EC-Council

Building A Culture Of Security

C|ND

Certified Network Defender

Certified Network Defender v3

MODULE 04

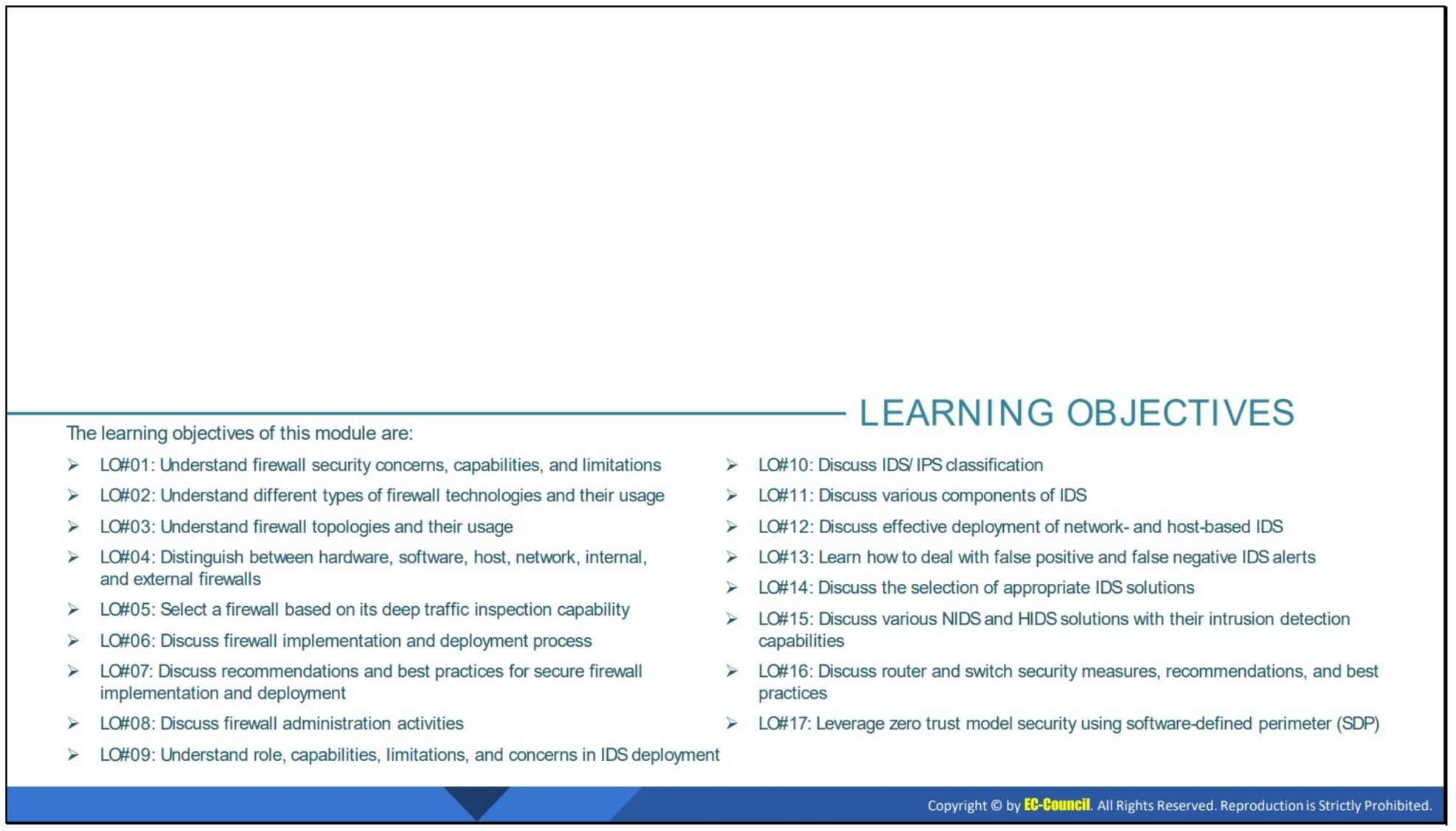
NETWORK PERIMETER SECURITY

EC-Council Official Curricula

https://t.me/learningnets

This page is intentionally left blank.

https://t.me/learningnets



Learning Objectives

Perimeter security is considered as the first line of defense against intruders and security breaches. An effective perimeter security should be an integral part of an organization's security. This module discusses security configuration of network perimeter devices such as firewalls, intrusion detection and intrusion protection systems (IDSs/IPSs), routers, switches, etc. for effective perimeter protection.

The objectives of this module are:

- Understand firewall security concerns, capabilities, and limitations
- Understand different types of firewall technologies and their usage
- Understand firewall topologies and their usage
- Distinguish between hardware, software, host, network, internal, and external firewalls
- Select a firewall based on its deep traffic inspection capability
- Discuss firewall implementation and deployment process
- Discuss recommendations and best practices for secure firewall implementation and deployment
- Discuss firewall administration activities
- Understand role, capabilities, limitations, and concerns in IDS deployment
- Discuss IDS/IPS classification
- Discuss various components of IDS

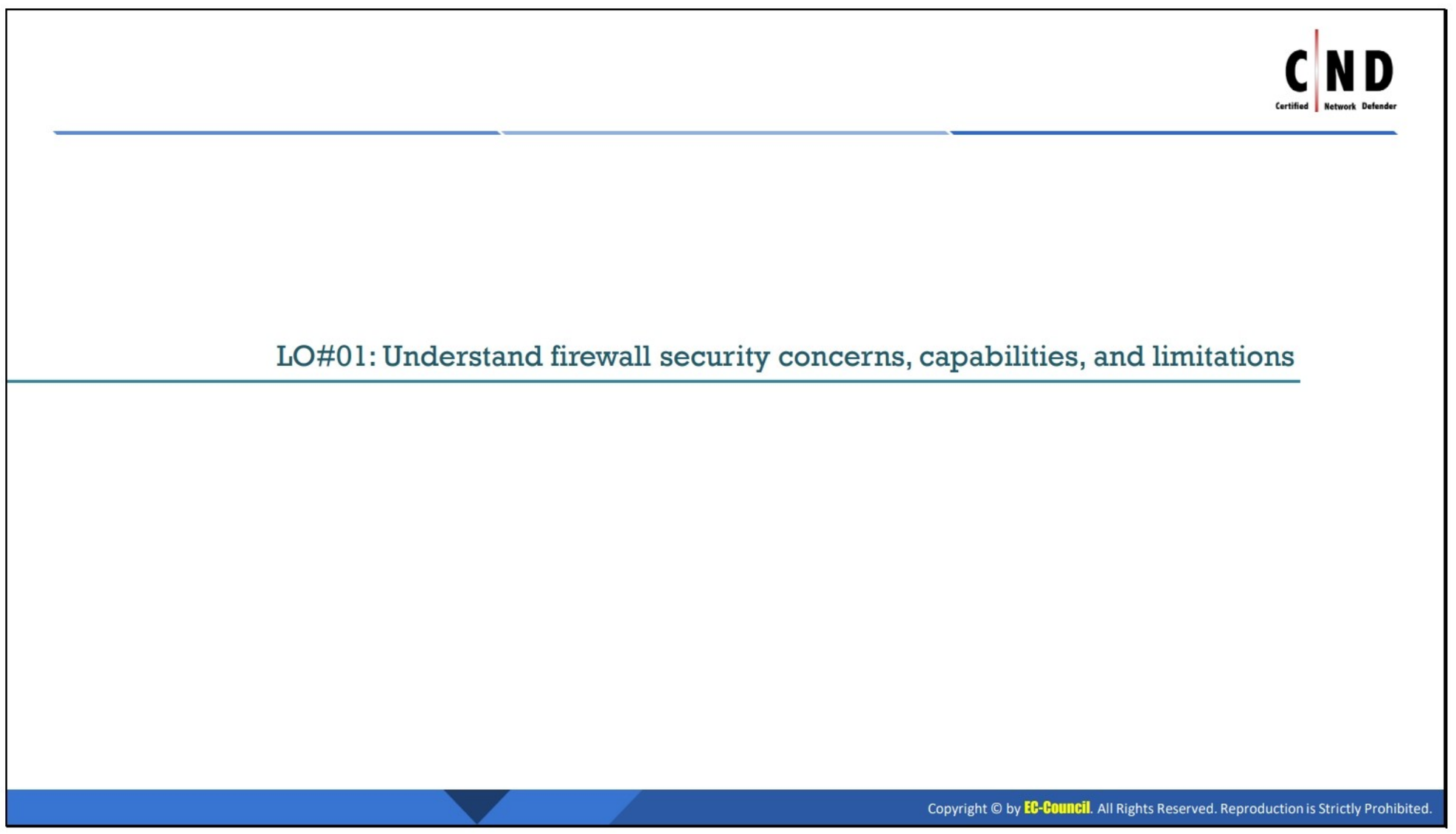
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- Discuss effective deployment of network- and host-based IDS
- Learn how to deal with false positive and false negative IDS alerts
- Discuss the selection of appropriate IDS solutions
- Discuss various NIDS and HIDS solutions with their intrusion detection capabilities
- Discuss router and switch security measures, recommendations, and best practices
- Leverage zero trust model security using software-defined perimeter (SDP)

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

https://t.me/learningnets

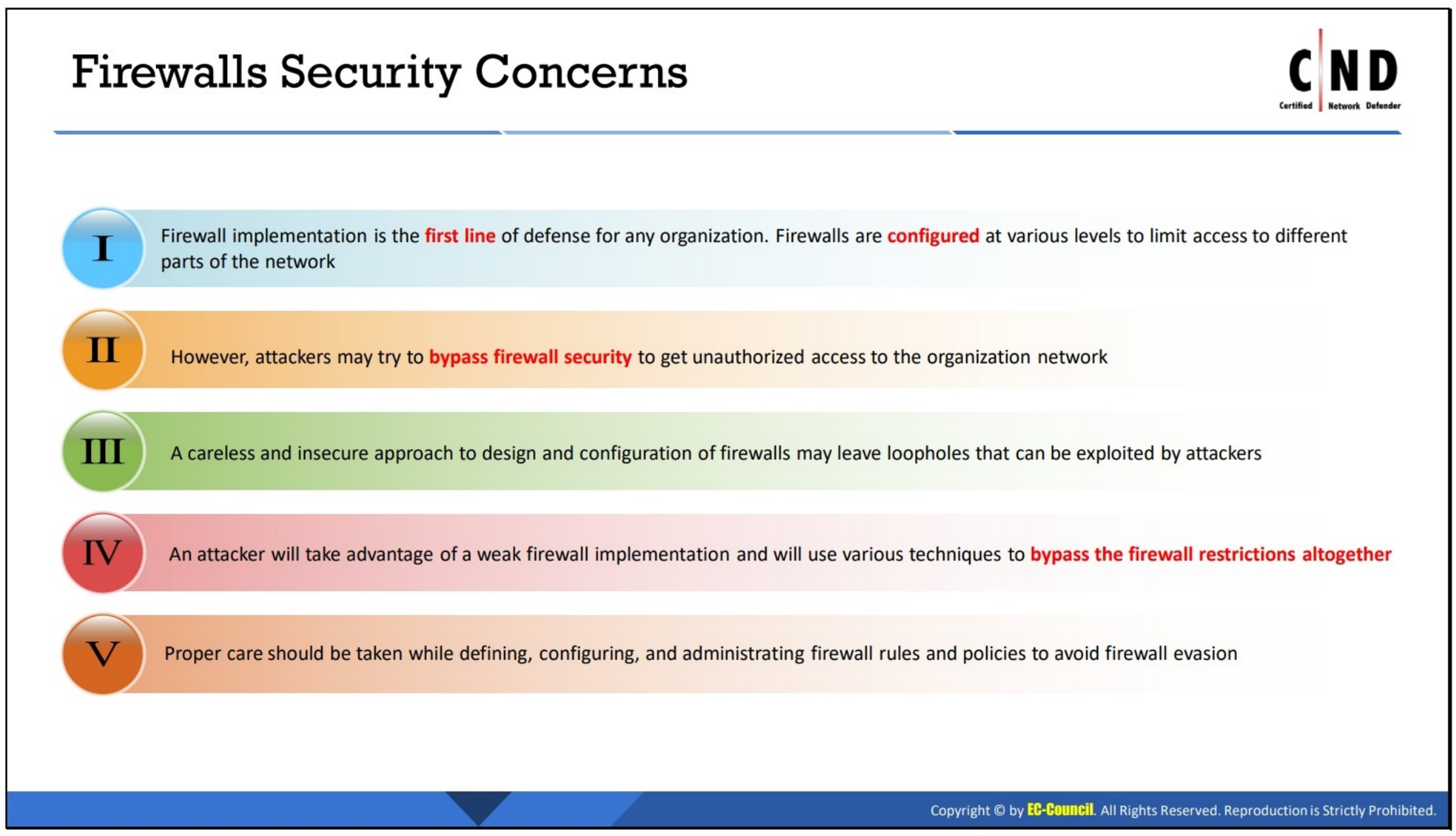


LO#01: Understand Firewall Security Concerns, Capabilities, and Limitations

The firewall plays a vital role in securing the link between private networks and the Internet in today's connected world. It acts as a gateway or as a filtering device that employs the network security policy and protects the network against external attacks. However, improper configuration and implementation of a firewall will diminish its ability to defend an organization's network. The objective of this section is to explain how a firewall can be configured securely to build effective perimeter protection for an organization.

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

https://t.me/learningnets

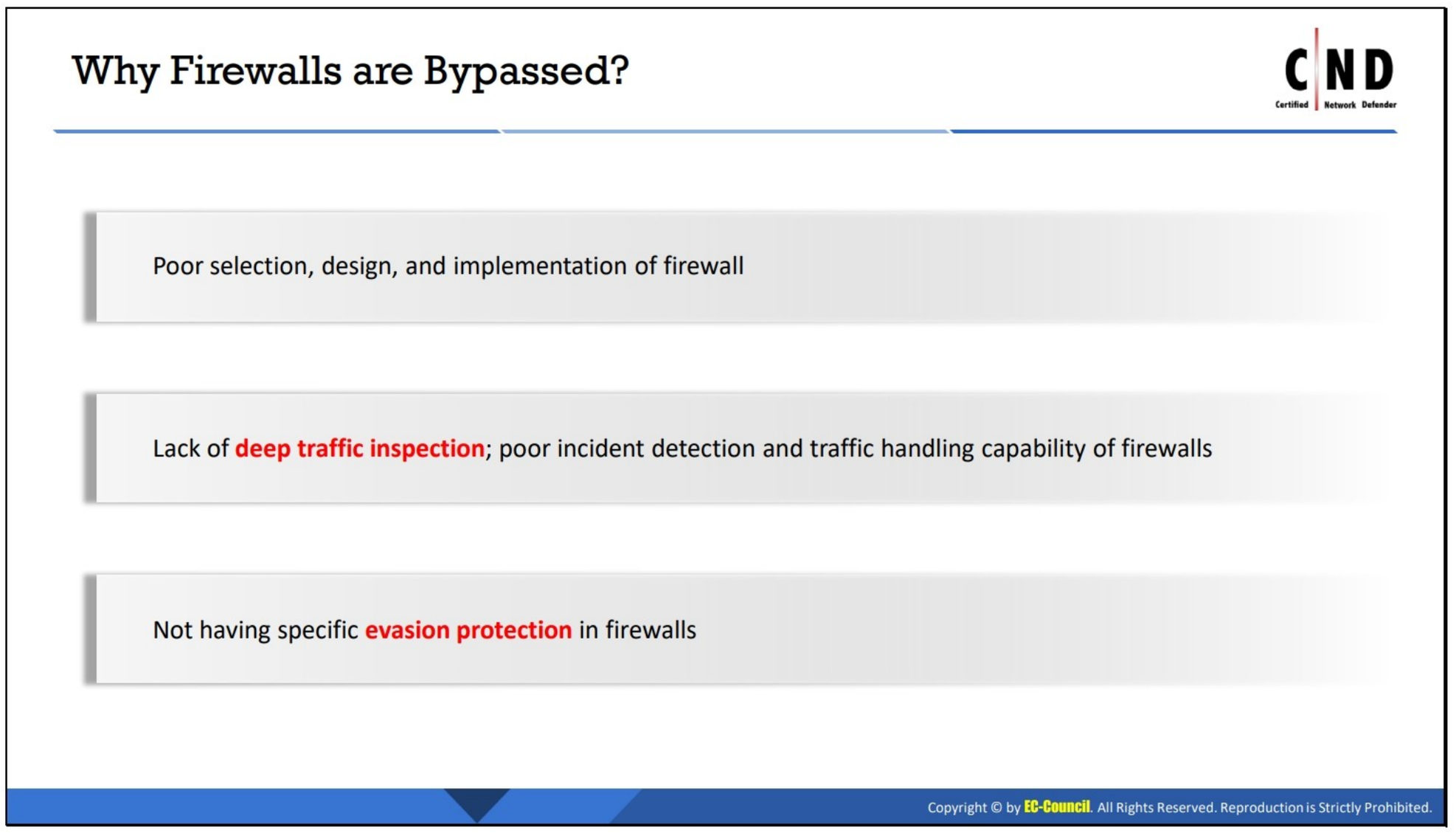


Firewalls Security Concerns

A firewall is the first line of defense for an organization's network. However, improper configuration and implementation of a firewall will diminish its ability to defend an organization's network.

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

https://t.me/learningnets

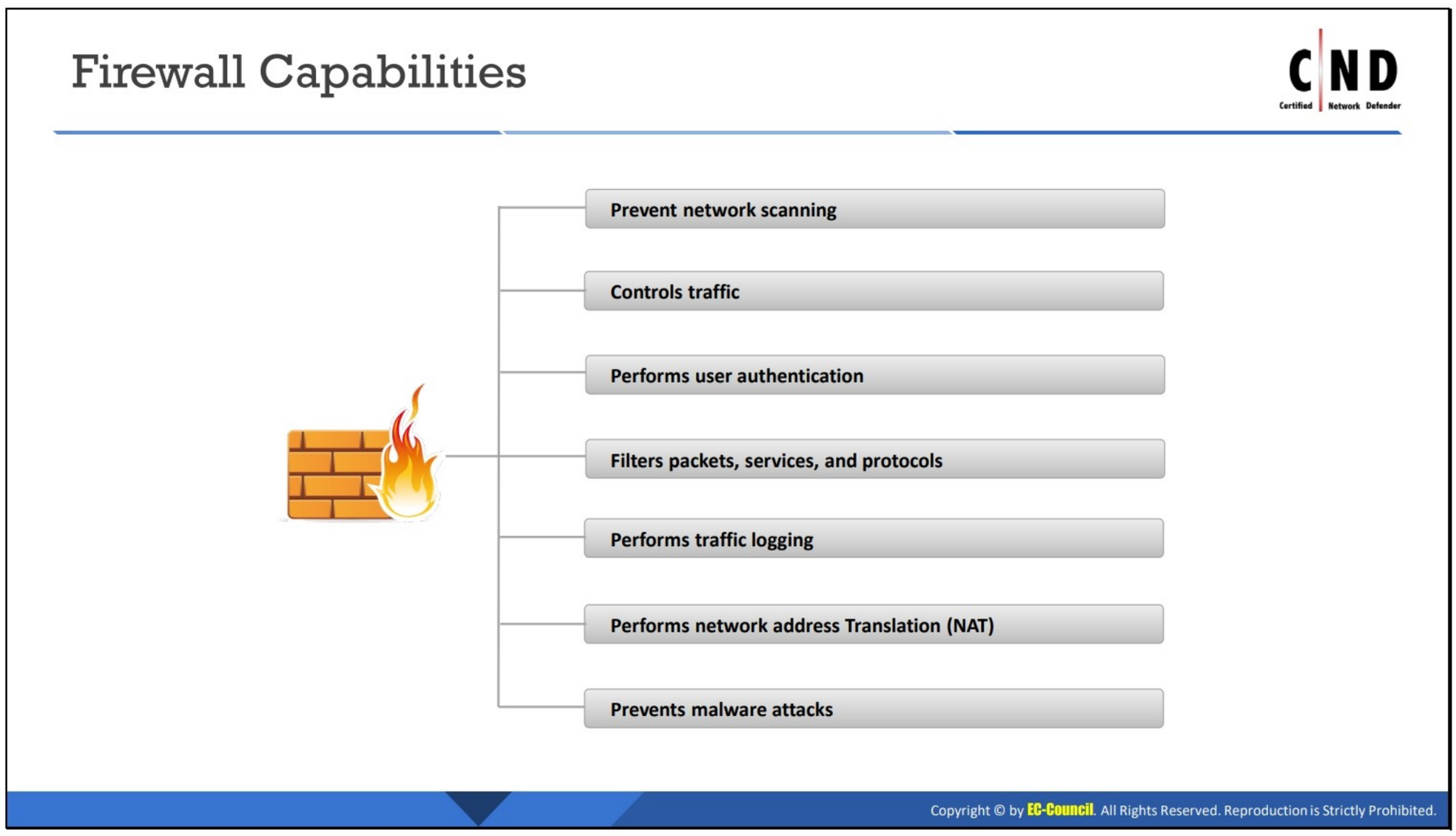


Why Firewalls are Bypassed?

Flawed designs and/or improper implementation of firewalls enable attackers to bypass them. An attacker can take advantage of improper traffic handling, inspection, or detection techniques of a firewall to bypass it. Most firewall vendors are unable to offer effective protection against evasions.

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

https://t.me/learningnets



Firewall Capabilities

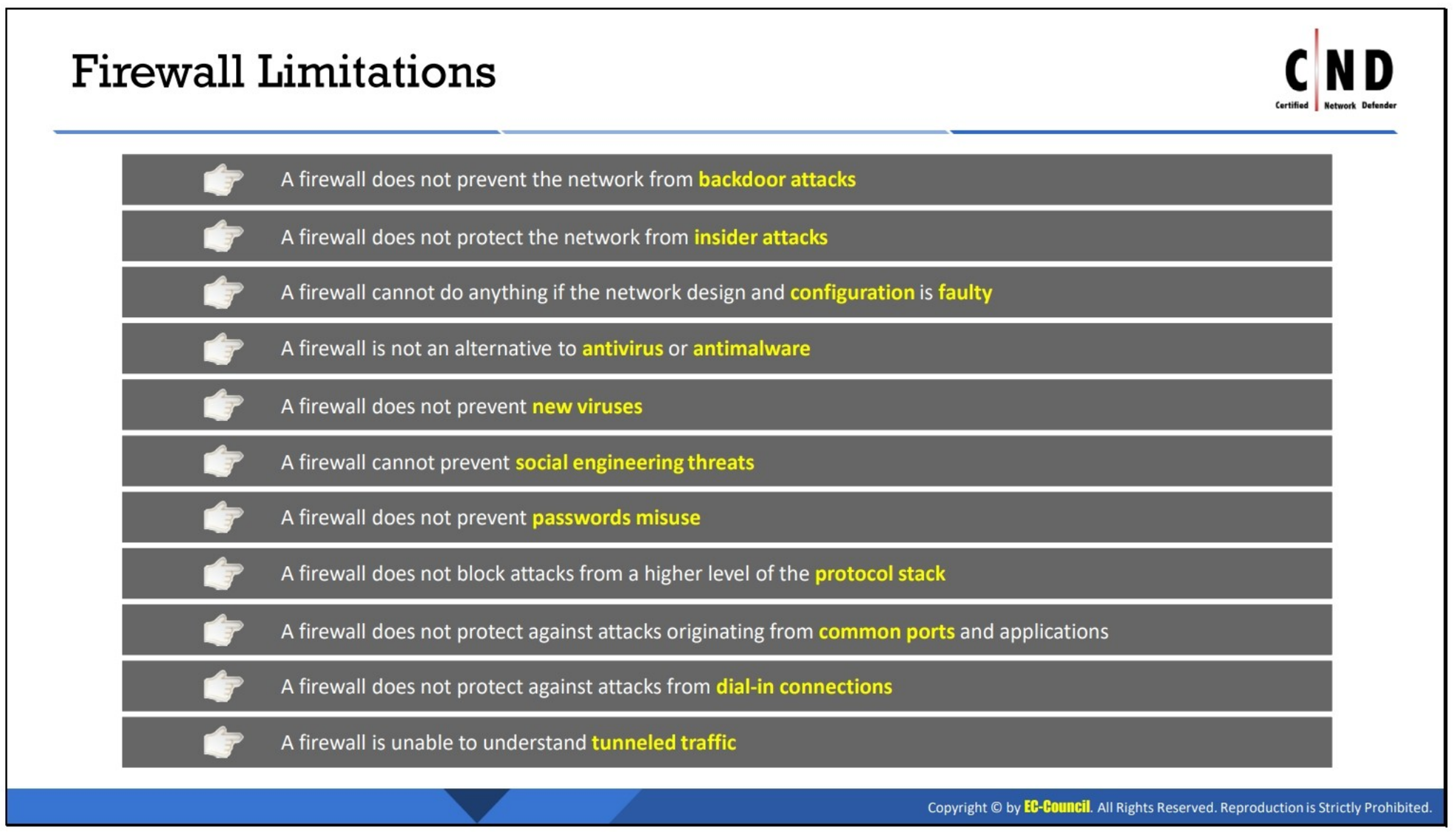
Be aware of a firewall's capabilities before planning for implementation. By knowing the capabilities of different types of firewalls, you will be able to decide what type to implement or whether a different security control or solution better suits your needs.

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.
- 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.

Certified Network Defender 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:

- Firewalls can restrict users from accessing valuable services such as FTP, Telnet, NIS, etc. and sometimes restrict Internet access as well.
- They cannot protect a network from internal (backdoor) attacks. For example, a disgruntled employee who cooperates with an external attacker.
- 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.
- 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.
- 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.
- Firewalls are unable to fully protect the network from all types of zero-day viruses that may try to bypass them.

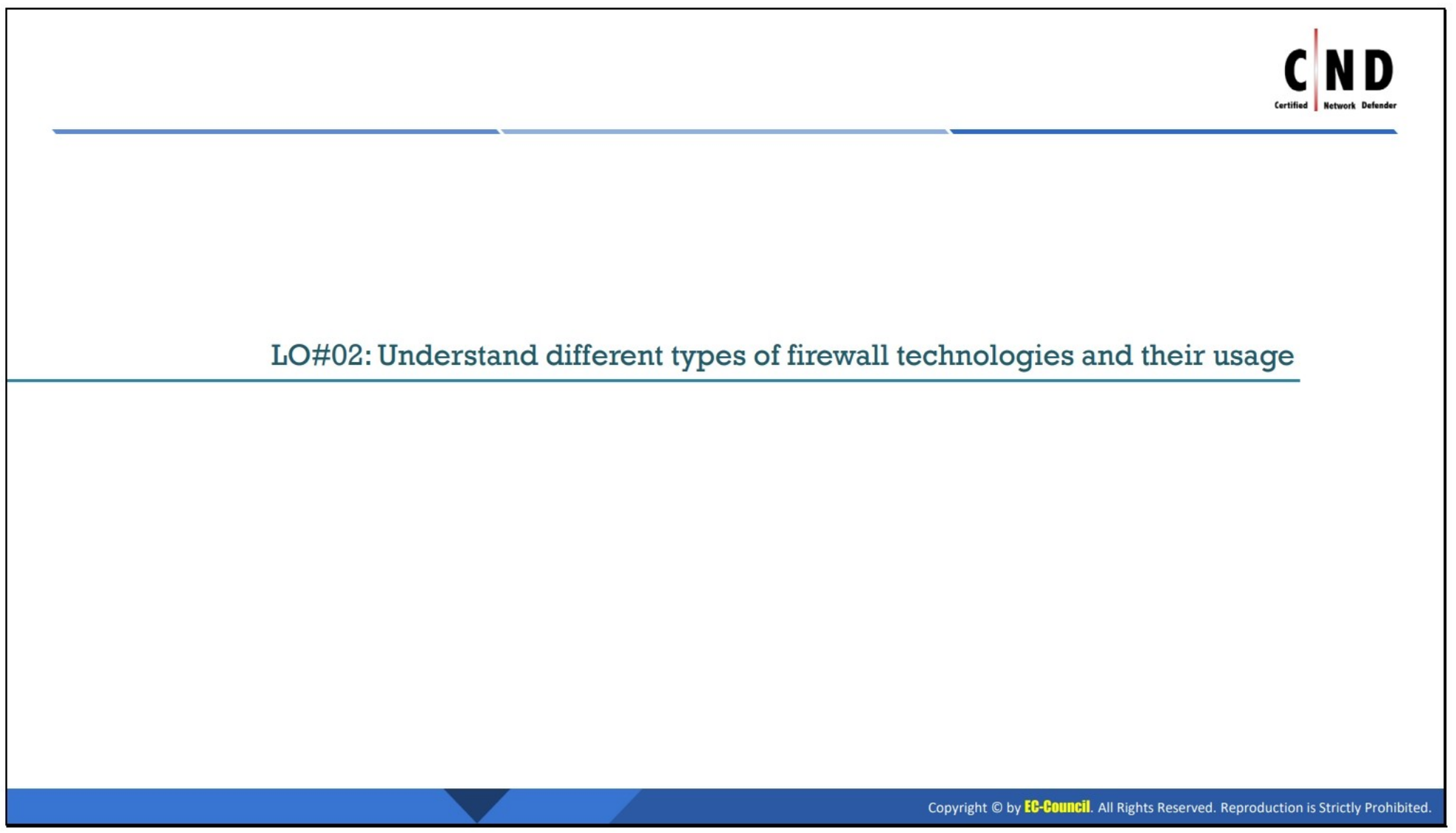
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- 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.

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

https://t.me/learningnets

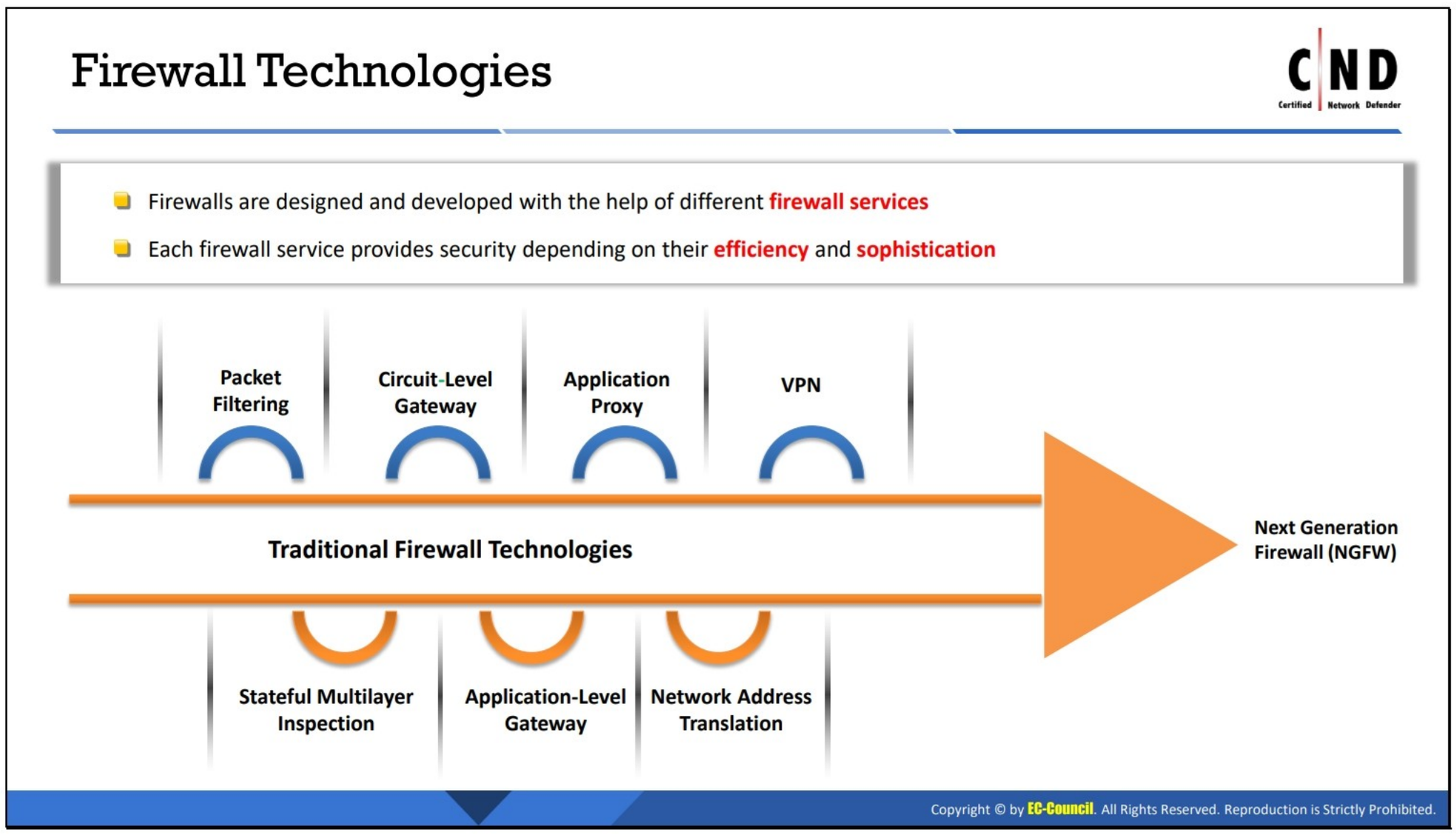


LO#02: Different Types of Firewall Technologies and Their Usage

This section describes 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).

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

https://t.me/learningnets



Firewall Technologies

Several firewall technologies are available for organizations to incorporate in their firewall security setup. Sometimes, firewall technologies are combined with other technologies to build new ones. For example, NAT is a routing technology, which when combined with a firewall, is considered a firewall technology instead.

The various firewall technologies used are:

- Packet filtering
- Stateful multilayer inspection
- Circuit-level gateway
- Application-level gateway
- Application proxy
- Network address translation NAT
- Virtual private network VPN
- Next-generation firewall (NGFW)
- Cloud firewall

The table below describes technologies working at different open systems interconnection (OSI) layers:

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

https://t.me/learningnets

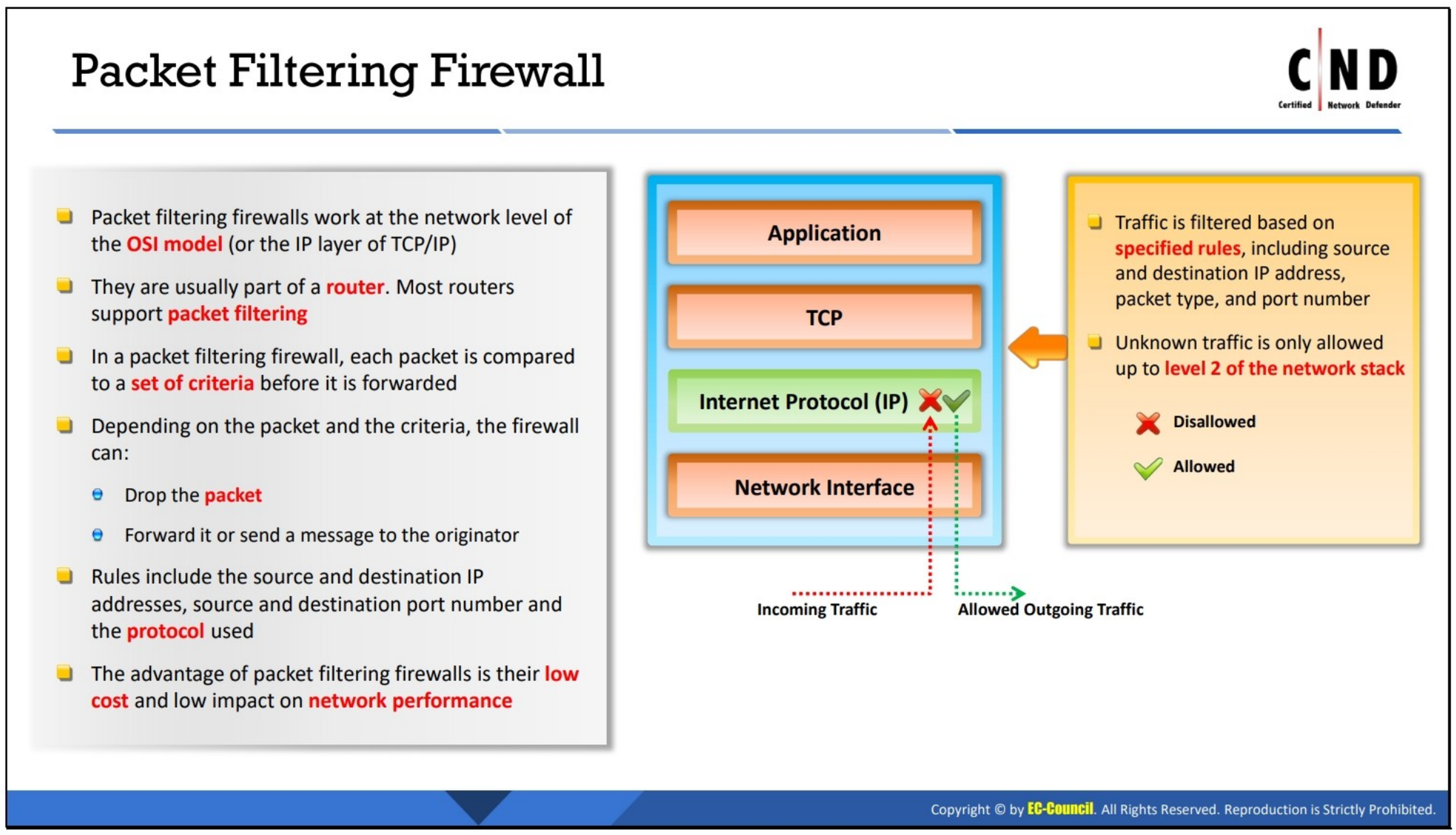
OSI Layer	Firewall Technology
Application	Virtual private Network (VPN) Application Proxies
Presentation	VPN
Session	VPN Circuit-level gateway
Transport	VPN Packet Filtering
Network	VPN Network Address Translation (NAT) Packet Filtering Stateful Multilayer Inspection

Table 4.1: Firewall Technologies at Different OSI Layers

The security level of these technologies varies according to their efficiency level. A comparison of these technologies can be made by allowing them to pass through the OSI layer between hosts. The data passes through the intermediate layers from the higher layer to the 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 thereafter to its destination.

Certified Network Defender 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 layer and are usually part of the router. 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.

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

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

https://t.me/learningnets

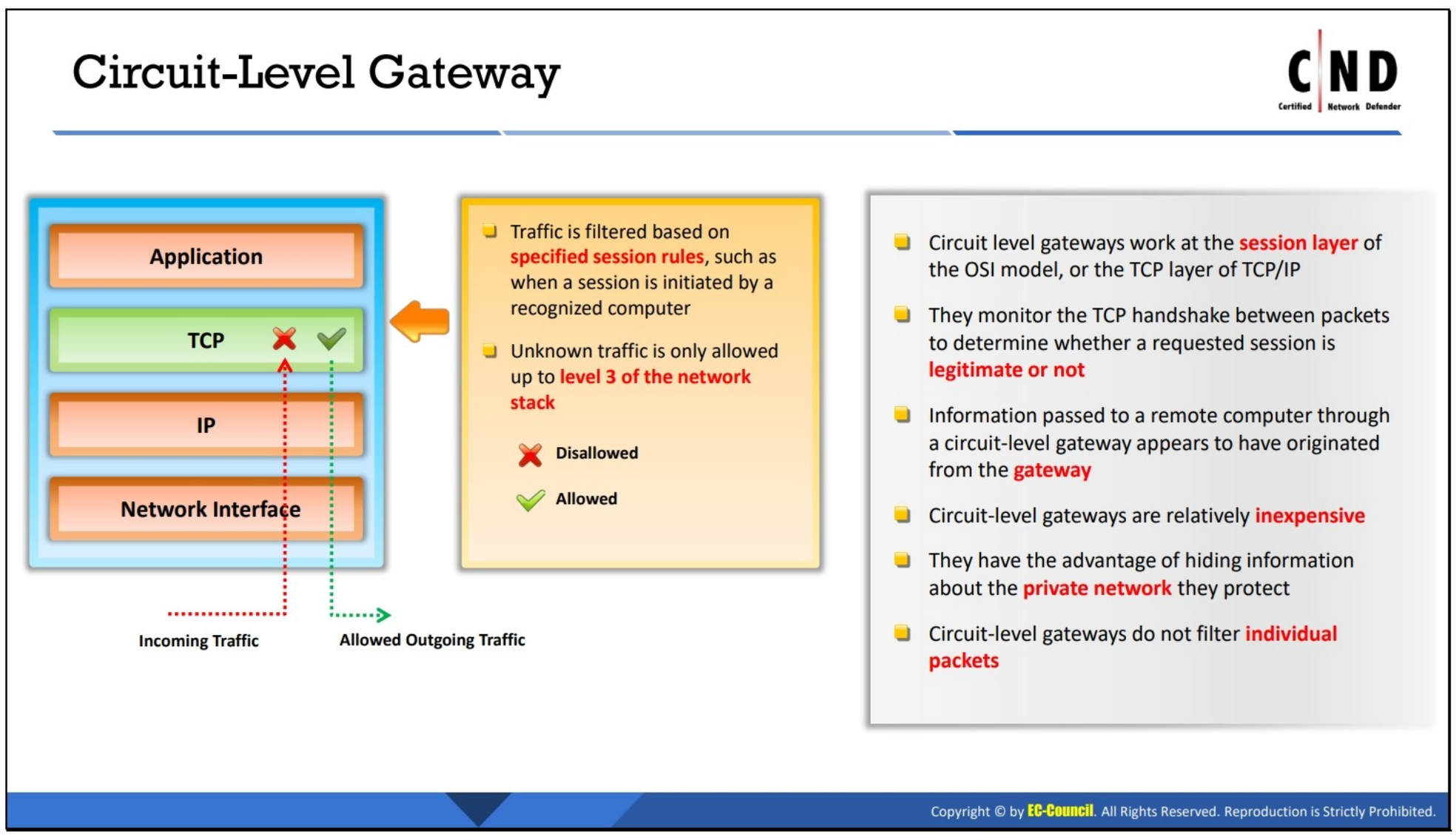
as packet spoofing, where the attacker crafts or replaces packet headers that are then unfiltered by the firewall.

