wajraj/physical-security-presentation-23717721?qid=f4e0b456-8a74-42a7-9543-d03f369c2a72&v=&b=&from_search=2.

76. Leminhvuong, (2009), Physical Security, from https://www.slideshare.net/leminhvuong/module-10-physical-security?qid=f4e0b456-8a74-42a7-9543-d03f369c2a72&v=&b=&from_search=6.

77. Sample internet usage policy, from https://www.gfi.com/pages/sample-internet-usage-policy.

78. Jonathan Gana KOLO, Umar Suleiman DAUDA, Network Security: Policies and Guidelines for Effective Network Management, from http://ljs.academicdirect.org/A13/007_021.htm.

79. Your guide to the Payment Card Industry Data Security Standard (PCI DSS) , from https://www.westpac.com.au/docs/pdf/bb/Guide_to_payment_card_indus1.pdf.

80. Electronic Communications Privacy Act (ECPA), from https://epic.org/privacy/ecpa/.

81. FISA 101: Why FISA Modernization Amendments Must Be Made Permanent, from https://www.justice.gov/archive/ll/.

82. 1927 (110th): Protect America Act of 2007, from https://www.govtrack.us/congress/bills/110/s1927/text.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

83. Sample acceptable internet use policy, from https://www.nibusinessinfo.co.uk/content/sample-acceptable-internet-use-policy.
84. Passwords Policy, from http://www.cpcstech.com/pdf/password_policy.pdf.
85. Information Security Compliance: Which regulations relate to me?, from https://www.tcdi.com/information-security-compliance-which-regulations/.
86. Compliance and Regulatory Frameworks, from https://www.rapid7.com/fundamentals/compliance-regulatory-frameworks/.
87. What Are IT Policies, Standards And Guidelines?, from https://binaryblogger.com/2015/02/11/policies-standards-guidelines/.
88. Jeff Battaglino, 7 Hidden Benefits of IT Security Compliance for Your Business, from https://www.cherwell.com/library/blog/it-security-compliance/.
89. Becky Metivier, (2017), Cybersecurity Compliance Assessments: It's All About Interpretation, from https://www.tylercybersecurity.com/blog/cybersecurity-compliance-assessments-its-all-about-interpretation.
90. Danny Palmer, (2019), What is GDPR?, from https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/.
91. General Data Protection Regulation, from https://en.wikipedia.org/wiki/General_Data_Protection_Regulation.
92. Gramm-Leach-Bliley, from https://dealers-insurance.com/gramm_leach_bliley_act.php.
93. What is Information System Security Policy (ISSP), from https://www.igi-global.com/dictionary/fear-appeals-threat-perceptions-and-protection-motivation-in-information-systems-security/42993.
94. Nehemiah Mavetera, Investigating Information System Security Policy and Awareness Training Programs in South African Organizations, from https://www.academia.edu/2409019/Investigating_Information_System_Security_Policy_and_Awareness_Training_Programs_in_South_African_Organizations.
95. Information Systems Security Policy, from https://www.temenos.com/wp-content/uploads/2019/07/governance-policy-information-systems-security-2019-jul-03.pdf.
96. Yash Tiwari, (2017), Security Awareness, from https://resources.infosecinstitute.com/security-awareness/#gref.
97. Corey Bleich, Top 10 Types of Employee Training Methods, from https://www.edgepointlearning.com/blog/top-10-types-of-employee-training/.
98. Michael Maughan, Employee Security Training Tips: Social Engineering, from https://www.securitymetrics.com/blog/employee-security-training-tips-social-engineering.
99. (2018), Data Protection Act 2018, from https://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf.

Module 04: Network Security Controls - Physical Controls

100. Tom Eston, (2008), Physical Security Assessments, from https://www.slideshare.net/agent0x0/physical-security-assessments-presentation.
101. Lisa Phifer, (2010), Removable storage device endpoint security and control, from https://searchsecurity.techtarget.com/magazineContent/Removable-storage-device-endpoint-security-and-control.
102. Dhani Ahmad, (2015), Physical security, from https://www.slideshare.net/emolagi/physical-security-45924353.
103. Tom Rubenoff, (2021), How to Create a Basic Mantrap System, from https://turbofuture.com/industrial/How-to-Create-a-Basic-Mantrap-System.
104. Stuart Gentry, (2021), Access Control: Models and Methods, from https://resources.infosecinstitute.com/certification/access-control-models-and-methods/.
105. (2004), Access Control Methodologies, from https://samples.jblearning.com/076372677X/chapple02.pdf.
106. (2009), Authorization and Access Control Technologies, https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc782880(v=ws.10)?redirectedfrom=MSDN.
107. Jeff A Sandine, (2009), What is the Difference Between Tailgating and Piggybacking Through an Access Controlled Secure Door?, from http://ezinearticles.com/?What-is-the-Difference-Between-Tailgating-and-Piggybacking-Through-an-Access-Controlled-Secure-Door?&id=1902821.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

108. Mohd Hamizi, (2015), 3 ensuring physical and data security, from https://www.slideshare.net/pdawackomct/3-ensuring-physical-and-data-security.

109. Deb Shinder, (2007), 10 physical security measures every organization should take, from https://www.techrepublic.com/blog/10-things/10-physical-security-measures-every-organization-should-take/.

110. Hudson K, Ruth A, Securing Network Cabling, from https://flylib.com/books/en/2.902.1.22/1/.

111. Mani Rathnam, (2015), Hardware Security, from https://www.slideshare.net/manirathnam39/hardware-security.

112. Securing Network Devices, from http://etutorials.org/Networking/Cisco+Certified+Security+Professional+Certification/Part+I+Introduction+to+Network+Security/Chapter+2+Securing+the+Network/Securing+Network+Devices/.

113. Faheem Ul Hasan, (2009), Physical Security Assessment, from https://www.slideshare.net/faheemi07/physical-security-assessment.

114. (2013), Physical Security Audit Checklist, from https://www.locknet.com/newsroom/physical-security-audit-checklist/.

115. John Kirtland, (2009), Challenges and benefits of physical IT security, from https://www.computerweekly.com/opinion/Challenges-and-benefits-of-physical-IT-security.

116. Vijay Luiz, (2015), Physical security challenges when vendors are on site, from https://www.linkedin.com/pulse/physical-security-challenges-when-vendors-site-vijay-luiz.

Module 05: Network Security Controls - Technical Controls

117. (2021), Network Segmentation Best Practices to Improve Security, from https://www.spamtitan.com/web-filtering/network-segmentation-best-practices/.

118. (2017), Becky Metivier, The Security Benefits of Network Segmentation, from https://www.tylercybersecurity.com/blog/the-security-benefits-of-network-segmentation.

119. Steve Petryschuk, (2019), Network Segmentation: What It Is & How It Works, from https://www.auvik.com/franklyit/blog/network-segmentation/#:~:text=Physical%20segmentation%20involves%20breaking%20down,%2C%20routers%2C%20and%20access%20points.&text=Typically%2C%20logical%20segmentation%20doesn't,the%20infrastructure%20is%20already%20managed..

120. Professor Messer, (2018), Network Segmentation – CompTIA Network+ N10-007 – 4.6, from https://www.professormesser.com/network-plus/n10-007/network-segmentation-3/.

121. (2014), Cisco Networking Academy's Introduction to VLANs, from https://www.ciscopress.com/articles/article.asp?p=2181837&seqNum=4.

122. Tom Olzak, (2021), VLAN Network Segmentation and Security- Chapter 5, from https://resources.infosecinstitute.com/topic/vlan-network-chapter-5/.

123. Basant Shrestha, (2013), VLAN, from https://basantshrestha.wordpress.com/2013/02/04/vlan/.

124. Firewall Design, from https://docstore.mik.ua/orelly/networking/firewall/ch04_02.htm.

125. DMZ (computing), from https://en.wikipedia.org/wiki/DMZ_(computing).

126. Firewalls, from http://mercury.webster.edu/aleshunas/COSC%205130/Chapter-22.pdf.

127. Donald Stoddard, Thomas M. Thomas, (2012), Network Security First-Step: Firewalls, from https://www.ciscopress.com/articles/article.asp?p=1823359&seqNum=7.

128. Habtamu Abie, (2000), An Overview of Firewall Technologies, from https://folk.universitetetioslo.no/abie/fwt.pdf.

129. Jeff Tyson, How Firewalls Work, from https://computer.howstuffworks.com/firewall1.htm.

130. How does a firewall work?, from https://www.bullguard.com/bullguard-security-center/pc-security/computer-security-resources/how-does-a-firewall-work.aspx.

131. Amandeep Kaur, (2010), Firewall presentation, from http://www.slideshare.net/adkpcte/firewall-presentation.

132. Firewall Defaults and Some Basic Rules, from https://www.downloads.netgear.com/docs/utm_qsgs/utm_fw.pdf.

133. (2009), Understanding Firewall Rules, from https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc730951(v=ws.11)?redirectedfrom=MSDN.