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.
- 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.

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

https://t.me/learningnets



Circuit-Level 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.

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

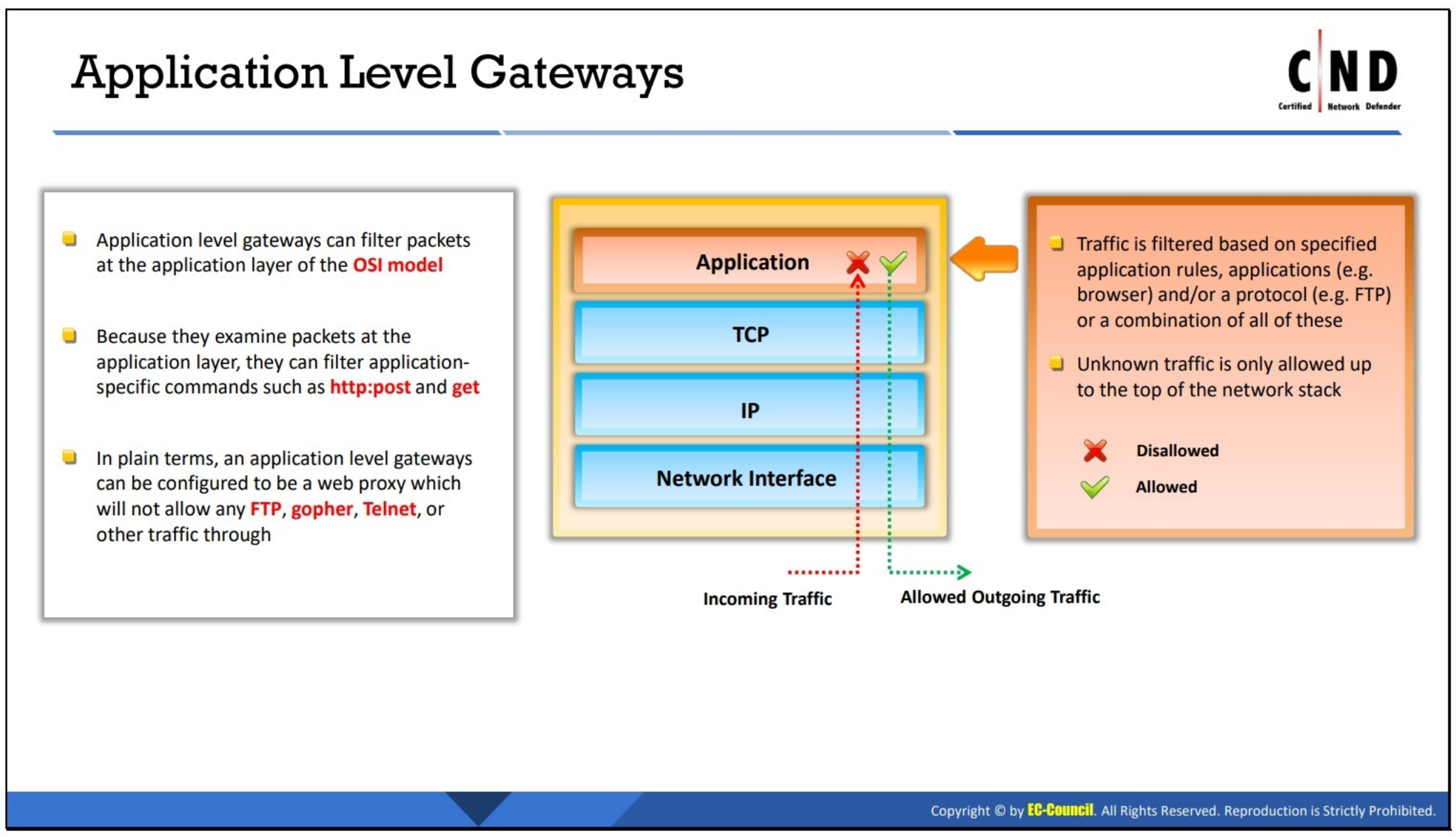
- Hides data of the private network
- Does not filter individual packets
- Does not require a separate proxy server for each application
- Easy to implement

Disadvantages

- Cannot scan active contents
- Can only handle TCP connections

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

https://t.me/learningnets



Application Level Gateways

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. 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.

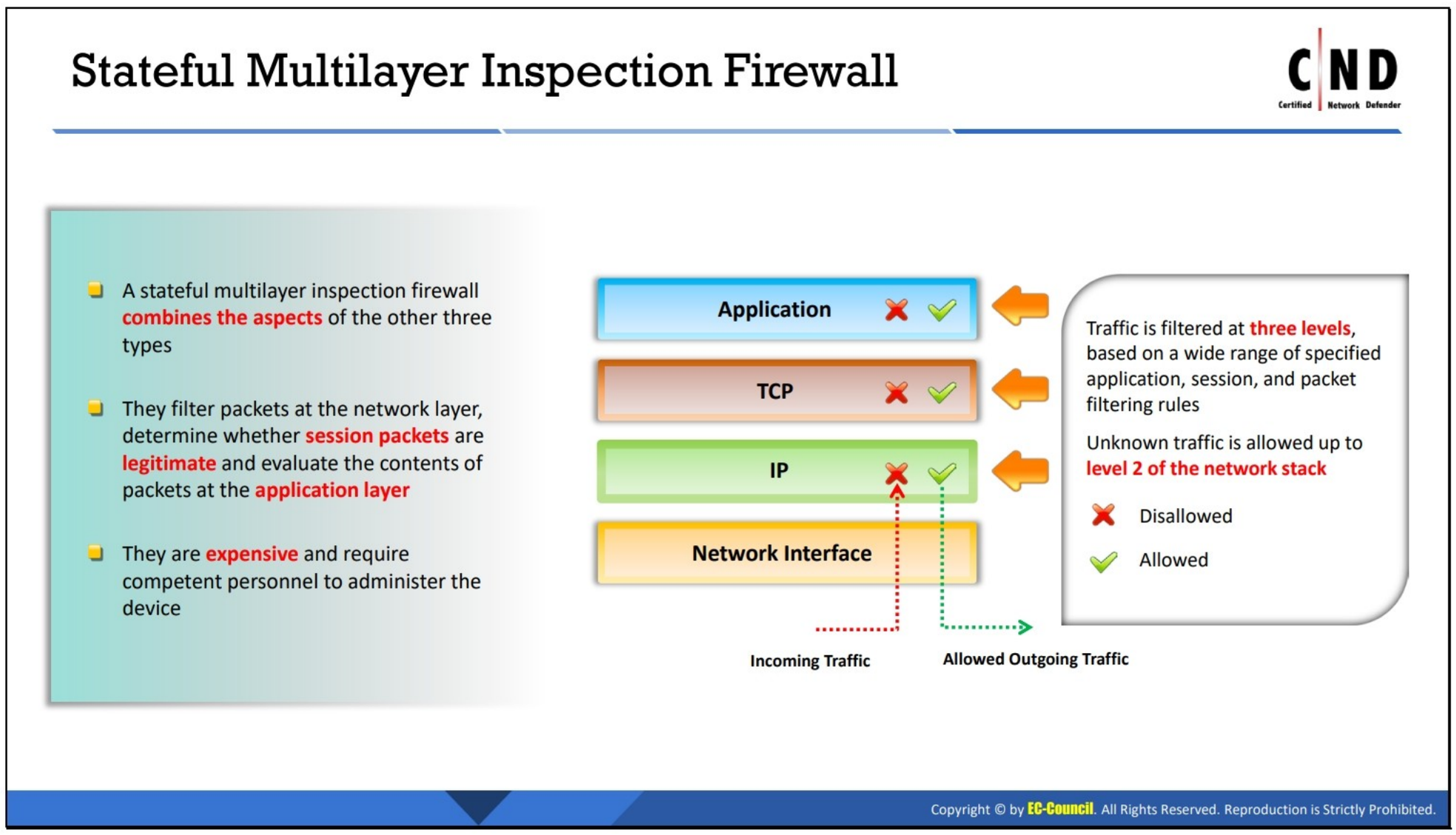
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

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.

Certified Network Defender 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.

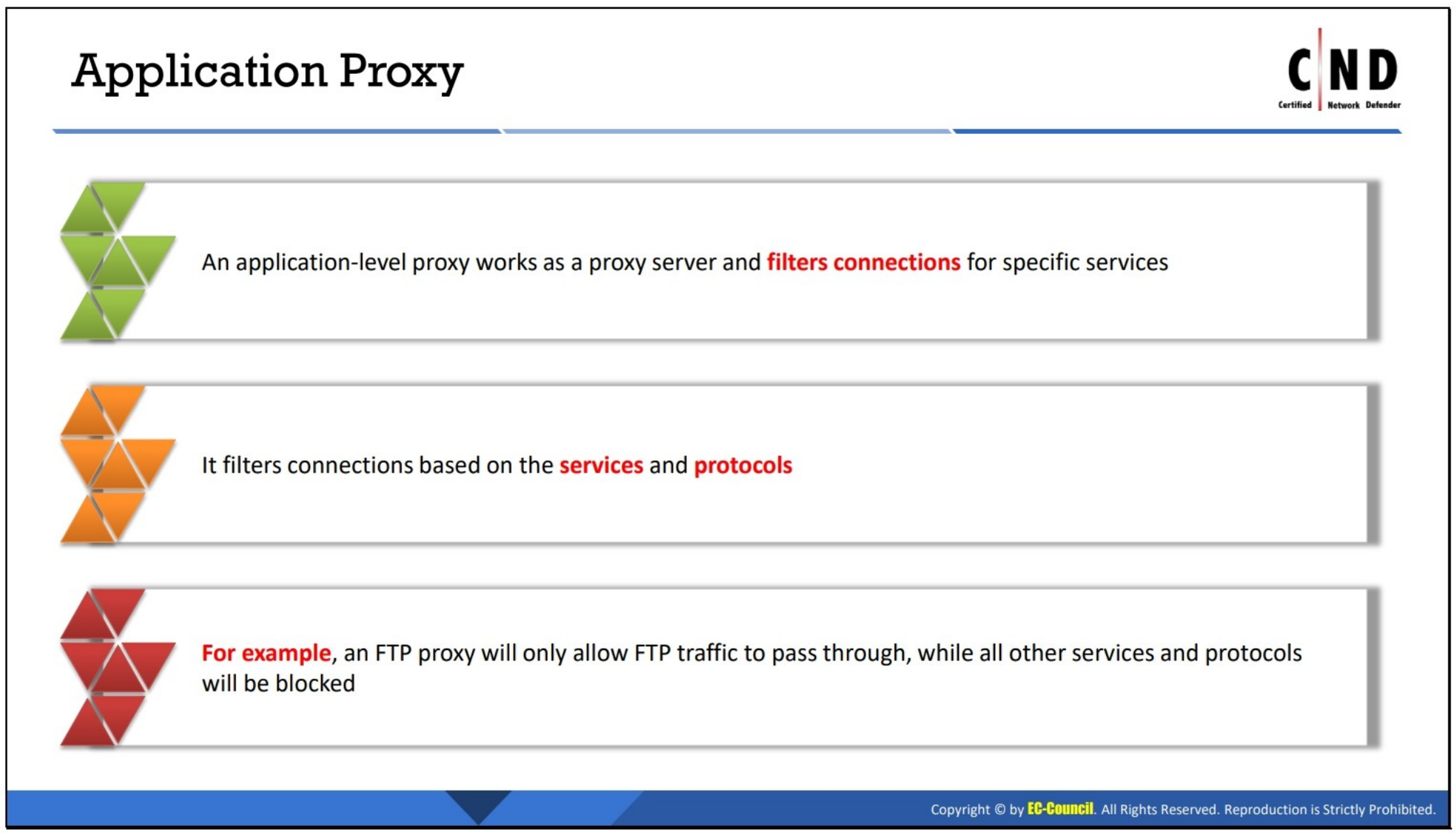
These firewalls eliminate the lack of transparency in application-level gateways as they allow a direct connection between the client and the host. These firewalls use algorithms to examine, filter, and process the application-layer data instead of using proxies. Stateful multilayer inspection firewalls 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.

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

https://t.me/learningnets



Application Proxy

An application proxy works as a proxy server. 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.

Advantages

- Proxy services can be good at logging because they can understand application protocols and allow logging in an effective way.

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

https://t.me/learningnets

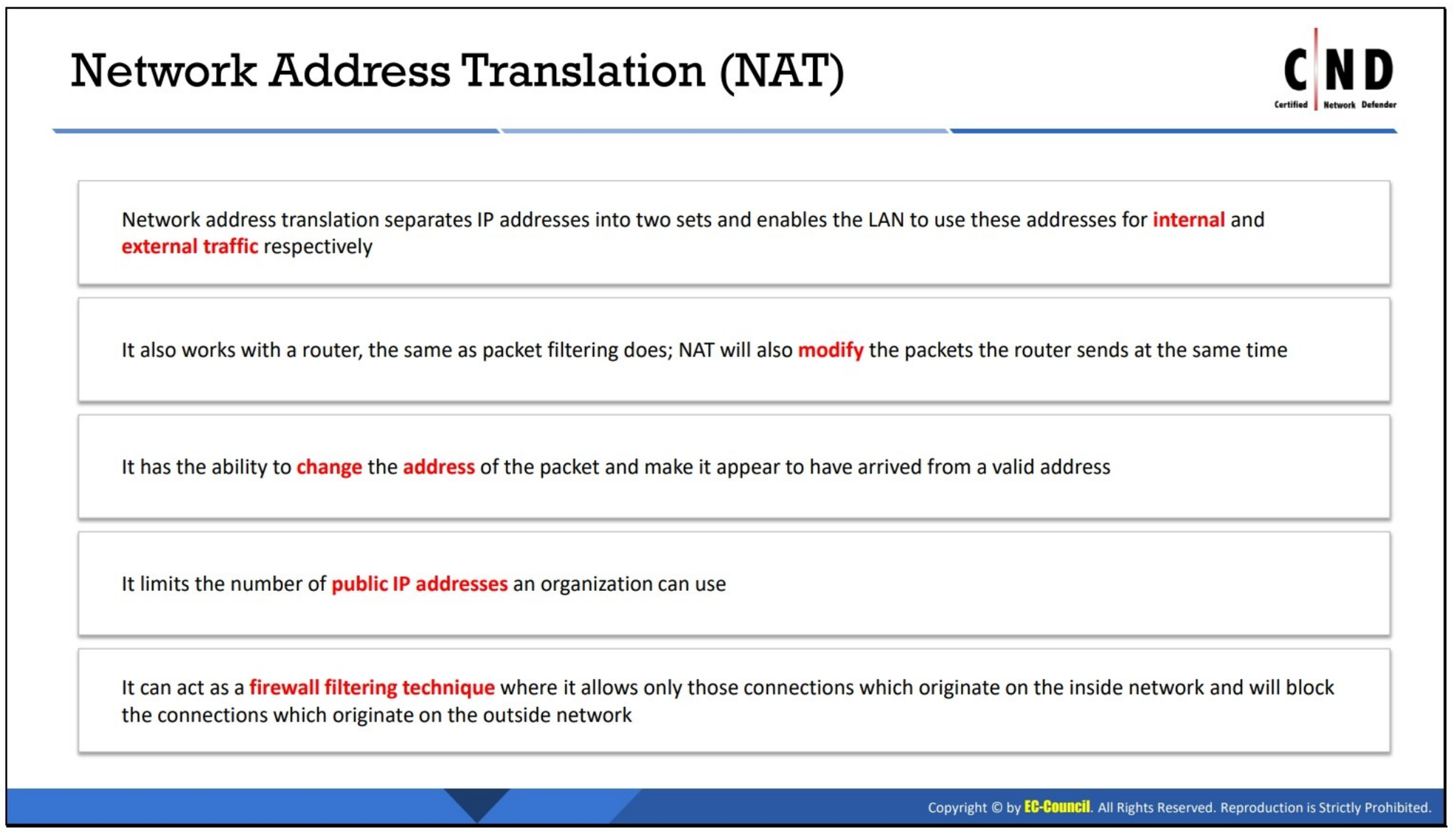
- Proxy services reduce the load on network links as they are capable of caching copies of frequently requested data and allow it to be directly loaded from the system instead of the network.
- Proxy systems perform user-level authentication, as they are involved in the connection.
- Proxy systems automatically 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.

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

https://t.me/learningnets



Network Address Translation (NAT)

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. 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.
- 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.

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

https://t.me/learningnets

Advantages

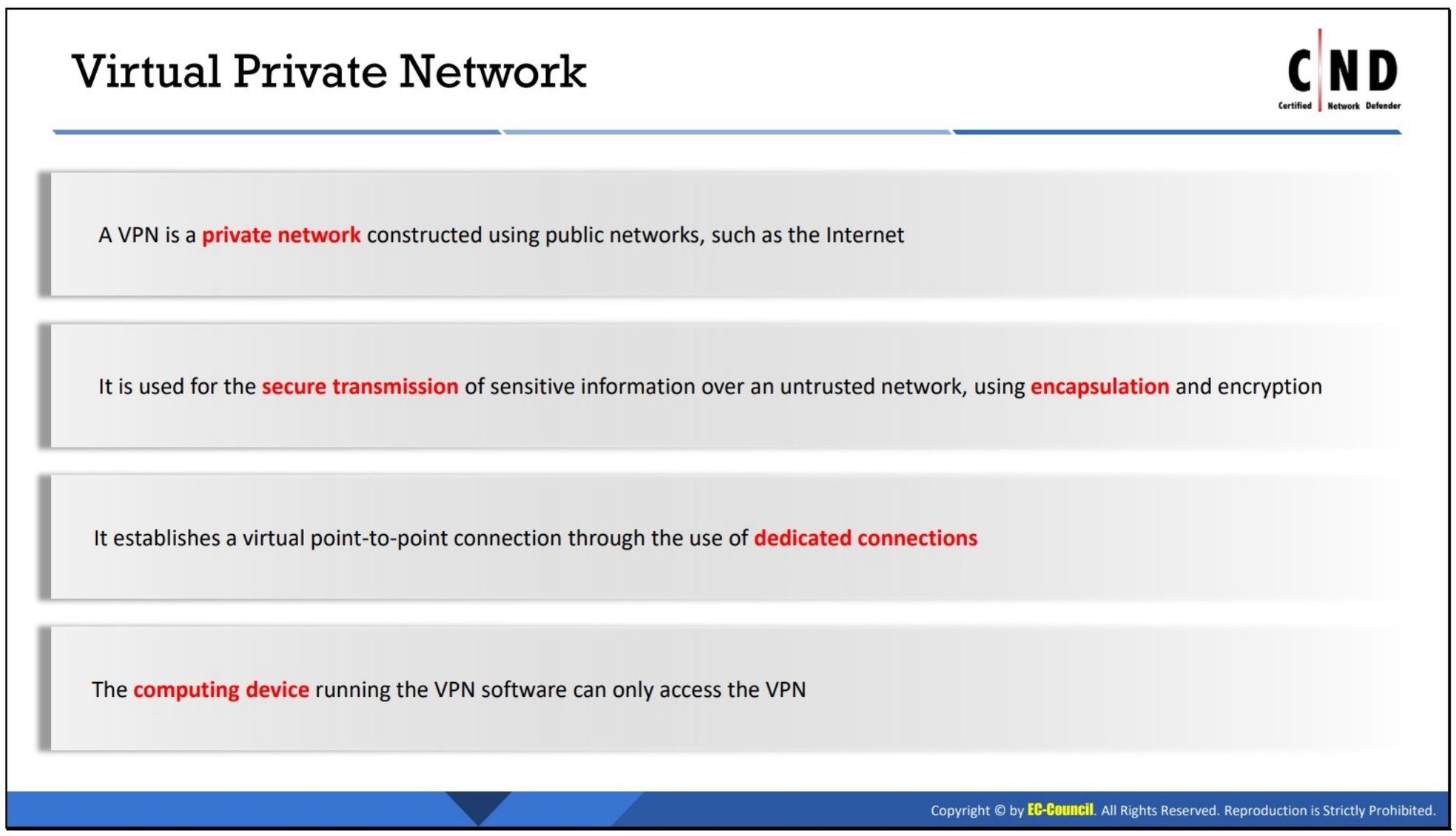
- NAT help enforce the firewall's control over outbound connections.
- It restricts incoming traffic and allows only packets that are part of a current interaction initiated from the inside.
- It helps hide the internal network's configuration and thereby reduces vulnerability of the network or system from outside attacks.

Disadvantages

- The NAT system has to guess how long it should keep a particular translation, which is impossible to guess correctly every time.
- NAT interferes with encryption and authentication systems that ensure security of the data.
- Dynamic allocation of ports may interfere with packet filtering.

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

https://t.me/learningnets



Virtual Private Network

A VPN is a network that provides secure access to the network through the Internet. Used for connecting wide area networks (WAN). It 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

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.

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

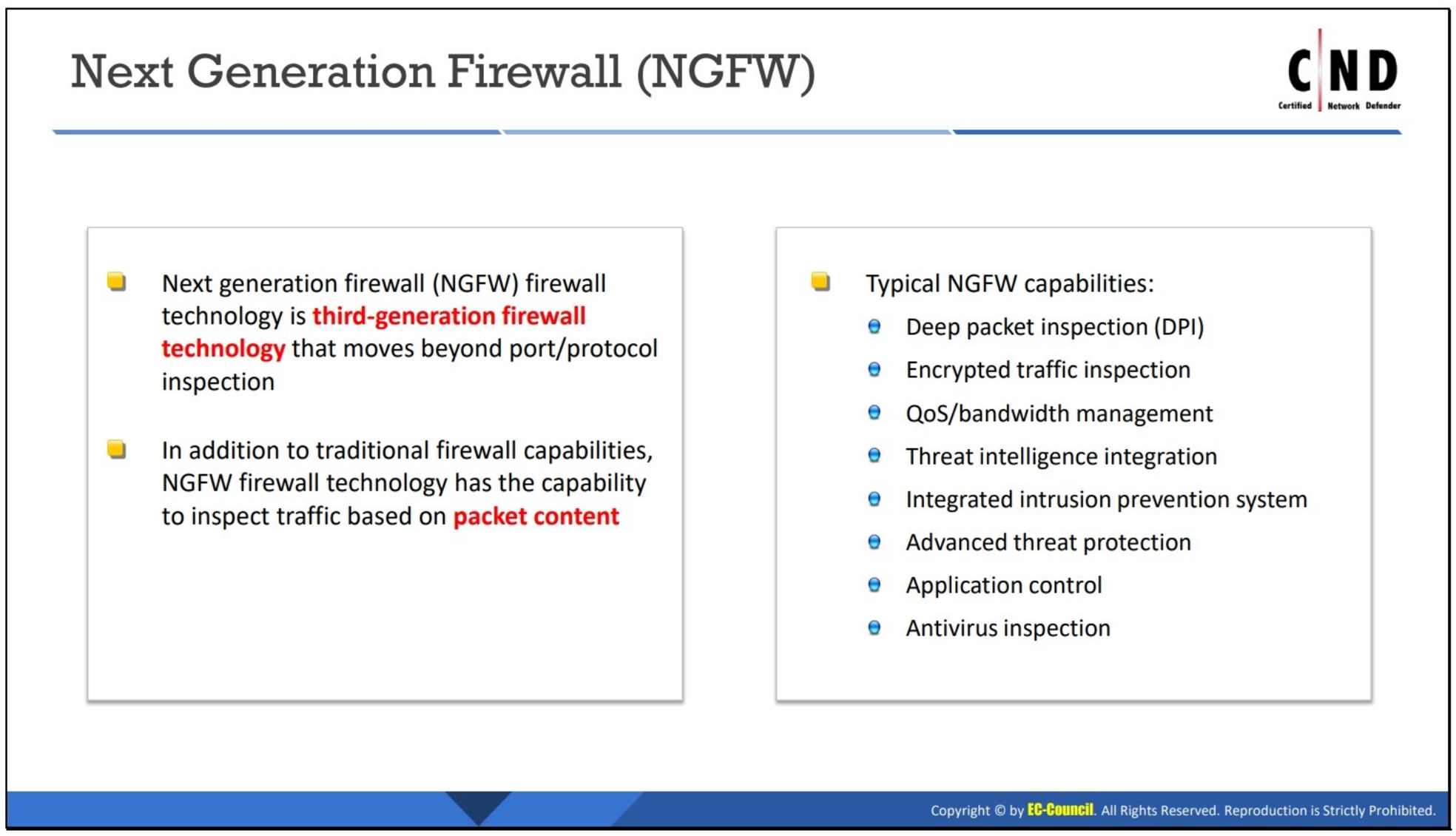
https://t.me/learningnets

Disadvantages

- As a VPN runs on a public network, the user remains vulnerable to an attack on the destination network.

Certified Network Defender 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. As with traditional firewalls, it also 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

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.

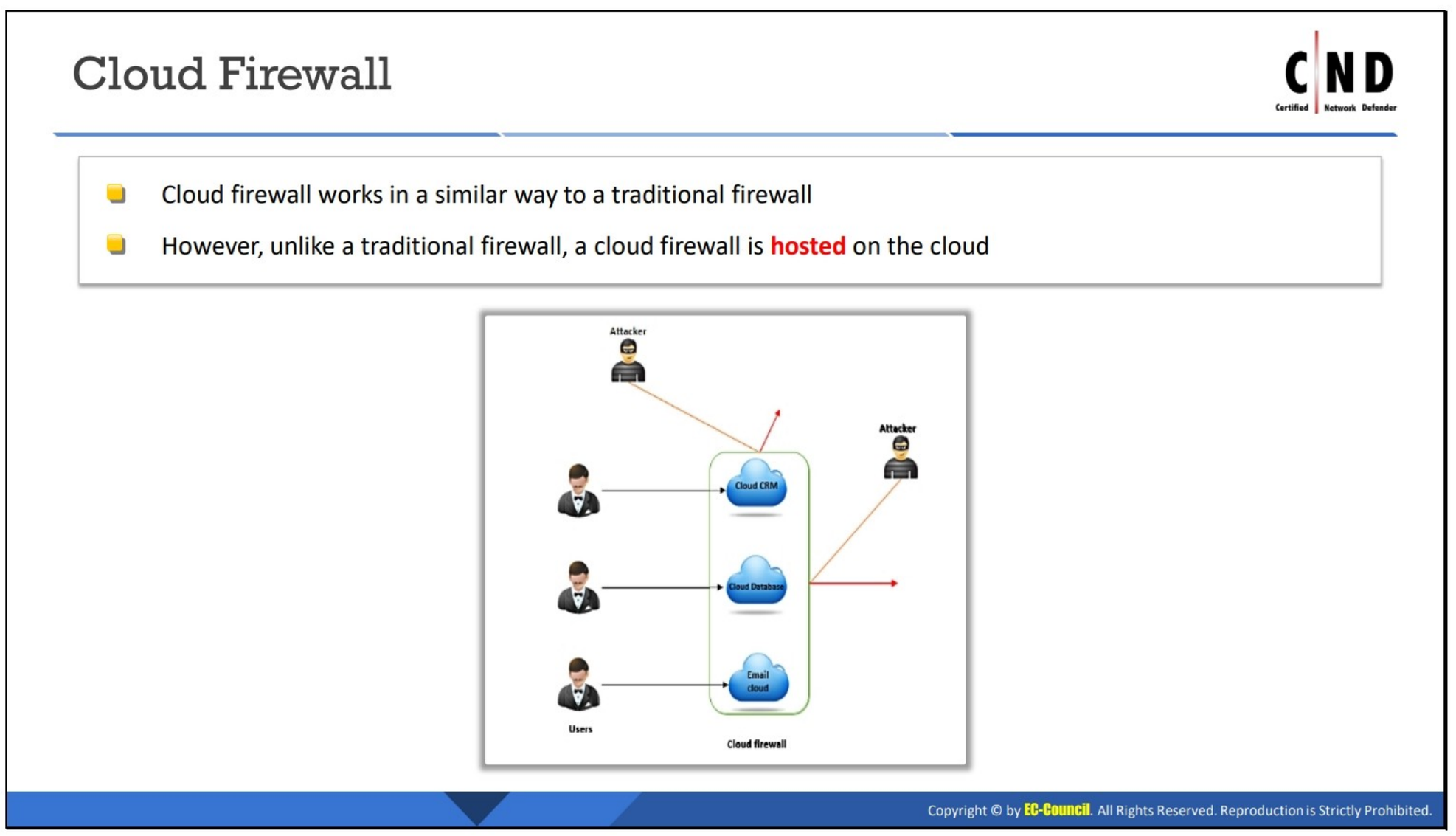
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

- 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.

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

https://t.me/learningnets



Cloud Firewall

A cloud firewall works in a similar way to a traditional firewall. It filters out potentially harmful network traffic. However, unlike a traditional firewall, a cloud firewall is hosted on the cloud. Cloud Firewalls are also known as FaaS (firewall as a service). Firewalls that are installed in the cloud are designed to provide a physical barrier between the cloud platform, its infrastructure, and its applications. It is used to protect on-site infrastructure.

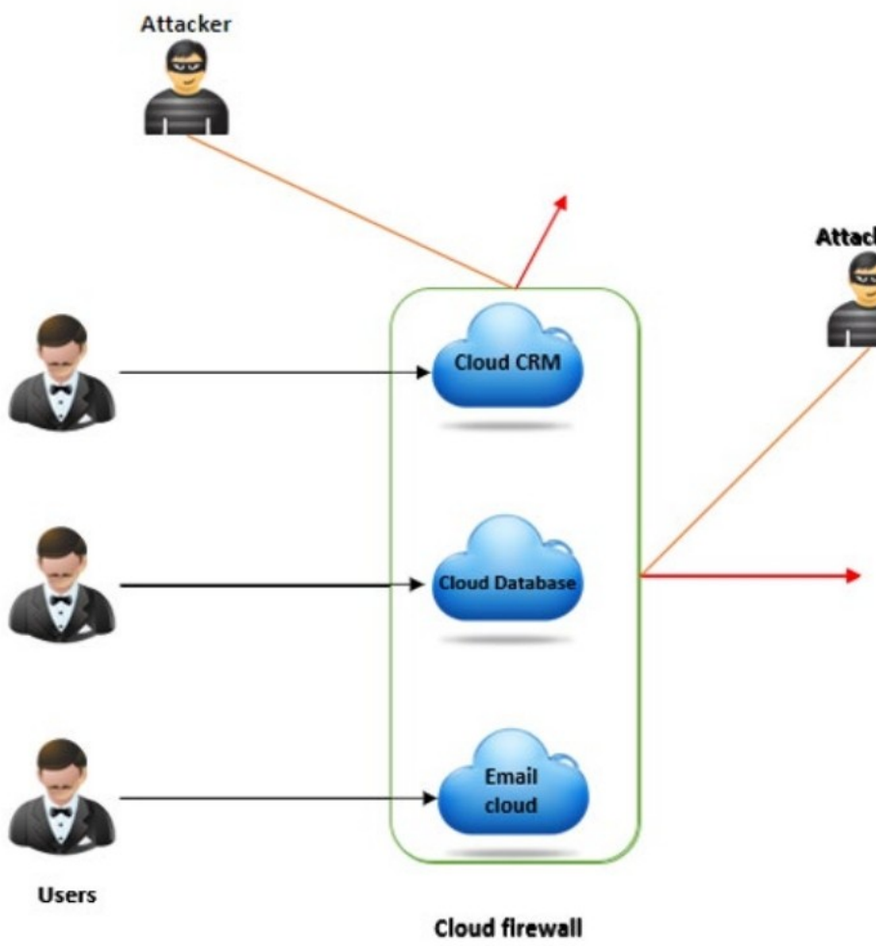


Figure 4.1: Cloud Firewall

Types of Cloud Firewalls

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

https://t.me/learningnets

- **SaaS Firewalls**

  These firewalls are designed to protect an organization's network and its users, just like a regular on-premises firewall or software firewall, but they're deployed from the cloud.

- **Next Generation Firewalls**

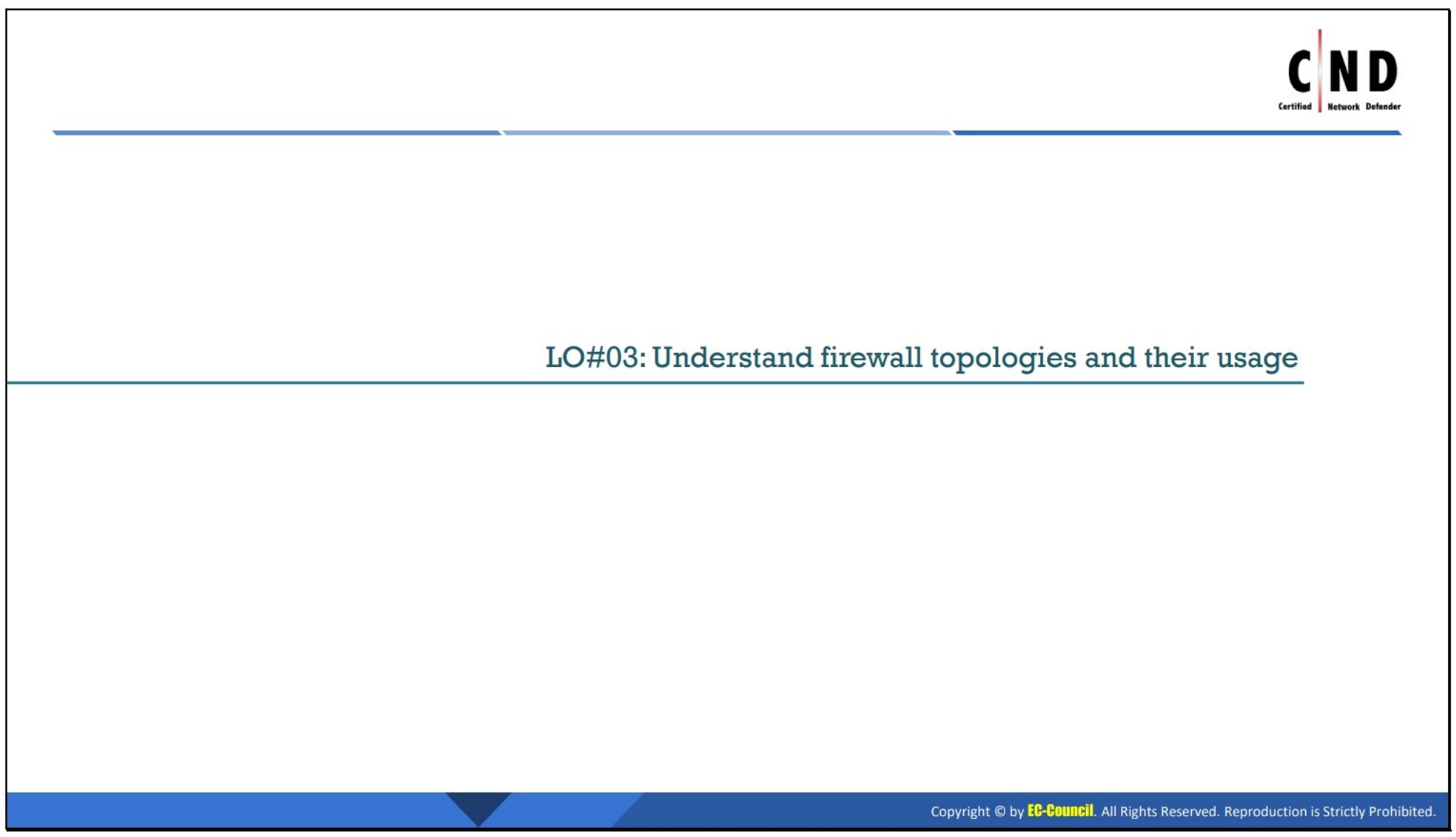
  These firewalls are designed to be deployed in a virtual data center environment. They provide protection for an organization's servers in a PaaS or IaaS framework. The firewall application resides on the virtual server and safeguards the flow of data between cloud-based applications.

Cloud Firewall Benefits

- **Scalability:** The ease of deployment allows organizations to scale up or down the scope of their security solutions without the difficulties associated with on-premises installation, maintenance, and upgrades.
- **Availability:** Cloud firewall providers consider the inherent expense associated with high availability by providing infrastructure support.
- **Extensibility:** Cloud firewalls are easily accessible and can be deployed anywhere an organization can offer a secure network communication channel.
- **Migration Security:** A cloud firewall can filter traffic from a wide range of sources, including the internet, virtual networks, tenants, and even virtual data centers.
- **Secure Access Parity:** Cloud Firewalls offer a level of security comparable to that of on-premises firewalls.
- **Identity Protection:** Cloud-based firewalls integrate with third-party access control vendors and provide users with granular visibility into filtering tools.
- **Performance Management:** Cloud Firewalls offer a range of features that enable users to manage performance, insight, utilization, settings, and logging.

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

https://t.me/learningnets



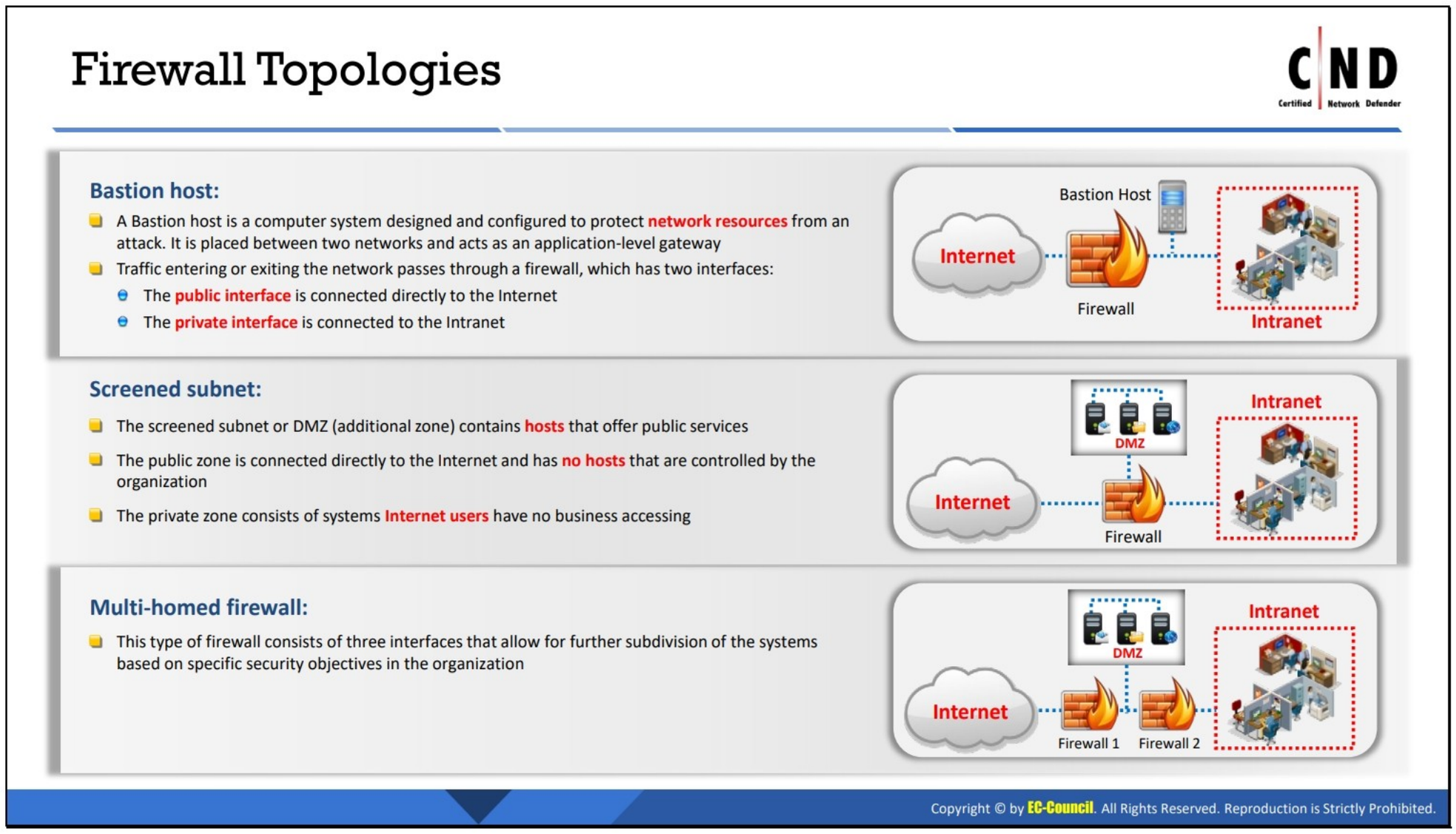
LO#03: Firewall Topologies and Their Usage

Choosing the appropriate firewall topology plays an important role in firewall configuration. This section describes various firewall topologies and parameters to be considered for appropriate selection of firewall topology.

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

https://t.me/learningnets

Technet24



Firewall Topologies

The three types of firewall architectures and their related use are explained below:

Bastion Host

A bastion host is a computer system designed and configured to protect network resources from attacks. It acts as a mediator between the inside and the outside network. The firewall resides between the Internet and the protected private network. It filters all incoming and outgoing traffic from the network. The bastion host provides a platform for an application-level or circuit-level gateway. It requires additional authentication for the user to access the proxy services. Install only the most essential services or applications on the bastion host. Simple networks that do not offer any Internet services use a bastion host topology. Suppose a system has two firewalls, then a bastion host is placed inside the two firewalls or on the public side of the demilitarized zone (DMZ). Examples of a bastion host include mail, DNS, and FTP servers.