134. Firewall, Internet Security, Anti Virus Protection - BullGuard, from https://www.bullguard.com/bullguard-security-center/pc-security/computer-security-resources/firewall-protection.aspx.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

135. How Firewalls work, from https://www.comodo.com/resources/home/how-firewalls-work.php.
136. G. Krishnam Raju, S. L. N. Reddy, Advantages of Firewall, http://www.scribd.com/doc/22594454/ADVANTAGES-OF-FIREWALL.
137. Vangie Beal, Firewall, from https://www.webopedia.com/definitions/firewall/.
138. Ben Lutkevich, What is firewall?, from https://searchsecurity.techtarget.com/definition/firewall.
139. Firewalling Fundamentals, from https://docs.netgate.com/pfsense/en/latest/firewall/fundamentals.html.
140. Per Thorsheim, Comparing Firewall Technologies, from http://www.ittoday.info/AIMS/DSM/84-10-26.pdf.
141. Karen Scarfone, Paul Hoffman, (2009), Guidelines on Firewalls and Firewall Policy, from http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf.
142. Ajay Yadav, (2020), Network Design: Firewall, IDS/IPS, from https://resources.infosecinstitute.com/topic/network-design-firewall-idsips/.
143. Firewall Technologies, from https://www.novell.com/documentation/nbm37/?page=/documentation/nbm37/over/data/ae70nts.html.
144. Habtamu Abie, (2000), An Overview of Firewall Technologies, from http://publications.nr.no/directdownload/publications.nr.no/3149/Abie_-_An_overview_of_firewall_technologies.pdf.
145. Network address translation, from https://en.wikipedia.org/wiki/Network_address_translation.
146. Firewall (computing), from https://en.wikipedia.org/wiki/Firewall_(computing).
147. Amy Larsen DeCarlo, Robert G. Ferrell, The 5 different types of firewalls explained, from https://searchsecurity.techtarget.com/feature/The-five-different-types-of-firewalls.
148. (2008), IP Packet Filtering, from https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc957881(v=technet.10)?redirectedfrom=MSDN.
149. Packet Filtering, from https://docstore.mik.ua/orelly/networking_2ndEd/fire/ch08_01.htm.
150. Application firewall, from https://en.wikipedia.org/wiki/Application_firewall.
151. Packet Filtering, from https://www.techopedia.com/definition/4038/packet-filtering.
152. Circuit-Level Gateway, from http://firewall-review.narod.ru/circuit_level_gateway.html.
153. Circuit-Level Gateway, from https://www.techopedia.com/definition/24780/circuit-level-gateway.
154. Application-level Gateway, from http://firewall-review.narod.ru/application_gateway.html.
155. Application Layer Filtering - Firewall Advanced Security, from http://www.internet-computer-security.com/Firewall/Application-Layer-Filtering.html.
156. Deb Shinder, (2004), Application Layer Filtering (ALF): What is it and How does it Fit into your Security Plan?, from https://techgenix.com/Application_Layer_Filtering/.
157. Rajesh K, (2009), What are: Packet filtering, Circuit level, Application Level and Stateful Multilayer inspection Firewalls, from http://www.excitingip.com/205/what-are-packet-filtering-circuit-level-application-level-and-stateful-multilayer-inspection-firewalls/.
158. Proxy Services, from https://docstore.mik.ua/orelly/networking_2ndEd/fire/ch05_03.htm.
159. Network Address Translation, from https://docstore.mik.ua/orelly/networking_2ndEd/fire/ch05_04.htm.
160. Virtual Private Networks, from https://docstore.mik.ua/orelly/networking_2ndEd/fire/ch05_05.htm.
161. Firewall Security, from http://www.ipcopper.com/firewalls.htm.
162. Firewall Architectures, from http://www.s-w-r.com/Firewall/link5.html.
163. Firewall Architectures, from http://www.invir.com/int-sec-firearc.html.
164. Bastion host, from https://en.wikipedia.org/wiki/Bastion_host.
165. (2002), Firewall Deployment for Multitier Applications, from https://zeltser.com/firewalls-for-multitier-applications/.
166. John R. Vacca, Scott Ellis, Firewalls: Jumpstart for Network and Systems Administrators, from https://books.google.co.in/books?id=ipvoml8c9zcC&pg=PA25&lpg=PA25&dq=Multi-homed+firewall+architecture&source=bl&ots=3E-Q8RRoS9&sig=KbpZfz1RrZmRAn3a5_Qt1QB6CJ4&hl=en&sa=X&ei=Zf0XVM-cEMeTuAT8yILgDg&ved=0CF8Q6AEwCg#v=onepage&q=Multi-homed%20firewall%20architecture&f=false.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

167. Firewall Architectures, from http://www.diablotin.com/librairie/networking/firewall/ch04_02.htm.
168. Firewall Facts, from https://sites.google.com/a/pccare.vn/it/security-pages/firewall-facts.
169. Network address translation, from https://en.wikipedia.org/wiki/Network_address_translation.
170. Network Address Translation, from https://docstore.mik.ua/orelly/networking_2ndEd/fire/ch05_04.htm.
171. Virtual Private Networks, from https://docstore.mik.ua/orelly/networking_2ndEd/fire/ch05_05.htm.
172. Firewalls and Virtual Private Networks, from https://www.wiley.com/legacy/compbooks/press/0471348201_09.pdf.
173. (2002), Firewall Deployment for Multitier Applications, from http://zeltser.com/multi-firewall/.
174. Laura Pelkey, (2012), Firewall Implementation: 3 Steps for Network Security, from https://blog.icorps.com/bid/138231/3-Steps-to-a-Successful-Firewall-Implementation.
175. Firewall implementation, from https://community.jisc.ac.uk/library/advisory-services/firewall-implementation.
176. Przemyslaw Kazienko, Piotr Dorosz, (2003), Intrusion Detection Systems (IDS) Part I, from http://googleweblight.com/?lite_url=http://www.windowsecurity.com/articles-tutorials/intrusion_detection/Intrusion_Detection_Systems_IDS_Part_I__network_intrusions_attack_symptoms_IDS_tasks_and_IDS_architecture.html&ei=wjgGk8gA&lc=en-IN&geid=7&s=1&m=328&ts=1443607601&sig=APONPFmMHyzAy-6SXYxgKzR70YUCJw_ing.
177. Patrick Harper, Secure IDS deployment best practices, from https://searchitchannel.techtarget.com/tip/Secure-IDS-deployment-best-practices.
178. Edward Yakabovicz, Intrusion detection system deployment recommendations, from https://searchsecurity.techtarget.com/tip/Intrusion-detection-system-deployment-recommendations.
179. K.Rajasekhar, B.Sekhar Babu , P.Lakshmi Prasanna, D.R.Lavanya, T.Vamsi Krishna, (2011), An Overview of Intrusion Detection System Strategies and Issues, from http://www.ijcst.com/vol24/1/krajasekhar.pdf.
180. 27-2-2012, What it is Network intrusion detection system?, from http://www.combofix.org/what-it-is-network-intrusion-detection-system.php.
181. How Intrusion Detection Works, from https://www.spamlaws.com/how-intrusion-detection-works.html.
182. Robert L. Barnard, Intrusion Detection Systems, from http://books.google.co.in/books?id=jo5ANoqS2MMC&pg=PA1&lpg=PA1&dq=Intrusion+detection+functions&source=bl&ots=40qoXTh7F0&sig=qkGHE9miEjvFCWK5x3OFFrYBKqY&hl=en&sa=X&ei=IS1HVKaUNZeMuATOzILgCw&ved=0CCwQ6AEwAjgK#v=onepage&q=Intrusion%20detection%20functions&f=false.
183. IDS Introduction, from http://etutorials.org/Networking/Router+firewall+security/Part+VII+Detecting+and+Preventing+Attacks/Chapter+16.+Intrusion-Detection+System/IDS+Introduction/.
184. Deb Shinder, (2005), SolutionBase: Understanding how an intrusion detection system (IDS) works, from https://www.techrepublic.com/article/solutionbase-understanding-how-an-intrusion-detection-system-ids-works/.
185. J. Forlanda, (2010), Intrusion Detection Systems: How They Work, from https://www.brighthub.com/computing/smb-security/articles/65416/.
186. Pastore M., Dulaney E, Intrusion Detection Systems, from https://flylib.com/books/en/4.213.1.49/1/.
187. Intrusion Detection Systems, from https://www.ipa.go.jp/security/fy11/report/contents/intrusion/ids-meeting/idsbg.pdf.
188. Fredrik Valeur, Giovanni Vigna, Christopher Kruegel and Richard A. Kemmerer, (2004), A Comprehensive Approach to Intrusion Detection Alert Correlation, from https://sites.cs.ucsb.edu/~vigna/publications/2004_valeur_vigna_kruegel_kemmerer_TDSC_Correlation.pdf.
189. Nazir Ahmad, (2012), Intrusion detection systems, from https://www.slideshare.net/King8117/intrusion-detection-systems-15218543.
190. Karen Scarfone and Peter Mell, (2007), Guide to Intrusion Detection and Prevention Systems, from https://csrc.nist.gov/publications/detail/sp/800-94/final.
191. Przemyslaw Kazienko, Piotr Dorosz, (2004), Intrusion Detection Systems (IDS) Part 2 – Classification, from https://techgenix.com/IDS-Part2-Classification-methods-techniques/.
192. Misuse detection, from https://en.wikipedia.org/wiki/Misuse_detection.
193. Kanika, Urmila, (2013), Security of Network Using Ids and Firewall, from http://www.ijsrp.org/research-paper-0613/ijsrp-p18150.pdf.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

194. Shiv Shakti Srivastava, Nitin Gupta, Saurabh Chaturvedi, Saugata Ghosh, (2011), A Survey on Mobile Agent based Intrusion Detection System, from https://www.ijcaonline.org/isdmisc/number6/isdm137.pdf.

195. Saidat Adebukola Onashoga, Adebayo D. Akinde and Adesina Simon Sodiya, (2009), A Strategic Review of Existing Mobile Agent Based Intrusion Detection Systems, from http://iisit.org/Vol6/IISITv6p669-682Onashoga623.pdf.

196. Nathan Einwechter, (2001), An Introduction To Distributed Intrusion Detection Systems, from https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=d4dcda2e-19b7-414d-826a-cfbcbfdc9353&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments.

197. Julie J.C.H. Ryan, (2002), Intrusion Detection, from http://www.seas.gwu.edu/~jjchryan/VAIDS051402.pdf.

198. Hudson K., Ruth A. Intrusion Detection Systems, from http://flylib.com/books/en/2.902.1.51/1/.

199. Intrusion detection system, from https://en.wikipedia.org/wiki/Intrusion_detection_system.

200. Intrusion Detection, from https://owasp.org/www-community/controls/Intrusion_Detection.

201. Kevin Timm, (2001), Strategies to Reduce False Positives and False Negatives in NIDS, from https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=56b0f35a-f1ed-480b-9fe9-16c0687435cd&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments.