Traffic entering or leaving the network passes through the firewall. It has two interfaces:

- The public interface is directly connected to the Internet.
- The private interface is connected to the Intranet.

Screened Subnet

It is also known as a “triple-homed firewall” and uses a single firewall with three network interfaces. The first interface connects the Internet, the second interface connects the DMZ, and the third interface connects the intranet. The screened subnet or DMZ (additional zone) contains hosts that offer public services. The public zone connects directly to the Internet and has no organization-controlled hosts. The main advantage with using the screened subnet is that it

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

https://t.me/learningnets

separates the DMZ and Internet from the intranet. If the firewall is compromised, access to the intranet will not be possible.

The screened subnet architecture consists of two screening routers: one is placed between the perimeter net and the internal network and the other is placed between the perimeter net and the external network. This architecture is more secure because to enter the internal network, the hacker/attacker has to pass both the routers.

Multi-homed Firewall

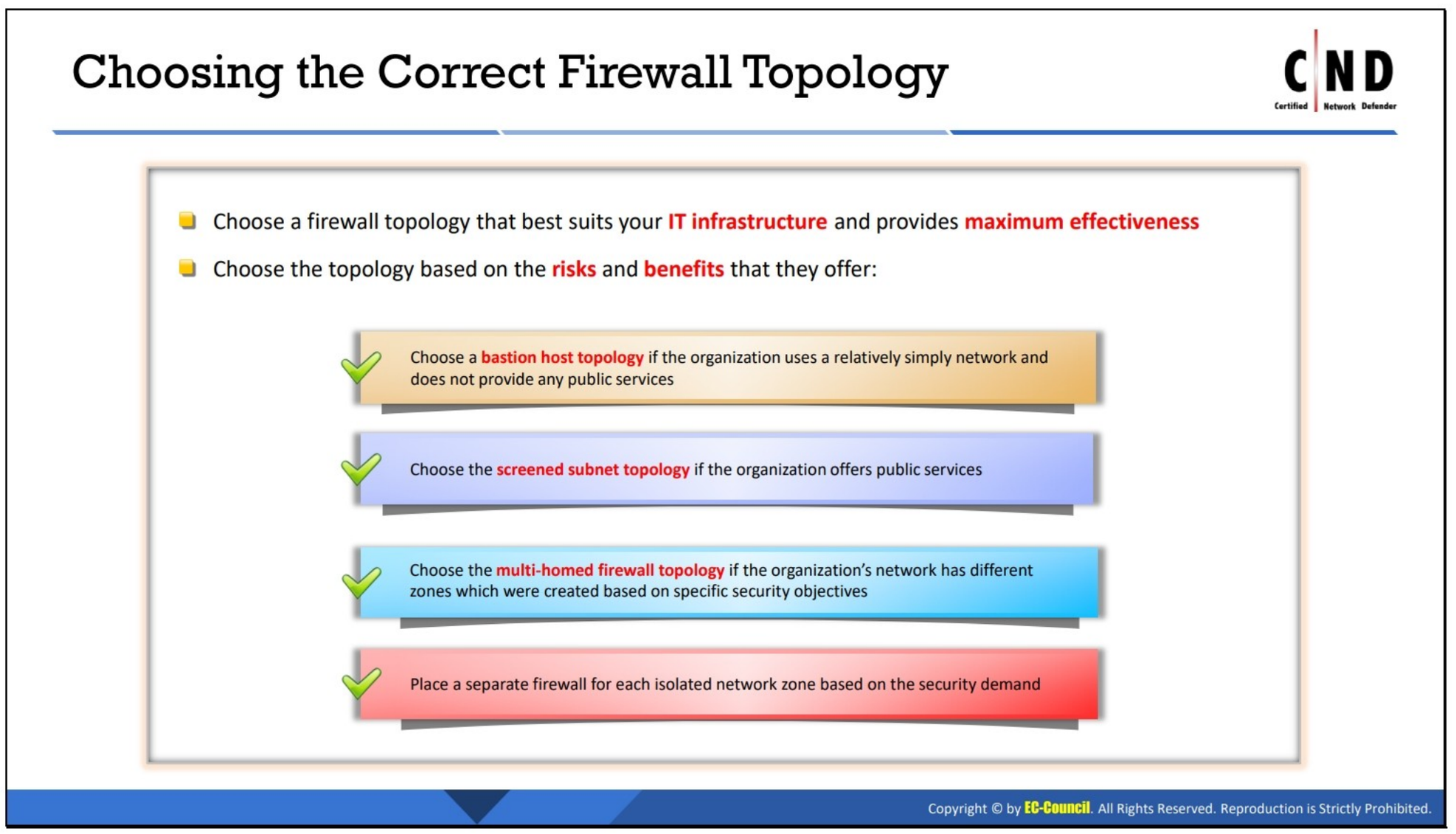
A multi-homed firewall refers to two or more networks. In this case, more than three interfaces are present, allowing for further subdivision of the systems based on the specific security objectives of the organization. Each interface connects with separate network segments logically and physically. A multi-homed firewall allows different security policy to be assigned to each interface. Internet users access only presentation servers, which have access to middleware servers that can access only data servers. A multi-homed firewall increases the efficiency and reliability of an IP network. It duplicates all the functions of a firewall in a single box and replaces the IP router that does not forward packets at the IP layer. The multi-homed host processes the packets through the application layer, which provides complete control over handling of the packets.

A dual-homed host is similar to the multi-homed host. It has two network interface cards (NICs): one connected to an external network (untrusted) and the other to an internal network (trusted). The key point here is that it does not allow traffic coming from the untrusted network to directly route on the trusted network—the firewall acts as an intermediary.

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

https://t.me/learningnets

Technet24



Choosing the Correct Firewall Topology

Before deploying a firewall on the network as part of their perimeter protection strategy, organizations should understand which firewall topology best suits their business needs.

Bastion Host

This type of topology is ideal for simple networks. It monitors the traffic between the private network and the outside world (Internet). This topology offers a single layer of protection, and the network may be compromised if an attacker penetrates through this layer. Restricting every user's Internet access through this firewall keeps the network relatively safe from threats. Organizations use this topology to protect a corporate network intended for surfing the Internet and other internal communications. It does not provide sufficient protection for web hosting or protecting an email server.

Screened Subnet

This type of topology is ideal for an organization hosting a website or an email server. A screened subnet topology provides secure services to Internet users. In this type of topology, the servers that provide public services are setup in a separate zone called a demilitarized zone (DMZ), keeping the trusted network secure from the Internet. Users inside the trusted network will have access to the Internet through the DMZ. Therefore, even if a malicious user compromises the firewall, they cannot access the network inside the DMZ.

Multi-homed Firewall

A multi-homed firewall offers the advantage of protecting your trusted network even if the DMZ is compromised. This topology operates on two or more network interfaces. Usually, one interface connects to the untrusted network (Internet), the other interface connects to the

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

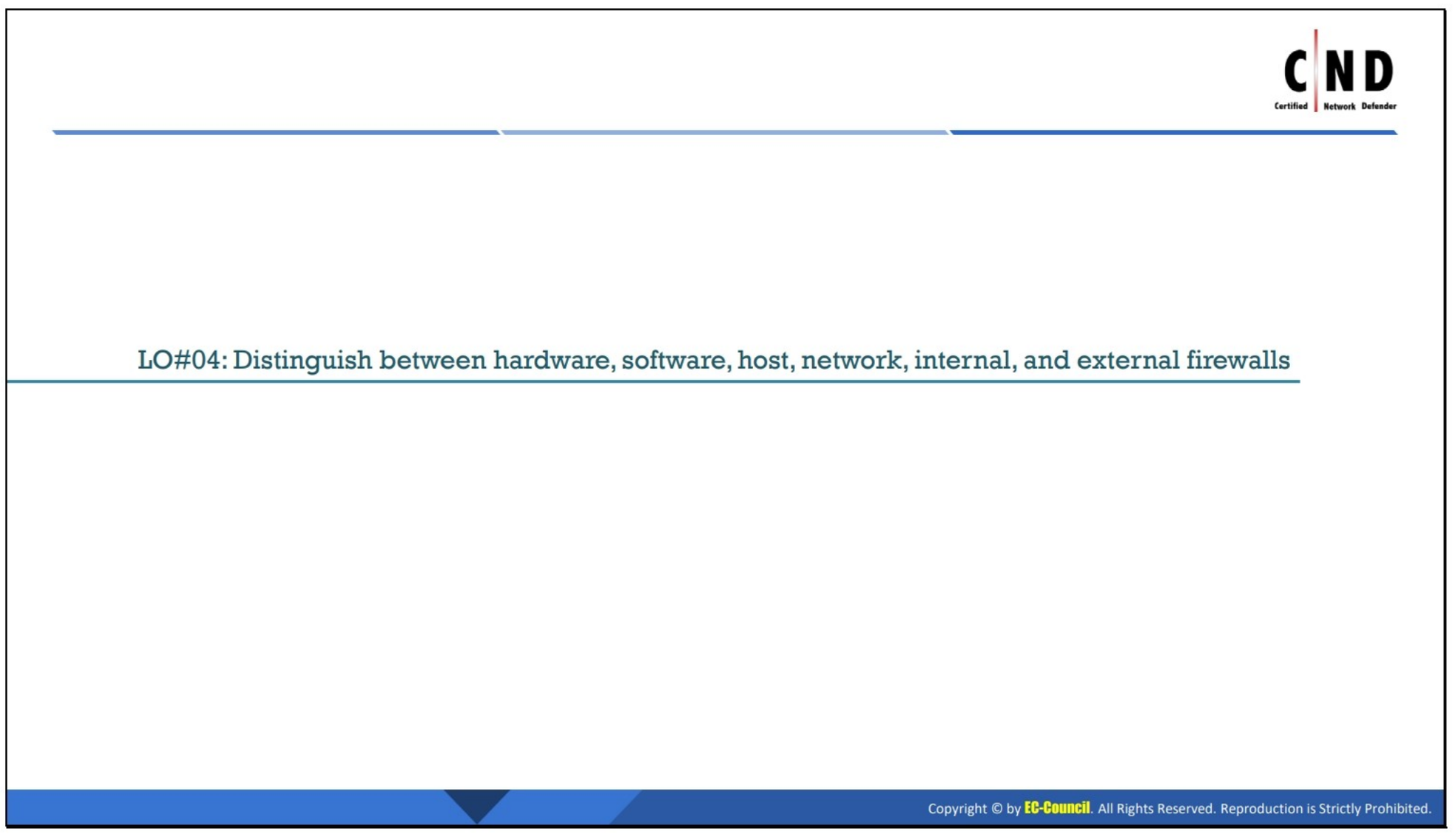
https://t.me/learningnets

trusted network, and the third interface to the DMZ. The rules for accessing the DMZ are less than those protecting the private network. This topology is ideal for organizations maintaining two or more network zones.

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

https://t.me/learningnets

Technet24

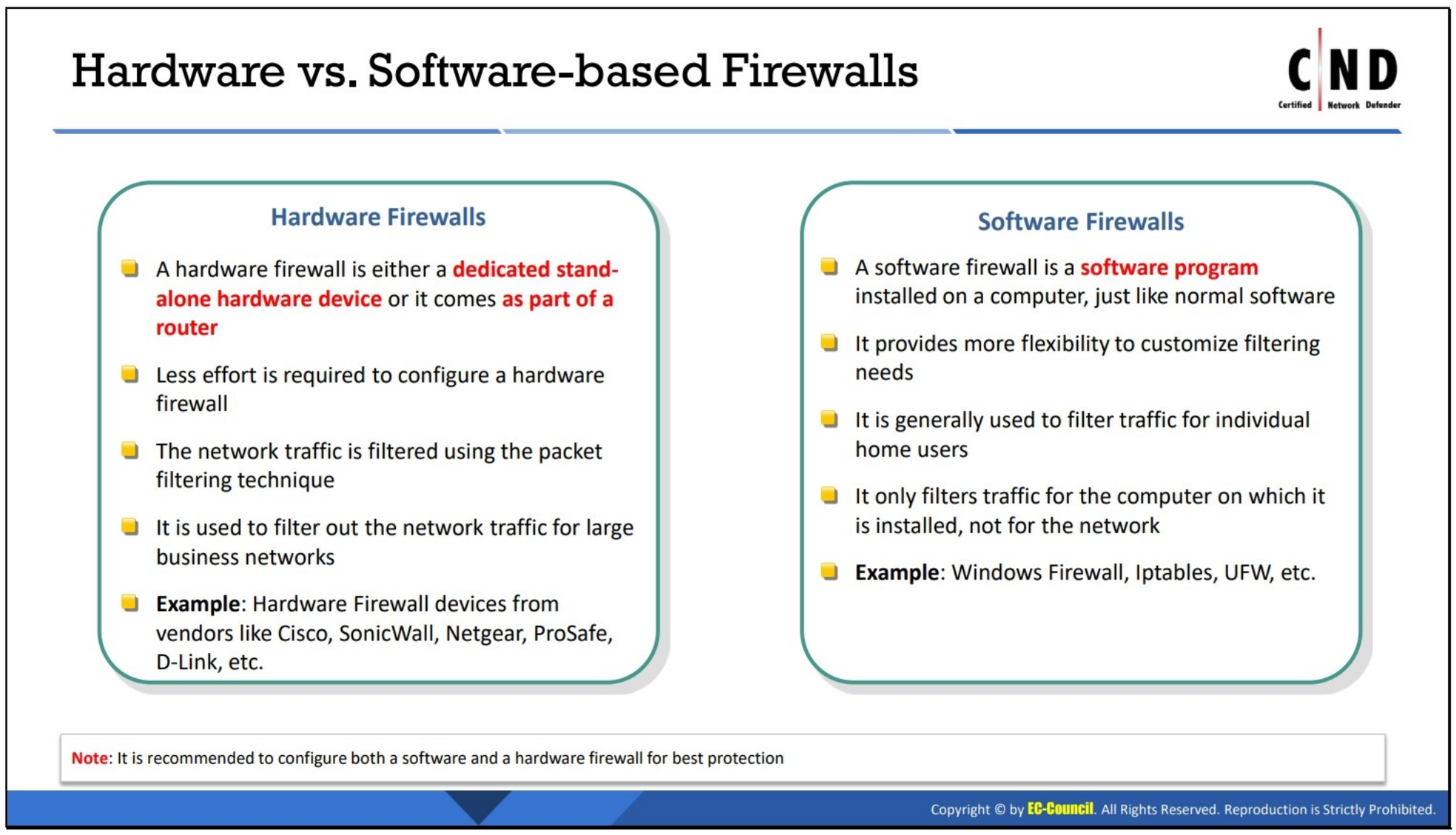


LO#04: Distinguish between Hardware, Software, Host, Network, Internal, and External Firewalls

The objective of this section is to explain the difference between hardware, software, host, network, internal, and external firewalls.

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

https://t.me/learningnets



Hardware vs. Software-based Firewalls

Hardware Firewalls

A hardware firewall is a dedicated firewall device placed on the perimeter of the network. It is an important part of a network setup, and it is either built-in to the broadband router or is a stand-alone product. A hardware firewall helps protect systems on the local network, and it is effective even with little to no configuration. Hardware firewalls usually employ packet filtering, wherein they read the header of a packet to identify the source and destination address and compare it with a set of predefined and/or user-created rules that determine whether they should forward or drop the packet. Hardware firewalls either function on an individual system or an individual network connected using a single interface. Examples of hardware firewall include Cisco ASA, FortiGate, etc.

Advantages

- A hardware firewall with its own operating system is considered to reduce security risks and provides better security control.
- Hardware firewalls initiate faster responses and enable more traffic.
- As a hardware firewall is a separate network component, it enables better management and allows the firewall to shutdown, move, or be reconfigured with less interference on the network.

Disadvantages

- They are more expensive than software firewalls.
- They are hard to implement and configure.

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

https://t.me/learningnets

Technet24

- They consume more space and need physical cabling.
- They are difficult to upgrade.

Software Firewalls

A software firewall is similar to a filter. It sits between the normal applications and the networking components of the operating system. It is more helpful for individual home users, is suitable for mobile users who need digital security when working outside of their corporate network, and it is easy to install on an individual's PC, notebook, or workgroup server. A software firewall implants itself in the key area of the application/network path. It analyzes data flow against the ruleset.

Configuration of a software firewall is simple compared to that of a hardware firewall. It intercepts all requests from a network to the computer to determine if they are valid and protects the computer from illicit attacks that try to access it. It incorporates user-defined controls, privacy controls, web filtering, content filtering, etc. to restrict unsafe applications from running on an individual system. Software firewalls utilize more resources and this reduces the speed of the system. Examples of software firewalls are those produced by Norton, McAfee, and Kaspersky, among others.

Advantages

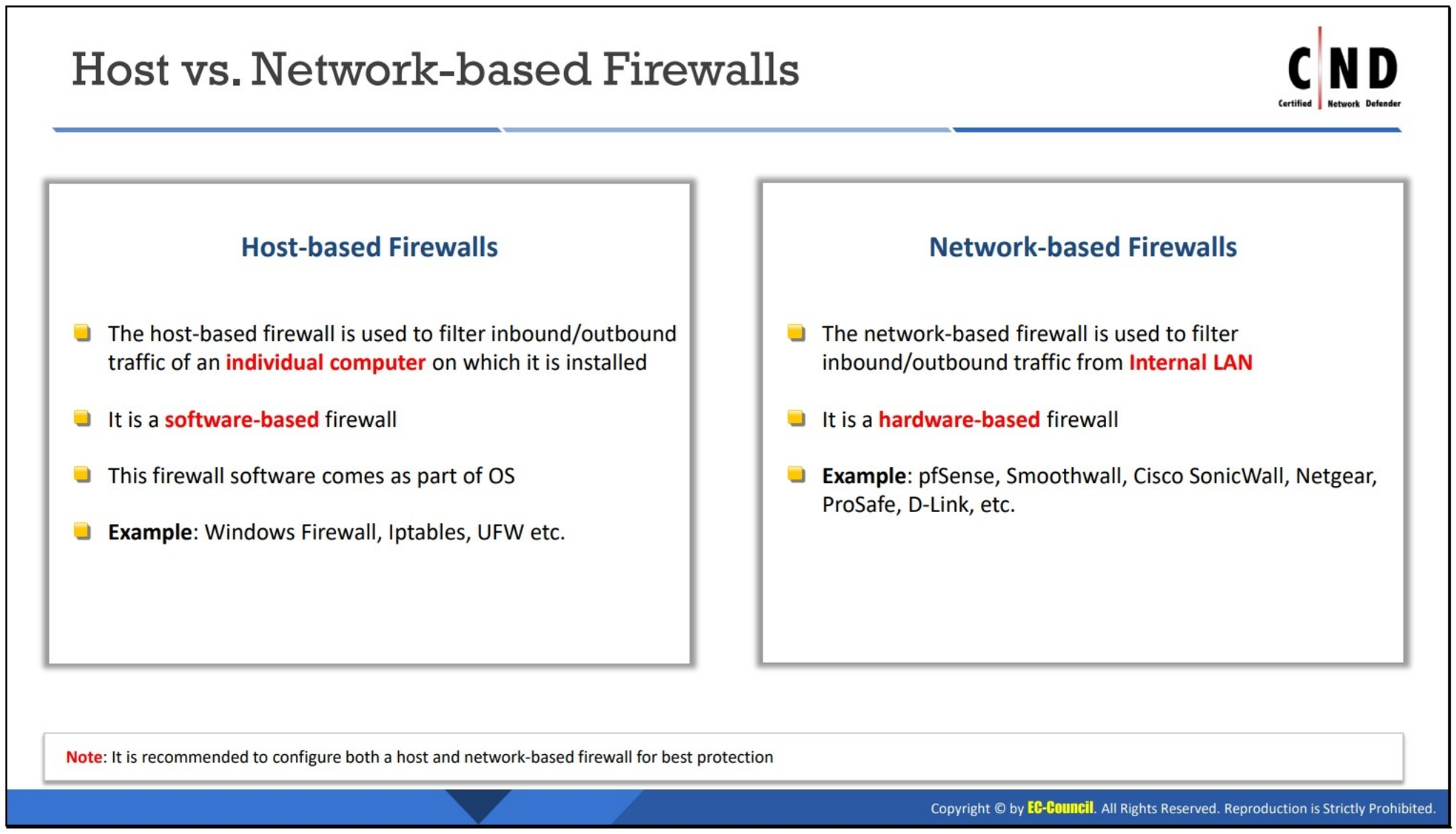
- Less expensive than hardware firewalls
- Ideal for personal or home use
- Easier to configure and reconfigure

Disadvantages

- Consume system resources
- Difficult to uninstall
- Not appropriate for environments requiring faster response times

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

https://t.me/learningnets



Host vs. Network-based Firewalls

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
- 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

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

https://t.me/learningnets
Technet24

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 managing 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.
- Their cost is lower in the case of big organizations.
- Incorrect maintenance of network firewalls that function as proxy servers may decrease network performance.

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

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

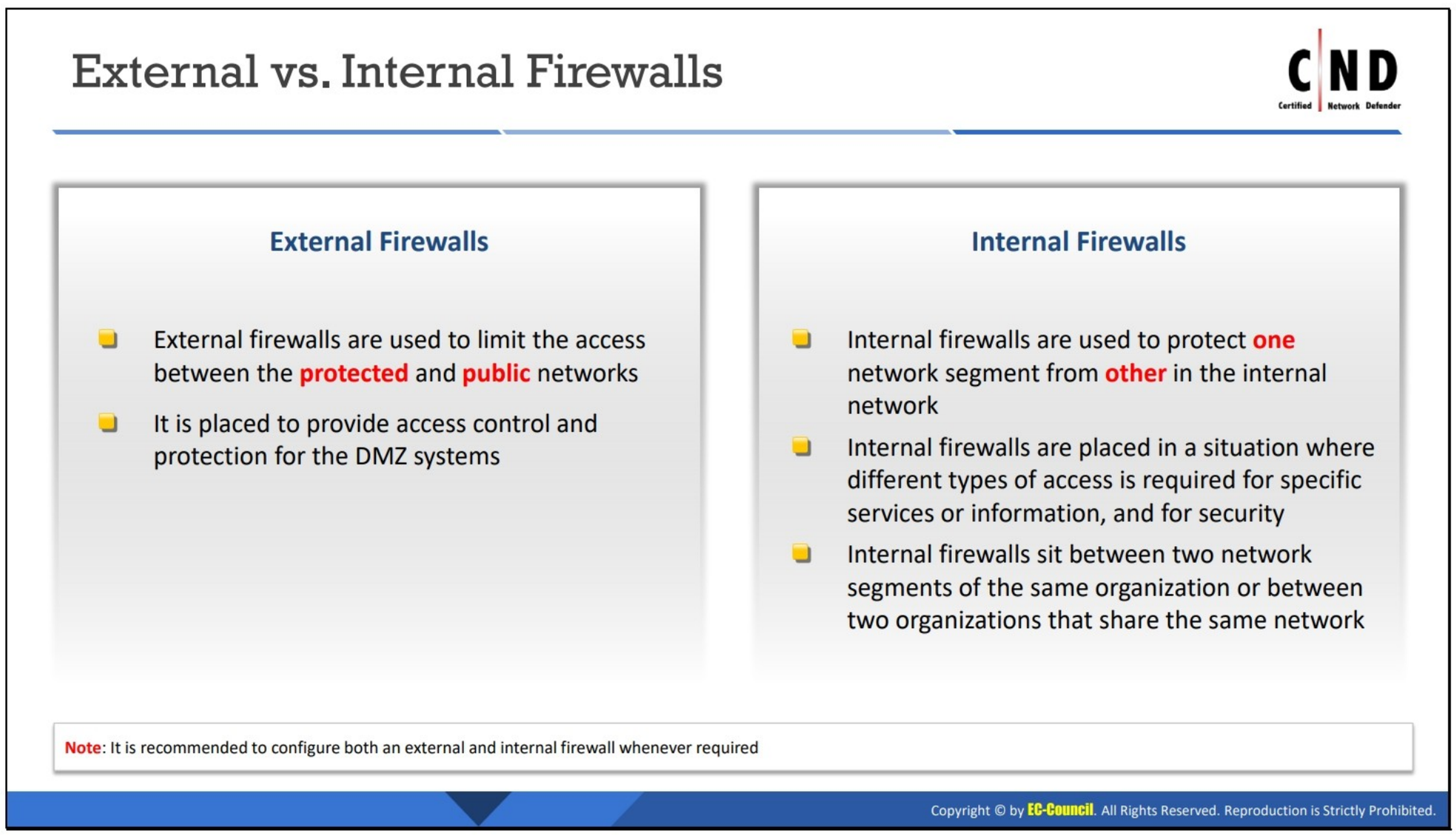
https://t.me/learningnets

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.

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

https://t.me/learningnets

Technet24



External vs. Internal Firewalls

External Firewalls

External firewalls are used to limit access between the protected network and the public network. They validate the inbound and outbound traffic of the internal network and translate addresses between the internal and public IP addresses. These firewalls are placed to provide access control and protection for the DMZ systems in which new connections are disallowed from the external to the internal network.

They provide security for legacy devices that do not have firewalls. They also provide security to systems that have issues preventing them from having protection capabilities. The implementation of external firewalls is done by placing the external firewall between the legacy device and the LAN. Even if the legacy device is compromised, the external firewall device can detect the malicious device and prevent it from spreading the attack to the remaining devices in the network and also prevent it from contacting applications on the Internet. Examples include Floodgate Defender by Icon Labs, Firebox M440 by WatchGuard (switch-oriented firewall), etc.

Advantages

- Operate independent of legacy devices
- Can be updated independently of legacy devices
- Ability to control systems with more open connections such as a web browser
- Allow quick installation and are easy to configure
- Useful for replacing the connection of a legacy device to a switch with a connection to the firewall device by combining the external firewall with a switch (this is applicable if an

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

https://t.me/learningnets

organization's legacy devices cannot be updated for security and replacing the system may not be feasible)

Internal Firewalls

Internal firewalls/internal network segmentation firewalls are used to protect one network segment from others in the internal network and ensure the application of stateful inspection and policies for the traffic that traverses through the internal network. These firewalls allow restricting the malicious activity in one segment of the network from spreading to other internal network segments.

These are placed in a situation where different types of access are required for specific services or information. Internal firewalls sit between two network segments of the same organization or between two organizations that share the same network. Instead of using switches, internal firewalls allow segmenting the network as well as monitoring its traffic by implementing stateful policies.

Advantages

- They isolate and secure critical servers and systems from internal users and external users accessing public servers while restricting the to access the network and will be under monitoring always.
- They block communication between two hosts and isolate the segment where malicious activity is identified
- They provide visibility into the internal network
- They allow segmentation and monitoring of even large L2 networks (but the internal firewalls need to be placed between two stacks of L2 aggregation switches)
- Traffic handling capacity is higher compared to placing the firewalls at the edge of the network
- They restrict remote users to a few network segments
- They allow containment and monitoring of VPN traffic

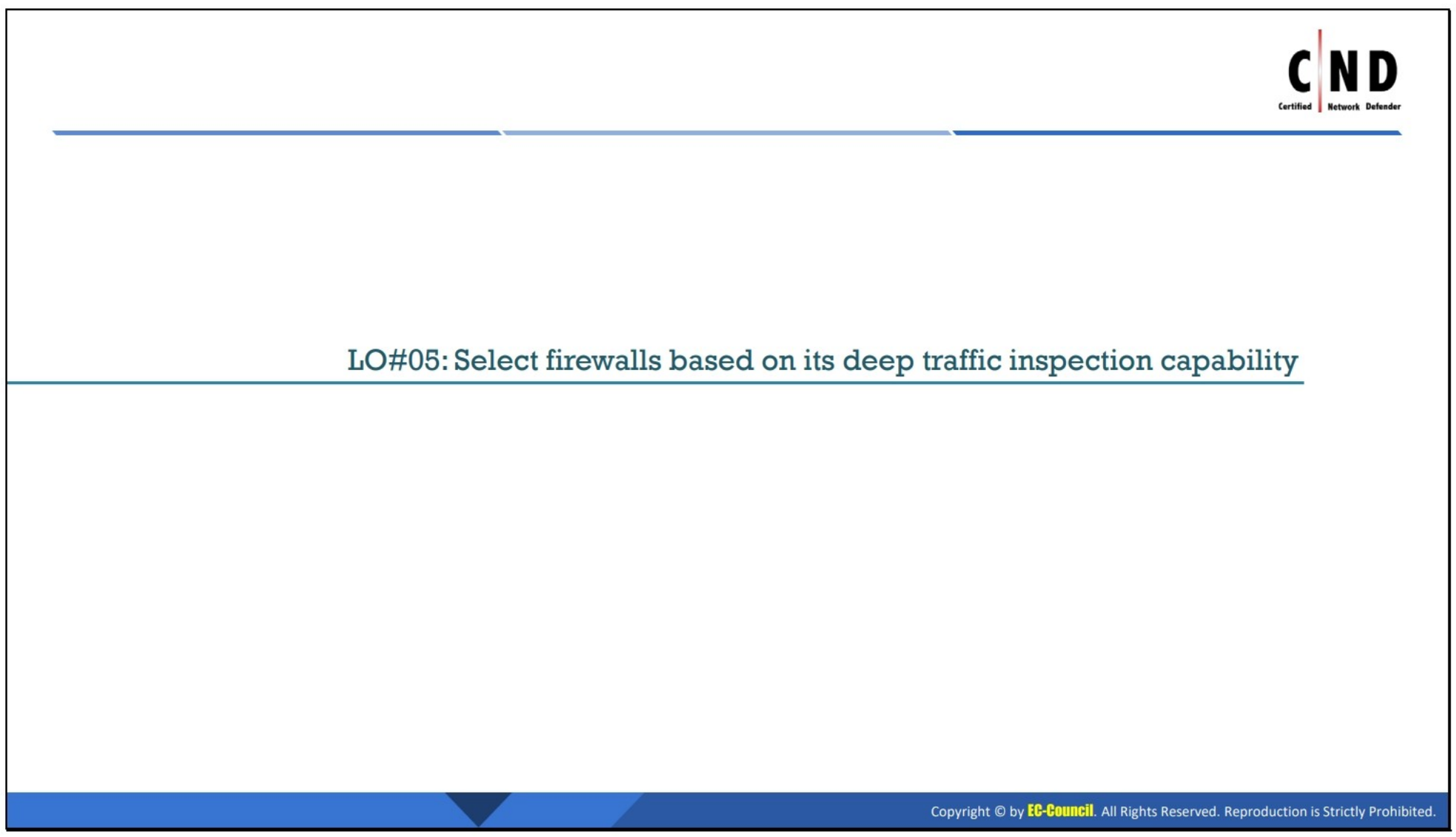
Disadvantages

- Internal firewalls need the creation of additional subnets
- Problematic for systems that move among different networks
- Expensive devices

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

https://t.me/learningnets

Technet24

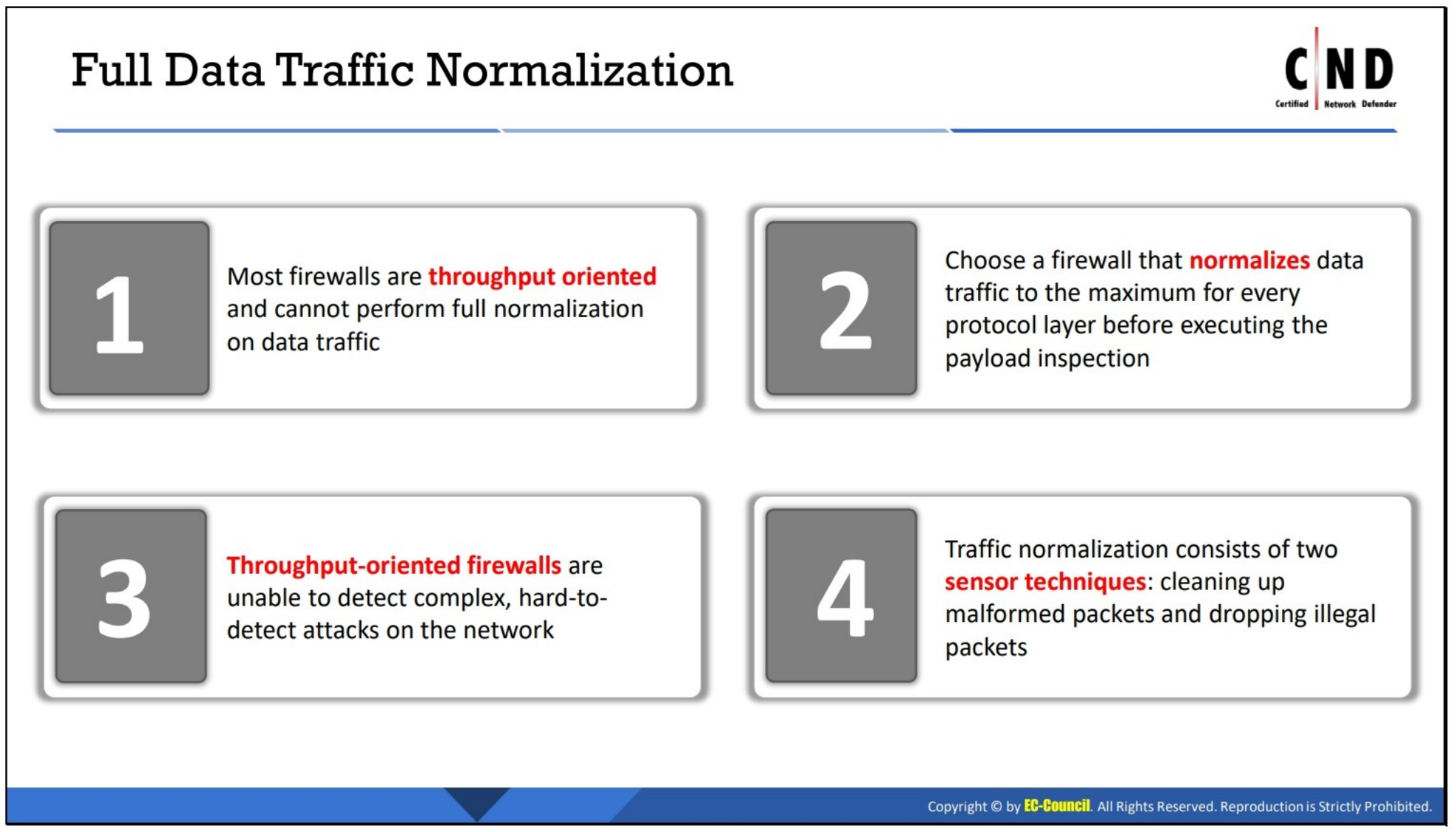


LO#05: Select Firewalls Based on Its Deep Traffic Inspection Capability

The objective of this section is to explain how to select the appropriate firewall by validating its deep traffic inspection capabilities.

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

https://t.me/learningnets



Full Data Traffic Normalization

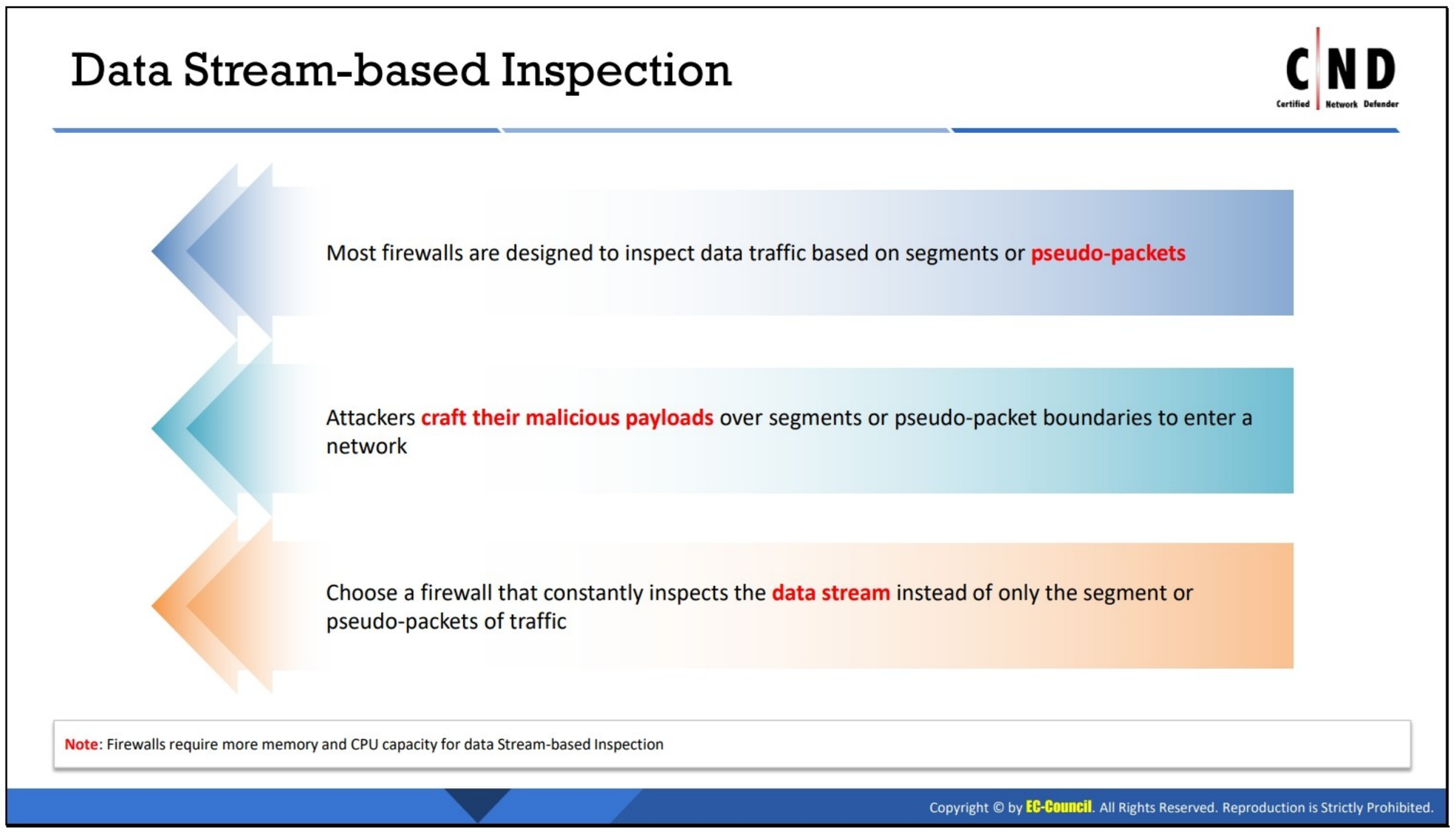
Normalization is a technique to prevent firewall evasion. Full data traffic normalization can prevent firewall evasion by preventing known attacks or by restricting access to internal machines from an external host when it detects a probe or an attack.

Firewall design must incorporate and optimize the inline throughput performance in a network to prevent attacks. Firewall vendors use shortcuts and execute only partial normalization and inspection. For instance, TCP segmentation handling is very limited and done only for selected protocols or ports (if not disabled by default). Evasions exploit these shortcuts and weaknesses in normalization and inspection processes. Only those firewalls should be utilized that normalize data traffic to the maximum on every protocol layer before executing the payload inspection. Traffic normalization comprises two sensor techniques. They are cleaning up malformed packets and dropping illegal packets.

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

https://t.me/learningnets

Technet24

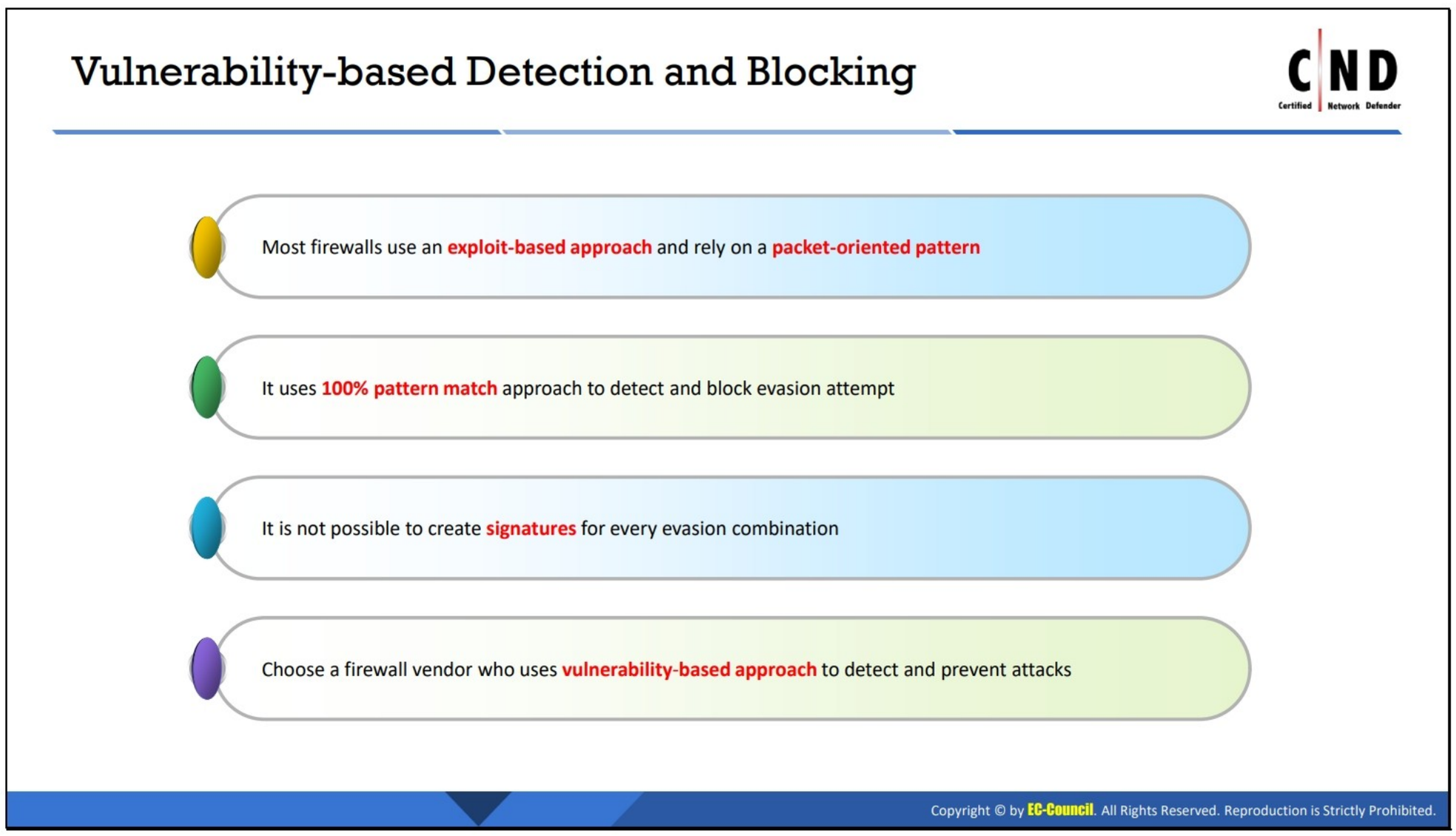


Data Stream-based Inspection

A firewall should be able to examine a constant data stream instead of fragments or pseudo-packets. This vital design issue is extremely difficult to fix, especially in the case of hardware-based products where a redesign of security devices would require significant R&D. Data stream–based inspection requires more memory and CPU capacity to perform efficiently. For many vendors, this is impossible and, thus, the inspection scope is sacrificed. The attacker can take advantage of this by spreading attacks over segments or pseudo-packet boundaries. Only those firewalls should be utilized that inspect constant data streams instead of segments or pseudo-packets of traffic.