202. Intrusion Detection Systems, from https://www.scribd.com/document/7148986/Intrusion-Detection-Systems.

203. Detecting Signs of Intrusion, from http://ptgmedia.pearsoncmg.com/images/020173723X/samplechapter/allench6.pdf.

204. Vangie Beal (15-7-2005), Intrusion Detection (IDS) and Prevention (IPS) Systems, from https://www.webopedia.com/insights/intrusion-detection-prevention/.

205. What is an Intrusion Prevention System?, from https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips.

206. (2013), How Intrusion Prevention Systems (IPS) Work in firewall?, from https://community.spiceworks.com/topic/362007-how-intrusion-prevention-systems-ips-work-in-firewall.

207. Ron Lepofsky, (2011), Intrusion Detection: Why do I need IDS, IPS or HIDS, from https://www.networkworld.com/article/2228598/intrusion-detection--why-do-i-need-ids--ips--or-hids-.html.

208. Ed Sale, Intrusion Detection and Intrusion Prevention, from https://www.cs.unh.edu/~it666/reading_list/Defense/ids_vs_idp.pdf.

209. Jennifer J. Minella, DS vs. IPS: How to know when I you need the technology, from https://searchsecurity.techtarget.com/tip/IDS-vs-IPS-How-to-know-when-you-need-the-technology.

210. (2014), Security: IDS vs. IPS Explained, from https://www.comparebusinessproducts.com/fyi/ids-vs-ips.

211. Jonathan Lister, What are the Advantages & Disadvantages of an Intrusion Detection System?, from https://www.hunker.com/12288156/what-are-the-advantages-disadvantages-of-an-intrusion-detection-system.

212. Brad Reese, (2008), Intrusion detection systems vs. network behavior analysis: Which do you need?, from https://www.networkworld.com/article/2346145/intrusion-detection-systems-vs--network-behavior-analysis--which-do-you-need-.html.

213. (2007), Intrusion Detection and Prevention Systems, from https://seclists.org/isn/2007/Mar/5.

214. Rebecca Bace and Peter Mell, (2001), Intrusion Detection Systems, from https://cryptome.org/sp800-31.htm.

215. (2006), Measuring Security Threats with Honeypot Technology, from http://www.honeynet.org/papers/individual/sane-2004.pdf.

216. (2006), SecurityFocus: Honeytokens -The Other Honeypot, from https://www.symantec.com/connect/articles/honeytokens-other-honeypot.

217. Satyajit, What is HoneyPot?, from https://www.securityhunk.in/2010/06/what-is-honeypot.html.

218. Niels Provos, (2003), A Virtual Honeypot Framework, from http://www.citi.umich.edu/techreports/reports/citi-tr-03-1.pdf.

219. Eric Peter and Todd Schiller, (2008), A Practical Guide to Honeypots, from https://www.cse.wustl.edu/~jain/cse571-09/ftp/honey/index.html#sec1.4.

220. Krishna Prasad P, (2017), Capturing Attacks on IoT Devices with a multi-purpose IoT Honeypot, from https://security.cse.iitk.ac.in/sites/default/files/15111021.pdf.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

221. Nishit Majitha, (2017), Honey-System: Design, Implementation, & Attack Analysis, from https://security.cse.iitk.ac.in/sites/default/files/15111024.pdf.
222. Honeypot (computing), from https://en.wikipedia.org/wiki/Honeypot_(computing).
223. Dolev.S., Application layer proxys, from http://www.cs.bgu.ac.il/research/atm_lab/ROUTING_.doc.
224. Proxy Server, from https://en.wikipedia.org/wiki/Proxy_server.
225. Proxy server, from https://whatis.techtarget.com/definition/proxy-server.
226. Steven J. Vaughan-Nichols, (2021), How to Set Up a Proxy Server on Your PC, Mac, or Web Browser, from https://www.avast.com/c-how-to-set-up-a-proxy#topic-1.
227. Raju PP, (2013), Different Types of VPN Protocols, from https://techpp.com/2010/07/16/different-types-of-vpn-protocols/.
228. VPN Technologies: Definitions and Requirements, from http://www.hit.bme.hu/~jakab/edu/litr/VPN/vpn-technologies.pdf.
229. VPN Technologies, from https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.html#vpn_tech.
230. Firewalls and Virtual Private Networks, from https://www.wiley.com/legacy/compbooks/press/0471348201_09.pdf.
231. (2014), What is VPN Concentrator?, from https://www.answers.com/Q/What_is_VPN_Concentrator.
232. Jeff Tyson, Chris Pollette, and Stephanie Crawford, (2021), How a VPN (Virtual Private Network) Works, from https://computer.howstuffworks.com/vpn.htm.
233. How Virtual Private Networks Work , from https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.html.
234. SSL VPN Security, from https://tools.cisco.com/security/center/resources/ssl_vpn_security.
235. SSL VPN (Secure Sockets Layer virtual private network), from https://searchsecurity.techtarget.com/definition/SSL-VPN.
236. Pradosh Kumar Mohapatra and Mohan Dattatreya, (2008), IPSec VPN Fundamentals, from https://www.eetimes.com/ipsec-vpn-fundamentals/#.
237. Paul Williams, What is a VPN? A Guide to Virtual Private Networks, from https://www.bandwidthplace.com/virtual-private-network-the-advantages-of-the-vpn-article/.
238. What Are the Main Benefits of VPNs?, from https://www.cactusvpn.com/vpn/benefits-of-vpn/.
239. (2014), What is VPN Concentrator?, from https://www.answers.com/Q/What_is_VPN_Concentrator.
240. Terry Slattery, How does the VPN concentrator work?, from https://searchnetworking.techtarget.com/answer/How-does-the-VPN-concentrator-work.
241. Configuring Site to Site IPsec VPN Tunnel Between Cisco Routers, from http://www.firewall.cx/cisco-technical-knowledgebase/cisco-routers/867-cisco-router-site-to-site-ipsec-vpn.html.
242. (2003), VPN Technologies: Definitions and Requirements, from http://www.hit.bme.hu/~jakab/edu/litr/VPN/vpn-technologies.pdf.
243. Andrew Tarantola, (2013), VPNs: What They Do, How They Work, and Why You're Dumb for Not Using One, from https://gizmodo.com/vpns-what-they-do-how-they-work-and-why-youre-dumb-f-5990192.
244. Andy Maxwell, (2012), How To Make VPNs Even More Secure, from https://torrentfreak.com/how-to-make-vpns-even-more-secure-120419/.
245. What is a VPN?, from https://www.ivpn.net/what-is-a-vpn/.
246. Usman Javaid, (2011), What Is VPN & Tunneling; How To Create And Connect To VPN Network [Beginner's Guide], from https://www.addictivetips.com/windows-tips/what-is-vpn-how-to-create-and-connect-to-vpn-network/.
247. What is Tunneling?, from http://www.dslreports.com/faq/5318.
248. Virtual Private Network, from https://en.wikipedia.org/wiki/Virtual_private_network.
249. Tunneling Protocol , from https://en.wikipedia.org/wiki/Tunneling_protocol
250. Tunneling Protocol, from https://www.pcmag.com/encyclopedia/term/tunneling-protocol.
251. Tunneling, from https://www.tech-faq.com/tunneling.html.
252. PPTP, from https://techterms.com/definition/pptp.
253. Layer 2 Tunneling Protocol, from https://en.wikipedia.org/wiki/Layer_2_Tunneling_Protocol.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

254. (2008), Layer Two Tunneling Protocol and Internet Protocol Security, from https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc958047(v=technet.10)?redirectedfrom=MSDN.

255. VPN Topologies Guide, from http://www.internet-computer-security.com/VPN-Guide/VPN-Topologies.html.

256. Advantages and Disadvantages of Hub-and-Spoke Operations, from http://aviationknowledge.wikidot.com/aviation:advantages-and-disadvantages-of-hub-and-spoke-opera.

257. Penna Sparrow, Mesh Topology: Advantages and Disadvantages, from https://www.ianswer4u.com/2011/05/mesh-topology-advantages-and.html#axzz3ElkXi5M9.

258. Penna Sparrow, Star Topology: Advantages and Disadvantages, from https://www.ianswer4u.com/2011/05/star-topology-advantages-and.html#axzz3ElkXi5M9.

259. (2012), RADIUS Protocol and Components, from https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc726017(v=ws.10)?redirectedfrom=MSDN.

260. Salvatore Salamone, (2002), Get IT Done: VPN reliability and scalability, from https://www.techrepublic.com/article/get-it-done-vpn-reliability-and-scalability/.

261. Guideline for setting up a functional VPN, from https://www.wingate.com/resources/WG/VPN_Setup_Guide.pdf.

262. (2016), Security Information and Events Management (SIEM), from https://blog.finjan.com/security-information-and-events-management-siem/.

263. Jatin Jain, (2015), What Is a SIEM?, from https://resources.infosecinstitute.com/certification/what-is-a-siem/#gref.

264. Karen Scarfone, (2015), A Comprehensive Guide to SIEM Products, from https://searchsecurity.techtarget.com/feature/Introduction-to-SIEM-services-and-products.

265. Linda Rosencrance, Security Information and Event Management (SIEM), from https://searchsecurity.techtarget.com/definition/security-information-and-event-management-SIEM.

266. Bip Khanal, (2015), Security Information and Event Management (SIEM), from https://www.linkedin.com/pulse/security-information-event-management-siem-bip-khanal.

267. Rajesh K, (2010), An Introduction to SIEM – Security Information & Event Management, from http://www.excitingip.com/920/an-introduction-to-siem-security-information-and-event-management/.

268. (2014), Security Information and Event Management (SIEM), from https://www.slideshare.net/k33a/security-information-and-event-management-siem#likes-panel.

269. Security Incident & Event Management (SIEM), from https://www.je.logicalis.com/globalassets/channel-islands/whitepapers/security-flyers/security-incident--event-management-siem.pdf.

270. Security Incident and Event Management (SIEM), from https://www.techopedia.com/definition/4097/security-incident-and-event-management-siem.

271. Security Information and Event Management (SIEM), from https://www.gartner.com/en/information-technology/glossary/security-information-and-event-management-siem.

272. (2020), How does SIEM logging work?, from https://cybersecurity.att.com/blogs/security-essentials/everything-you-wanted-to-know-about-siem-and-log-management-but-were-afraid.

273. The Essential Guide to User Behavior Analytics, from https://www.ciosummits.com/Online_Assets_Balabit_Essential_Guide_to_User_Behavior_Analytics.pdf.

274. Idan Tendler, (2016), User behavior analytics is key to identifying nefarious use of insider credentials, from https://www.networkworld.com/article/3027168/security/user-behavior-analytics-is-key-to-identifying-nefarious-use-of-insider-credentials.html.

275. Greg Schaffer, (2016), User Behavior Analytics (UBA), from https://info.varonis.com/hubfs/docs/research_reports/SC_UBA_Report16_Final.pdf.

Module 06: Virtualization and Cloud Computing

276. (2016), What is Software Defined Networking (SDN)? Definition, from https://www.sdxcentral.com/networking/sdn/definitions/what-the-definition-of-software-defined-networking-sdn/.

277. What is Software-Defined Networking (SDN)?, from https://www.blueplanet.com/resources/What-is-SDN.html.

278. (2016), What Is NFV Infrastructure (NFVI)? Definition, from https://www.sdxcentral.com/networking/nfv/definitions/nfv-infrastructure-nfvi-definition/

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

279. Eugene, (2017), Virtualization Techniques in Cloud Computing, from https://www.sam-solutions.com/blog/virtualization-techniques-in-cloud-computing/.

280. Namrata Bisht, (2021), Virtualization in Cloud Computing and Types, from https://www.geeksforgeeks.org/virtualization-cloud-computing-types/.

281. Shaikh Abdul Azeem, Satyendra Kumar Sharma, (2017), Role of Network Virtualization in Cloud Computing and Network Convergence, from http://www.iraj.in/journal/journal_file/journal_pdf/3-400-1512365019136-140.pdf.

282. Gabor Nagy, (2015), Operating System Containers vs. Application Containers, from https://blog.risingstack.com/operating-system-containers-vs-application-containers/.

283. Murugiah Souppaya, John Morello, Karen Scarfone, (2017), Application Container Security Guide, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-190.pdf.

284. Docker Architecture, from https://www.aquasec.com/cloud-native-academy/docker-container/docker-architecture/.

285. Khaja Ibrahim, (2019) Docker Networking Series – I, from https://directdevops.blog/2019/10/05/docker-networking-series-i/.

286. (2021), Kubernetes Components, from https://kubernetes.io/docs/concepts/overview/components/.

287. Prasad Katti, Kubernetes Design and Architecture, from https://github.com/kubernetes/community/blob/master/contributors/design-proposals/architecture/architecture.md#the-kubernetes-node.

288. Amir Jerbi, (2017), 8 Docker security rules to live by, from https://www.infoworld.com/article/3154711/8-docker-security-rules-to-live-by.html.

289. Aria, (2018), Security Challenges Related to Containers, from https://www.ariacybersecurity.com/container-security-challenges-blog/.

290. Christopher Tozzi, (2018), 3 Container Security Advantages and 3 Security Challenges, from https://containerjournal.com/topics/container-security/3-container-security-advantages-and-3-security-challenges/.

291. (2019), Container Security: Examining Potential Threats to the Container Environment, from https://www.trendmicro.com/vinfo/us/security/news/security-technology/container-security-examining-potential-threats-to-the-container-environment.

292. Shira Caldie, (2017), Using Docker containers? Beware of these security risks, from https://www.ontrack.com/uk/blog/the-world-of-data/using-docker-containers-beware-of-these-security-risks/.

293. Chuck Hegarty, (2018), Understanding Container Security: Kernel Exploits, DDoS Attacks & Poisoned Images, from https://www.siriuscom.com/2018/08/understanding-container-security/

294. Patrick Kleindienst, (2016), Exploring Docker Security – Part 2: Container flaws, from https://blog.mi.hdm-stuttgart.de/index.php/2016/08/16/exploring-docker-security-part-2-container-flaws/.

295. Karthik, (2012), Virtualization Security in Cloud Computing, from https://resources.infosecinstitute.com/virtualization-security-cloud-computing/#gref.

296. Docker Security, from https://docs.docker.com/engine/security/.

297. Jack Wallen, (2017), 5 tips for securing your Docker containers, from https://www.techrepublic.com/article/5-tips-for-securing-your-docker-containers/.

298. Docker Image Security Best Practices, from https://res.cloudinary.com/snyk/image/upload/v1551798390/Docker_Image_Security_Best_Practices_.pdf.

299. What is virtualization?, from https://www.citrix.com/en-in/glossary/what-is-virtualization.html.

300. Virtualization, from https://www.techopedia.com/definition/719/virtualization.

301. What is Virtualization, from https://www.igi-global.com/dictionary/an-evolutionary-approach-for-load-balancing-in-cloud-computing/31852.

302. Clare Hopping, (2021), What is virtualisation?, from https://www.itpro.co.uk/612016/what-is-virtualisation.

303. Virtualisation - Server Virtualisation, from http://www.artofcomputing.com/virtualisation-virtual-servers.html.

304. Vikas Garg, Virtualization, from http://www.ijoart.org/papers/VIRTUALIZATION.html.

305. What is Network Virtualization (NV)?, from https://www.vmware.com/topics/glossary/content/network-virtualization.

306. Network Virtualization and Virtual Networks, from https://docs.oracle.com/cd/E19120-01/open.solaris/819-6990/gfkbw/index.html.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

307. Network Virtualization, from https://www.techopedia.com/definition/655/network-virtualization.
308. Network Virtualization, from https://networksandservers.blogspot.com/2011/10/virtualization-ii.html.
309. Overview of Network Virtualization, from https://docs.oracle.com/cd/E26502_01/html/E28992/gfkbw.html.
310. Anatomy of Container Attack Vectors and Mitigations, from https://www.bankinfosecurity.com/anatomy-container-attack-vectors-mitigations-a-12490.
311. A sleeping security threat: How to protect against container compromise, from https://www.scmagazine.com/home/opinion/executive-insight/a-sleeping-security-threat-how-to-protect-against-container-compromise/.
312. Robail Yasrab, Mitigating Docker Security Issues, from https://arxiv.org/ftp/arxiv/papers/1804/1804.05039.pdf.
313. Steven Vaughan-Nichols, (2019), 5 ways to secure your containers, from https://www.hpe.com/us/en/insights/articles/5-ways-to-secure-your-containers-1904.html.
314. Devdatta Mulgund, (2019), Best Practices for Application Container Security, from https://securityintelligence.com/posts/8-best-practices-for-application-container-security/.
315. Chandani Vaya, (2019), A journey to Kubernetes security, from https://developer.ibm.com/technologies/containers/articles/journey-to-kubernetes-security/.
316. Connor Gilbert, (2019), 9 Kubernetes Security Best Practices Everyone Must Follow, from https://www.cncf.io/blog/2019/01/14/9-kubernetes-security-best-practices-everyone-must-follow/.
317. Chris Cooney, (2019), Security as Standard in the Land of Kubernetes, from https://www.freecodecamp.org/news/security-as-standard-in-the-land-of-kubernetes-50bfad74ca16/.
318. (2019), 15 Kubernetes security best practice to secure your cluster, from https://www.mobilise.cloud/15-kubernetes-security-best-practice-to-secure-your-cluster/.
319. Ajmal Kohgadai, (2019), Docker Container Security 101: Risks and 33 Best Practices, from https://www.stackrox.com/post/2019/09/docker-security-101/.
320. Docker Images, from https://www.katacoda.com/courses/docker/2.
321. Ajmal Kohgadai, (2020), Kubernetes Security 101: Risks and 29 Best Practices, from https://www.stackrox.com/post/2020/05/kubernetes-security-101/.
322. Kirsten Newcomer, 4 Kubernetes security challenges and how to address them, from https://techbeacon.com/enterprise-it/4-kubernetes-security-challenges-how-address-them.
323. Anastasios Arampatzis , (2020), What Are The Top 5 Kubernetes Security Challenges And Risks?, from https://informationsecuritybuzz.com/articles/what-are-the-top-5-kubernetes-security-challenges-and-risks/.
324. Arunvignesh Venkatesh, (2017), Cloud Computing Security: Provider & Consumer Responsibilities, from https://www.mindtree.com/blog/cloud-computing-security-provider-consumer-responsibilities.
325. Stratoscale, (2016), Security in Cloud Networking: FW, ACLs and More, from https://www.stratoscale.com/blog/data-center/security-cloud-networking-fw-acls/.
326. Natalie Boyd, (2018), Achieving Network Security in Cloud Computing, from https://www.sdxcentral.com/cloud/definitions/achieving-network-security-in-cloud-computing/.
327. (2018), Top 6 Methods to Protect Your Cloud Data from Hackers, from https://www.idexcel.com/blog/top-6-methods-to-protect-your-cloud-data-from-hackers/.
328. Naomi Assaraf, (2015), 5 Safety Concerns with Cloud Data Storage, Answered, from https://blog.cloudhq.net/5-safety-concerns-with-cloud-data-storage-answered/.
329. (2017), 7 Effective Tips to Secure Your Data in the Cloud, from https://hackernoon.com/7-effective-tips-to-secure-your-data-in-the-cloud-820bfe438d2.
330. Ed Moyle, (2019), 3 best practices for cloud security monitoring, from https://searchcloudsecurity.techtarget.com/tip/Cloud-security-monitoring-Challenges-and-guidance.
331. Mike Mason, (2018), Key Considerations for Compliance in the Cloud, from https://www.corporatecomplianceinsights.com/key-considerations-compliance-cloud/.
332. (2013), Introduction to Cloud Computing, from https://www.slideshare.net/ProfEdge/introduction-to-cloud-computing-23970527.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

333. Martin Gontovnikas, (2018), What Is Identity as a Service (IDaaS)?, from https://auth0.com/blog/identity-as-a-service-in-2018/.