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

https://t.me/learningnets



Vulnerability-based Detection and Blocking

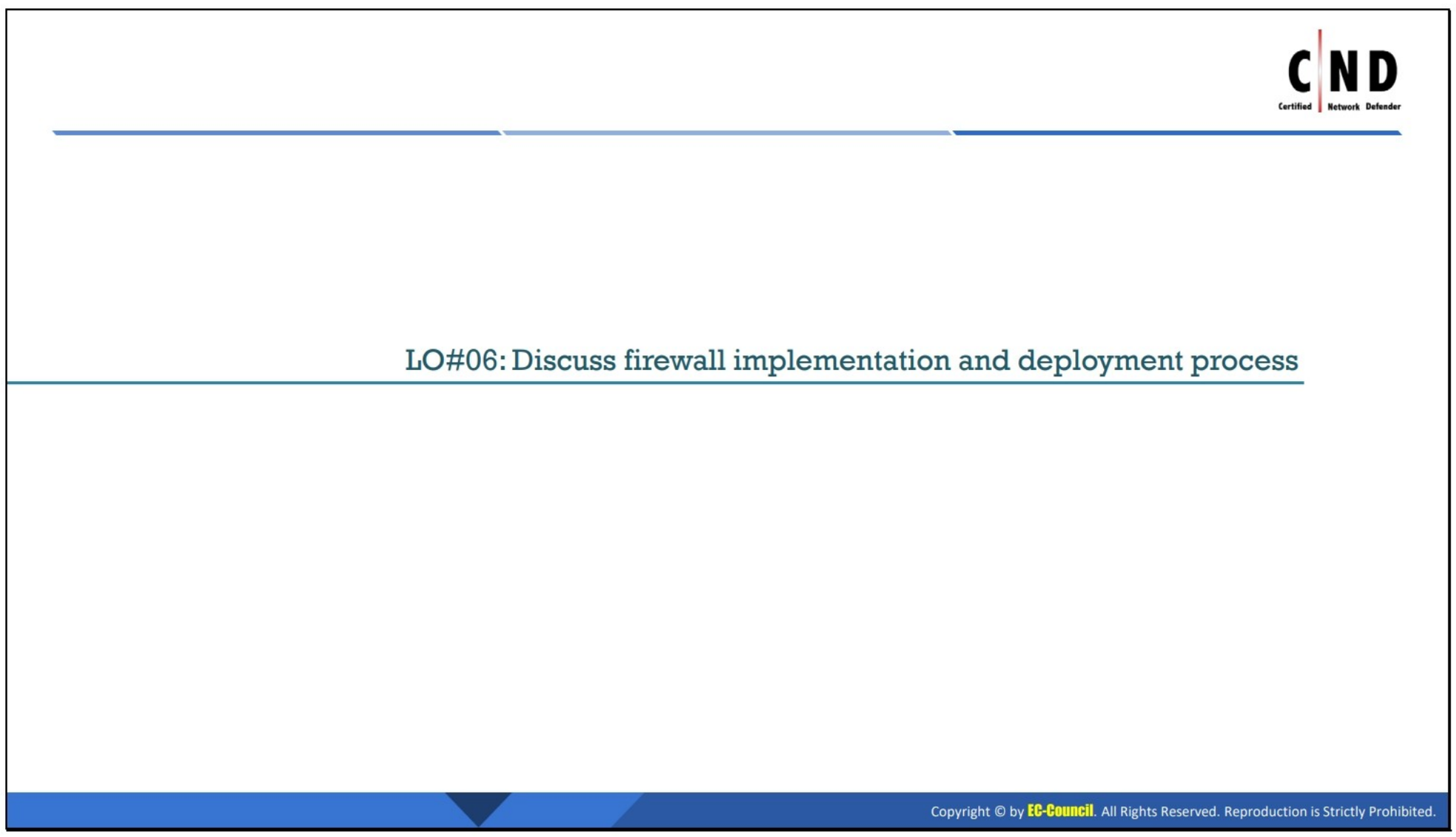
Some firewall vendors implement an exploit-based approach to detect and block network exploitation attempts. An exploit-based approach works on the principle of a packet-oriented pattern (signature), and if the there is a 100% match, the evasion is detected and blocked. However, it is not possible to create signatures for every evasion combination. Moreover, new attack patterns and signatures are invented daily. Therefore, firewalls with exploit-based approaches cannot detect and block all firewall evasion attempts. Relying on such firewalls can pose a risk to the organization's network.

Hence, a firewall based on the vulnerability approach is preferred instead. Such firewalls block exploitation attempts at both the network and the application layers.

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

https://t.me/learningnets

Technet24

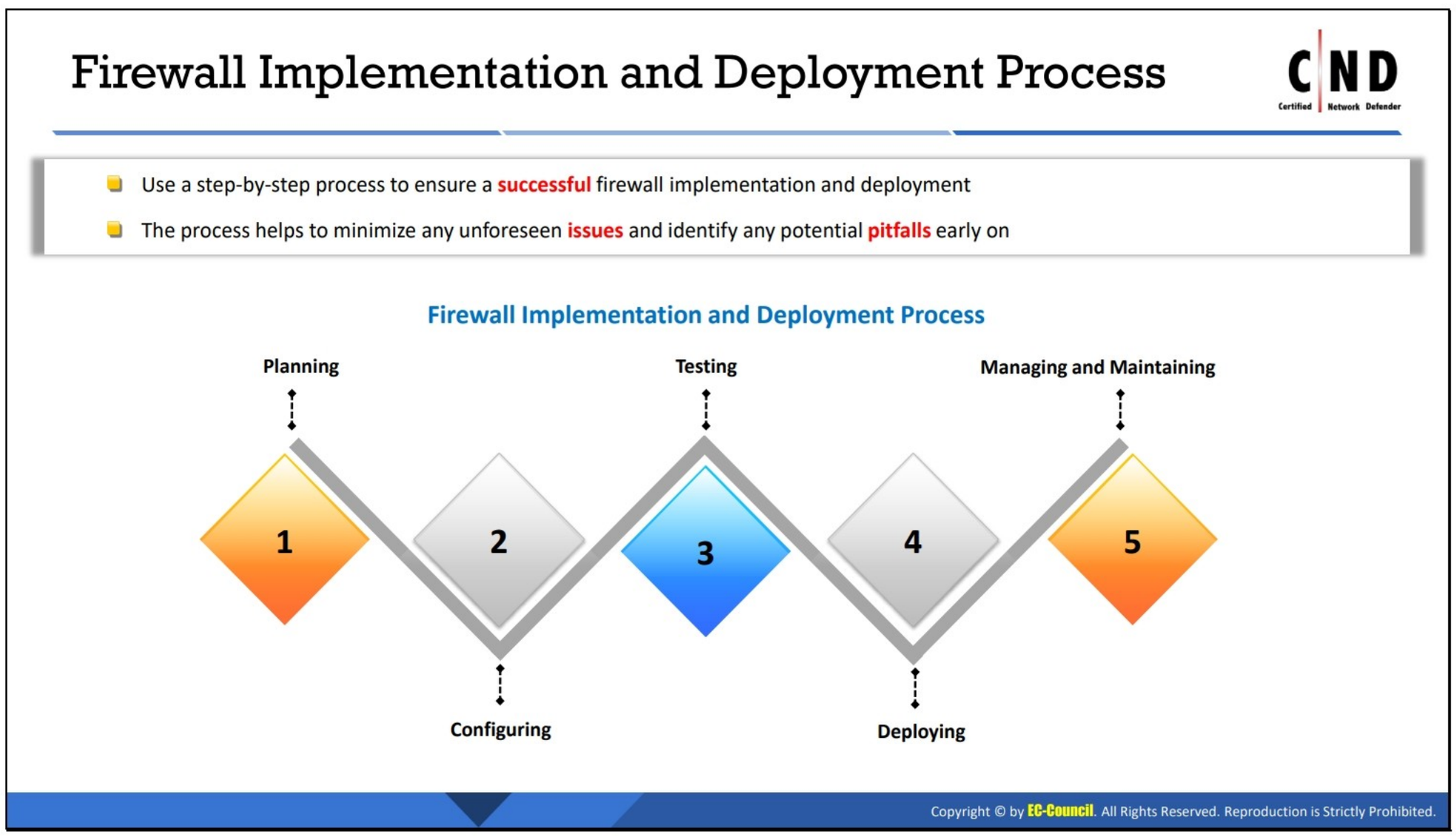


LO#06: Firewall Implementation and Deployment Process

The objective of this section is to explain the implementation and deployment process of firewalls.

Certified Network Defender 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. 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.

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

https://t.me/learningnets

Technet24

Firewall Implementation and Deployment: Planning

Assess the Need for Implementing Firewall

- Conduct a security **risk assessment** to identify all possible threats to the organization
- Identify the **potential impact of threats** to confidentiality, integrity, and availability of an organization's information system
- Build an organization's **security policy** from the results of the risk assessment
- Organization must determine if they need to implement a firewall to **enforce** the new security policies

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

Firewall Implementation and Deployment: Planning (Cont'd)

Things to Consider before Implementing Firewalls

- Define the **technical objectives** behind your firewall implementation. Objectives will drive the firewall selection process
- Decide on whether your selected firewall **fits** your existing network topology. This drives the selection of appropriate firewall topology
- Decide on the **type of traffic** that you want to inspect. This drives the appropriate selection of firewall technology
- Decide **type of firewall** that suites your need. This drives the selection of an appliance or a software firewall solution

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

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

https://t.me/learningnets

Firewall Implementation and Deployment: Planning (Cont'd)

Points of Consideration while Implementing Firewall

- Identify and consider all **requirements** to determine which firewall to implement
  - Don't construct a firewall using any other **networking equipment** such as a **router**, which are not meant for use as a firewall. It causes overload on the equipment and does not provide the security intended
  - Don't overload firewall with **non-security services** such as configuring it to be a web server, email server, etc.
  - Use firewalls at **multiple levels**
  - Sensitive network data, resources or systems should not be placed **behind a firewall** to avoid inside attacks from within the organization
  - Perform extensive market research to find out the **capabilities** and **limitations** of each firewall model has

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

Firewall Implementation and Deployment: Planning (Cont'd)

Factors to Consider before Purchasing any Firewall Solution

- **Management:** Will it provide **remote** and **centralized** management capabilities?
- **Performance:** What will be its **throughput**, maximum simultaneous connections, connections per second, and latency time?
- **Integration:** Will it be **easy to integrate** into the existing network infrastructure or require specific hardware?
- **Security Capabilities:**
  - What do you need to **secure**?
  - Which types of **firewall technologies** should it support?
  - What kind of **additional security** features does it have?
- **Physical Requirements:** Will it require any additional physical requirements such as **additional power**, backup power, cooling system, or **network connections**?
- **Personnel:** Will the administrator require any **training** to implement, deploy, administer and manage the firewall?
- **Future Needs:** Will it **meet** the future needs of the organization?

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

Firewall Implementation and Deployment: Planning

Assess the need of implementing firewall

There are some factors to consider before implementing a firewall solution on the network. It is your responsibility to specify network security issues and address them during firewall implementation.

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

https://t.me/learningnets

Technet24

Therefore, a proper risk assessment should be conducted before planning a firewall implementation.

This includes the following:

- Detecting possible threats and vulnerabilities in the network
- Evaluating possible impacts of a threat
- Identifying appropriate security controls

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. Depending on the potential origin of threats, a layout for firewall implementation should then be built. 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.

Consider the following things before implementing firewalls:

- Define the technical objectives behind the firewall implementation. Know why the organization is implementing a firewall. These objectives can help to drive the firewall selection process. For example, it can be an easy task to choose between a simpler and a complex feature-rich firewall if an organization knows its objectives behind the firewall implementation.
- Decide on whether the selected firewall fits the existing network topology. Know whether the selected firewall can sit at the perimeter of the organization's network or isolate a LAN in the organization. Know how much traffic the selected firewall can process and how many interfaces the selected firewall will need to segment the traffic. These performance requirements should drive the selection of an appropriate firewall topology.
- Decide on the type of traffic to be inspected based on the requirements as vendors come up with different trademarks for their traffic-inspection technology. For example, packet-filtering firewalls use simple rules for packet evaluation, stateful-inspection firewalls track the three-way TCP handshake, and application proxy firewalls offer breaking the connection between client and server in addition to offering stateful inspection. Knowing about these can drive the appropriate selection of firewall technology.
- Decide on whether the organization is suited for a hardware or a software firewall solution. Physical devices are easy to install but are usually the more expensive option. On the other hand, software firewall solutions are tricky to install and need tweaking; they are often less secure than hardware firewalls too.
- Decide on which OS (Windows, UNIX, etc.) is suited best for the organization's requirements as most firewall hardware runs on an OS and the firewall administrators should be able to work with it.

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

https://t.me/learningnets

Points to consider while implementing a firewall:

- Do not configure a firewall on a device not is not meant for firewalling. For example, configuring a firewall to function on a router can put additional burden on the router's functionality and affect its performance.
- Do not enable additional non-security services such as a web server or email server on the firewall. This will overload the device and reduce its efficiency in providing network security.
- Consider deploying firewalls at different locations at the perimeter, department, and individual host level.
- Consider a policy that requires the use of a firewall.
- Concentrating on external threats leaves the network vulnerable to internal threats or inside attacks. Consider keeping all sensitive and critical systems behind internal firewalls.
- Be careful while deploying a specific type of firewall. It should be done based on their techniques and limitations. Organizational security policies have a great impact on the type of firewall used.

Factors to Consider Before Purchasing and Implementing any Firewall Solution

The organization should consider the following factors before purchasing and implementing any firewall solution for their network.

- Management: The firewall should support encrypted protocols such as HTTPS, SSH, and access over a serial cable for remote management. Check whether any of these remote management protocols are acceptable for use with the organization's policies. Ensure that it is possible to restrict remote management to certain firewall interfaces and source IP addresses. In firewalls, look for centralized management from the same vendor. If it is available, check whether it is a vendor-specific application that performs this operation or not.
- Performance: Consider the performance of the firewall based on throughput, number of connections, time required for each connection, and its latency time. Check its resistance against bottleneck problems. Evaluate its failover and load balancing functionality.
- Integration: Consider the hardware requirements for firewall implementation. The implemented firewalls need to be compatible with all other security devices. Check the compatibility of the firewall log system with the existing log management system.
- Security capabilities: Consider all the possible areas of the organization that require security. Choose the appropriate firewall technology that best addresses the kind of traffic that needs to be monitored. Additionally, consider other network security capabilities such as IDS, VPN, and content filtering while choosing a firewall.
- Physical requirements: Consider the physical space and protection required for a firewall. For example, extra shelf or rack space, adequate power backup facilities, and air conditioning facilities at the location of the placement.

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

https://t.me/learningnets

Technet24

- Personnel: Management should choose network operators or the personnel responsible for managing the firewall. The organization must train network defenders on managing and maintaining the firewall before deploying it.
- Future needs: Choose a firewall that meets the future needs of the organization such as plans to move to IPv6, anticipated bandwidth requirements, and compliance with regulations expected to be implemented.

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

https://t.me/learningnets

Firewall Implementation and Deployment: Configuring

- **Firewall configuration requires** a series of steps for successful firewall configuration

Hardware and Software Installation

- Install the hardware, OS, patches, vendor updates, and any underlying **firewall software** when a software firewall is being implemented
- Install patches and vendor updates on the system when a **hardware-based firewall** is implemented
- Configure the firewall to protect **unauthorized access**
- Configure the **admin account** for firewall administration duties

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

Firewall Implementation and Deployment: Configuring (Cont'd)

Creating ad Configuring Firewall Policies

- Create and configure the firewall **policies**
- The policy should explain how the firewall is to be **updated** and **managed**

The Steps Involved in Creating a Firewall Policy:

1. Identify the **network applications** that are of utmost importance
2. Identify the **vulnerabilities** that are related to the network applications
3. Prepare a **cost-benefits analysis** to secure the network applications
4. Create a **network application traffic matrix** to identify the protection method
5. Create a **firewall ruleset** that depends on the application's traffic matrix

Conduct Periodic Review of Firewall Policies:

- Conduct periodic reviews of firewall policies to achieve **accuracy** and **timeliness**
- If a firewall application is upgraded, then the firewall's ruleset must be **formally changed as well**
- Firewall installs, systems, and other resources must be **audited** on a regular basis
- Review and update firewall **policies** every six months

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

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

https://t.me/learningnets

Technet24

Firewall Implementation and Deployment: Configuring (Cont'd)

Creating and Configuring Firewall Rules

Firewall Rules:

- A firewall rule defines the parameters against which **network connection** is compared and takes one of following **two actions**:
  - Allow the connection
  - Block the connection
- Firewall rules help an administrator impose **customized access control** on inbound and outbound network traffic
- You need to **define a ruleset**, specifying what services, source addresses, destination addresses, protocols, etc. to permit through the firewall and what should be denied

Build an Appropriate Firewall Ruleset:

- **Design** and **configure** a firewall ruleset based on the organizational security need
- The firewall ruleset consists of the rules that establish the **functionality** of the firewall
- A firewall ruleset contains the following information: (based on the firewall platform architecture):
  - Packet source address
  - Packet destination address
  - Traffic type
  - Action (allow, deny, Drop)

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

Firewall Implementation and Deployment: Configuring (Cont'd)

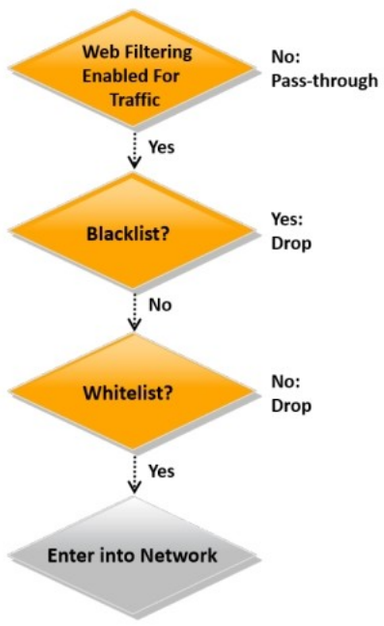
How Does a Firewall Rule Work?

Blacklist:

- All packets are allowed, except those set to **deny**

Whitelist:

- All packets are denied, except those set to **allow**



Example: Packet Filter Firewall Ruleset

- The following tables illustrates a **sample packet filter firewall ruleset**, helping you to configure the packet filtering rules in software as well as hardware firewalls

S. No	Source Address	Source Port	Dest Address	Dest Port	Action
1	Any	Any	10.1.1.0	>1023	Allow
2	10.1.1.1	Any	Any	Any	Deny
3	Any	Any	10.1.1.1	Any	Deny
4	10.1.1.1	Any	Any	Any	Allow
5	Any	Any	10.1.1.2	HTTP	Allow
6	Any	Any	10.1.1.3	SMTP	Allow
7	Any	Any	Any	Any	Deny

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

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

https://t.me/learningnets

Firewall Implementation and Deployment: Configuring (Cont'd)

Firewall Rule Tester: Firewalk

Firewalk can help you in **discovering** your firewall rules

Example:

```
nmap --script=firewalk --traceroute <host>

nmap --script=firewalk --traceroute --
script-args=firewalk.max-retires=1 <host>

nmap --script=firewalk --traceroute --
script-args=firewalk.probe-timeout=400ms
<host>

nmap --script=firewalk --traceroute --
script-args=firewalk.max-probed-ports=7
<host>
```

```
root@alice-Virtual-Machine: /home/alice

root@alice-Virtual-Machine:/home/alice# nmap --script=firewalk --traceroute 10.10.10.1
Starting Nmap 7.80 ( https://nmap.org ) at 2023-12-08 01:18 EST
Nmap scan report for 10.10.10.1
Host is up (0.00097s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Host script results:
| firewalk:
| HOP  HOST         PROTOCOL  BLOCKED PORTS
| 0    20.20.10.20  tcp       4,6-7,13,19-20
|_1    20.20.10.53  tcp       1,3,9,17

TRACEROUTE (using port 443/tcp)
HOP RTT     ADDRESS
1   0.64 ms _gateway (20.20.10.53)
2   1.42 ms 10.10.10.1

Nmap done: 1 IP address (1 host up) scanned in 14.66 seconds
root@alice-Virtual-Machine:/home/alice#
```

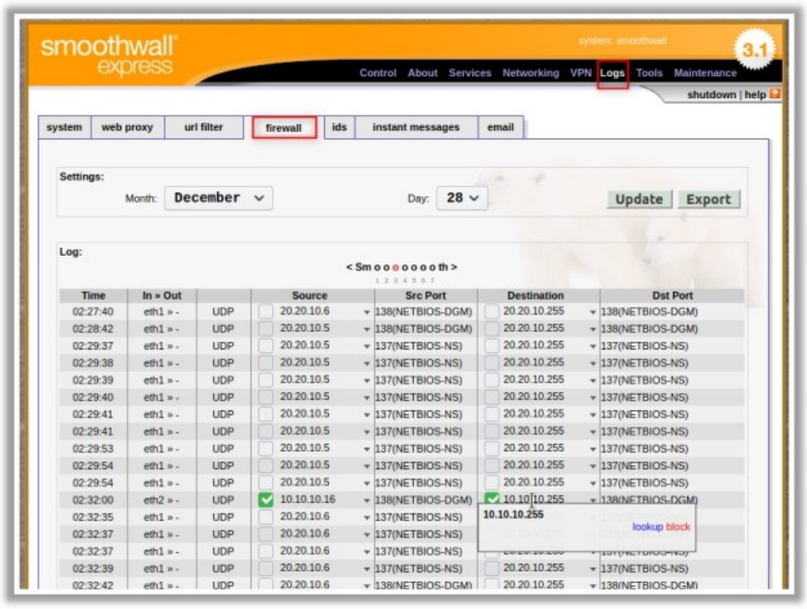
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Firewall Implementation and Deployment: Configuring (Cont'd)

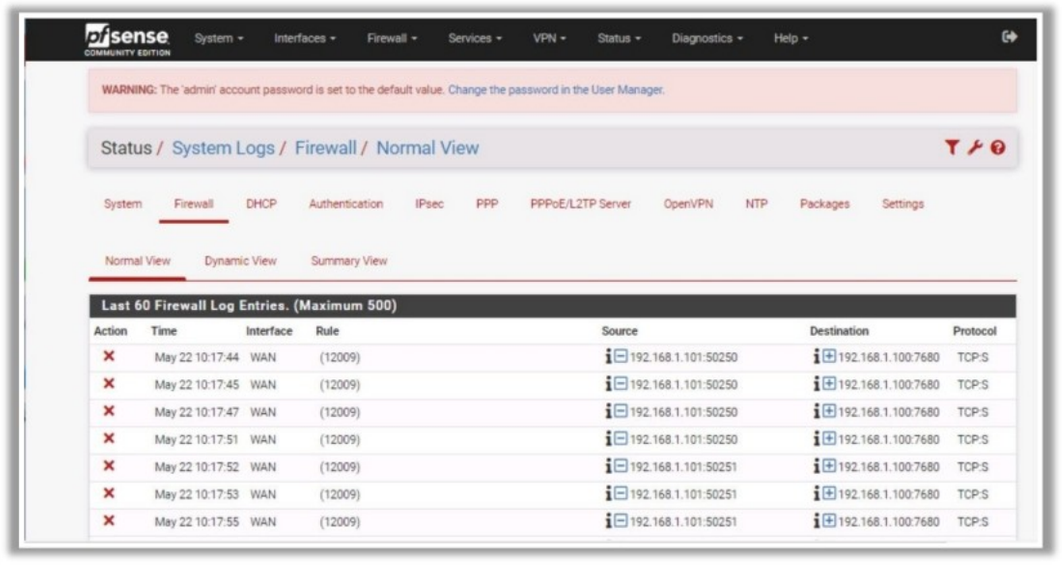
Configuring Logging and Alerting

- Setup logging and alerts to **detect security incidents**

Smoothwall Firewall Logging



pfSense Firewall Logging



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

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

https://t.me/learningnets

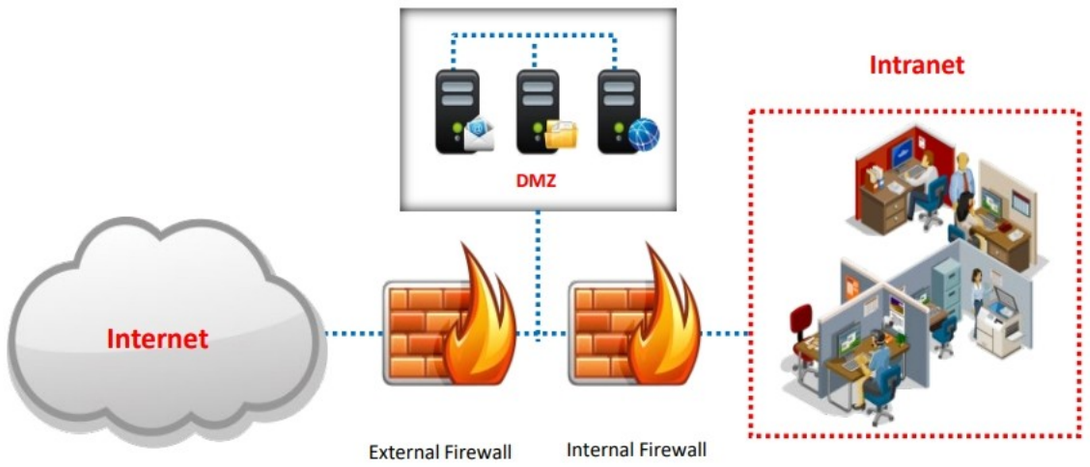
Technet24

Firewall Implementation and Deployment: Configuring (Cont'd)

C|ND Certified Network Defender

Integrating Firewall into Network Architecture

- Integrate the firewall with the **existing network infrastructure**, with or without specific hardware depending on the selection of the firewall



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

Firewall Implementation and Deployment: Configuring

Configuring a firewall involves configuring various components and features such as hardware, software, policy configuration, implementing logging, and alerting mechanisms.

Hardware and Software Installation

After selecting a certain type of firewall for implementation, proceed with the installation and configuration of the hardware and operating system. If a software-based firewall is being implemented, consider installing the necessary software first. It is important to perform a timely installation of patches and vendor updates for both types of firewalls. Install the remote management capability software to remotely access the firewall console and manage it to prevent any unauthorized access. Access to the firewall should be restricted to only those who are responsible for managing the firewall. Also, disable management services for the firewall, such as simple network management protocol (SNMP). Configure new admin accounts, if the firewall supports having a separate administrator account to perform firewall administration duties.

Creating ad Configuring Firewall Policies

After installing the firewall hardware and software, it is now time to focus on creating the firewall's policies.

Firewall policy implementation should be performed following the organization's system security plan with regard to network traffic, types of traffic protocols, source addresses, and destination addresses, as required by applications of the organization.

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

https://t.me/learningnets

Define a firewall policy, which explains how the firewall is setup, operated, updated, and maintained. The policy includes the scope of the firewall, services offered, and the types of communications supported.

The steps involved in creating a firewall policy are listed below.

- Step 1: Identify the network applications that are of utmost importance, especially the traffic they generate, bandwidth required, and the type of connection they use.
- Step 2: Identify the vulnerabilities that are related to the network applications and their impact over the network as well as the systems.
- Step 3: Prepare a cost-benefit analysis to secure the network applications.
- Step 4: Create a network application traffic matrix to identify the protection method.
- Step 5: Create a firewall ruleset that depends on the application's traffic matrix.

Checklist: Implementing a Basic Firewall Policy

- Always confirm that the policies implemented meet the needs of the organization.
- Always create one or more firewall rules for inbound traffic to allow voluntary inbound network traffic.

Conducting Periodic Review of Firewall Policies

According to recent studies, almost 80% of the firewalls installed were misconfigured. Any small error in the firewall configuration increases risk for an organization. Security, regulatory compliance, network availability, and performance are altered if there are any issues in the firewall.

Firewall policies should align with day-to-day advancements in threat levels in order to deploy a protected network. It is essential to verify the policy that defines the processes regularly to check if they are able to combat any new risks and attacks.

The steps to review the policies include the following:

- Create periodic reviews for firewall policies to achieve accuracy and timeliness.
- Review and update firewall policies every six months.
- If a firewall's application is upgraded, then the firewall's ruleset must be formally changed.
- Firewall installs, systems, and other resources must be audited on a regular basis.

The scheduled periodic firewall policy reviews include the following:

- Actual audits and vulnerability assessments of production that give a good idea on what systems are being used, internal communications patterns deployed, and the type of attacks they are prone to.
- Backup infrastructure components help create a backup in case an attack leads to data loss.

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

https://t.me/learningnets

Technet24

- Computer systems, shared drives, email servers, web servers, and secured networks placed at various locations must also be reviewed in order to keep the system updated, which offers the utmost speed and efficiency.

Scheduled reviews should examine the following:

- Whether proper firewall policies are implemented for each firewall
- Firewall rules that are not used often and whether they can be eliminated
- Any changes in network security that gives rise to additional or new security exposures

Periodic firewall reviews help increase security, availability, and performance of the organization's network.

Creating and Configuring Firewall Rules

Firewall Rules

A firewall uses one or more sets of "rules" to inspect network packets as they come in or go out of the firewall and either allows the traffic through or blocks it.

A firewall rule defines the process to inspect one or more characteristics of network packets such as the protocol type, source or destination host address, and source or destination port of the network connection. The firewall takes the required action based on the network policy of the organization.

Rules of the firewall should comply with the company's goals and security policies as well as offer convenience and cater to the organizational needs for averting all threats. It is recommended to frame the guidelines for sampling the work of a firewall and updating it at scheduled intervals.

A firewall follows three basic rules in order to secure an organization's systems:

- Allow**:** A firewall allows "safe" traffic to flow that has been defined as such.
- Block**:** A firewall will block traffic that looks suspicious.
- Ask**:** A firewall initially asks whether to allow incoming and outgoing traffic to access the organization's network resources. It also remembers the responses for future use.

With the help of rules, firewalls decide which actions to be taken if the traffic coming from specific IP addresses and ports breaks the firewall rules. These firewall rules are set according to an organization's security policy.

Building Appropriate Firewall Ruleset

A ruleset's design depends on the type of traffic flowing through the network, including the protocols of the firewall such as DNS, SNMP, and NTP. If multiple firewalls need to have the same rules, synchronize all the rules across all the firewalls.

Build rulesets that support and implement the organization's firewall policy while also offering better performance. These should be specific and dependent on the network traffic they interact with and include information such as traffic types required and protocols used for management purposes. The type of firewall and specific products affect the ruleset's development process.

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

https://t.me/learningnets

Firewall rules allow a computer to send or receive packets from a program, services, computers, and/or users. Firewall rules allow three actions:

- Allow the connection.
- Allow the connection only if secured through IPsec.
- Block the connection.

These rules are applicable for both inbound and outbound traffic. Rules can be applied to a variety of network adapters including LAN, wireless, and remote access.

Most firewall platforms use rulesets as their common system for implementing security controls. The contents of the firewall ruleset will establish the functionality of the firewall. Based on the firewall's platform architecture, firewall rulesets contain the following information:

- Packet source address
- Packet destination address
- Traffic type

The ruleset should ensure that port filtering is performed both at the outer edge of the network and inside the network. The ruleset should also be capable of raising an alert if a user logs on or changes any of the rules.

It is recommended that every firewall include the following in their ruleset:

- Enable port filtering at the outer edge and inside the network
- Create rules to perform content filtering close to the content receiver

How does a firewall rule work?

There are two ways to define firewall rules based on the appropriate approach selected when creating protocols, reducing vulnerabilities on a network, and selecting the desired functionalities that are offered. These two approaches are outlined below:

Blacklist

- In this approach, estimate and define all the properties of malicious traffic and the firewall will prevent such traffic from entering the internal network.
- With this type of configuration, it is easier to protect the internal network when using a firewall.
- The firewall allows all packets, except the ones set to deny.

Whitelist

- In this approach, the firewall contains the properties of acceptable traffic.
- All packets are denied by the firewall, except those, that are set to allow.

As an example, the following table shows how to build the ruleset for packet filtering firewalls.

The first rule in the table is described below:

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

https://t.me/learningnets

Technet24

This row states that if traffic originates from any IP address and port source and for a specified destination IP address (10.1.1.0 in this case) and the port source is greater than 1023, this type of traffic will be allowed to pass through the firewall.

S.No	Source Address	Source Port	Dest Address	Dest Port	Action
1	Any	Any	10.1.1.0	>1023	Allow
2	10.1.1.1	Any	Any	Any	Deny
3	Any	Any	10.1.1.1	Any	Deny
4	10.1.1.1	Any	Any	Any	Allow
5	Any	Any	10.1.1.2	HTTP	Allow
6	Any	Any	10.1.1.3	SMTP	Allow
7	Any	Any	Any	Any	Deny

Table 4.2: Packet Filtering Firewall Ruleset

If you want to allow all IP traffic between a trusted external host and your internal hosts, the firewall rule will be as shown in following table.

Rule	Direction	Source Address	Destination Address	ACK Set	Action
A	Inbound	Trusted external host	Internal	Any	Permit
B	Outbound	Internal	Trusted external host	Any	Permit
C	Either	Any	Any	Any	Deny

Table 4.3: IP Traffic Between a Trusted External Host and Internal Hosts

Use the following tricks to build packet filtering firewall rulesets more effectively and securely.

- Edit your filtering rules offline.
- Reload rulesets from scratch each time.
- Always use IP addresses, and never hostnames.

The above rules are also known as “explicit allow/deny.” However, most of the firewalls have an "implicit deny" rule configured, which by default blocks all traffic that is not explicitly allowed. The firewall access list ends with “implicit deny,” which blocks all the packet the do not meet the requirements

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

https://t.me/learningnets

Firewall Rule Tester: Firewalk

Firewalk is an active reconnaissance network security tool for enumerating firewalls rules. Firewalk sends out TCP or UDP packets with a TTL one greater than the targeted gateway/firewall. If the gateway/firewall allows the traffic, it will forward the packets to the next hop where they will expire and elicit an ICMP_TIME_EXCEEDED message. If the gateway host does not allow the traffic, it will likely drop the packets and there will be no response.

To get the correct IP TTL that will result in expired packets you need to ramp up the hop-counts.

Example Usage

- `nmap --script=firewalk --traceroute <host>`
- `nmap --script=firewalk --traceroute --script-args=firewalk.max-retries=1 <host>`
- `nmap --script=firewalk --traceroute --script-args=firewalk.probe-timeout=400ms <host>`
- `nmap --script=firewalk --traceroute --script-args=firewalk.max-probed-ports=7 <host>`

Figure 4.2: Firewalk Example

Configuring Logging and Alerting

The firewall should have the capability to store logs and send and synchronize them in a centralized log management system. Logging should be done on a case-by-case basis to determine what to log and how long to keep logs. Create user accounts with read-access enabled to perform read-only tasks such as auditing and evaluation of the logs, and enable alarm systems that notify network defenders in the event of any attack on the firewall. The sign of attacks can include the following:

- Any attempt of manipulation for any of the firewall rules
- Events such as system reboots or disk shortages
- Any system status changes

Firewall Logs

Firewall logs contain information about activities such as port scans, unauthorized connection attempts, failed authentication attempts, abnormal protocols, virus attacks, activities from compromised systems, and security threat attempts at the boundary of the network. It helps trace the source of the network attacks.

Firewall logs are huge datasets to look into, especially for big enterprises with more than one or two firewalls. Firewalls record many log files with a very large number of log file entries every day. Firewall logs are stored locally or in a centralized logging server (Syslog server) on the network. The collection of firewall log data can help in analyzing the transactions between the source IP address and the destination IP address. If a firewall creates a huge log volume (approximately 10000 or even more events per second), it is necessary to use specialized software to collect and analyze them.

Firewall log data includes activities such as the following:

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

https://t.me/learningnets

Technet24

- Virus logs
- Network and device attacks
- Audit trail
- Event logs
- Network traffic
- VPN connection establishment

Importance of firewall logs:

- The firewall logs provide details regarding the status of the firewall.

Benefits of firewall logs include the following:

- Enhances network administration, troubleshooting and debugging
- Creates baseline information for comparison
- Provides a clearer outlook of the system
- Provides solutions for better forensic analysis

Firewall Logging

Firewall logging is the ability of a firewall to record or log the details of user's activities on a network. Log file maintenance is crucial to overcoming security breaches, as the attackers unknowingly leave their footprints when trying to pass through a firewall. Firewall logs can help investigate such incidents.

A centralized secure server should contain the firewall logs so as to protect it from attackers. Otherwise, an attacker could delete the logs that contain their footprints.

If any suspicious activity is detected in a firewall log, it should be handled immediately and all necessary actions taken to avoid any security incidents.

Using an Analyzer to Inspect Firewall Logs

A firewall analyzer is an application for analysis of firewall logs; it providing many tools to help gather, analyze, and report any logs found. Examples of firewall analyzers include ManageEngine Firewall Analyzer, SolarWinds Firewall Analyzer, etc.

ManageEngine Firewall Analyzer:

Source: https://www.manageengine.com

ManageEngine firewall analyzer is a program that collects, correlates, and analyzes security device information from enterprise-wide heterogeneous firewalls, proxy servers from Cisco, Fortinet, CheckPoint, WatchGuard, NetScreen, and more. It is a browser-based firewall/VPN/proxy server reporting solution.

SolarWinds Firewall Analyzer:

Source: https://www.solarwinds.com

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

https://t.me/learningnets

This firewall analyzer analyzes firewall logs, automates threat remediation, and secures the network against cyberattacks.

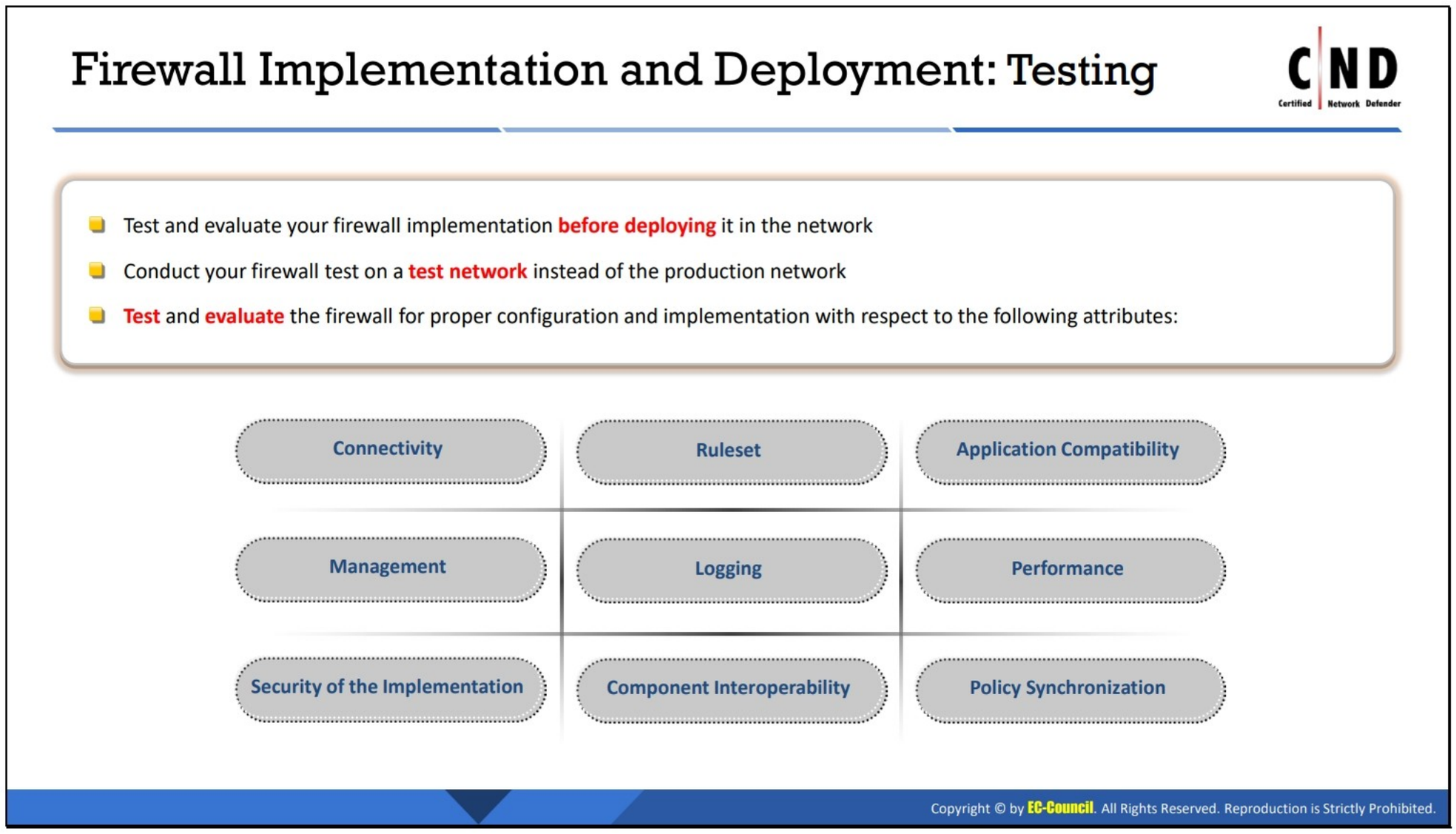
Integrating Firewall into Network Architecture

There are certain requirements for integrating a firewall with existing network devices that will interact with the firewall as well as the network's routing structure. Configuring the network router at the boundary of the network enables it to handle firewall addressing.