334. Multi-Cloud, from https://avinetworks.com/glossary/multi-cloud/.

335. (2019), Multicloud, from https://en.wikipedia.org/wiki/Multicloud.

336. Rich Caldwell, (2019), Pros and Cons of a Multi-Cloud Strategy, from https://centricconsulting.com/blog/pros-and-cons-of-a-multi-cloud-strategy/.

337. Jignesh Solanki, 6 Multi-Cloud Architecture Designs for an Effective Cloud Strategy, from https://www.simform.com/multi-cloud-architecture/.

338. (2020), Cloud storage, from https://en.wikipedia.org/wiki/Cloud_storage.

339. Laxmi Ashrit, What is Cloud Storage – Architecture, Types, Advantages & Disadvantages, from https://electricalfundablog.com/cloud-storage-architecture-types/.

340. Basic Cloud Storage Architecture Information Technology Essay, from https://www.uniassignment.com/essay-samples/information-technology/basic-cloud-storage-architecture-information-technology-essay.php.

341. (2019), What is Containers as a service (CaaS)?, from https://www.ibm.com/services/cloud/containers-as-a-service.

342. Using an IAM Role to Grant Permissions to Applications Running on Amazon EC2 Instances, from https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-ec2.html.

343. Lock Away Your AWS Account Root User Access Keys, from https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#lock-away-credentials.

344. Stuart Scott, (2015), AWS Security: Identity and Access Management (IAM), from https://cloudacademy.com/blog/aws-security-identity-and-access-management-iam/.

345. Setting an Account Password Policy for IAM Users, from https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html.

346. AWS Managed Policies, from https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_managed-vs-inline.html#aws-managed-policies.

347. Brad Lyman, An Easier Way to Manage Your Policies, from https://aws.amazon.com/blogs/security/an-easier-way-to-manage-your-policies/.

348. Create Individual IAM Users, from https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#create-iam-users.

349. Creating Your First IAM Admin User and Group, from https://docs.aws.amazon.com/IAM/latest/UserGuide/getting-started_create-admin-group.html.

350. Adding and Removing Users in an IAM Group, from https://docs.aws.amazon.com/IAM/latest/UserGuide/id_groups_manage_add-remove-users.html.

351. Rob Moncur, Now Create and Manage Users More Easily with the AWS IAM Console, from https://aws.amazon.com/blogs/security/now-create-and-manage-users-more-easily-with-the-aws-iam-console/.

352. Jeff Barr, IAM: AWS Identity and Access Management – from Now Generally Available, https://aws.amazon.com/blogs/aws/iam-identity-access-management/.

353. Overview of Access Management: Permissions and Policies, from https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction_access-management.html.

354. AWS IAM features, from https://aws.amazon.com/iam/features/.

355. AWS IAM, from https://www.simplilearn.com/aws-iam-tutorial-article.

356. The AWS Account Root User, from https://docs.aws.amazon.com/IAM/latest/UserGuide/id_root-user.html.

357. Roles Terms and Concepts, from https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_terms-and-concepts.html.

358. Creating a Role to Delegate Permissions to an IAM User, from https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-user.html.

359. Abhishek Pandey, Introducing an Easier Way to Delegate Permissions to AWS Services: Service-Linked Roles, from https://aws.amazon.com/blogs/security/introducing-an-easier-way-to-delegate-permissions-to-aws-services-service-linked-roles/.

360. Using Temporary Credentials With AWS Resources, from https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp_use-resources.html.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

361. Creating an IAM User in Your AWS Account, from https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users_create.html.

362. Anything as a Service (XaaS), from https://timesofcloud.com/cloud-tutorial/xaas/.

363. Natallia Sakovich, Everything-as-a-Service (XaaS): Definition and Examples, from https://www.sam-solutions.com/blog/everything-as-a-service-xaas-definition-and-examples/.

364. Forrest Stroud, (2021), XaaS – Anything-As-A-Service, from https://www.webopedia.com/definitions/anything-as-a-service-xaas/.

365. What is XaaS (anything as a service)?, fromhttps://www.netapp.com/knowledge-center/what-is-anything-as-a-service-xaas/#:~:text=%E2%80%9CAnything%20as%20a%20service%E2%80%9D%20(,a%20service%20over%20the%20internet.

366. Ryan Squires, (2018), Everything-as-a-Service (XaaS): From Software to Property, from https://jumpcloud.com/blog/xaas.

367. (2018), Everything-as-a-Service: Have Federal CIOs Found Their Holy Grail?, from https://www.eglobaltech.com/post/everything-as-a-service-have-federal-cios-found-their-holy-grail.

368. Brett Mundell, (2019), On-premise vs Cloud vs Hosted: What's the difference?, from https://www.leveragetech.com.au/blog/on-premise-vs-cloud-vs-hosted/.

369. John Moore, Hosted Services, from https://searchitchannel.techtarget.com/definition/hosted-services.

370. Susan Meyer, Understanding the Differences Between On-Premise vs Hosted vs SaaS + How to Pick the Right Choice for Your Ecommerce, from https://www.bigcommerce.com/blog/on-prem-vs-hosted-vs-saas/#pros-and-cons-of-on-prem-hosted-and-saas.

371. Cloud Security, from https://slideplayer.com/slide/6204150/.

Module 07: Wireless Network Security

372. What is WiFi?, from https://scambusters.org/wifi.html.

373. Wireless Network, from https://en.wikipedia.org/wiki/Wireless_network#Difficulties.

374. Types of Wireless Network Explained with Standards, from https://www.computernetworkingnotes.com/ccna-study-guide/types-of-wireless-network-explained-with-standards.html.

375. Wireless Network, from https://www.techopedia.com/definition/26186/wireless-network.

376. Wireless Technology, from https://www.nibusinessinfo.co.uk/content/pros-and-cons-wireless-networking.

377. IEEE 802.11i-2004, from https://en.wikipedia.org/wiki/IEEE_802.11i-2004.

378. 802.11i, from https://searchmobilecomputing.techtarget.com/definition/80211i.

379. Wireless Access Point, from https://en.wikipedia.org/wiki/Wireless_access_point.

380. Agustina, J. V. Peng Zhang, and Kantola, (2003), Performance evaluation of GSM handover traffic in a GPRS/GSM network, from https://ieeexplore.ieee.org/document/1214113?isnumber=27298&arnumber=1214113&count=217&index=21.

381. Peter Loshin, (2019), Defending against the most common wireless network attacks, from https://searchsecurity.techtarget.com/feature/A-list-of-wireless-network-attacks.

382. Chris Weber and Gary Bahadu, (2009), Wireless Networking Security, from https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-xp/bb457019(v=technet.10)?redirectedfrom=MSDN.

383. (2009), How 802.11 Wireless Works, from https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc757419(v=ws.10)?redirectedfrom=MSDN.

384. TKIP (Temporal Key Integrity Protocol), from https://www.tech-faq.com/tkip-temporal-key-integrity-protocol.html.

385. Kevin Beaver and Peter T. Davis, Understanding WEP Weaknesses, from https://www.dummies.com/programming/networking/understanding-wep-weaknesses/.

386. Bradley Mitchell, (2021) Wired vs. Wireless Networking, from https://www.lifewire.com/wired-vs-wireless-networking-816352.

387. Bradley Mitchell, (2019), Wireless Standards - 802.11b 802.11a 802.11g and 802.11n, from https://www.lifewire.com/wireless-standards-802-11a-802-11b-g-n-and-802-11ac-816553.

388. Wi-Fi Protected Access, from https://searchmobilecomputing.techtarget.com/definition/Wi-Fi-Protected-Access.

389. WPA (Wi-Fi Protected Access), from https://www.tech-faq.com/wpa-wi-fi-protected-access.shtml.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

390. Paul Arana, (2006), Benefits and Vulnerabilities of Wi-Fi Protected Access 2 (WPA2), from https://cs.gmu.edu/~yhwang1/INFS612/Sample_Projects/Fall_06_GPN_6_Final_Report.pdf.

391. Lisa Phifer, Service set identifier, from https://searchmobilecomputing.techtarget.com/definition/service-set-identifier.

392. Antenna Cabling Guide, from http://wireless.gumph.org/content/3/12/011-antenna-cabling.html.

393. Mateusz Buczkowski, (2018), Introduction to Wi-Fi Security, from https://www.grandmetric.com/2018/07/06/ended-wpa3-wi-fi-security-evolution/.

394. Wireless Security Protocols: WEP, WPA, WPA2 and WPA3, from https://www.cyberpunk.rs/wireless-security-protocols-wep-wpa-wpa2-and-wpa3.

395. Penny Hoelscher, (2018), What is WPA3, is it secure and should I use it?, from https://www.comparitech.com/blog/information-security/what-is-wpa3/.

396. Discover Wi-Fi Security, from https://www.wi-fi.org/discover-wi-fi/security.

397. (2018), WPA3 Explained, from https://medium.com/@reliancegcs/wpa3-explained-wi-fi-is-getting-major-security-update-2b6dca8f3aff.

398. Wi-Fi Protected Access, from https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access.

399. Tips For Securing Your Wireless Connection, from https://www.sophos.com/en-us/security-news-trends/best-practices/wi-fi.aspx.

400. Eric Geier, (2011), Wi-Fi security do's and don'ts, from https://www.networkworld.com/article/2182865/wi-fi-security-do-s-and-don-ts.html.

401. Pablo Estrada, (2011), 10 Best Practices for Designing Your Event Wi-Fi Deployment, from https://meraki.cisco.com/blog/2011/06/10-best-practices-for-designing-your-event-wi-fi-deployment/.

402. Beryl George, Wireless Technologies, from https://slideplayer.com/slide/6835910/.

Module 08: Mobile Device Security

403. Mike Chapple, (2017), Mobile Connection Method, from https://www.linkedin.com/learning/comptia-security-plus-sy0-501-cert-prep-2-technologies-and-tools/mobile-connection-methods?trk=lynda_redirect_learning.

404. Ankit Anand, Cellular Wireless Network Security, from https://www.slideshare.net/AnkitAnand126/cellular-wireless-network-security#:~:text=Conclusion%20Cellular%20Networks%20are%20open,authentication%2C%20confidentiality%2C%20integrity%20etc..

405. (2021), Point-to-point (telecommunications), from https://en.wikipedia.org/wiki/Point-to-point_(telecommunications)#:~:text=In%20telecommunications%2C%20a%20point%2Dto,be%20heard%20by%20the%20other..

406. (2019), Differences between Point-to-Point and Multi-point Communication, from https://www.geeksforgeeks.org/differences-between-point-to-point-and-multi-point-communication/.

407. (2017), Point-to-Point and Point-to Multipoint Wireless, from https://www.cablefree.net/wireless-technology/difference-point-point-point-multipoint/.

408. Jerry Hildenbrand, (2020), How does GPS work on my phone?, from https://www.androidcentral.com/how-does-gps-work-my-phone.

409. Suzanne Smiley, (2016), 7 Types of Security Attacks on RFID Systems, from https://www.atlasrfidstore.com/rfid-insider/7-types-security-attacks-rfid-systems.

410. Kate O'Flaherty, (2020), How safe is 5G really?, from https://www.raconteur.net/technology/5g/5g-security/.

411. Erica Mixon, Mobile Device Management (MDM), from https://searchmobilecomputing.techtarget.com/definition/mobile-device-management.

412. Vangie Beal, (2021), Mobile Device Management, from https://www.webopedia.com/definitions/mobile-device-management/.

413. Mykhayl Tserr, Eugene Koshel, (2020), How to Build a Mobile Device Management (MDM) System?, from https://www.apriorit.com/dev-blog/473-how-to-build-an-mdm-system.

414. Muhammad Raza, (2019), Mobile Device Management (MDM): An Introduction, from https://www.bmc.com/blogs/mdm-mobile-device-management/.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

415. Colin Steele, Mobile Application Management (MAM), from https://searchmobilecomputing.techtarget.com/definition/mobile-application-management-MAM.

416. Mobile content management system (CMS), from https://www.contentful.com/r/knowledgebase/mobile-cms/.

417. Mobile content management (MCM), from https://www.manageengine.com/mobile-device-management/mobile-content-management.html.

418. (2020), Introduction to Mobile Content Management, from https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/MCM/GUID-AWT-MCM-INTRO.html.

419. Forrest Stroud, (2021), MCM – Mobile Content Management , from https://www.webopedia.com/definitions/mcm-mobile-content-management/.

420. (2020), Mobile content management system, from https://en.wikipedia.org/wiki/Mobile_content_management_system.

421. Joel Snyder, (2021), 3 things you should know about remote wipe, from https://insights.samsung.com/2020/05/28/3-things-you-should-know-about-remote-wipe-2/.

422. Cliff White, Remote Wipe: a Must for Mobile Security, from https://www.accellion.com/blog/remote-wipe-must-for-mobile-security/.

423. A Beginner's Guide to Geofencing for Mobile Apps , from https://clearbridgemobile.com/a-beginners-guide-to-geofencing-for-mobile-apps/.

424. Aasif, (2021), A Simple Guide to Geofencing for Mobile App Marketing, from https://www.appypie.com/geofencing-app-marketing.

425. Rahul Singh, (2018) , Understanding geolocation in mobile apps: How location based services in apps enhance their appeal?, from https://www.promaticsindia.com/blog/understanding-geolocation-in-mobile-apps-how-location-based-services-in-apps-enhance-their-appeal/.

426. Lock screen, from https://en.wikipedia.org/wiki/Lock_screen.

427. Amer Owaida, (2020), How secure is your phone's lock screen?, from https://www.welivesecurity.com/2020/06/05/how-secure-is-your-phone-lock-screen/.

428. Maud Panier, (2021), Before We Start: What Are Mobile Push Notifications And How To Use Them, from https://thetool.io/2020/top-push-notifications-tools-services#:~:text=A%20Push%20Notification%20(also%20called,a%20request%20from%20the%20user.&text=They%20are%20the%20opposite%20side,Notifications%20originate%20from%20a%20server..

429. Ian Blair, What is a Push Notification? And Why It Matters?, from https://buildfire.com/what-is-a-push-notification/.

430. Push Notification Kat King, from https://www.twilio.com/docs/glossary/what-is-push-notification.

431. (2020), PINs vs. Passwords: What's the Difference?, from https://www.allclearid.com/2020/01/15/pins-vs-passwords-whats-difference/.

432. Password and PIN security, from https://www.paypal.com/us/webapps/mpp/security/secure-passwords.

433. Leonardo Sam Waterson, (2019), Why Biometrics is a Must for Mobile App Security, from https://www.m2sys.com/blog/guest-blog-posts/biometrics-mobile-app-security/.

434. KamalBenzekkia, AbdeslamEl Fergouguia, AbdelbakiElBelrhiti ElAlaoui, (2018), A Context-Aware Authentication System for Mobile Cloud Computing, from https://www.sciencedirect.com/science/article/pii/S1877050918301479.

435. Ben Kepes, (2016), Forget two-factor authentication, here comes context-aware authentication, from https://www.computerworld.com/article/3105866/forget-two-factor-authentication-here-comes-context-aware-authentication.html.

436. Bridget Botelho, (2013), Context-aware security, from https://searchsecurity.techtarget.com/definition/context-aware-security.

437. Containerization of Android devices, from https://www.manageengine.com/mobile-device-management/mdm-containerization.html.

438. Alma Evans, (2018), What is Containerization and why is it important for your business?, from https://www.hexnode.com/blogs/what-is-containerization-and-why-is-it-important-for-your-business/.

439. (2021), Full-Disk Encryption, from https://source.android.com/security/encryption/full-disk.

440. Joel Snyder, (2021), BYOD, CYOD, COPE, COBO — What Do They Really Mean?, from https://insights.samsung.com/2018/05/09/byod-cyod-cope-cobo-what-do-they-really-mean/.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

441. Rene Millman, (2021), What is BYOD?, from https://www.itpro.co.uk/strategy/28072/what-is-byod.

442. (2018), Enterprise Mobility Management: Models and Solutions, from https://www.altexsoft.com/blog/cloud/enterprise-mobility-management-models-and-solutions/.

443. Jo Davis, (2014), 5 things to consider before implementing BYOD, from https://realbusiness.co.uk/5-things-to-consider-before-implementing-byod/.

444. Choose Your Own Device (CYOD), from https://www.techopedia.com/definition/29909/choose-your-own-device-cyod.

445. (2021), BYOD vs. CYOD vs. COBO vs. COPE: How to Know When to Change or Adjust Your Mobile Strategy, from https://blog.caleromdsl.com/byod-vs-cyod-vs-cope-choose-right-enterprise-mobility-strategy/.

446. BRING YOUR OWN DEVICE (BYOD) VS. CHOOSE YOUR OWN DEVICE (CYOD), from https://www.utgjiu.ro/rev_ing/pdf/2018-4/18_S.%20Iovan,%20C.%20Ivanus%20-BRING%20YOUR%20OWN%20DEVICE%20(BYOD)%20VS.%20CHOOSE%20YOUR%20OWN%20DEVICE%20(CYOD).pdf.

447. Josh Bouk, (2018), Josh Bouk, CYOD vs BYOD: A Comparative Analysis, from https://www.cassinfo.com/telecom-expense-management-blog/cyod-vs-byod-a-comparative-analysis.

448. Best Practices to Make BYOD, CYOD and COPE Simple and Secure, from https://www.citrix.com/en-in/products/citrix-endpoint-management/byod-best-practices.html.

449. Liarna La Porta, (2018), What's the best mobile device ownership model for your business?, from https://www.wandera.com/cope-byod-cyod/.

450. Iskren Tairov, (2016), Enterprise Mobility – A Solution For Increased Business Efficiency, from https://www.researchgate.net/profile/Iskren_Tairov/publication/314286291_ENTERPRISE_MOBILITY_-_A_SOLUTION_FOR_INCREASED_BUSINESS_EFFICIENCY/links/58bfe640458515bc83906d6e/ENTERPRISE-MOBILITY-A-SOLUTION-FOR-INCREASED-BUSINESS-EFFICIENCY.pdf.

451. Corporately-Owned, Personally-Enabled: When is COPE the Right Mobility Model for Agencies?, from https://www.accenture.com/t20150523T024231__w__/gr-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_14/Accenture-Corporately-Owned-Personally-Enabled-When-COPE-Right-Mobility-Model-Agencies.pdf.

452. BYOD, CYOD, COPE, COBO — What Do They Really Mean?, from https://www.wired.com/brandlab/2018/06/byod-cyod-cope-cobo-really-mean/.

453. Ines Reinhardt, (2019), Mobility Basics Part III: What's The Difference Between Byod, Cobo And Cope?, from https://blog.cortado.com/mobility-basics-whats-the-difference-between-byod-and-cobo/.

454. Sunil Lalvani, (2014), Transition from BYOD to COBO, from https://cio.economictimes.indiatimes.com/tech-talk/transition-from-byod-to-cobo/325.

455. How to choose the right mix: BYOD/COPE/CYOD/COBO, from http://docs.media.bitpipe.com/io_12x/io_122848/item_1123795/Mobile%20Device%20Ownership%20-%20How%20to%20Choose%20the%20Right%20Mix.pdf.

456. Ed Tittel, (2014), 7 Enterprise Mobile Security Best Practices, from https://www.cio.com/article/2378779/7-enterprise-mobile-security-best-practices.html.

457. Mobile device management (MDM) for iOS, Android, and Windows devices., from https://www.manageengine.com/products/desktop-central/mobile-device-management-mdm.html.

458. Bocholt, (2019), Everything under control TISLOG MDM - centralized management for your hardware, from https://www.tis-gmbh.de/en/tislog-mdm-mobile-device-management/.

459. Manasdeep, (20130, Mobile Device Management (MDM) – Challenges and Solutions, from https://niiconsulting.com/checkmate/2013/07/mobile-device-management-challenges-and-solutions/.