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

https://t.me/learningnets

Technet24



Firewall Implementation and Deployment: 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.

Before deploying a firewall, run a test on a test network, replicating the original network. Different aspects of the firewall are evaluated in this phase, as discussed below.

- Connectivity: Testing whether users can establish a connection through the implemented firewall.
- Ruleset: Check whether the firewall permits/blocks the traffic as per security policies. An analysis of the firewall ruleset includes manual testing to verify if the rules work according to the outlined security rules.
- Application compatibility: Check whether the implemented firewall solution is compatible with the existing application or communications.
- Management: Test whether the firewall can be managed in an effective manner.
- Logging: Test whether logging and data management functions adhere to the organization's policies and strategies.
- Performance: Test the performance of a firewall on a live network using simulated traffic generators. The testing process needs to include applications that can affect the network throughput and latency.
- Security of the implementation: Conduct a vulnerability assessment to identify any vulnerabilities and weaknesses in the firewall implementation.

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

https://t.me/learningnets

- Component interoperability: Evaluate the functioning of different components of the firewall. Using different firewall components from different vendors can create performance issues.
- Policy synchronization: Test how synchronized policies or rulesets work when multiple firewalls are used in multiple scenarios.

Testing a firewall includes the following steps:

- Developing an appropriate test case
- Deriving the test packets from the test case
- Sending the test packets to the firewall
- Examining the performance of the firewall

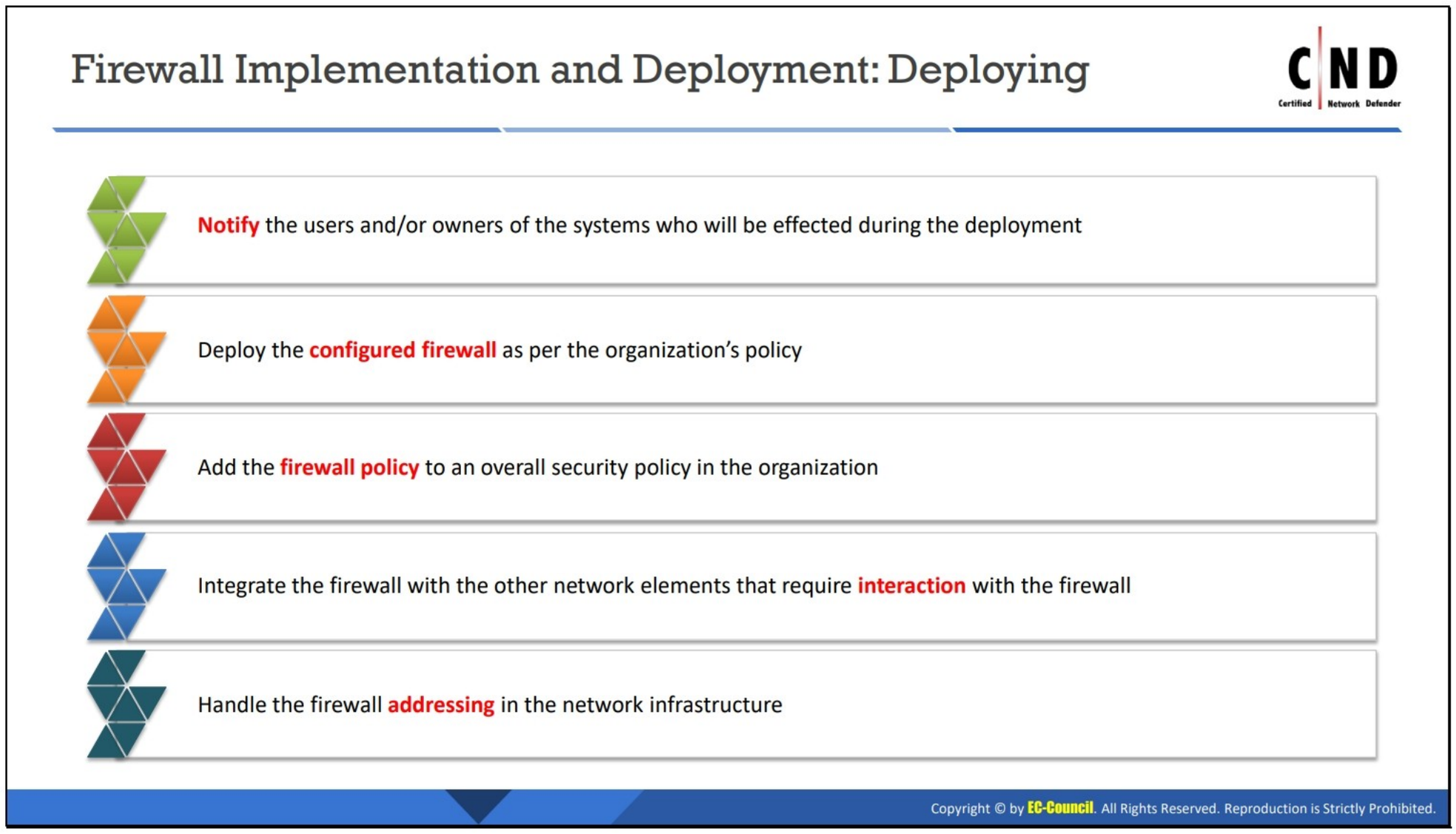
The following are some of the factors that contribute to firewalls not working as per configuration:

- Development of incorrect test cases, which leads to an incorrect prediction of firewall performance
- Incorrect implementation of security policies when designing the firewall rules
- Errors in implementation of the firewall
- Lose of packets in the network
- Buggy test environment
- Faulty hardware components

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

https://t.me/learningnets

Technet24



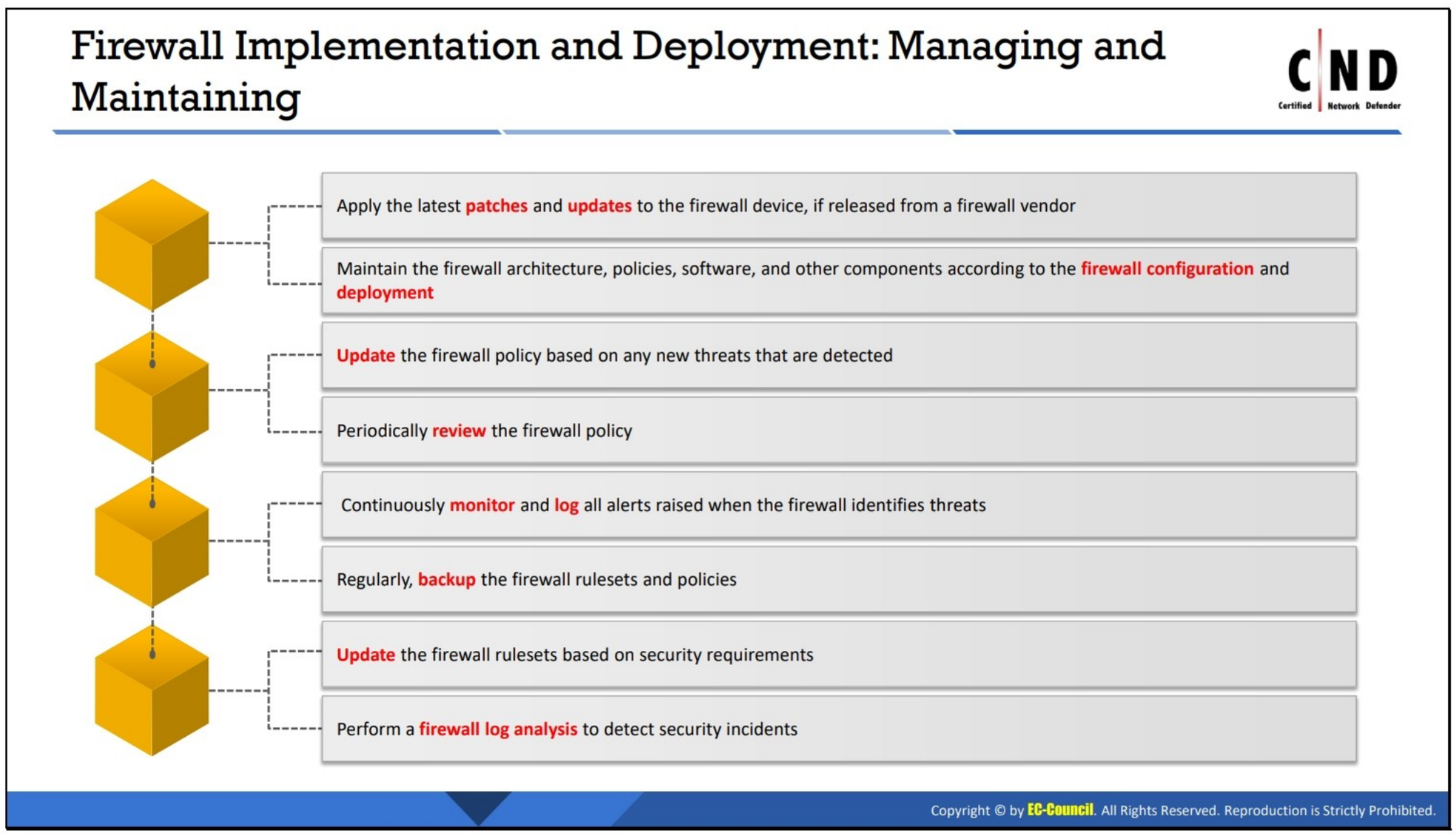
Firewall Implementation and Deployment: Deploying

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.

- Reconfigure the network device on the outside of the network to handle addressing of the firewall. Proper deployment of a firewall facilitates the sending and receiving of traffic from the newly configured firewall system.
- Update all hosts for the new firewall deployment.
- Alert all the users regarding the deployment of a new firewall into their operational environment.
- Finally, allow private traffic through the newly deployed firewall.

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

https://t.me/learningnets



Firewall Implementation and Deployment: 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 regular backups of the firewall policies and rulesets depending on the rule format used by the firewall. Use restrictions offered by firewalls on who can change a ruleset and from which addresses. Review the firewall policy regularly to uncover the following:

- Rules that are not required.
- Adding new rules to the firewall

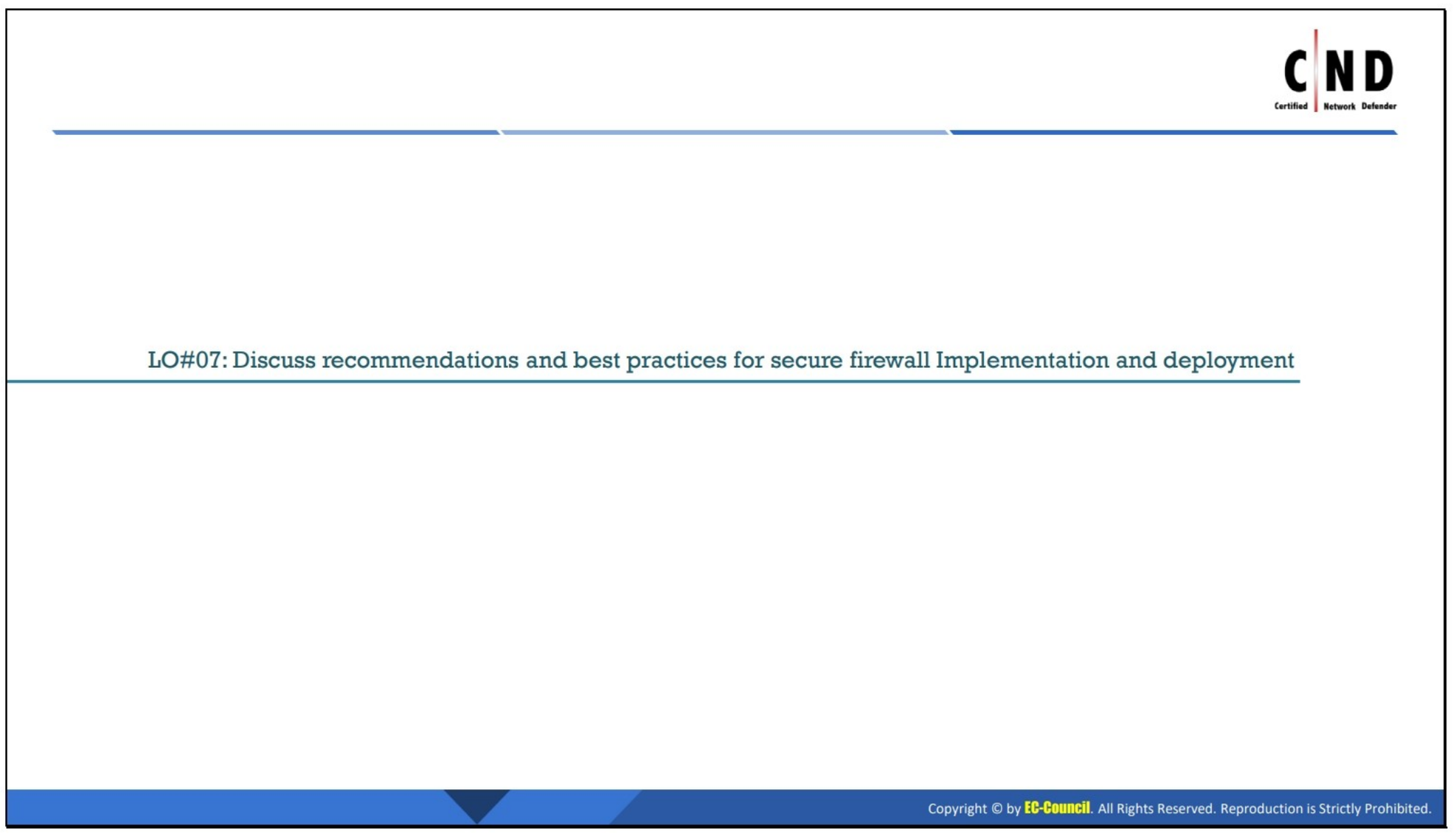
Management and maintenance of a firewall includes the following:

- Extending its life
- Making sure it is operating properly
- Confirming it provides a protective layer to the operational environment
- Improving performance.
- Checking for required updates
- Confirming that the components are working properly

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

https://t.me/learningnets

Technet24



LO#07: Recommendations and Best Practices for Secure Firewall Implementation and Deployment

The objective of this section is to explain the recommendations and best practices for secure firewall implementation and deployment.

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

https://t.me/learningnets

Secure Firewall Implementation: Best Practices

- Filter unused and common **vulnerable** ports
- Configure a **remote syslog server** and apply strict measures to protect it from malicious users
- If possible, create a **unique user ID** to run the firewall services. Rather than running the services using the administrator or root IDs
- Monitor **firewall logs** at regular intervals. Include them in your data retention policy
- Set the firewall ruleset to deny all traffic and enable only the services required
- Immediately investigate all **suspicious log** entries found
- 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.
- Backup the firewall logs on a set **schedule**. Store these backups on a secondary storage device for future reference or for any legal issues arising from an incident
- To enhance the **performance** of the firewall, limit the applications that are running
- Perform **audits** at least once a year on the firewalls. This is done to evaluate the standards implemented in securing an organization's IT resources

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

Secure Firewall Implementation: Best Practices

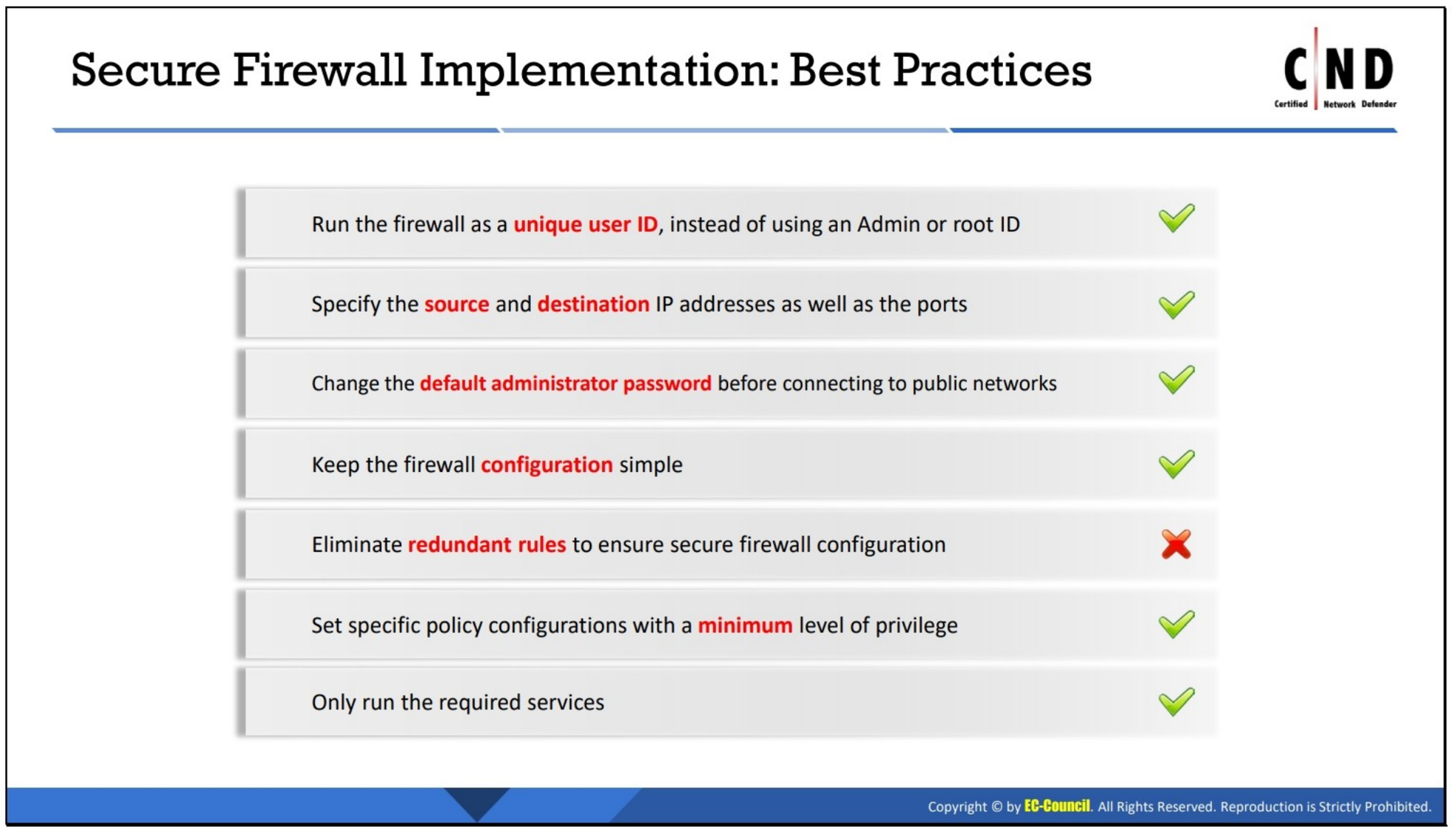
- Clearly define a firewall **change management** plan
- Ensure the implementation passes business and technology-based **risk assessments**
- By default, **disable** all FTP connections to/from the network
- Allow **secure email access** through the firewall
- Catalog and review all **inbound** and **outbound traffic** allowed through the firewall
- Set a default "**deny**" rule for inbound traffic with explicit "**allow**" rules
- Keep firewall rules as **granular** as possible
- Ensure all rules and objects follow standard **naming conventions**
- Prioritize the rules in a proper **logical order**
- For easy management, always **group** similar rules together

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

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

https://t.me/learningnets

Technet24



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.

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

https://t.me/learningnets

- 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.
- 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 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.
- Clearly defining a centralized firewall management plan and a documented process can help prevent unwanted changes to the current configuration of the network. It can limit the chance of a change, opening vulnerabilities in network security.
- The effectiveness of any firewall solution depends on the rules with which it is configured. In general, a firewall is configured to monitor inbound and outbound traffic and to protect

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

https://t.me/learningnets
Technet24

a network in which it is configured. It also monitors the source and type of traffic traversing the network.

- Most organizations use a firewall for protecting the network environment from threats and in tracking the source of a threat. Augmenting a firewall ruleset with an effective logging mechanism makes it an effective security mechanism to protect the network.
- Set a default 'deny' rule for inbound traffic with explicit 'allow' rules. A deny policy at the end of a ruleset ensures that traffic trying to go to the wrong zone is caught. It is essential to cover every possible combination.
- Firewall rules should be appropriately prioritized based on the security requirement of the organization.
- Organizations should consider monitoring employee's email messages through the firewall. They should create a separate email network zone that is firewalled from both the DMZ and the internal network. Then place both the email and the webmail servers in that zone. This enables the organization to allow secure email access through the firewall.
- Manage the lifecycle of a firewall rule policy by enforcing an expiration date. This will help clean up newly created temporary rules for new services. When an expiration date is set for a rule, it is either deleted after its lifetime or it can be extended (if needed).
- Always test the firewall policies before implementing them in the network. Testing a firewall can discover unexpected implementation errors by assessing firewall performance, network traffic, and other devices. These details provide a view of how the proposed changes in the firewall configuration will affect the environment.
- Auditing firewall security policies ensures the firewall rules implemented are according to the security regulations of an organization. It is your responsibility to perform firewall security audits to identify policy violation activities.
- The organization needs to ensure they upgrade their firewall to the latest patches and updates released by the firewall's vendor. Any delay in upgrading to the latest version can affect the security of the network. Upgrading to the latest firewall version minimizes the chances of a vulnerability in the network. It is also possible to conduct vulnerability assessments on the firewall, enabling easy assessment of the flaws and weaknesses.
- Ensure the removal of firewall rule base regularly as it improves firewall security, firewall performance, and efficiency. Cleaning the firewall rule base also prevents security and management issues.
- Restrict unauthorized access to prevent any modification in the firewall configuration. Organizations can implement access permissions that will only permit authorized users to make changes to the firewall configuration.
- Most organizations implement firewalls from different vendors. The firewall configuration architecture differs from one organization to another. The organization needs to ensure that only skilled personnel are looking after the firewall administration and maintenance.

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

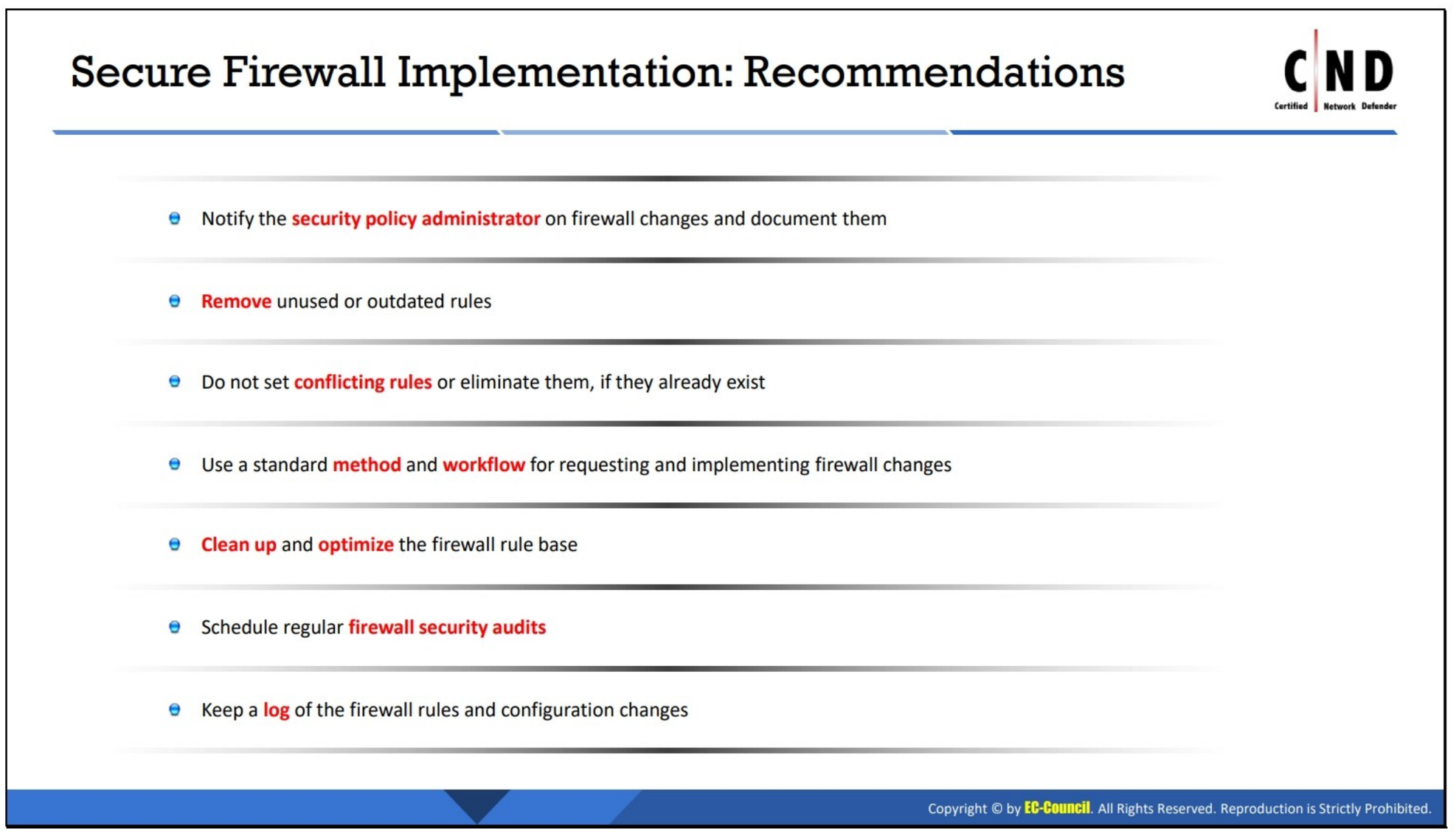
https://t.me/learningnets

- Always filter packets for the correct source and destination address in order to prevent attackers from accessing the network.
- Always make sure to change the passwords regularly, at least every six months.
- Configuration of the firewall should be kept simple and should meet company requirements. Periodic review of the firewall configuration helps maintain firewall security.
- Always provide minimal access to the firewall in order to avoid any security incidents.

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

https://t.me/learningnets

Technet24

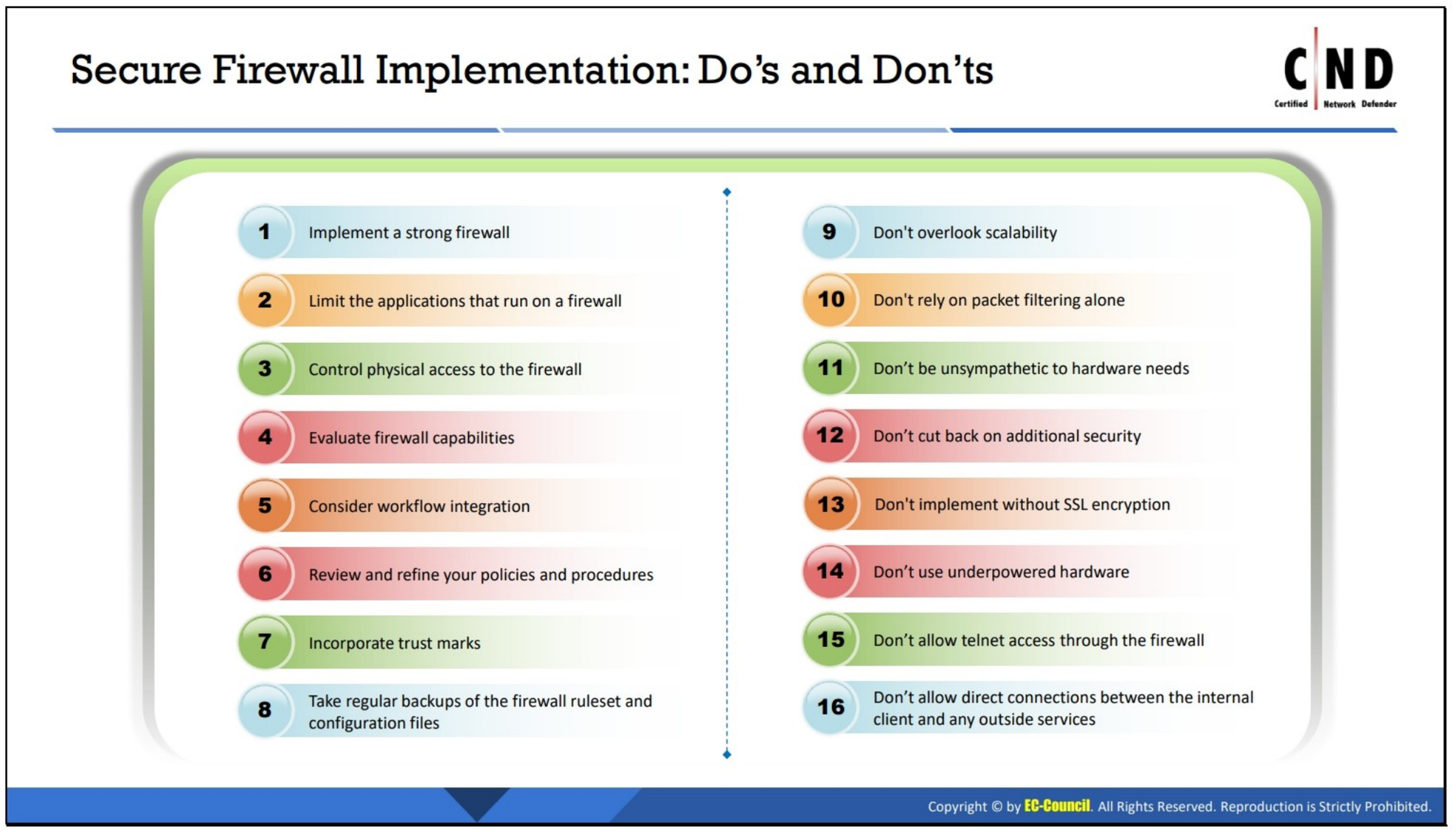


Secure Firewall Implementation: Recommendations

- 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 network defender is unable to understand.
- 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.

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

https://t.me/learningnets



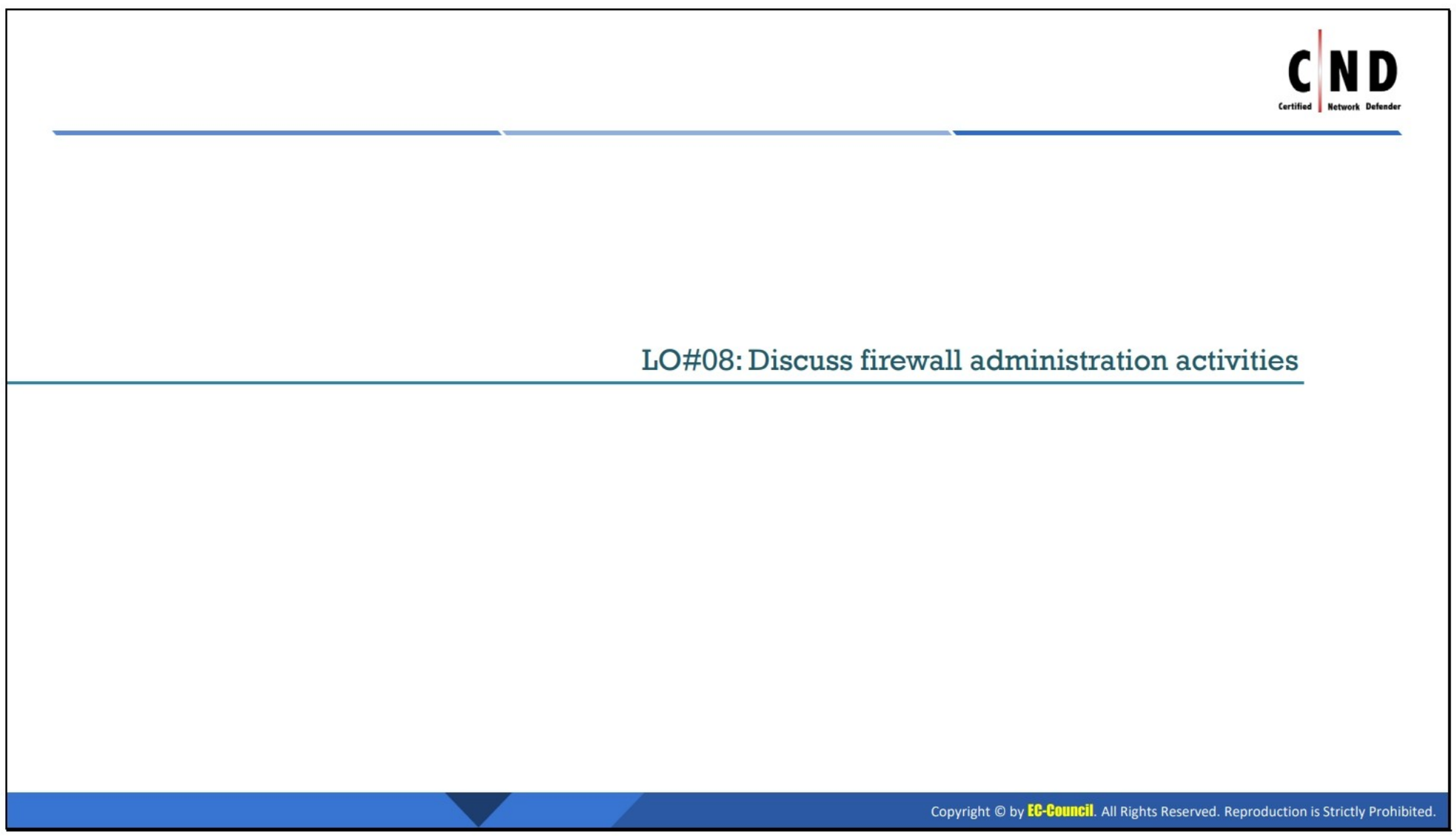
Secure Firewall Implementation: Do's and Don'ts

- A firewall should include intrusion prevention and detection capabilities to guard against denial of service (DDoS) attacks. The consequences of not having these measures in place will be severe if a DDoS incident occurs in future.
- While implementing a firewall do not overlook scalability. Most firewall vendors claim they can scale up to thousands of devices. Determine what that actually means in terms of management and the ability to perform under stress.
- After choosing a firewall that meets the business requirements of an organization, test the firewall on a live production environment. The organization should determine the network requirements and evaluate the product capabilities accordingly. The test should determine whether the selected solution actually performs as expected.
- Installation of proxy servers assures security as it provides access only to selective users.
- When implementing a firewall solution, organizations need to focus on the hardware required for the implementation. Refrain from buying more technology. First, make sure that what is currently available works for the organization and improves its security.
- The idea behind a workflow in firewall management is a natural extension of change management functionality. Manage the change process to ensure only the correct rules are created. Most vendors offer complimentary workflow products to integrate their core capabilities with workflow tools of change management. This may not be important if your organization has a well-defined process and supporting tools already in place.

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

https://t.me/learningnets

Technet24



LO#08: Firewall Administration Activities

The objective of this section is to explain the various administrative activities required for managing and maintaining firewall security.

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

https://t.me/learningnets

Firewall Administration

Accessing Firewall Platform

- Threats to firewalls arise from exploiting **remote management resources** such as the graphical management interface
- **Control access** to the firewall management using encryption, strong authentication, and limiting access through the IP address

Build Operating System Platform for Firewall

- Implement the firewalls on systems tailored to specifically **strong security applications**; e.g., Bastion host
- Patch and remove any unnecessary **features** and **services** before implementing the firewall on the platform

Firewall Failover Strategies

- Use failover services like **heartbeat-based** services in case of primary firewall service failure
- A heartbeat mechanism initiates the backup systems when a failover event **triggers**. It includes the back-end/customized network interfaces

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

Firewall Administration (Cont'd)

Firewall Logging

- By default, all firewalls have a method for **logging capabilities**
- Use a **centralized logging service** such as a UNIX syslog application which also provides log examination and parsing

Firewall Backups

- Use **full backups** instead of incremental backups

Security Incidents

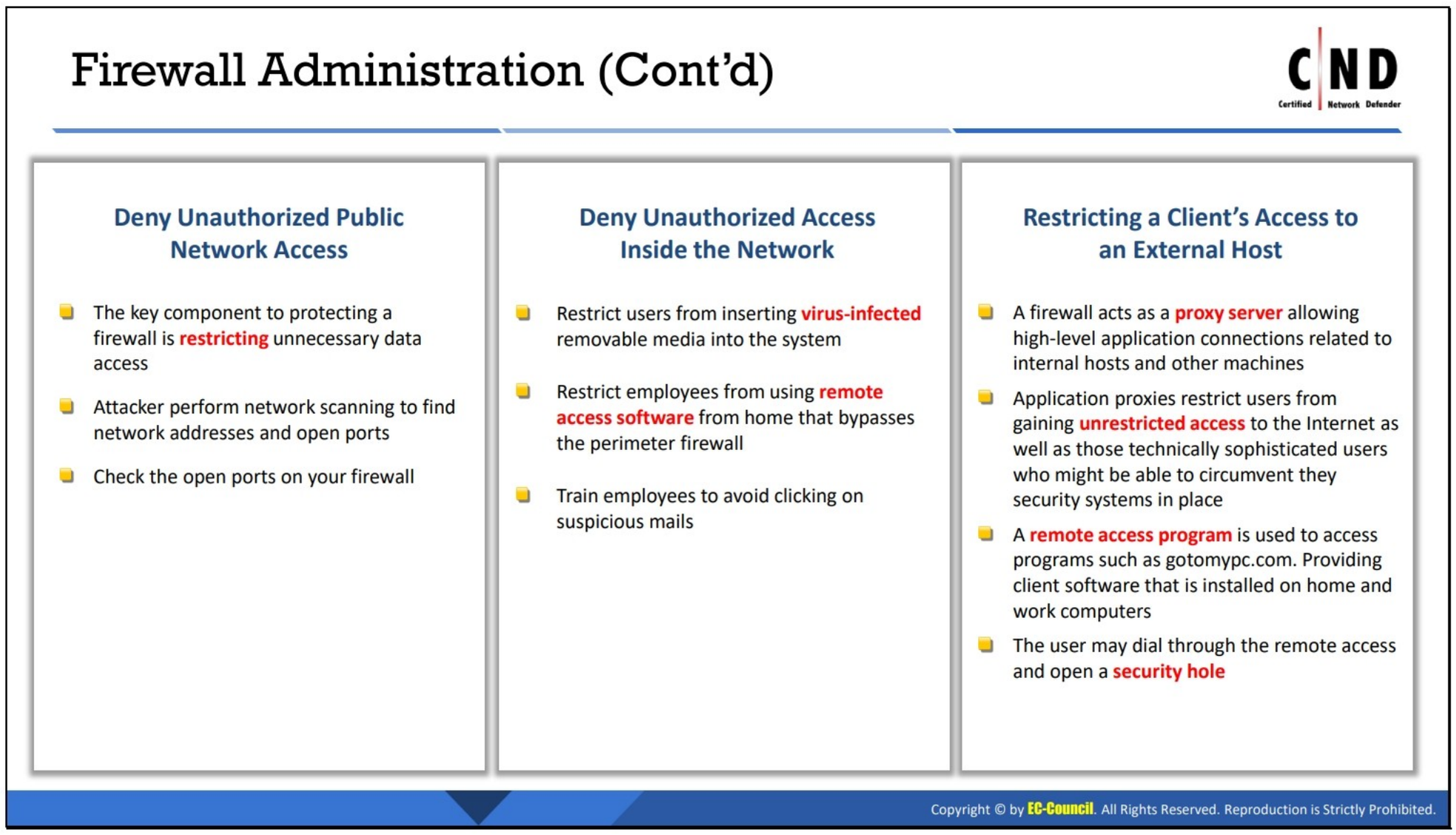
- Firewalls play a critical role in **security incidents**. They correlate all the events which have passed through it, especially where network attacks are concerned
- Synchronize the firewall with **network time protocol** (NTP) to effectively correlate the incident events

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

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

https://t.me/learningnets

Technet24



Firewall Administration

Firewall administration is the process of maintaining security by managing firewall devices and/or software. It includes access to the firewall platform, operating system builds, firewall failover strategies, firewall logging functionality, security incidents, firewall backups, etc.

Firewall administration includes the modification of security policies, assessment of vulnerabilities, identification, detection of new threats, and development of counter measures to combat them. Monitor firewall activities regularly to ensure proper functionality to prevent the network from attacks.

Firewall Administration Activities:

- Access to the firewall platform/accessing firewall platform: Threats to firewalls arise from exploiting remote management resources such as the graphical management interface or an operating system console. To prevent unauthorized access to these resources, manage the firewall using encryption and strong user authentication techniques. The graphic management interface uses secure socket layer (SSL) which relies on the hypertext transfer protocol (HTTP) for secure communication over the network.