460. Mobile Device Management, from https://www.ecom-ex.com/solutions/mobile-device-management/.

461. Forrest Stroud, (2021), Mobile Application Management (MAM), from https://www.webopedia.com/TERM/M/mam-mobile-application-management.html.

462. Mobile application management, from https://en.wikipedia.org/wiki/Mobile_application_management.

463. What is Mobile Application Management (MAM)?, from https://www.manageengine.com/mobile-device-management/mobile-application-management.html.

464. Mobile content management system, from https://en.wikipedia.org/wiki/Mobile_content_management_system#Key_features.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

465. What is Mobile Threat Defense?, from https://www.lookout.com/products/mobile-threat-defense/.

466. Robin Gray, What is Mobile Threat Defense (MTD)?, from https://www.wandera.com/what-is-mobile-threat-defense-mtd/.

467. What Is Mobile Threat Defense?, from https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=b211ab8a-0b3b-4177-8a4d-61bfd8a7f1a7&CommunityKey=63909be8-ed89-4445-bfd4-55f7374256ce&tab=librarydocuments.

468. Scott King, (2017), Gartner Mobile Threat Defense and Enterprise Mobile Security Guide, from https://blog.zimperium.com/your-guide-to-mobile-threat-defense/.

469. Mobile E-mail Management (MEM), from https://www.manageengine.com/mobile-device-management/mobile-email-management.html.

470. 42Gears Mobile Email Management, from https://www.42gears.com/white-papers/42gears-mobile-email-management/.

471. Understanding Unified Endpoint Management, from https://docs.42gears.com/whitepapers/Understanding%20Unified%20Endpoint%20Management.pdf.

472. KC Karnes, (2020), Mobile App Security Threats and Secure Best Practices, from https://clevertap.com/blog/mobile-app-security/.

473. David Oragui, (2018), 7 Steps You Should Take to Improve Mobile App Security, from https://themanifest.com/mobile-apps/7-steps-you-should-take-improve-mobile-app-security.

474. 5 Mobile App Security Best Practices you can't Ignore!, from https://www.preludesys.com/mobile-app-security-best-practices/.

475. Vijay Singh, (2020), Security Checklist for Mobile Development, from https://hackr.io/blog/mobile-app-security-standards-checklist.

476. Daniel Hein, (2019), Mobile Data Security: How to Protect Corporate Data on Mobile Devices, from https://solutionsreview.com/mobile-device-management/mobile-data-security-how-to-protect-corporate-data-on-mobile-devices/.

477. 6 Steps to Rapidly Improve Mobile Data Security, from https://www.imei.com.au/mobile-data-security#datasecurity.

478. 4 Practical Stapes to Safeguard your Mobile Data, from https://www.imei.com.au/mobile-data-security#legislationregulations.

479. Mobile Security – Introduction, from https://www.tutorialspoint.com/mobile_security/mobile_security_quick_guide.htm.

Module 09: IoT Device Security

480. Gamal H. Eladl, Technical Requirements for the Application of Internet of Things, from http://ijcsn.org/IJCSN-2017/6-4/Technical-Requirements-for-the-Application-of-Internet-of-Things.pdf.

481. Enterprise Internet of Things, from http://www.enterox.com/IoT/articles/enterprise-internet-of-things.htm.

482. Ronak Patel, (2019), IoT for Business Enterprises: Everything You Need to Know, from https://dzone.com/articles/iot-for-business-enterprises-attributes-challenges.

483. Jonathan Greig, (2020), IoT device security: 5 tips for enterprises, from https://www.techrepublic.com/article/iot-device-security-5-tips-for-enterprises/.

484. Vishruta Rudresh, (2018), IoT Security Reference Architecture, from https://cdn2.hubspot.net/hubfs/2539908/Whitepapers/IoT%20Security%20Reference%20Architecture_September-2018.pdf.

485. Steven Lerner, (2019), 12 IoT Security Challenges And How to Address Them in the Enterprise, from https://www.enterprisedigi.com/iot/articles/iot-security-challenges.

486. Andrey Nikishin, (2018), What is a secure internet of things?, from https://os.kaspersky.com/2018/05/31/what-is-a-secure-internet-of-things/.

487. Nick Carstensen, (2019), Improving IOT Security With Log Management, from https://www.graylog.org/post/improving-iot-security-with-log-management.

488. David Strom, (2017), 9 ways to improve IoT device security, from https://www.hpe.com/us/en/insights/articles/9-ways-to-make-iot-devices-more-secure-1701.html.

489. Alex Grizhnevich, (2018), IoT architecture: building blocks and how they work, from https://www.scnsoft.com/blog/iot-architecture-in-a-nutshell-and-how-it-works.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

490. Priya Pedamkar, IoT Ecosystem, from https://www.educba.com/iot-ecosystem/.

491. What Is the Internet of Things Ecosystem?, from https://etma.org/what-is-iot-ecosystem/.

492. Uwazie Emmanuel Chinanu, Onoja Emmanuel Oche, Joy O. Okah-Edemoh, (2018), Architectural Layers of Internet of Things: Analysis of Security Threats and Their Countermeasures, from https://arpgweb.com/pdf-files/sr4(10)80-89.pdf.

493. Murat Aydos, Yılmaz Vural, Adem Tekerek, (2019), Assessing risks and threats with layered approach to Internet of Things security, from https://journals.sagepub.com/doi/full/10.1177/0020294019837991.

494. Hezam Akram Abdul-Ghani, Dimitri Konstantas, Mohammed Mahyoub, (2018), A Comprehensive IoT Attacks Survey based on a Building-blocked Reference Model, from https://thesai.org/Downloads/Volume9No3/Paper_49-A_Comprehensive_IoT_Attacks_Survey.pdf.

495. Ehsan ul Haq, Tariq Aziz Rao, (2018), Security Challenges Facing IoT Layers and its Protective Measures, from https://www.researchgate.net/publication/323892938_Security_Challenges_Facing_IoT_Layers_and_its_Protective_Measures.

496. (2016), Strategic Principles for Securing the Internet of Things (IoT), from https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf.

497. IoT Security Guidelines for Network Operators, from https://www.gsma.com/iot/iot-security-guidelines-for-network-operators/.

498. (2019), IoT Security Guidelines for Network Operators, from https://www.gsma.com/iot/wp-content/uploads/2019/10/CLP.14-v2.1.pdf.

499. (2019), Internet of Things (IoT) security: 9 ways you can help protect yourself, from https://us.norton.com/internetsecurity-iot-securing-the-internet-of-things.html.

500. (2019), 12 tips to help secure your smart home and IoT devices, from https://us.norton.com/internetsecurity-iot-smart-home-security-core.html.

501. Jacob Arellano, (2019), Best Practices for Securing IoT Devices, from https://www.verypossible.com/blog/best-practices-for-securing-iot-devices.

502. Dean Hamilton, (2018), Best practices for IoT security, from https://www.networkworld.com/article/3266375/best-practices-for-iot-security.html.

503. George Corser, Internet of Things (IOT) Security Best Practices, from https://internetinitiative.ieee.org/images/files/resources/white_papers/internet_of_things_feb2017.pdf.

504. Conner Forrest, (2017), Ten best practices for securing the Internet of Things in your organization, from https://www.zdnet.com/article/ten-best-practices-for-securing-the-internet-of-things-in-your-organization/.

Module 10: Cryptography and PKI

505. Yuan Xue, (2009), Digital Signature, from https://tao.truststc.org/Members/yuanxue/network_security/Public resources/lecture12.

506. Hash Function, from https://en.wikipedia.org/wiki/Hash_function.

507. Andrew Zola, Hashing, from https://searchsqlserver.techtarget.com/definition/hashing.

508. Vangie Beal, (2021), Hashing, from https://www.webopedia.com/definitions/hashing/.

509. Ben Lutkevich, Vicki-Lynn Brunskill, Peter Loshin, Digital Signature, from https://searchsecurity.techtarget.com/definition/digital-signature.

510. Dawid Czagan, (2019), Non-repudiation and Digital signature, from https://resources.infosecinstitute.com/topic/non-repudiation-digital-signature/.

511. Vangie Beal, (2021), Digital Certificate, from https://www.webopedia.com/definitions/digital-certificate/.

512. Peter Loshin, Digital Certificate, https://searchsecurity.techtarget.com/definition/digital-certificate.

513. (2012), Digital Certificates, from https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc962029(v=technet.10)?redirectedfrom=MSDN.

514. (2001), Announcing the Advanced Encryption Standard (AES), from https://csrc.nist.gov/csrc/media/publications/fips/197/final/documents/fips-197.pdf.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

515. John Talbot and Dominic Welsh, (2006), Complexity and Cryptography an introduction, from https://www.cambridge.org/gb/academic/subjects/mathematics/discrete-mathematics-information-theory-and-coding/complexity-and-cryptography-introduction?format=PB&isbn=9780521617710.

516. What is Public-Key Cryptography?, from http://www.x5.net/faqs/crypto/q3.html.

517. Josh Ryder, (2000), Introduction to Encryption, from https://www.developer.com/guides/introduction-to-encryption/.

518. HMAC, from https://en.wikipedia.org/wiki/HMAC.

519. Hash-based Message Authentication Code (HMAC), from https://searchsecurity.techtarget.com/definition/Hash-based-Message-Authentication-Code-HMAC.

520. How and when do I use HMAC?, from https://security.stackexchange.com/questions/20129/how-and-when-do-i-use-hmac/20301.

521. Krishna Gehlot, (2015), Message Authentication Code & HMAC, from, https://www.slideshare.net/PRINCEOFSUNCITY/message-authentication-code-hmac.

522. Umesh Hodeghatta RaoUmesha Nayak, (2014), Cryptography, from https://link.springer.com/chapter/10.1007/978-1-4302-6383-8_8.