  Under an internal individual authentication process, the user should have a unique user ID and password to gain access to the interface. Some firewalls also support token-based authentication to grant access to centralized servers using remote authentication dial-in user service (RADIUS).

- Build an operating system platform for a firewall: Platform consistency plays a vital role in successful implementation of a firewall such as an OS with hardened security features for the applications. Do not install a firewall on systems that offer all possible installation options, especially after removing unnecessary OS features. Firewall installations should

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

https://t.me/learningnets

not affect the functioning of the OS. Install all security patches on the OS before installing the firewall. Unused network services, network protocols, applications, and user accounts must be disabled.

- Firewall failover strategies: Failover strategies are required to balance the security of the network when a firewall failure occurs. Failover strategies such as heartbeat-based services help balance the firewall failover by shifting all the inbound and outbound traffic to the backup firewall. They reduce the chances of a network failure. Both primary and backup firewalls are kept behind a single MAC address to provide seamless functionality.
- Firewall logging: Manage, examine, and parse all firewall logs. Various operating systems such as Windows, UNIX, and Linux variants support firewall logging. The firewall preserves these logs on the centralized server for maximum security and uses only few software packages to examine them. A firewall that does not support a syslog interface will have their own internal logging functionality.
- Firewall backups: All firewall backups should be "day zero" or full backups instead of incremental backups immediately before the production release. Because firewall access control does not permit a centralized backup scheme, firewalls have in-built backup facilities.

  It is desirable to have all critical file systems backed up to external devices in Windows operating systems. In UNIX the /var file system directory and sub directories require write access and contain all the system logs and spool directories.
- Security incidents: In case of a security incident, temporarily disable remote access to the resources and revoke user authentication until the situation comes under control.

  In a minor security incident, the attacker can use basic network probes. Due to its lower severity, many companies do not treat these incidents as threats. In medium security incidents, the attacker tries to get unauthorized access to the resources or the system.

  A high-end incident describes a situation, where an attacker is successful in obtaining access to the system. Such incidents usually restrict resource availability.

  A firewall uses an event-correlation technique, which works based on the time synchronization rolling back the state of the firewall to a unique state in order to reconstruct the phases of the incident.
- System administration: Proper system administration also contributes to firewall administration, as described below.
  - Standardize the OSes and make them ready for updates and fixes
  - Centralized system administration, which contributes to better firewall security
  - Examine the communication path between the firewall and the system in order to uncover any errors or faults in the configuration
  - Decide on the type of firewall that is best suited for the organization

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

https://t.me/learningnets

Technet24

Deny Unauthorized Public Network Access

Weak network access controls increase the chances of unauthorized public network access. This leads to the manipulation of data, services, and DoS attacks. Proper controls such as user access restrictions and security controls for granting permissions can limit unauthorized public network access.

Organizations should use SSL and HTTPS protocol services while accessing corporate resources using public networks, which will ensure consistency with firewall policy as these protocols pass only encrypted information.

To prevent unauthorized public network access, scan the network regularly for open ports and disable them to ensure proper utilization of any remotely accessible resources. Utilities such as Nmap can help discover open ports.

Deny Unauthorized Access Inside the Network

Restriction of unauthorized access from inside the network prevents the user from running malicious programs, installation of suspected software, etc.

Necessary security measures to prevent unauthorized access inside the network are:

- Prohibit users from installing plug-and-play devices such as flash drives, which may be virus-infected and when executed can corrupt the data present in the host system or network.
- Restrict employees from using remotely available corporate resources from public networks such as an internet cafés or free public Wi-Fi (e.g., hotels), which bypasses the perimeter of the firewall.
- Educate employees on the topic of social engineering, which is an attack involving hackers who build confidence with the unsuspecting user to trick them into collecting personal information such as user credentials, server information, IP addresses, etc. which is then used to perform network attacks against an organization.
- Firewall instructions should be provided by well-trained firewall administrators enabling users to configure their firewall to filter IP packets for detection of unauthorized packets.
- Emails containing viruses can spread through all the computers on a network when the user attempts to open the mail. Using an updated internet security solution can prevent such email attacks.
- Provide access only to required documents and files.
- Account rights should be carefully structured in order to facilitate proper data access.
- Proper training to users can prevent unauthorized access inside an internal network. While there are limits to this strategy, educating users has many threat prevention benefits.

Restricting a Client's Access to an External Host

A client should not have direct access to an external host, which could make it vulnerable to threats. Therefore, all clients should access the host through the firewall. The firewall would act as a proxy server allowing high-level application connections related to internal hosts and other

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

https://t.me/learningnets

machines. A single firewall acts as both packet filtering at the application level and a proxy server at the domain level. Application proxies restrict users from gaining unrestricted access to the Internet. However, technically sophisticated users might be able to circumvent the security systems altogether.

Vulnerable external hosts gather sensitive information from clients such as IP addresses, types of security, level of security, server locations, and remote access credentials. Remote access to programs can be useful (such as gotomypc.com) for providing remote access to work systems, but there are many risks associated with such tools due to techniques such as password sniffing, packet stealing, and IP spoofing.

The user might dial through the remote access to connect with an illicit server and application, which can open a security hole.

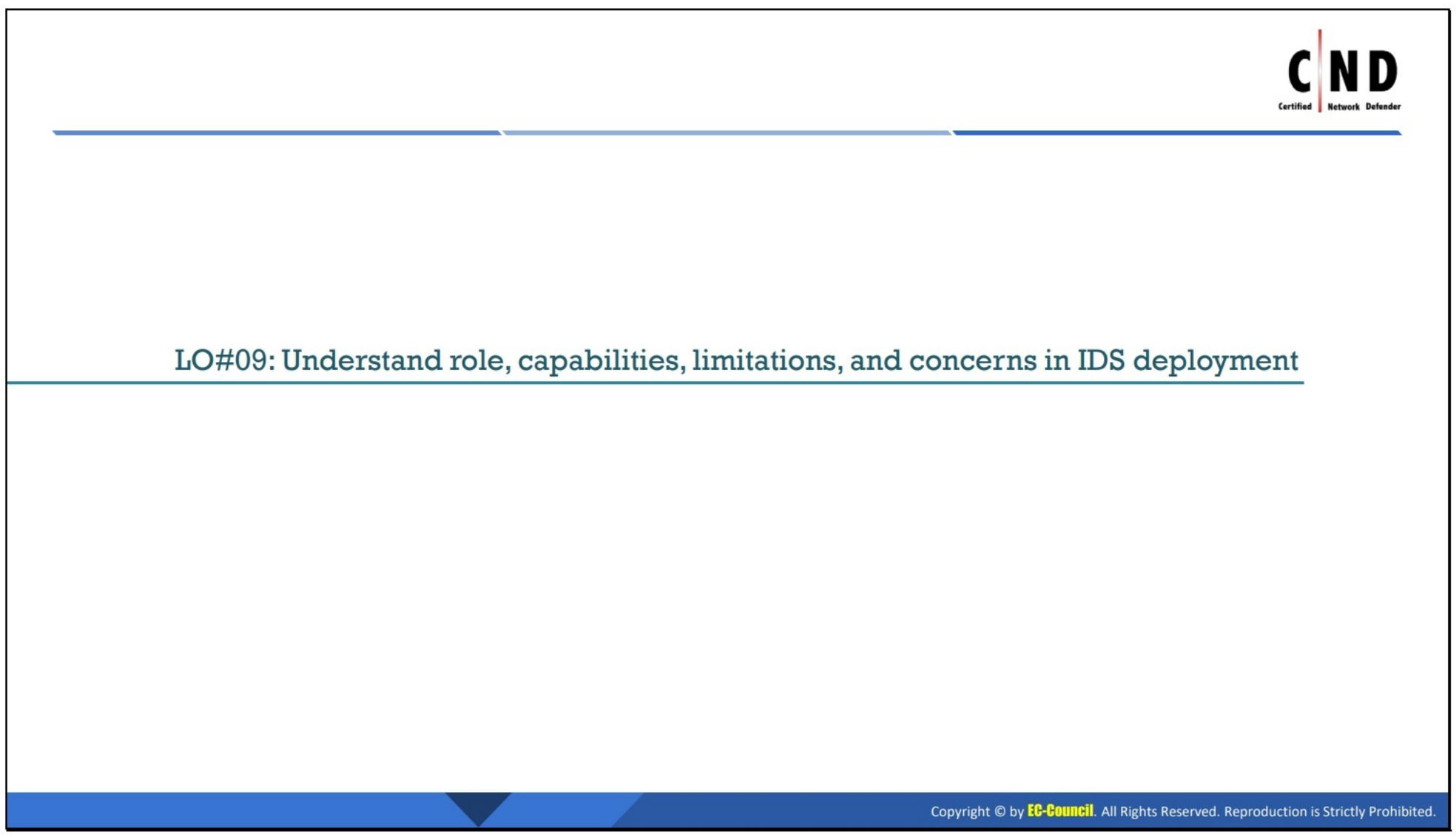
It is possible to restrict authorized access to areas by employing the following policies:

- Allow only internal IP addresses to pass through the firewall.
- Block traffic containing private addresses.
- Block all outbound traffic from VLAN workgroups.
- Block broadcast traffic and all traffic from servers that require no connectivity with any of the external networks.

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

https://t.me/learningnets

Technet24

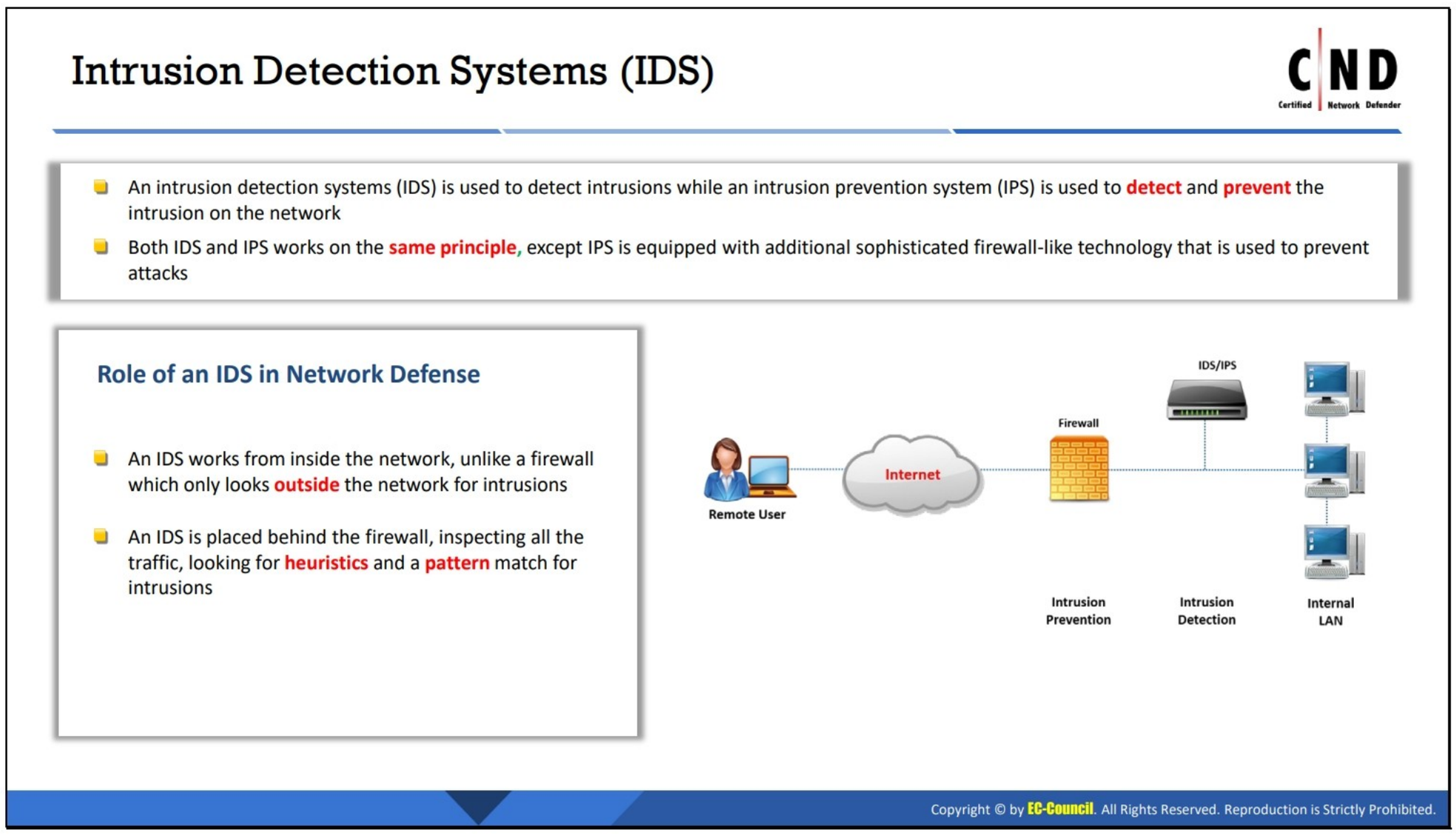


LO#09: Understand Role, Capabilities, Limitations, and Concerns in IDS Deployment

The objective of this section is to explain the role, capabilities, limitations, and concerns in implementing IDS security.

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

https://t.me/learningnets



Intrusion Detection Systems (IDS)

Intrusion detection systems (IDS) are network security devices used to monitor and detect malicious activity in a private network. Intrusion prevention systems (IPS) are considered as extensions of IDS. Unlike IDS though, IPS is placed inline and detects the incident as well as blocks it from getting into the network.

An IDS identifies and alerts regarding an intrusion attempt. However, besides these activities, an IPS can detect and stop the intrusion attempt. IPS systems can also correct cyclic redundancy check (CRC) errors, defragment packet streams, detect TCP sequencing issues, and manage the options in the transport and network layers.

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.

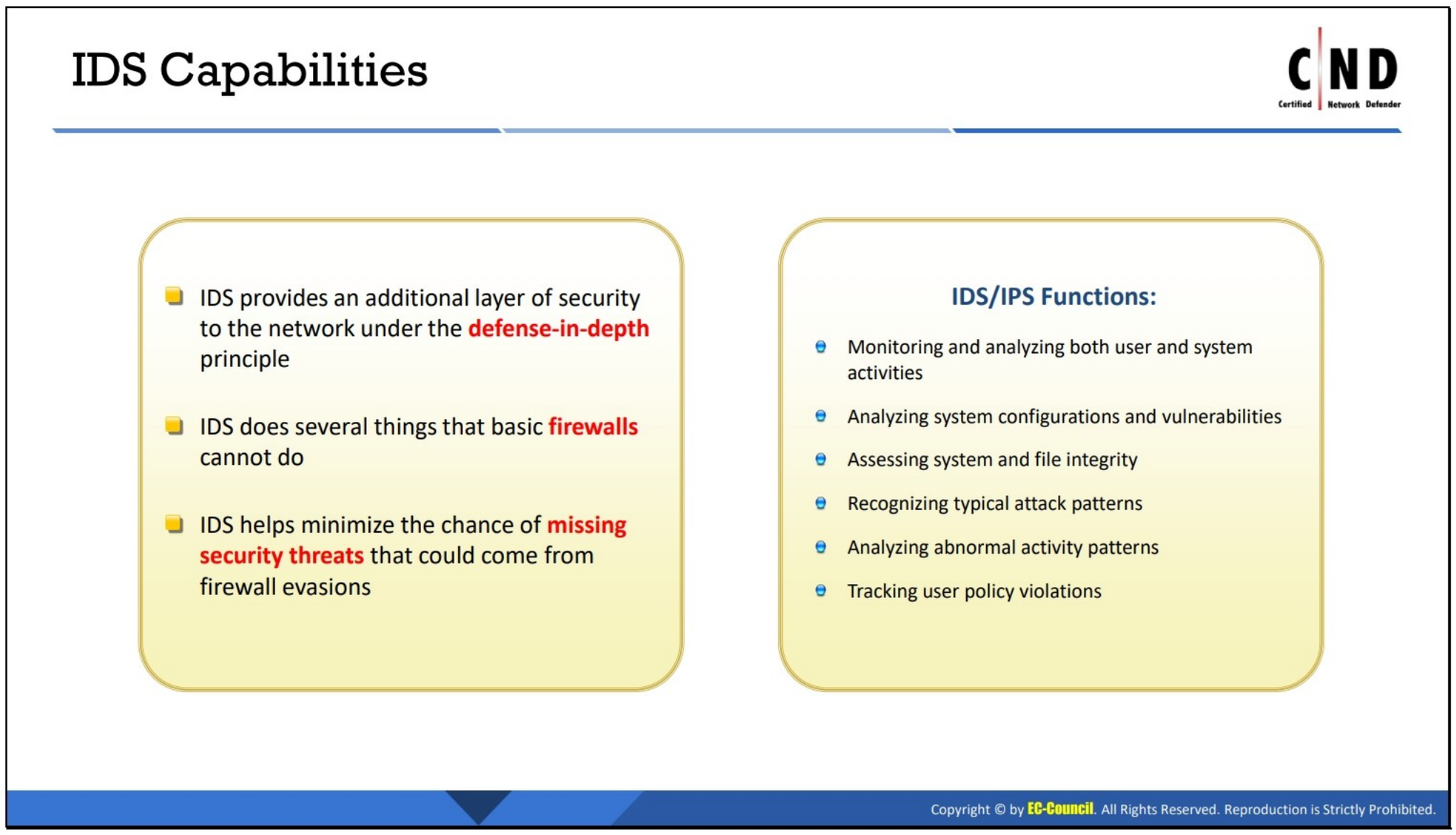
As an example, a firewall can be configured to pass traffic solely to port 80 of the Web server and to port 25 of the email server but it will not inspect the nature of the traffic flowing through either of these ports.

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 network defenders.

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

https://t.me/learningnets

Technet24



IDS Capabilities

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 network defenders 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.

An IDS works by gathering information about illicit attempts made to compromise security and then verifying them. It also records the event data and network defender can use this data to take future preventive measures and make improvements to network security.

In addition to its core functionality of identifying and analyzing intrusions, an IDS can perform the following types of activities related to intrusion detection:

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

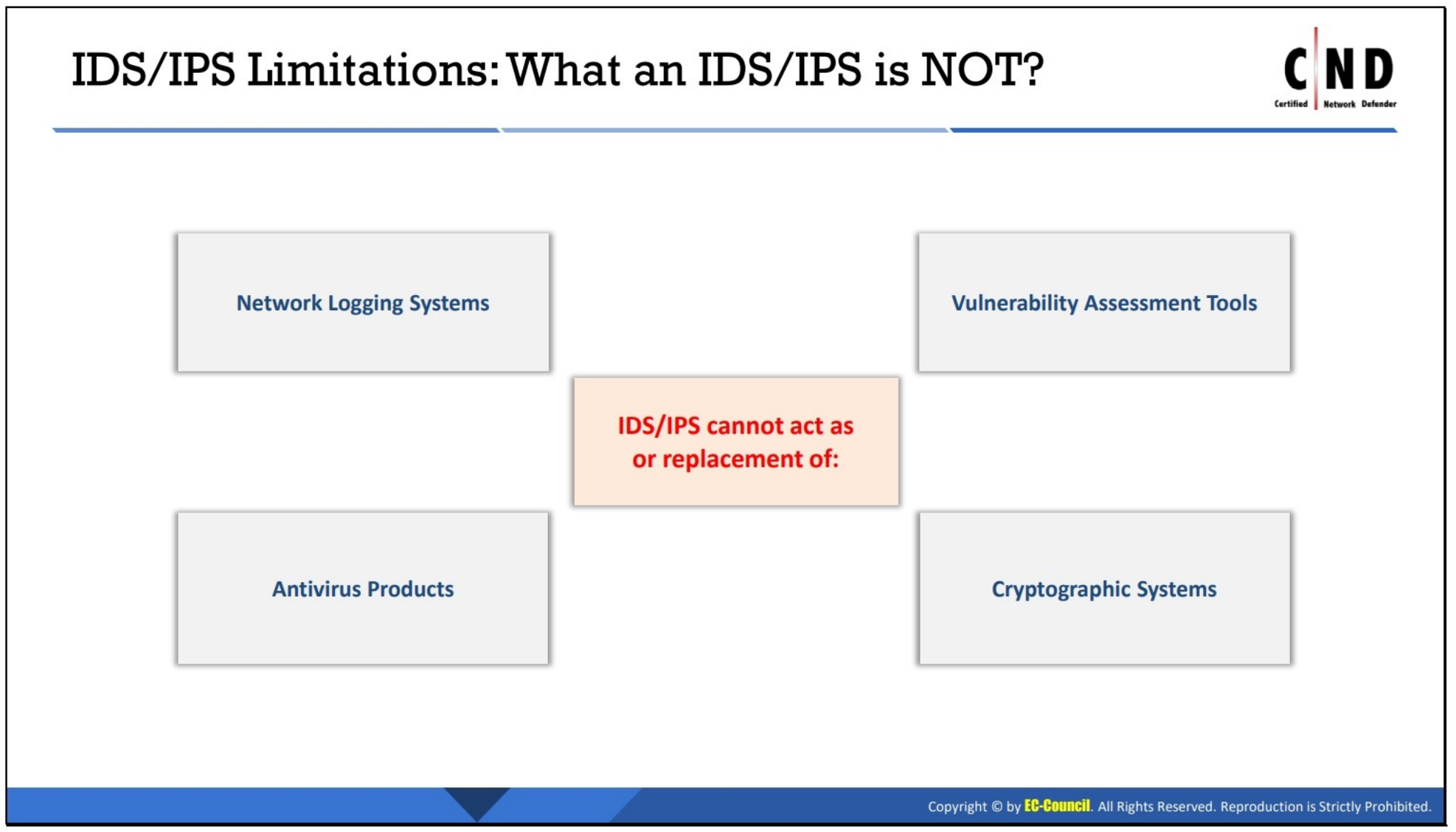
https://t.me/learningnets

- 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 network defender 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.

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

https://t.me/learningnets

Technet24



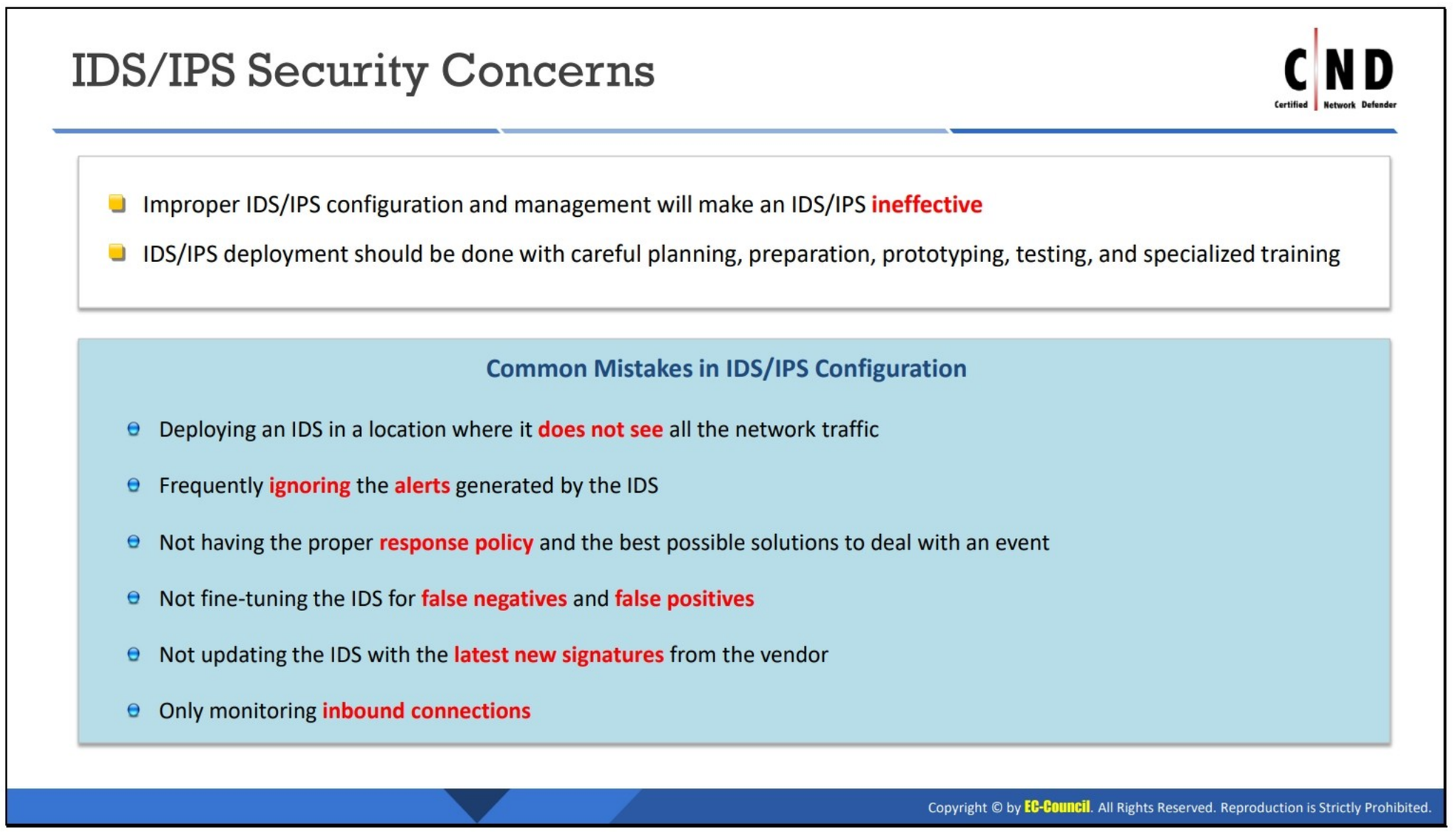
IDS/IPS Limitations: What an IDS/IPS is NOT?

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 are 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.

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

https://t.me/learningnets



IDS/IPS Security Concerns

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 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.

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

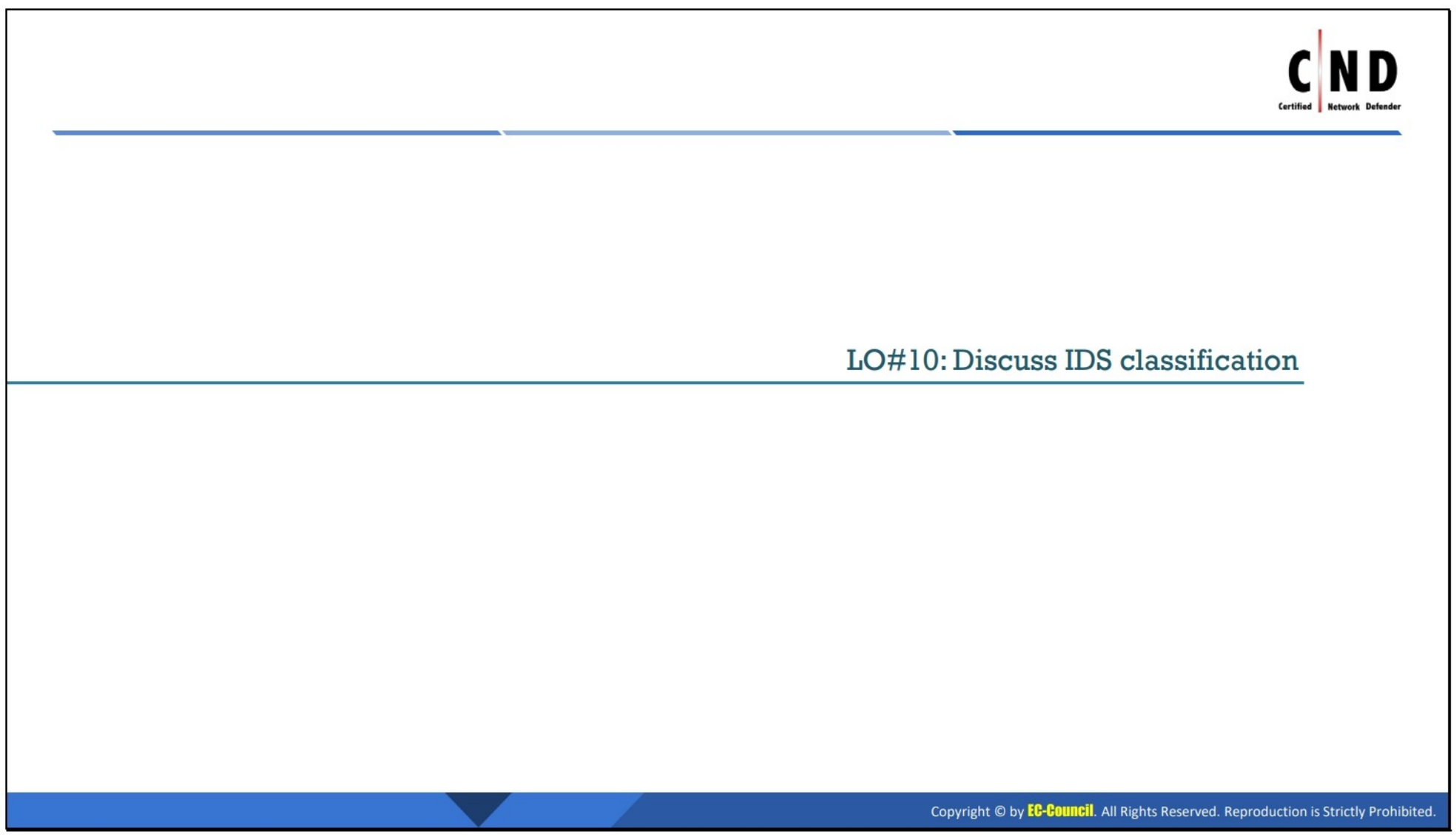
https://t.me/learningnets

Technet24

- 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.

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

https://t.me/learningnets



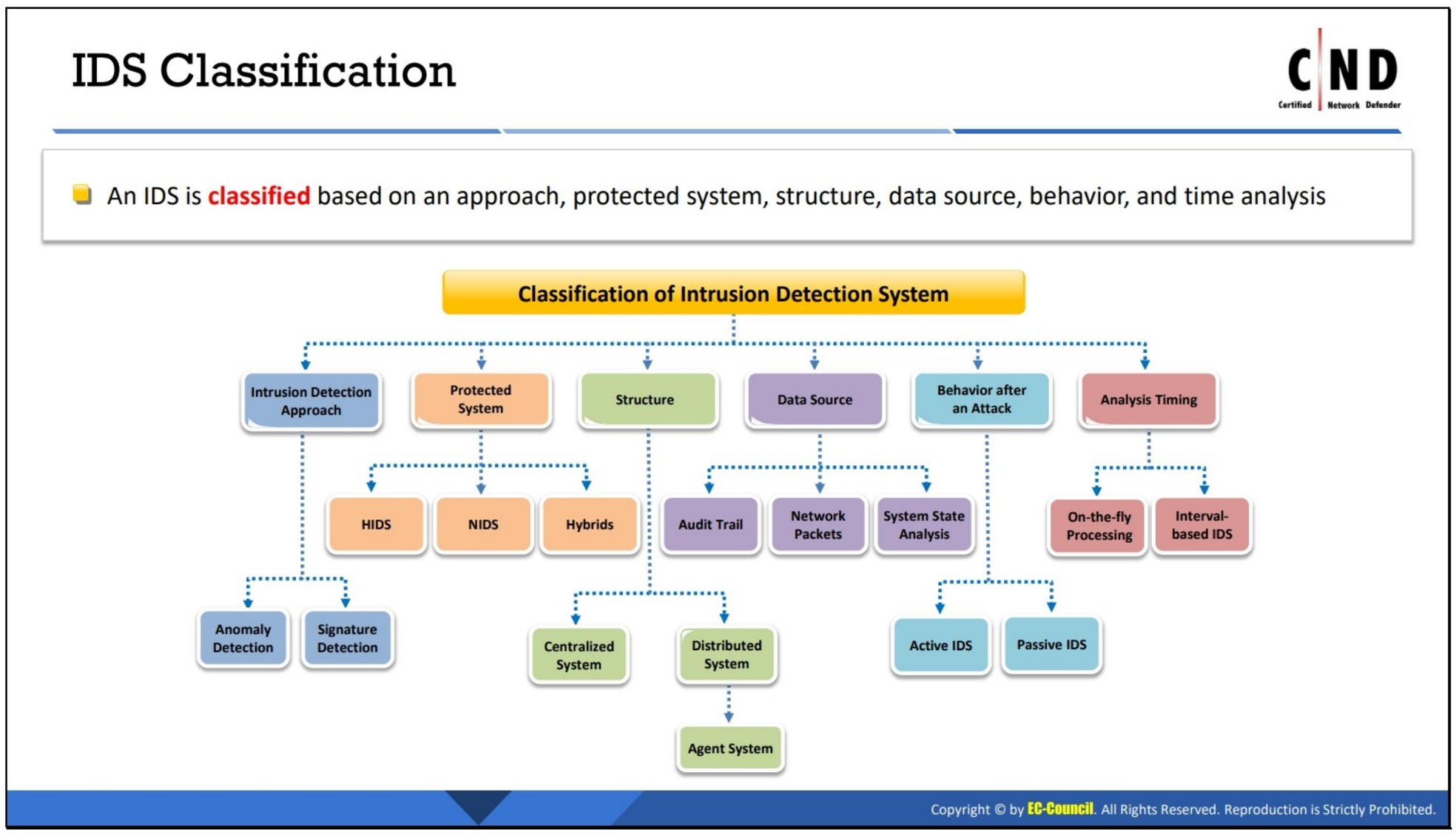
LO#10: IDS Classification

The objective of this section is to describe the different types of IDS/IPS and their working.

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

https://t.me/learningnets

Technet24



IDS Classification

Generally, an IDS uses anomaly-based detection and signature-based detection methods to detect intrusions. 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.

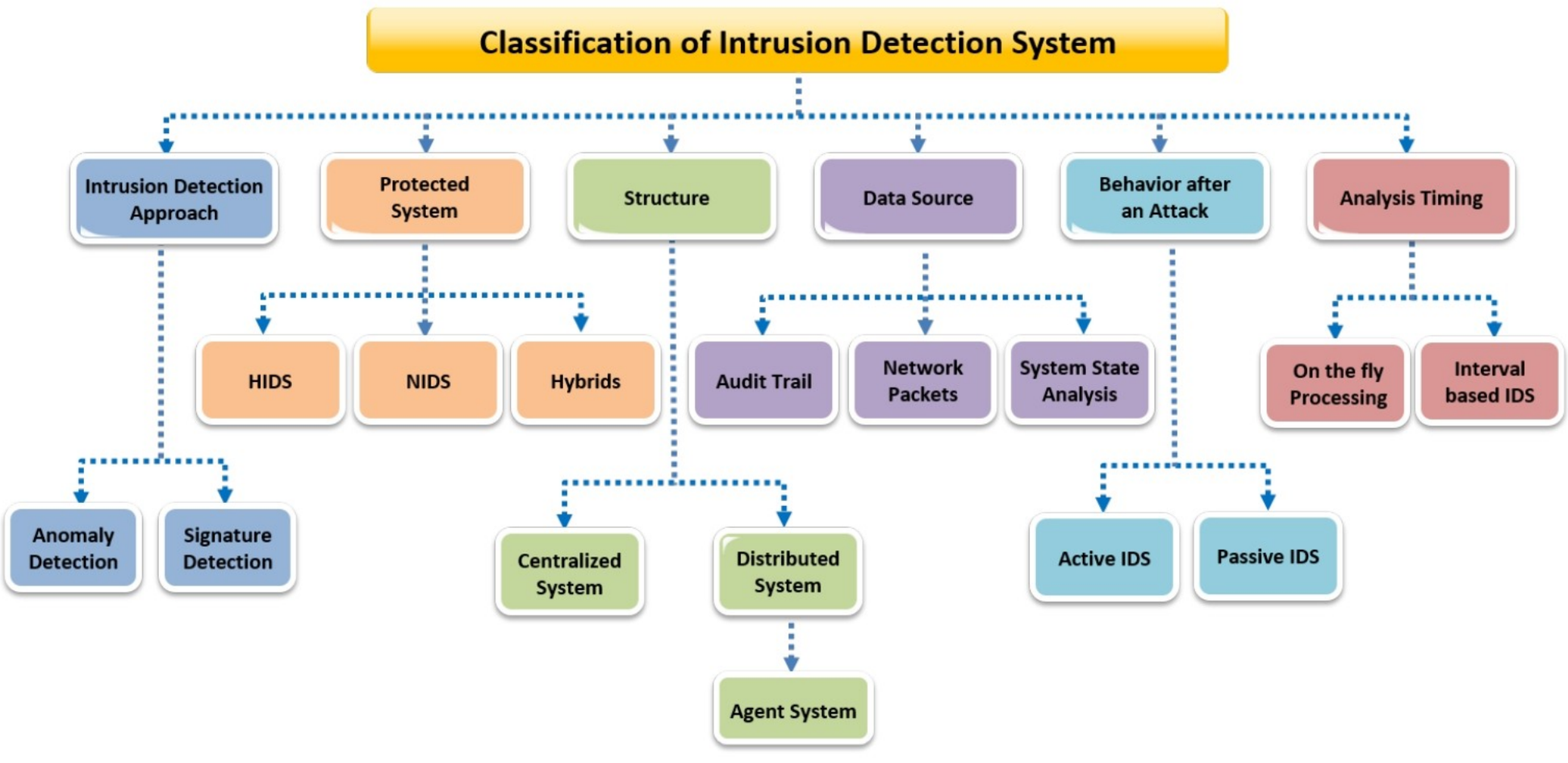


Figure 4.3: Classification of Intrusion Detection System

Certified Network Defender 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

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

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

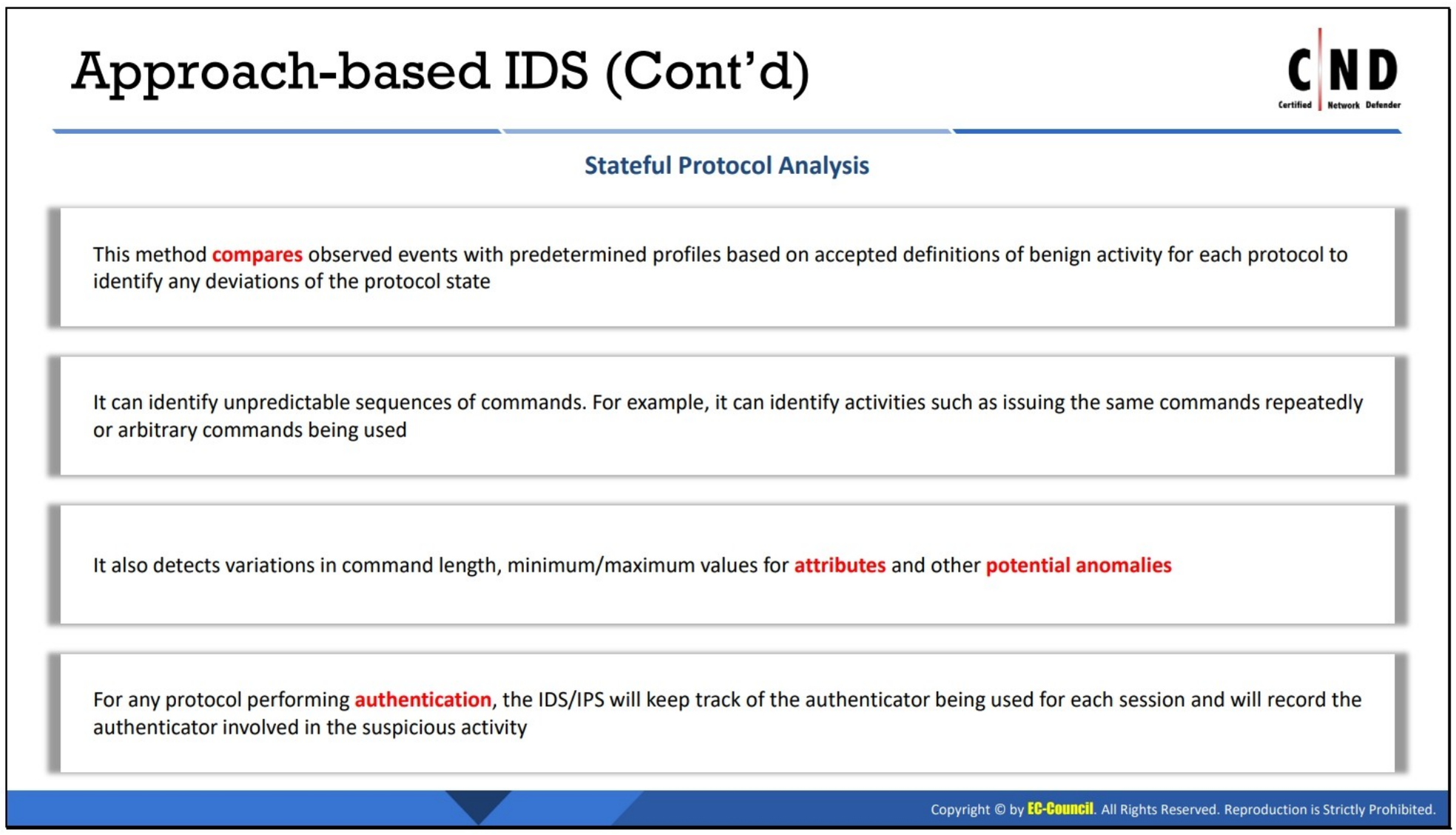
- The rate of generating **false alarms** is high due to unpredictable behavior of users and networks
- The need to create an **extensive set of system events** in order to characterize normal behavior patterns

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

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

https://t.me/learningnets

Technet24



Approach-based IDS

Signature-based Detection

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 in to the 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. 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.

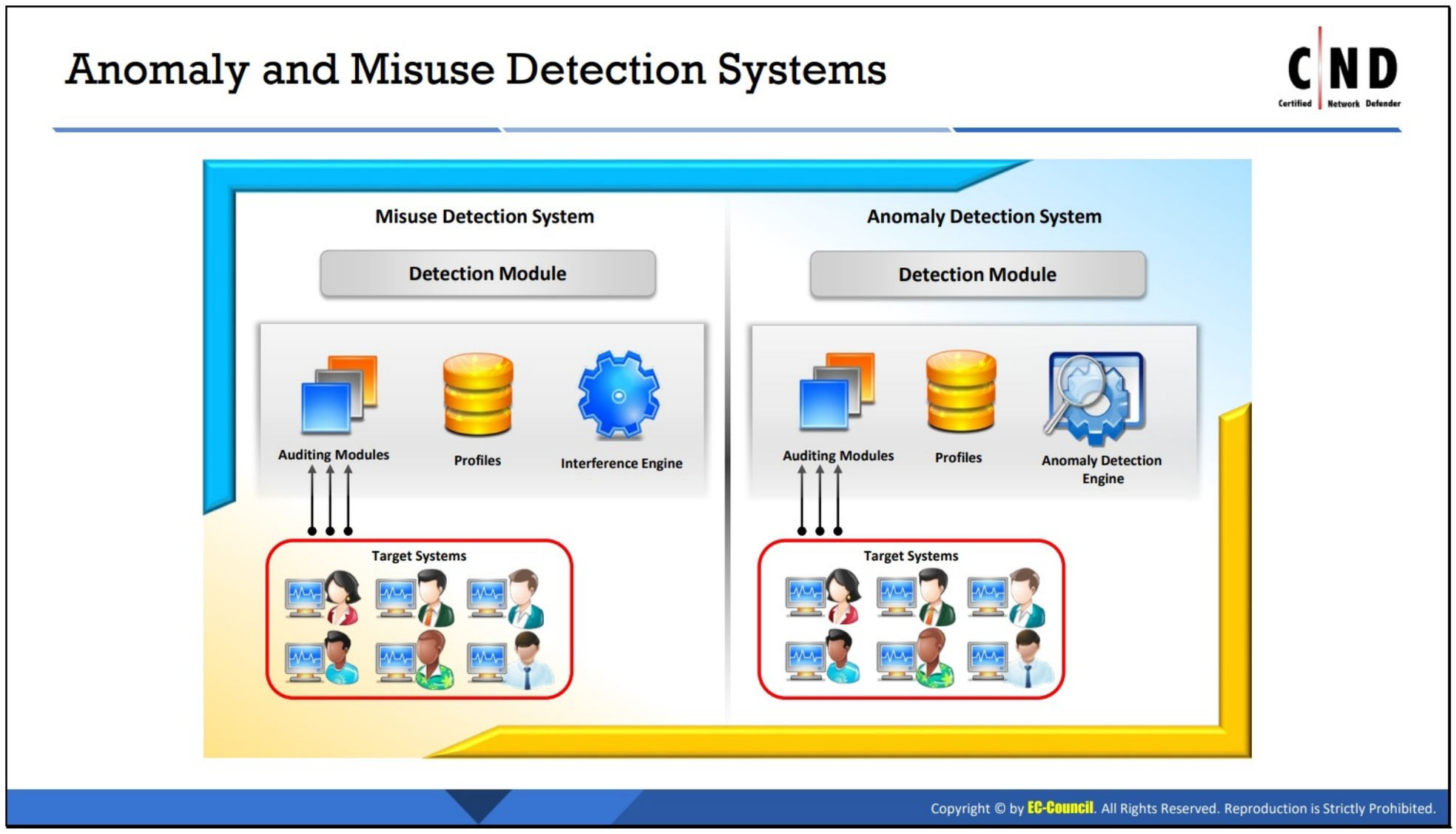
Stateful Protocol Analysis

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.

Certain IDSs can specify suitable activities for each class of users in accordance with the authenticator information.

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

https://t.me/learningnets



Anomaly and Misuse Detection Systems

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.

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.

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

https://t.me/learningnets

Technet24

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.

Advantages

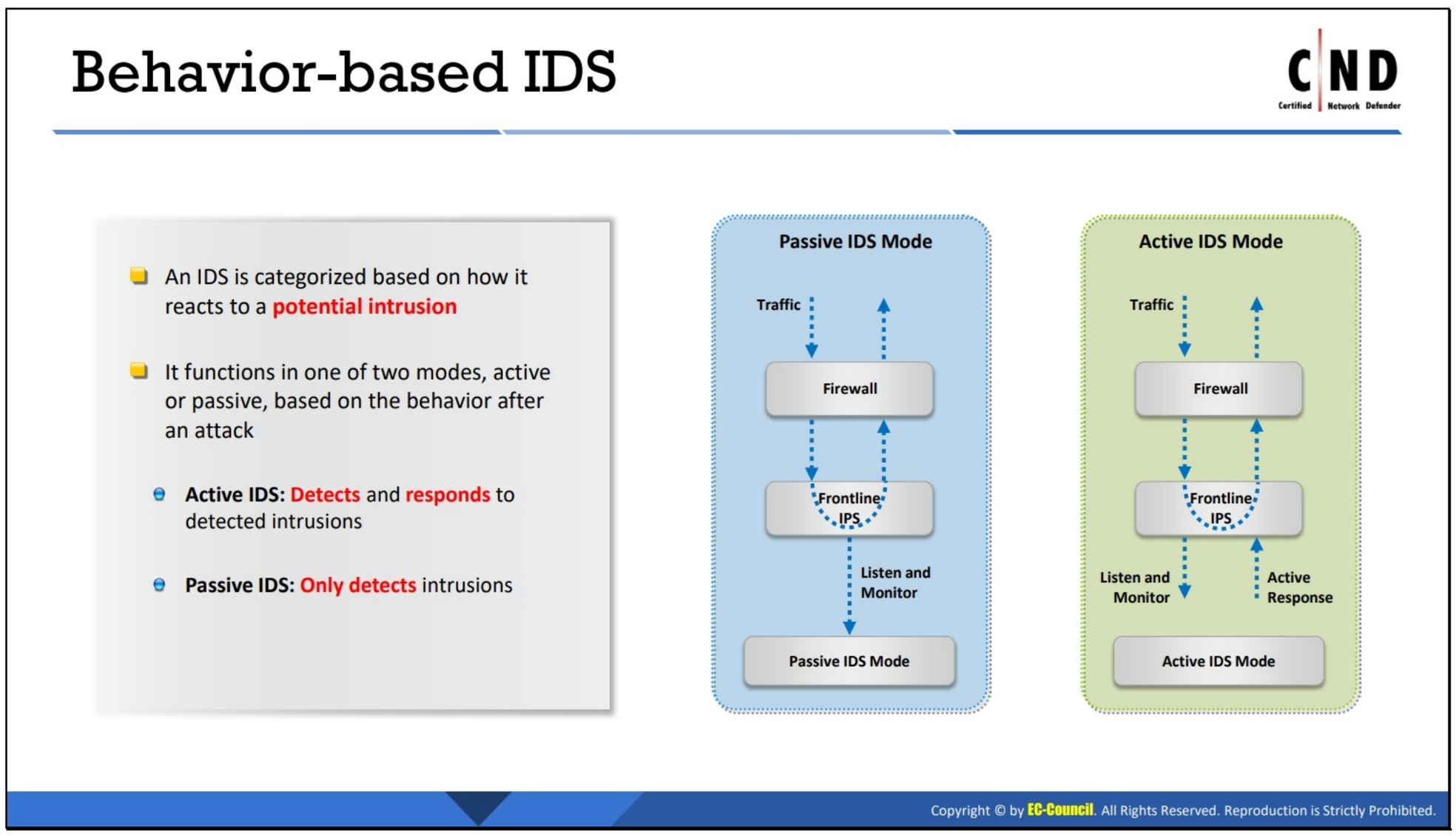
- More accurate detection than an anomaly detection system
- Fewer false alarms

Disadvantage

- Unable to detect new attacks due to predefined rules

Certified Network Defender 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. In terms of behavior, IDSs are classified into two types: active and passive.

Active IDS

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.

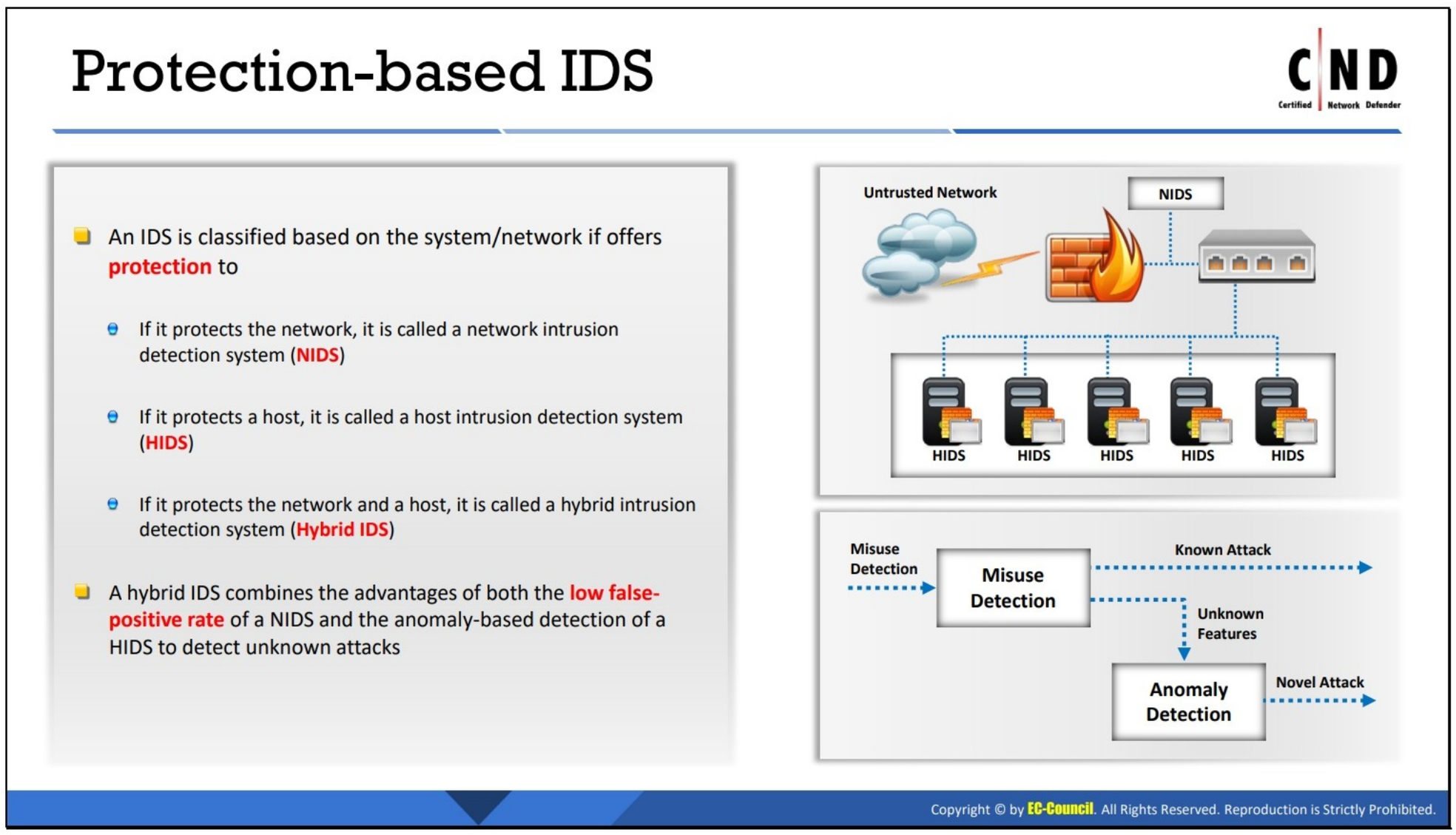
Passive IDS

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.

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

https://t.me/learningnets

Technet24



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).

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 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.

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

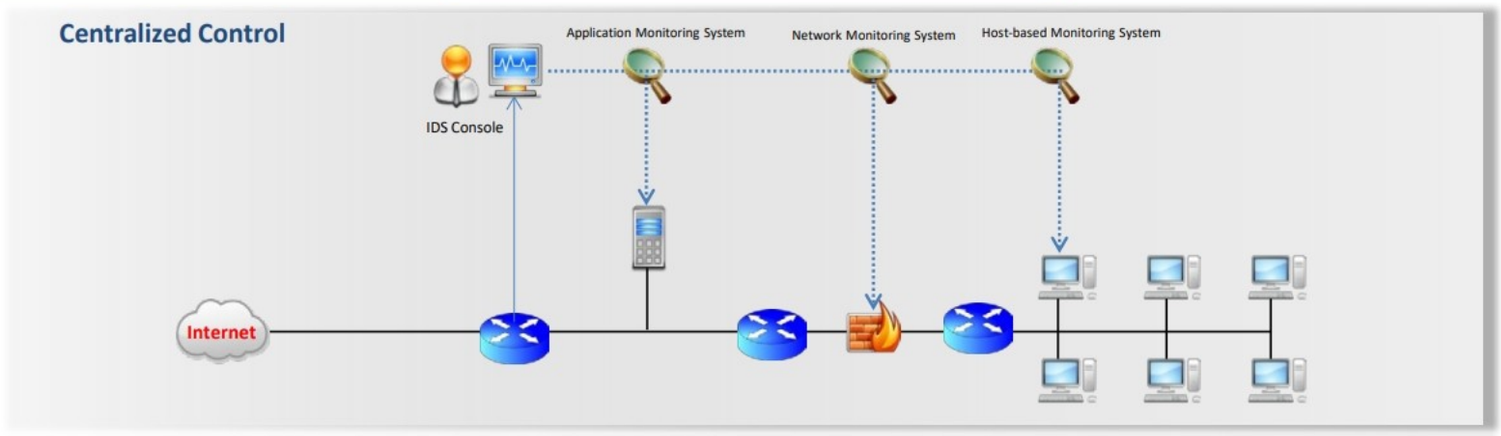
https://t.me/learningnets

Structure-based IDS

1. An IDS is also classified as a **centralized IDS** or a **distributed IDS**, this classification is based on the structure of the IDS
2. In a centralized IDS, all data is shipped to a **central location** for analysis, independent of the number of hosts that are monitored
3. In a distributed IDS, **several IDS** are deployed over a large network and each IDS communicates with each other for traffic analysis

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

Structure-based IDS (Cont'd)



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

Structure-based IDS

Depending on the structure, traditional IDSs can be categorized into two types:

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 advanced network of monitoring, incident analysis, and instant attack data. By having these cooperative

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

https://t.me/learningnets

Technet24

agents distributed across a network, network operators can get a broader view of what is occurring on their network as a whole.

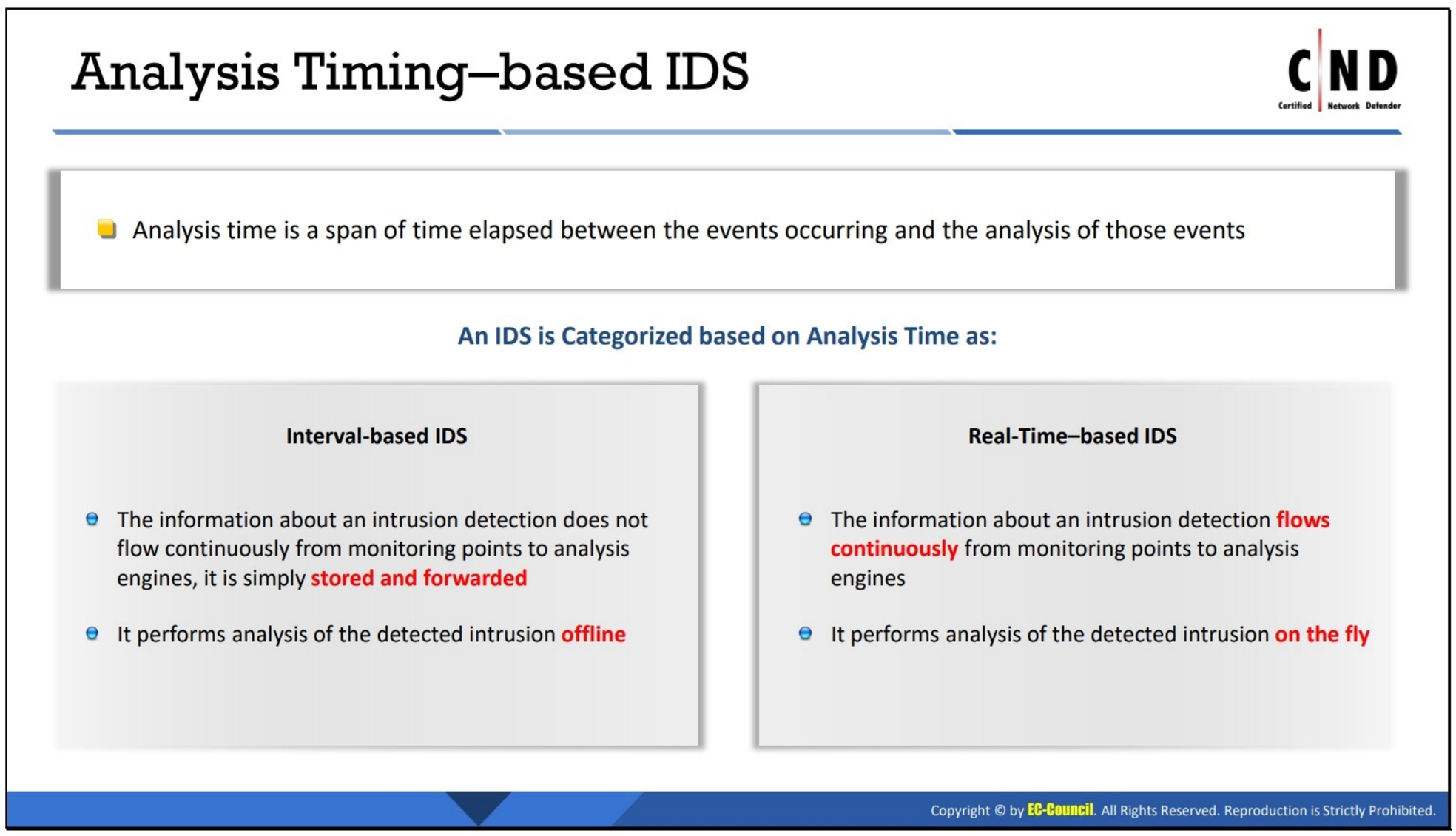
dIDS also allows a company to efficiently manage its incident analysis resources by centralizing its attack records and by giving the analyst a way to spot new trends or patterns and identify threats to the network across multiple network segments.

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.

Certified Network Defender 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 flow from monitoring points to the analysis engine is not continuous. Information is handled in a fashion similar to "store and forward" communication schemes. 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.

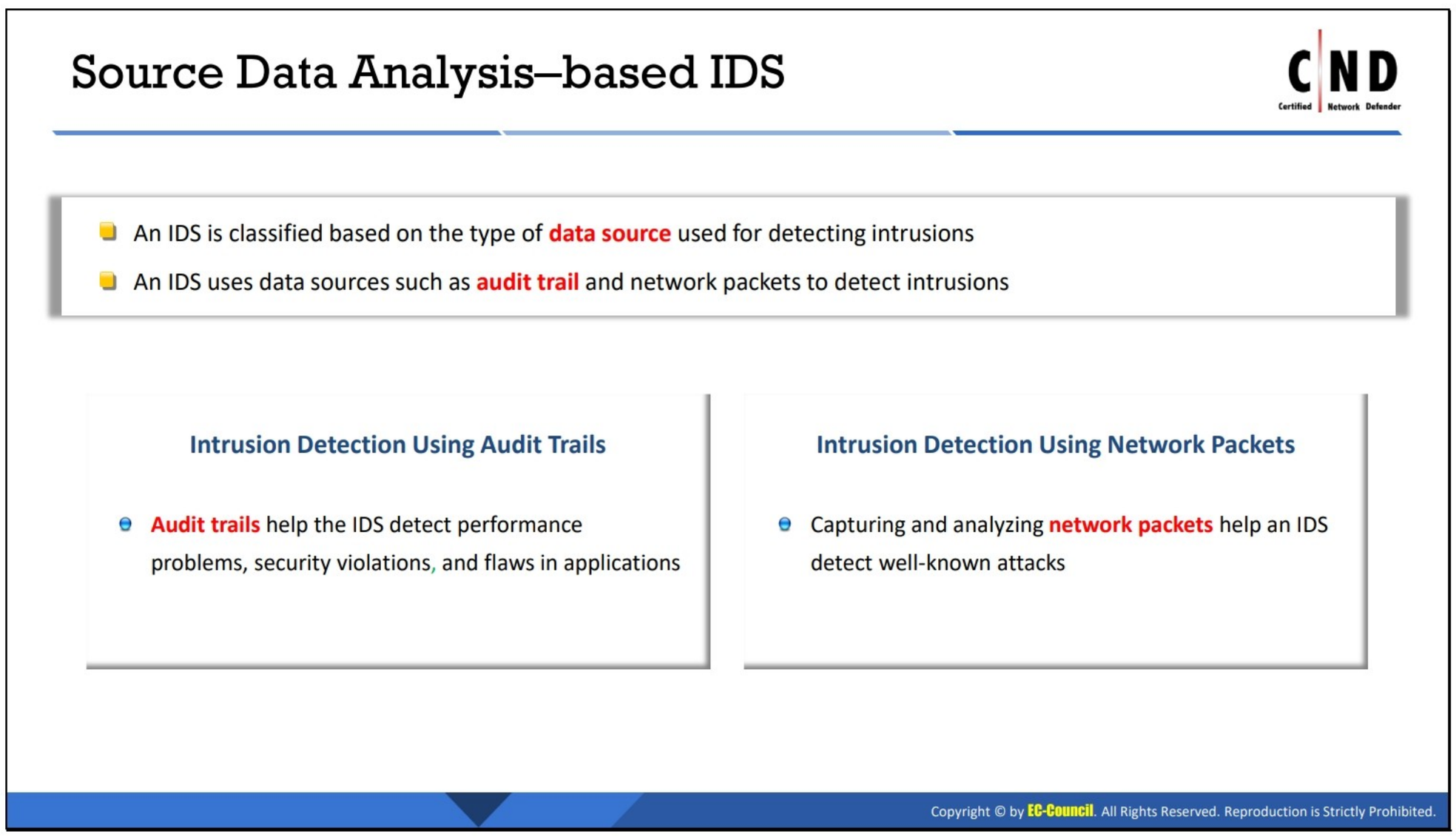
Real-time–based IDS

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.

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

https://t.me/learningnets

Technet24



Source Data Analysis–based IDS

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
  - Identifying system vulnerabilities

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

https://t.me/learningnets

- 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

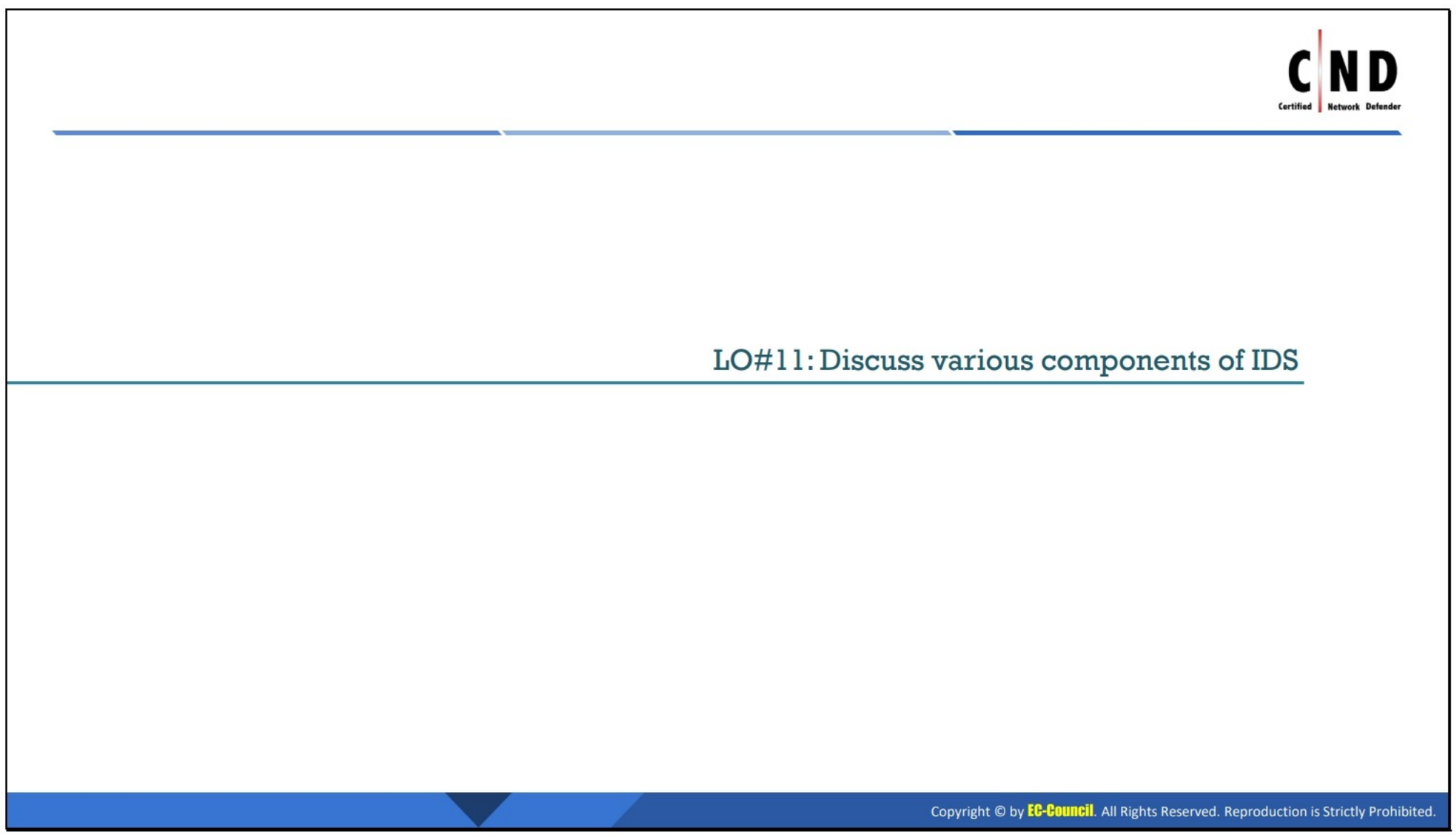
Intrusion Detection Using Network Packets

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.

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

https://t.me/learningnets

Technet24

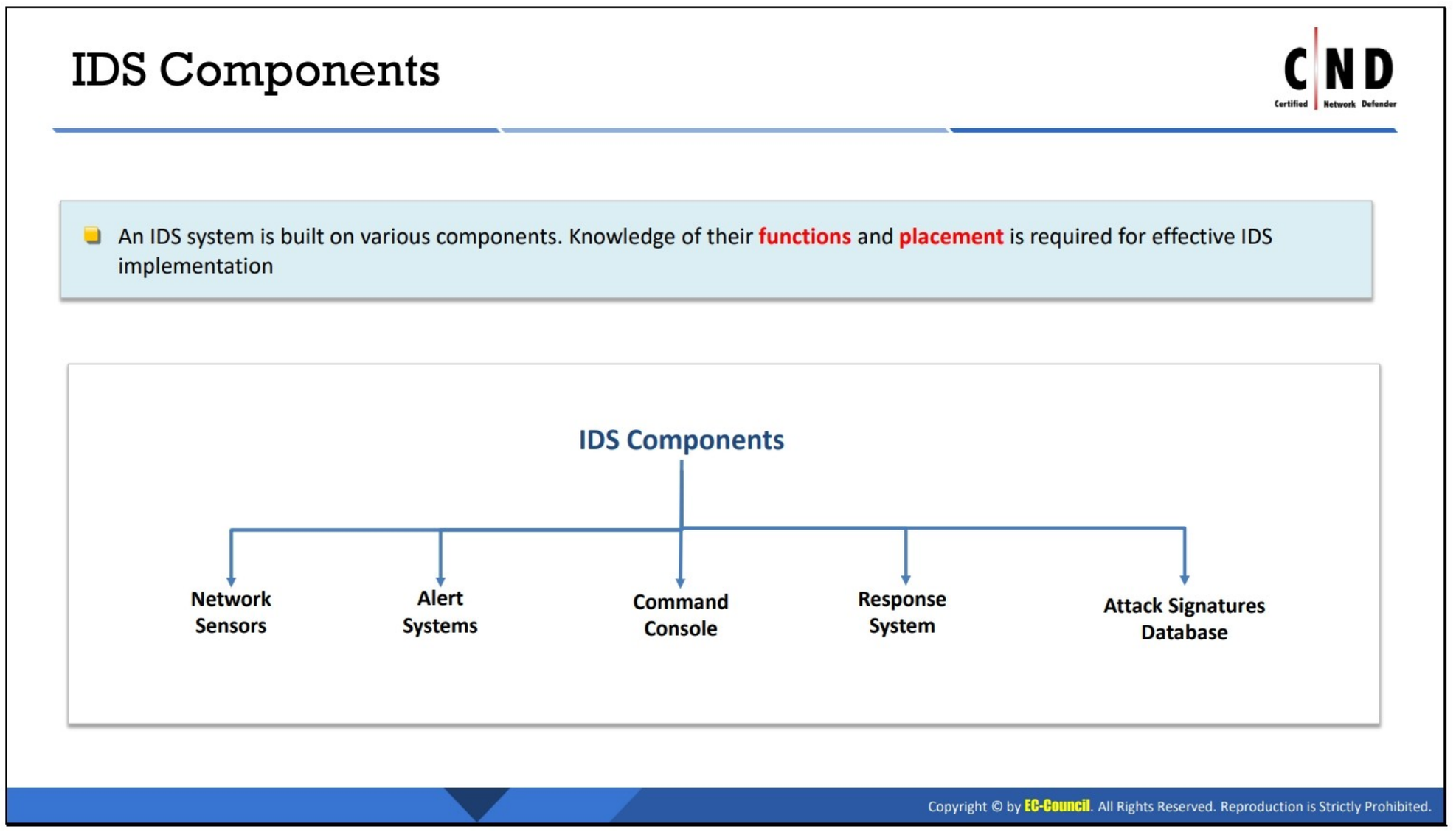


LO#11: Various Components of IDS

This section describes the different components that constitute IDS/IPS systems.

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

https://t.me/learningnets



IDS Components

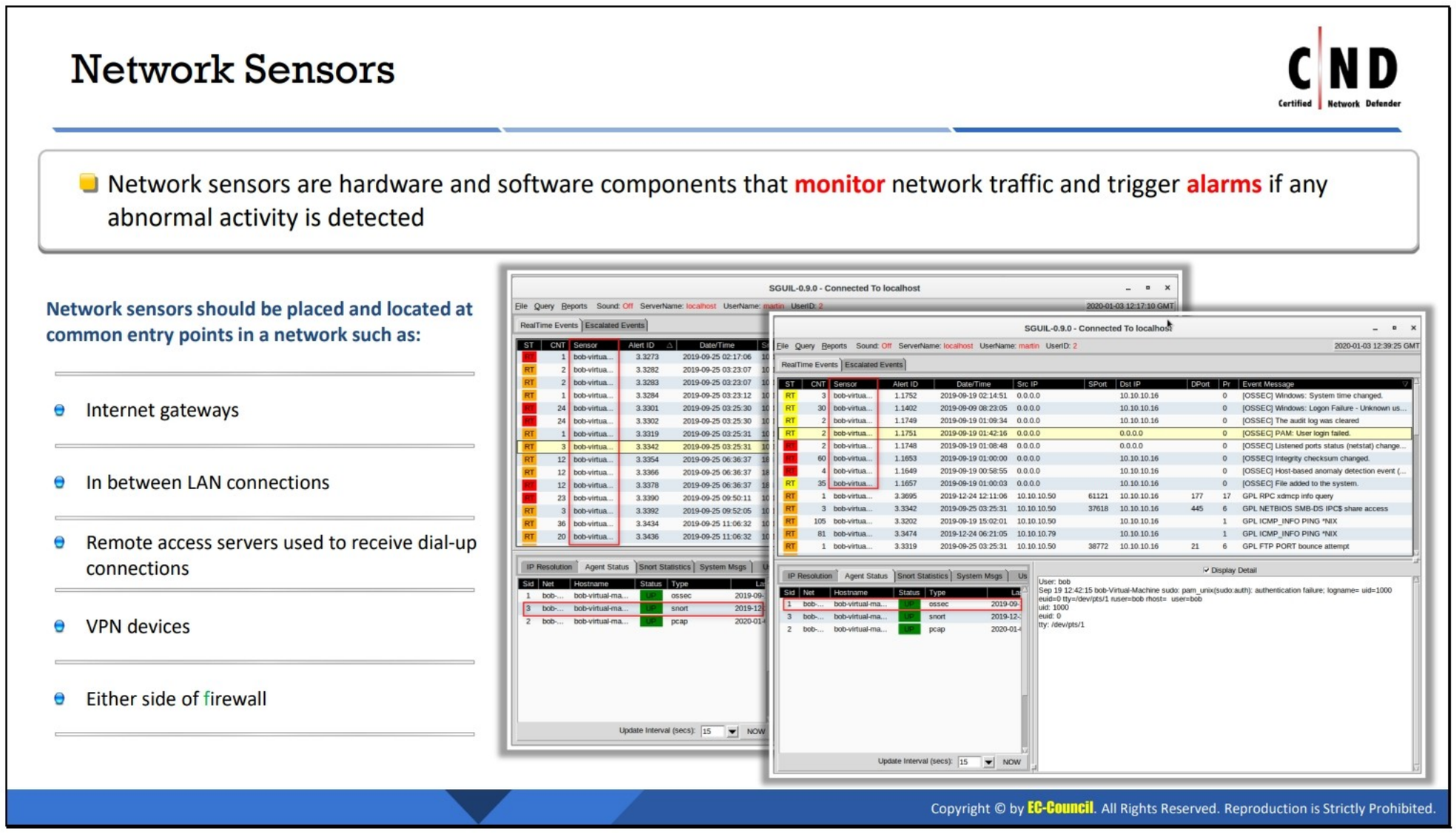
An IDS is comprised of different components. These components are used to collect information from a variety of systems and network sources, and then analyze the information for any abnormalities. Major components of an IDS are listed below.

- 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.

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

https://t.me/learningnets

Technet24



Network Sensors

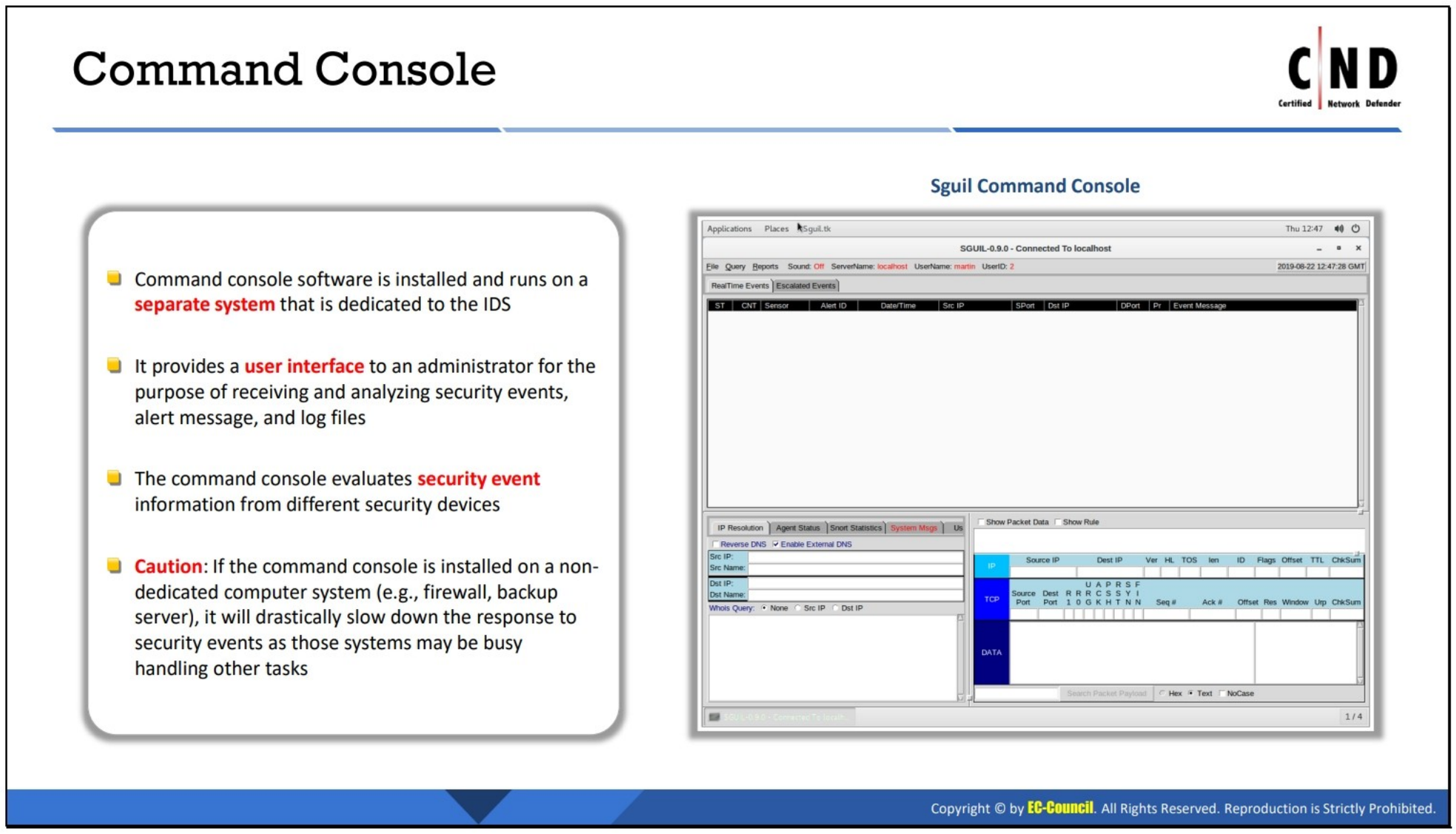
A network sensor is a hardware and/or software device that is connected to the network and reports to the IDS. It is a primary data collection point for the IDS. Network sensors collect data from the data source and pass it to the alert systems.

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.

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

https://t.me/learningnets



Command Console

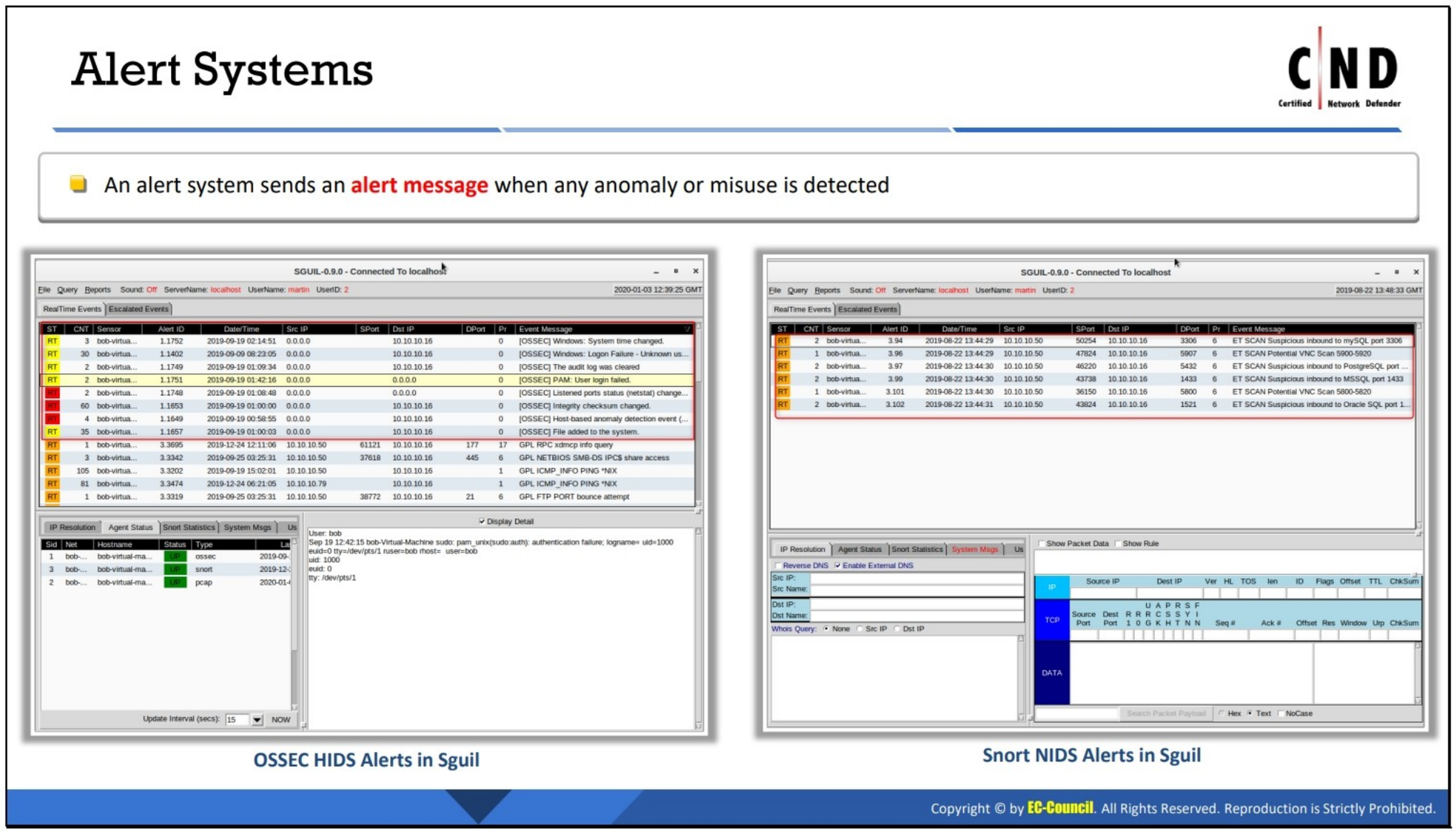
The command console is software that acts as an interface between an administrator and the IDS. The IDS collects all the data from security devices and analyzes it using the command console. Administrators use the console to analyze alert messages triggered by the alert system and manage log files. The 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.