Module 11: Data Security

523. Data Loss Prevention, from https://www.futuretech-group.com/datalossprevention.html.

524. What Is Backup and Recovery?, from https://www.netapp.com/data-protection/backup-recovery/what-is-backup-recovery/.

525. (2017) How to Encrypt Your Device, from https://spreadprivacy.com/how-to-encrypt-devices/.

526. Ayush, (2018), How to encrypt files with EFS Encryption on Windows 10, from https://www.thewindowsclub.com/encrypt-files-efs-encryption-windows-10.

527. Why back up? The importance of protecting your data , from http://static.highspeedbackbone.net/pdf/hp_why_backup.pdf.

528. (2010), Choosing backup media is easy when you know how, thanks to this handy guide, from https://www.top-windows-tutorials.com/backup-media/.

529. Simplifying NAS/SAN Backup and Recovery with Barracuda Backup, from https://www.barracuda.com/assets/docs/White_Papers/Barracuda_Backup_SB_NAS_US.pdf.

530. What is the difference between cold backup and hot backup, from http://www.geekinterview.com/question_details/49691.

531. Difference between: Full, Differential, and Incremental Backup, from http://www.backup.info/difference-between-full-differential-and-incremental-backup.

532. What Is System Backup?, from https://www.ubackup.com/help/system-backup.html.

533. What is a Data Backup?, from https://support.winzip.com/hc/en-us/articles/115011428608-What-is-a-Data-Backup-.

534. Backup, from https://en.wikipedia.org/wiki/Backup.

535. Backup, from https://searchdatabackup.techtarget.com/definition/backup.

536. Ed Palmer, (2002), Seven steps to backup and restore, from https://searchdatabackup.techtarget.com/magazineContent/Seven-steps-to-backup-and-restore.

537. Kris Bushover,Eric Osterholm, (2008), Disaster Recovery & Data Backup Strategies, from https://www.slideshare.net/spiceworks/disaster-recovery-data-backup-strategies-presentation.

538. How Often Do You Need to Back Up Your Files?, from https://www.allbusiness.com/how-often-do-you-need-to-back-up-your-files-1202-1.html.

539. How Often Should You Backup Your Files?, from https://www.datarecoverylabs.com/company/resources/how-often-should-you-backup-your-files.

540. Selecting the backup medium, from https://tldp.org/LDP/sag/html/backup-media.html.

541. Alexander S. Gillis, RAID (redundant array of independent disks), from https://searchstorage.techtarget.com/definition/RAID.

542. Vangie Beal, RAID, from https://www.webopedia.com/definitions/raid/.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

543. What is RAID?, from http://www.freeraidrecovery.com/library/what-is-raid.aspx.

544. Rich Castagna, Kim Hefner, RAID controller, from https://searchstorage.techtarget.com/definition/RAID-controller.

545. Serial ATA (Serial Advanced Technology Attachment or SATA), from https://searchstorage.techtarget.com/definition/Serial-ATA.

546. Disk array controller, from https://en.wikipedia.org/wiki/Disk_array_controller.

547. RAID, from https://www.prepressure.com/library/technology/raid.

548. Ankur Niyogi, (2005), RAID Redundant Array of Independent Disks, from https://www.slideshare.net/raid-recovery/understanding-raid-levels-raid-0-raid-1-raid-2-raid-3-raid-4-raid-5?qid=18a133f3-4e28-4e69-aa94-2029a17dae35&v=qf1&b=&from_search=11.

549. Antony Adshead, (2009), Software RAID vs hardware RAID: Pros and cons , from https://www.computerweekly.com/news/1367590/Software-RAID-vs-hardware-RAID-Pros-and-cons.

550. Brien Posey, (2011), Best practices for setting up RAID groups, from https://searchdatacenter.techtarget.com/tip/Best-practices-for-setting-up-RAID-groups.

551. Scott Lowe, (2010), Choose a RAID level that works for you, from https://www.techrepublic.com/blog/the-enterprise-cloud/choose-a-raid-level-that-works-for-you/.

552. Storage area network, from https://en.wikipedia.org/wiki/Storage_area_network.

553. (2012), Storage Area Network (SAN), from https://www.slideserve.com/ula/storage-area-network-san.

554. Sarath Pillai, (2014), SAN vs NAS - Difference between a Storage Area Network and Network Attached Storage, from https://www.slashroot.in/san-vs-nas-difference-between-storage-area-network-and-network-attached-storage.

555. Brien Posey, Advantages and disadvantages of using a SAN, from https://searchstorage.techtarget.com/tip/Advantages-and-disadvantages-of-using-a-SAN.

556. Syed Ubaid Ali Jafri, (2013), Storage Area Network, from https://www.slideshare.net/masterubaid/storage-area-network-25251039.

557. Raphael Ejike, Stroage Area Network (SAN), from https://pt.slideshare.net/raphaelejike/storage-area-network-san-4892728.

558. Storage Area Network Architecture (SAN Architecture), from https://www.techopedia.com/definition/30211/storage-area-network-architecture-san-architecture.

559. Keith Spayth, (2010), Storage Area Network, from https://www.slideshare.net/itsec/san-review.

560. Network-attached storage, from https://en.wikipedia.org/wiki/Network-attached_storage.

561. Vangie Beal, NAS - Network Attached Storage, from https://www.webopedia.com/definitions/network-attached-storage/.

562. Garry Kranz, What is network-attached storage (NAS) and how does it work?, from https://searchstorage.techtarget.com/definition/network-attached-storage.

563. Network Attached Storage (NAS) Review: Pros and Cons, from https://www.bffnas.com/network-attached-storage-nas-overview-on-its-pros-and-cons/.

564. Rajesh K, (2010), NAS – Advantages, Limitations & Recommendations for Ethernet Storage over TCP/IP Networks, from http://www.excitingip.com/819/network-attached-storage-advantages-limitations-ethernet-storage-ip-network-best-practices/.

565. (2012), Network Attached Storage (NAS), from https://www.slideshare.net/sandeepgodfather/network-attached-storage-nas.

566. Ed Hannan, Cold Backup (Offline Backup), from https://searchdatabackup.techtarget.com/definition/cold-backup.

567. Paul Crocetti, Hot Backup (Dynamic Backup), from https://searchdatabackup.techtarget.com/definition/hot-backup.

568. Erin Sullivan, Brien Posey, (2020), Data backup types explained: Full, incremental, differential and incremental-forever backup, from https://searchdatabackup.techtarget.com/tip/Data-backup-types-explained-Full-incremental-differential-and-incremental-forever-backup.

569. Types of backup, (2009), from https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc784306(v=ws.10)?redirectedfrom=MSDN.

570. Data Recovery, from https://en.wikipedia.org/wiki/Data_recovery

571. Stephen Watts, (2018), Data Masking: An Introduction, from https://www.bmc.com/blogs/data-masking/.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

572. Brien Posey, Paul Crocetti, Andrew Burton, Data Retention Policy, from https://searchdatabackup.techtarget.com/definition/data-retention-policy.

573. Mike Mariano, (2018), 5 Key Steps to Developing a Solid Data Retention Policy, from https://www.ispartnersllc.com/blog/5-steps-developing-data-retention-policy/.

Module 12: Network Traffic Monitoring

574. Packet analyzer, from https://en.wikipedia.org/wiki/Packet_analyzer.

575. Packet Analyzer, from https://www.techopedia.com/definition/25323/packet-analyzer.

576. Chris Sanders, Practical Packet Analysis Using Wireshark To Solve Real-World Network Problems, from http://repository.root-me.org/R%C3%A9seau/EN%20-%20Practical%20packet%20analysis%20-%20Wireshark.pdf.

577. Wireshark Display Filters, from https://packetlife.net/media/library/13/Wireshark_Display_Filters.pdf.

578. Bobby Rogers, TCP/IP Packet Analysis Course, from https://www.vtc.com/products/TCP-IP-Packet-Analysis-Tutorials.htm.

579. (2020), Packet Sniffing, from https://thedatalist.com/pages/packet-sniffing/.

580. Detect/Analyze Scanning Traffic Using Wireshark, from https://www.koenig-solutions.com/documents/PenTestExtra-06-2013.pdf.

581. Alisha Cecil, A Summary of Network Traffic Monitoring and Analysis Techniques, from https://www.cse.wustl.edu/~jain/cse567-06/ftp/net_monitoring.pdf.

582. Karen Kent Frederick, (2001), Network Intrusion Detection Signatures, from https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=d6b5a639-dba9-442a-b6ad-460d495cff4a&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments.

583. Network Traffic Analysis, from https://www.techopedia.com/definition/29976/network-traffic-analysis.

584. Randy Weaver, Dawn Weaver, Dean Farwood, (2013), Guide to Network Defense and Countermeasures, from https://books.google.co.in/books?id=qbwuj_Umh9YC&pg=PA83&lpg=PA83&dq=Normal+traffic+signatures&source=bl&ots=WfHdWGSJS0&sig=5MKhVDfvmYh9N0Q6hbVf1-IFhD0&hl=en&sa=X&ved=0ahUKEwi1wtXk57XKAhWUj44KHQoXCv4Q6AEIbzAQ#v=onepage&q=Normal%20traffic%20signatures&f=false.

585. Packet Capture, from https://www.techopedia.com/definition/25333/packet-capture.

586. (2009), Capturing network communication packets with Wireshark Utility, from https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=1421bc97-5808-43d8-8485-6fa2ceba5586&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments.

587. How To Set Up a Capture, from https://wiki.wireshark.org/CaptureSetup.

588. Working with captured packets, from https://www.wireshark.org/docs/wsug_html_chunked/ChWorkDefineFilterSection.html.

589. Capturing Live Network Data, from https://www.wireshark.org/docs/wsug_html_chunked/ChCapCaptureFilterSection

590. Chris Hoffman, (2017), How to Use Wireshark to Capture, Filter and Inspect Packets, from http://www.howtogeek.com/104278/how-to-use-wireshark-to-capture-filter-and-inspect-packets/.

Network Defense Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

N|DE™

Network Defense Essentials

EC-Council

https://t.me/learningnets

EC-COUNCIL OFFICIAL CURRICULA