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

https://t.me/learningnets

Technet24



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

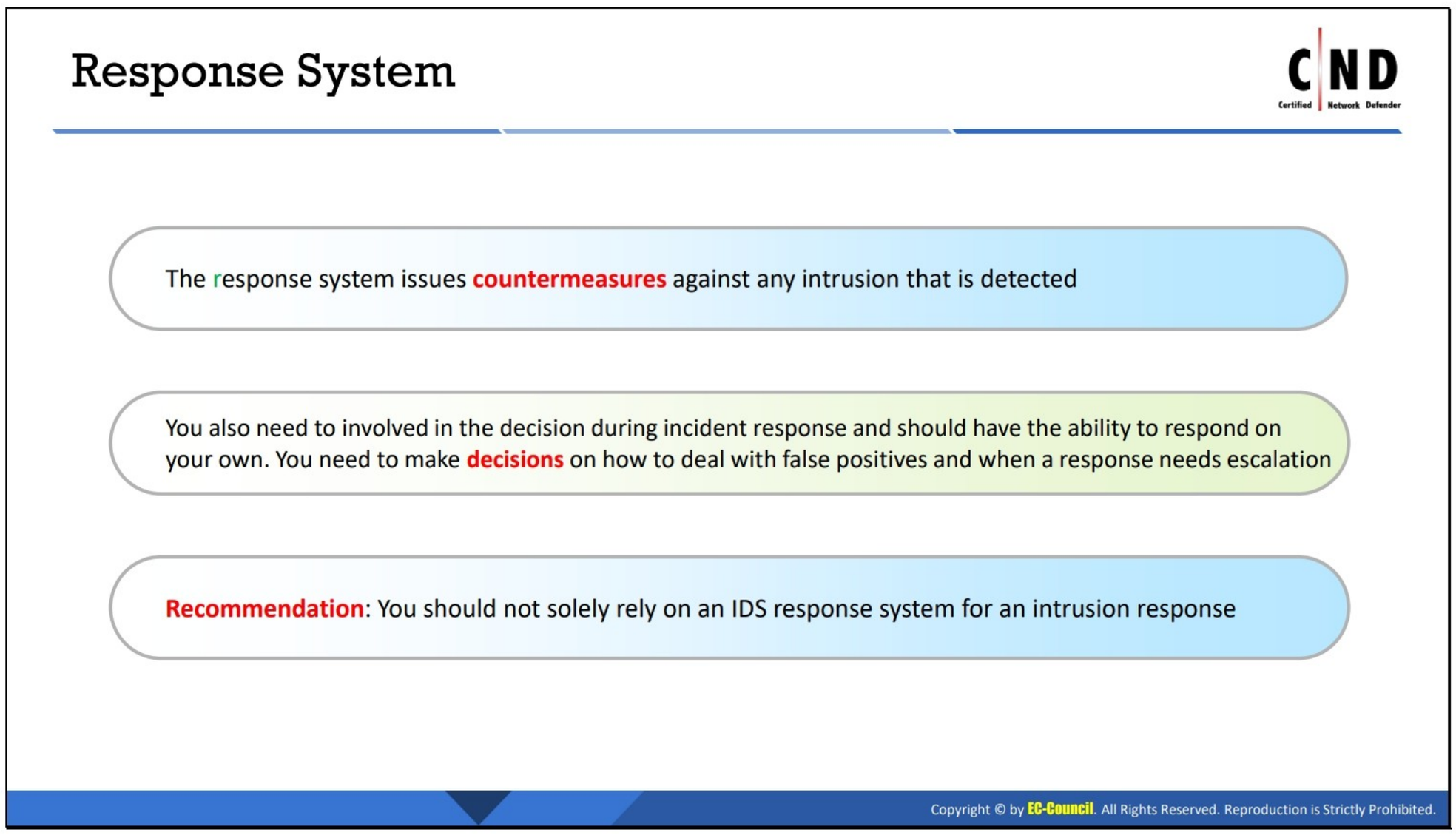
When a sensor triggers an alert, there are three possibilities:

- 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, network defenders 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.

Certified Network Defender 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.

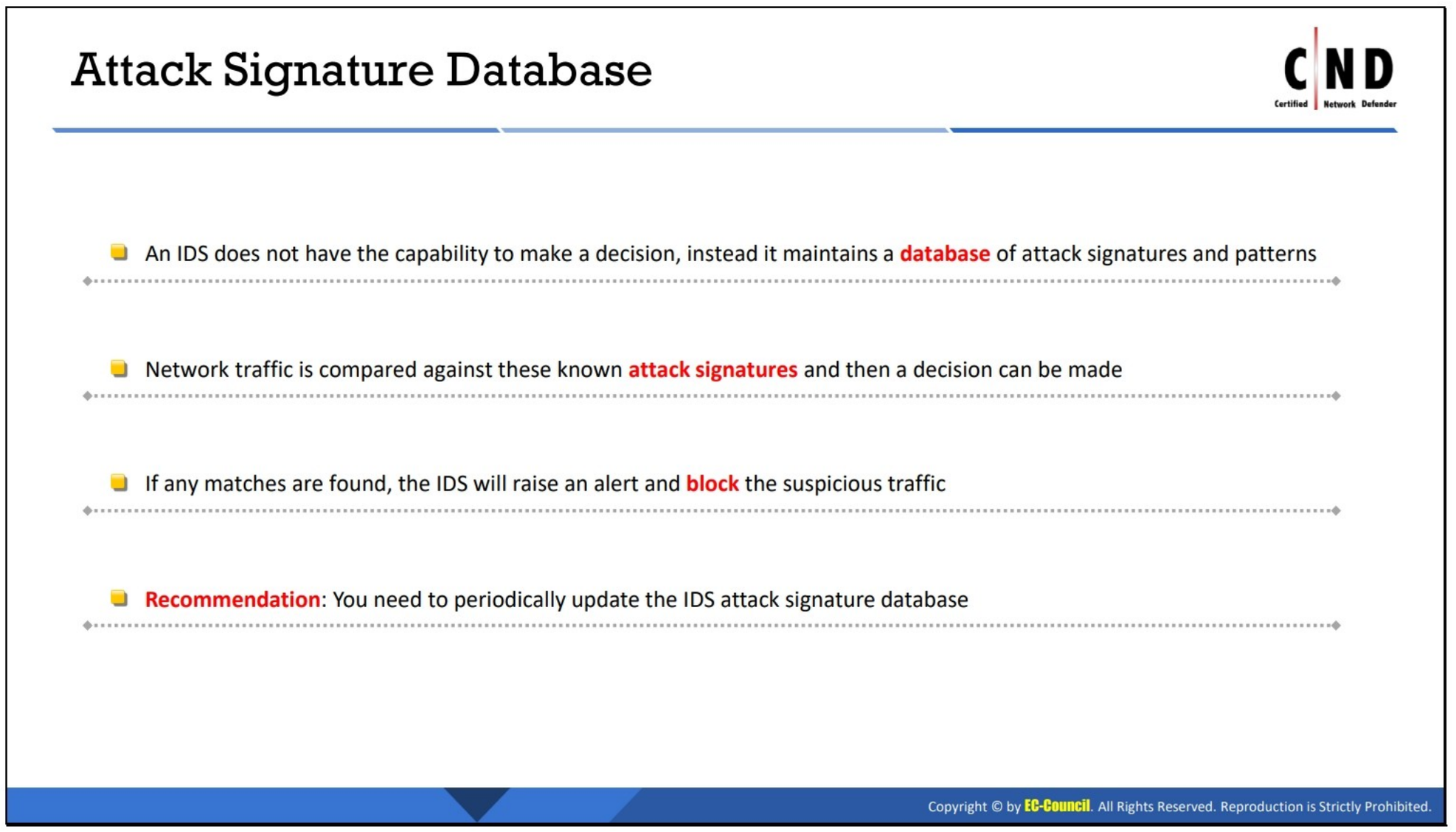
Network defenders can setup an IDS to allow the response system to take actions against intrusions or they can respond on their own. In the case of false positives, administrators need to respond to allow this traffic into the network without blocking it. Using the response system, administrators can 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. Network defenders are responsible for determining the appropriate response and ensuring that the response is executed.

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

https://t.me/learningnets

Technet24



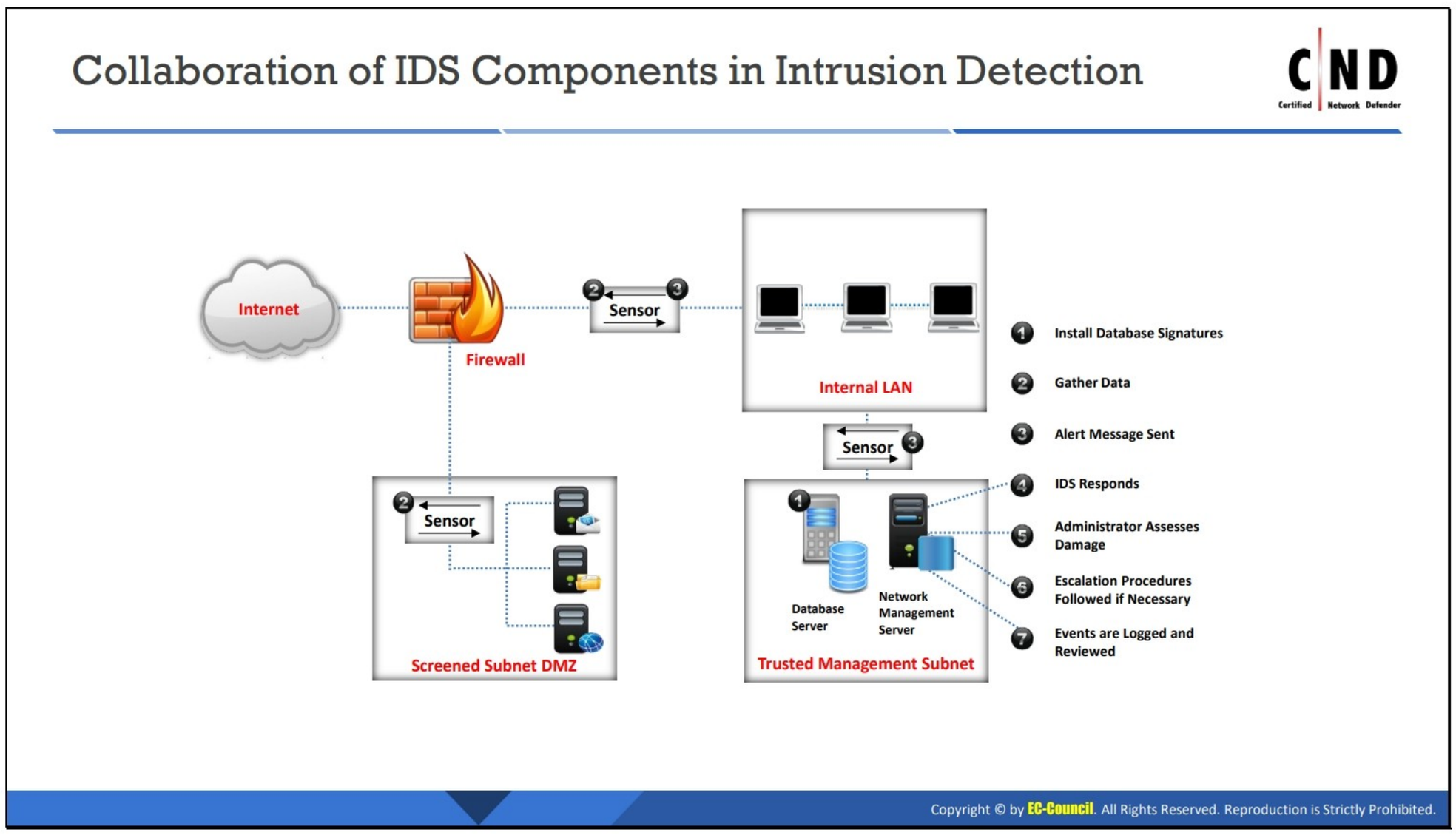
Attack Signature Database

Network defenders 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.

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

https://t.me/learningnets



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.

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

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

https://t.me/learningnets

Technet24

alert and takes a counter action such as dropping the packet, restarting the network traffic, and so on.

Administrator Assesses the Damage

The network defender 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)

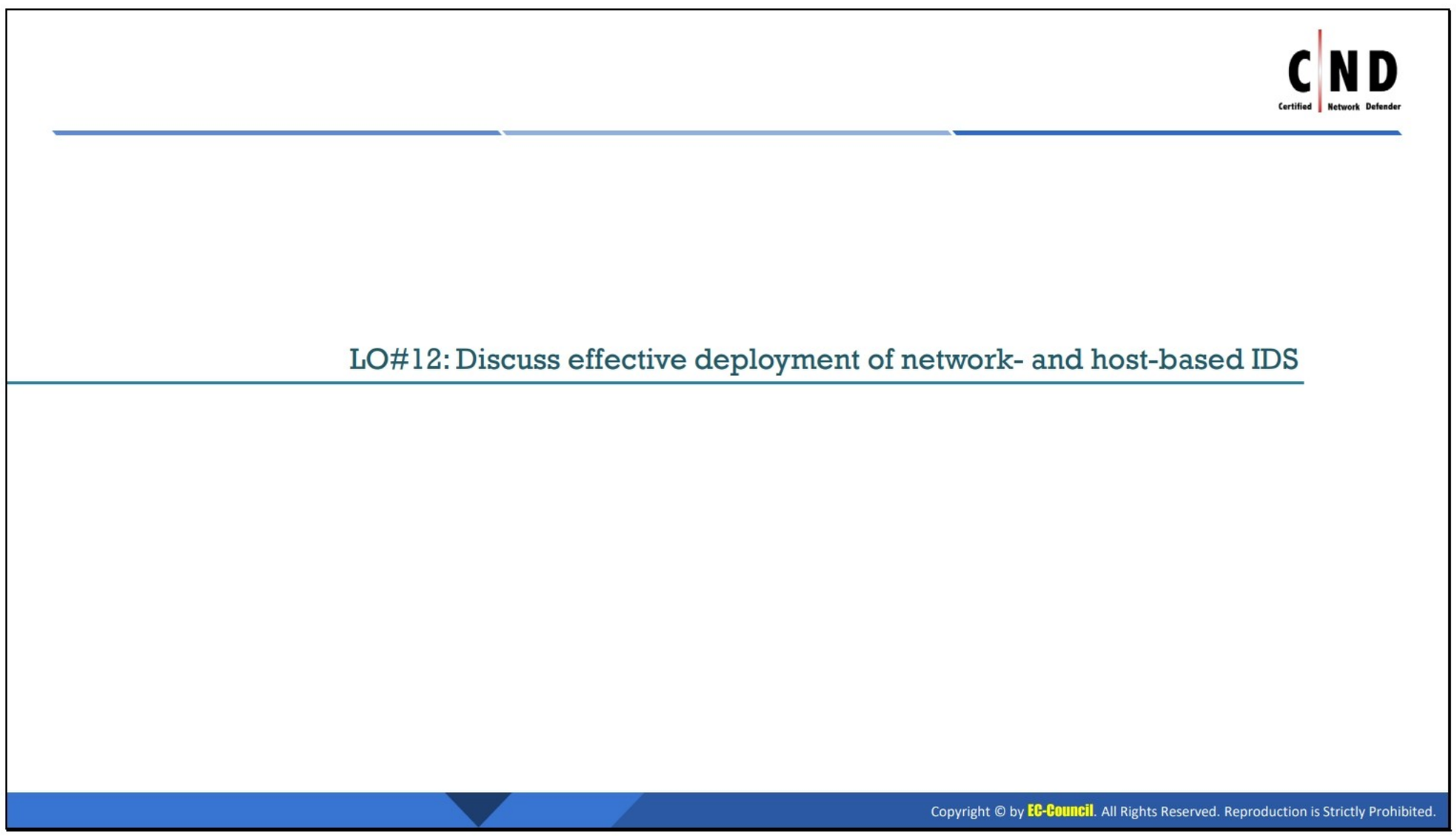
Escalation procedures are a set of actions written in the security policy and followed if the IDS detects a true positive (attack). These procedures vary depending on the severity of the incident.

Events are Logged and Reviewed

Network defenders 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 network defender in updating the database of attack signatures with new events and in detecting future attacks.

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

https://t.me/learningnets



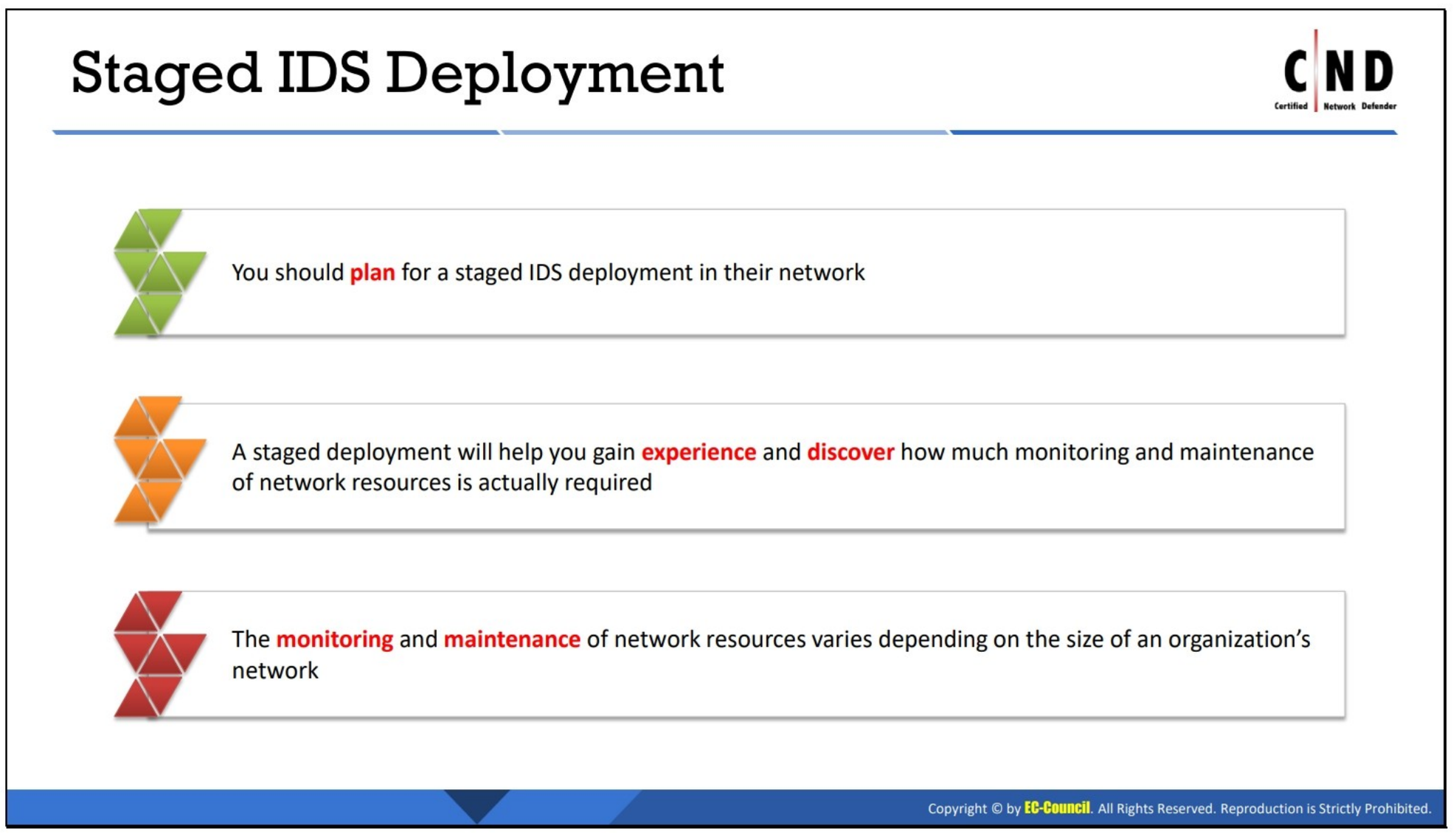
LO#12: Effective Deployment of Network and Host-Based IDS

This section discusses the deployment strategies for network- and host-based IDS/IPS.

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

https://t.me/learningnets

Technet24



Staged IDS Deployment

Before effectively deploying an IDS, network defenders must understand their network infrastructure and organizational security policies. 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.

Certified Network Defender 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)

Location 1

Place an IDS sensor behind each **external firewall** and in the **network DMZ**

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**

Advantages:

- Ability to identify the number and types of attack originating from the Internet to the network

Location 3

Place an IDS sensor on major **network backbones**

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**

Advantages:

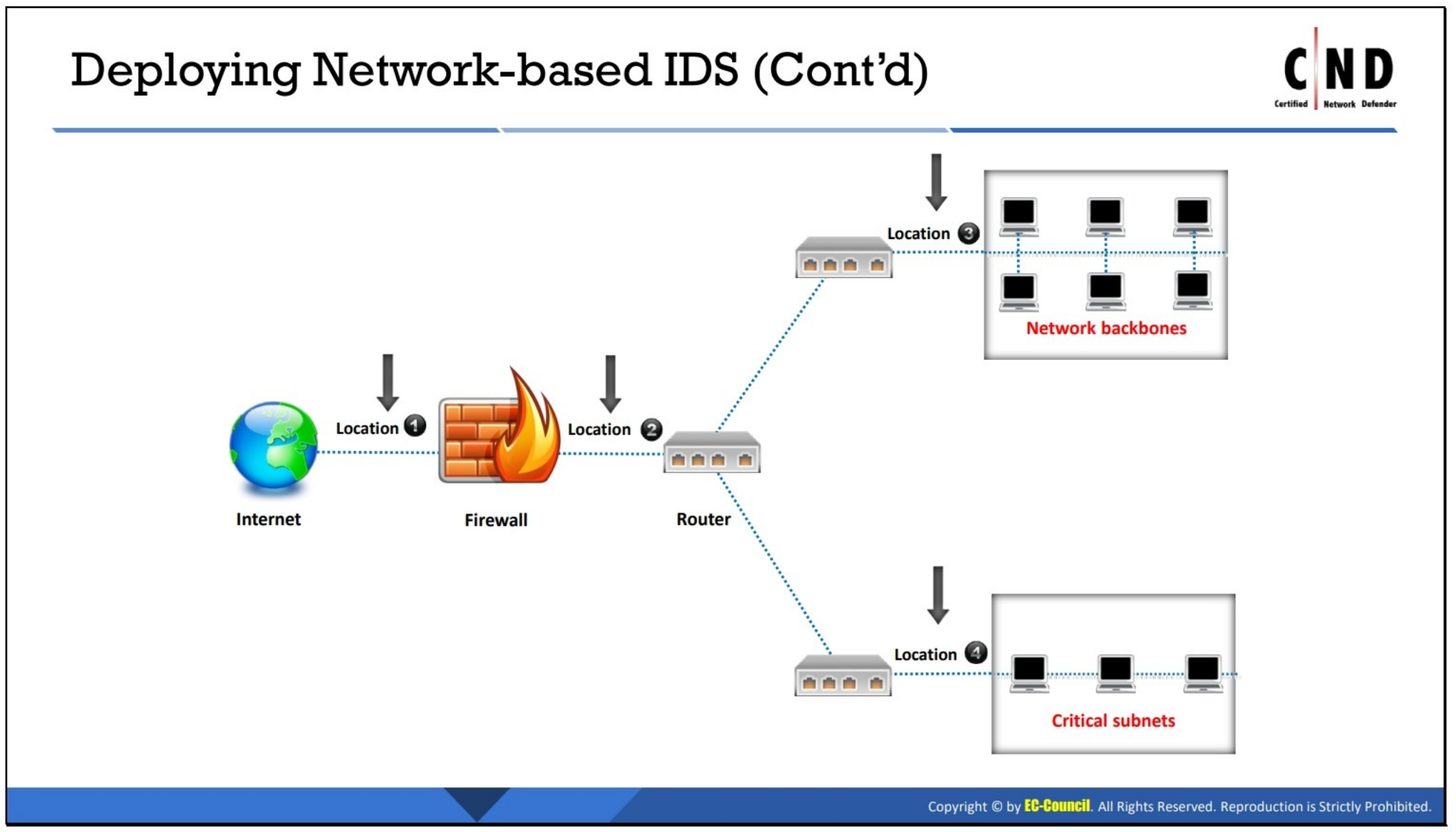
- Detects attacks on critical systems and resources
- Focuses on specific critical systems and resources

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

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

https://t.me/learningnets

Technet24



Deploying Network-based IDS

As a NIDS protects multiple hosts from a single location, the network defender can also consider customizing it to provide security for the entire network. The network defender should consider deploying an IDS management console before adding its sensors.

network defenders need to deploy IDS sensors incrementally throughout the network. Network defender must consider various factors such as the difference in traffic, logging, reporting, and alerts received when they deploy a new sensor for an IDS.

Network defender 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

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

https://t.me/learningnets

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.

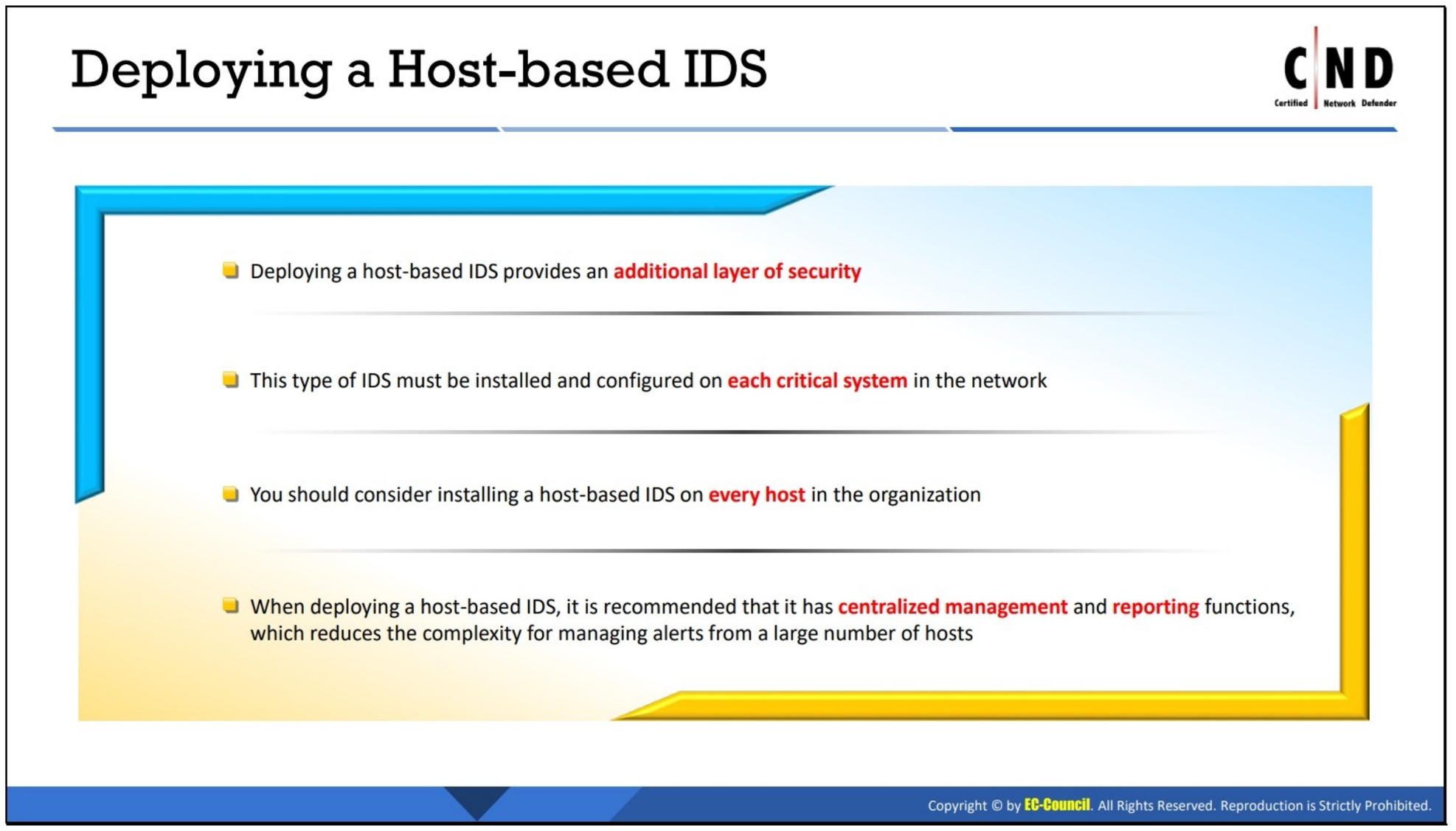
Different options for the deployment of sensors in the network are discussed below.

- Location 1: The sensor is placed outside the organizational network and perimeter firewall. 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.
- Location 2: 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.
- Location 3: 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.
- Location 4: 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.

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

https://t.me/learningnets

Technet24



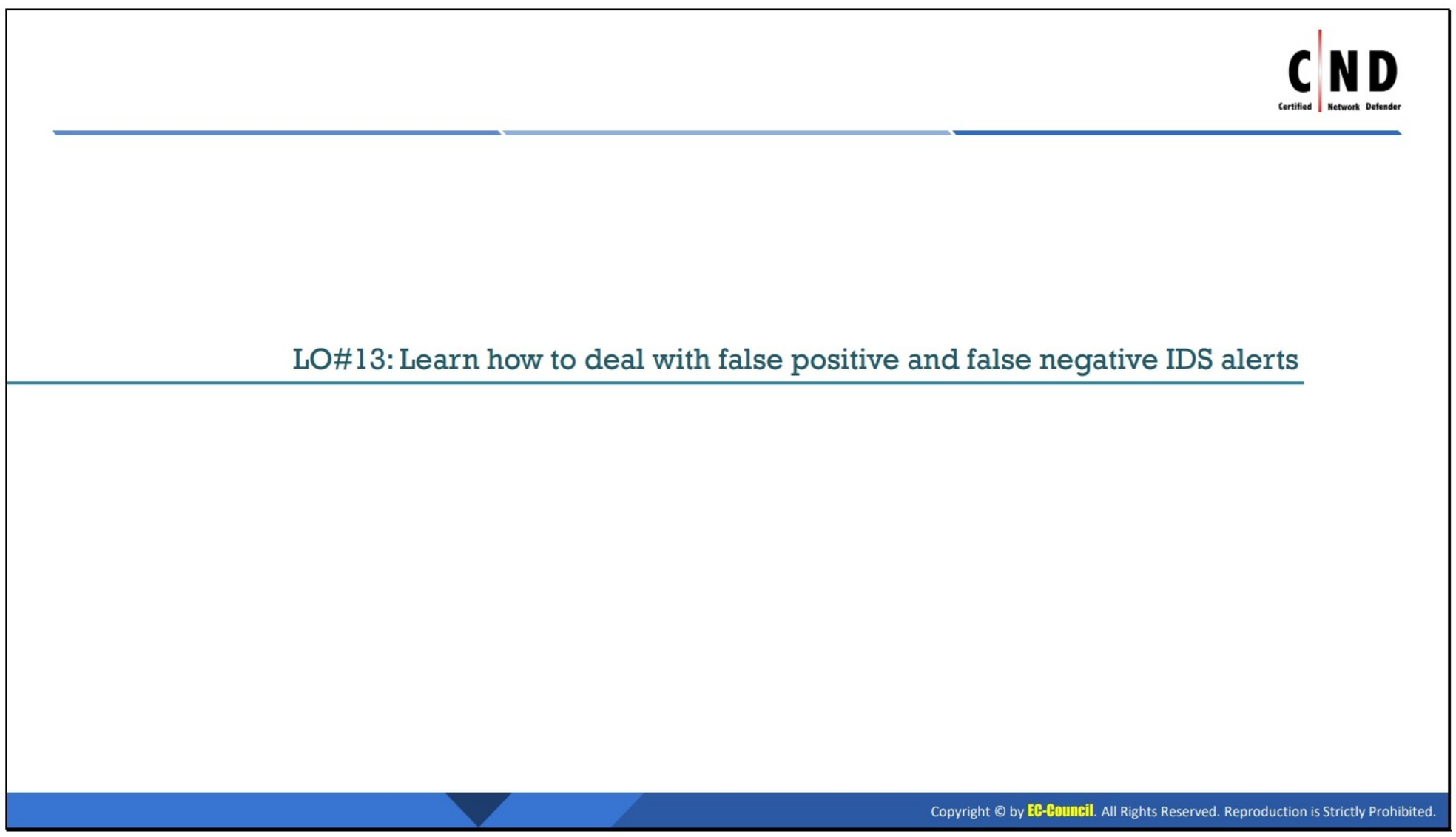
Deploying a Host-based IDS

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. Network defenders must consider implementing an IDS management console before adding additional hosts.

If network defender comfortably manages the HIDS on critical servers at the initial stage, then and only then can they consider deploying the HIDS on all remaining hosts in the network. This allows network defender 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.

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

https://t.me/learningnets



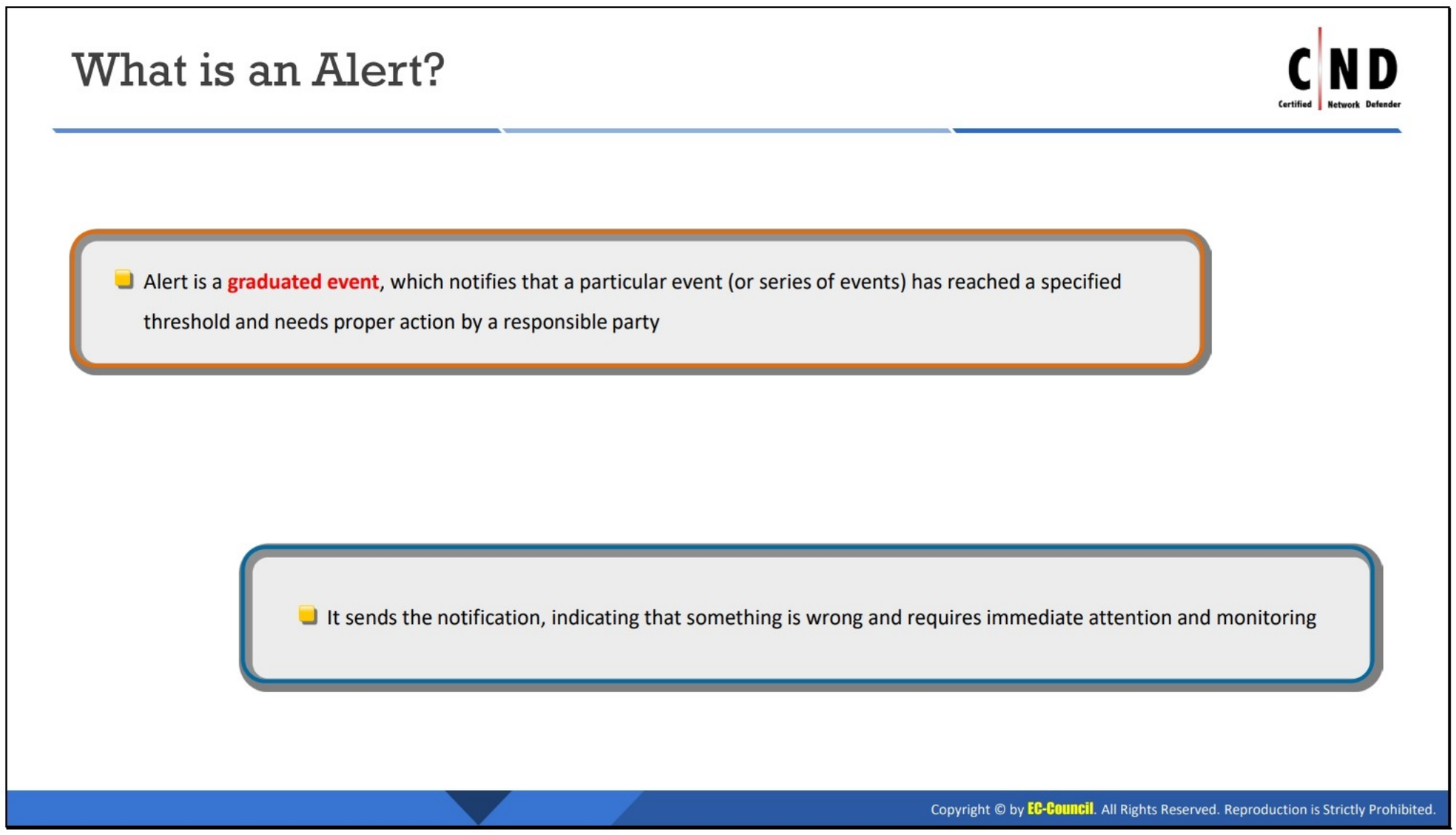
LO#13: How to Deal with False Positive and False Negative IDS Alerts

This section provides tips on fine-tuning IDS/IPS to decrease the number of false positive alerts.

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

https://t.me/learningnets

Technet24



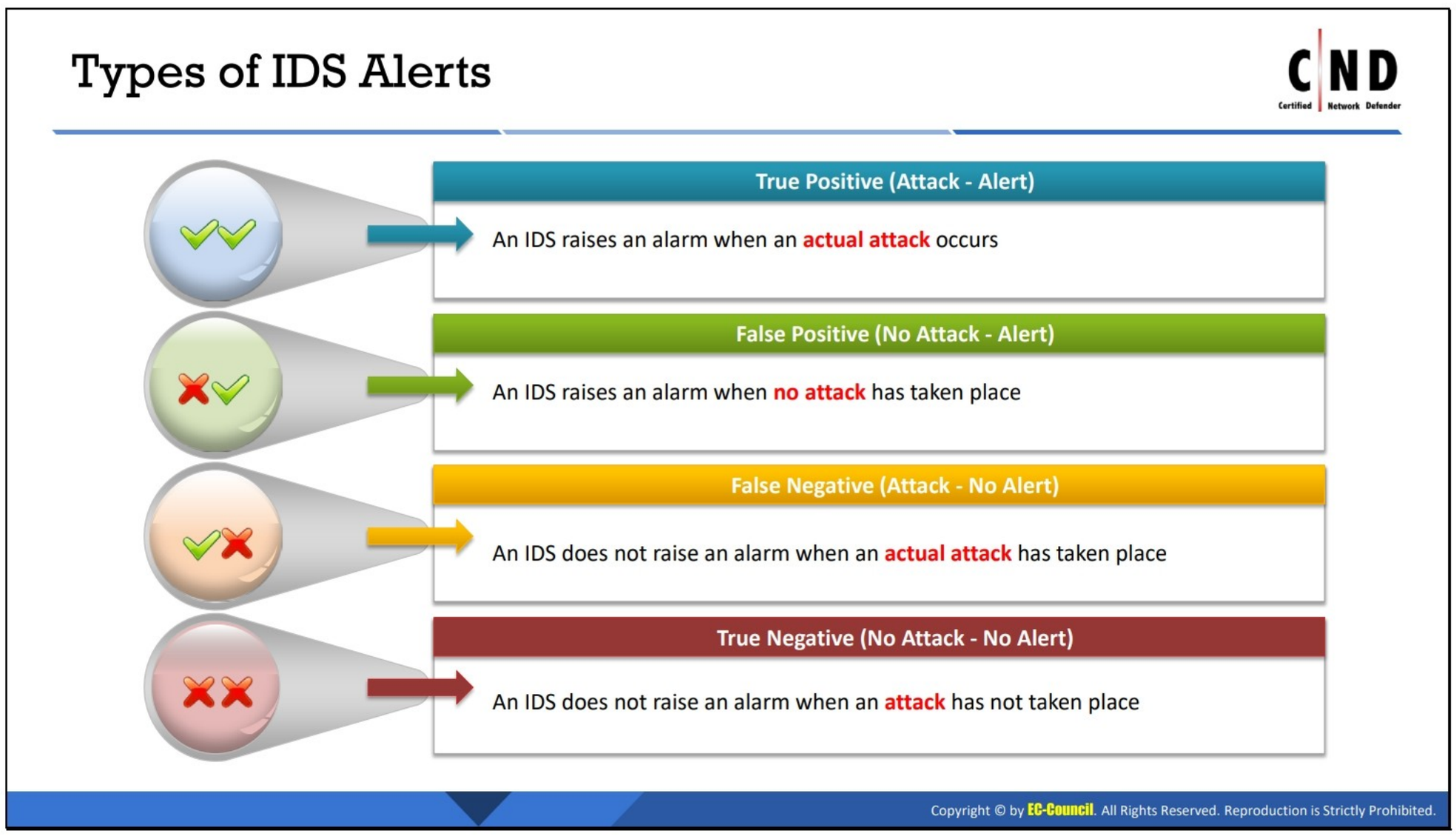
What is an Alert?

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.

Certified Network Defender 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, which include true positives, false positives, false negatives, and true negatives.

True Positive (Attack - Alert)

A true positive is a condition occurring 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 is actually attempting to compromise the network; or it may be a drill, in which case security personnel are using hacker tools to conduct tests of 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. A false positive occurs when an IDS treats normal system activity as an attack. False positives tend to make users insensitive to alarms and reduce their reactions to actual intrusion events. While testing the configuration of an IDS, administrators use false positives to determine if the IDS can distinguish between false positives and real attacks or not.

False Negative (Attack - No Alert)

A false negative is a condition occurring when an IDS fails to react to an actual attack event. This is the most dangerous type of failure as the purpose of an IDS is to detect and respond to attacks.

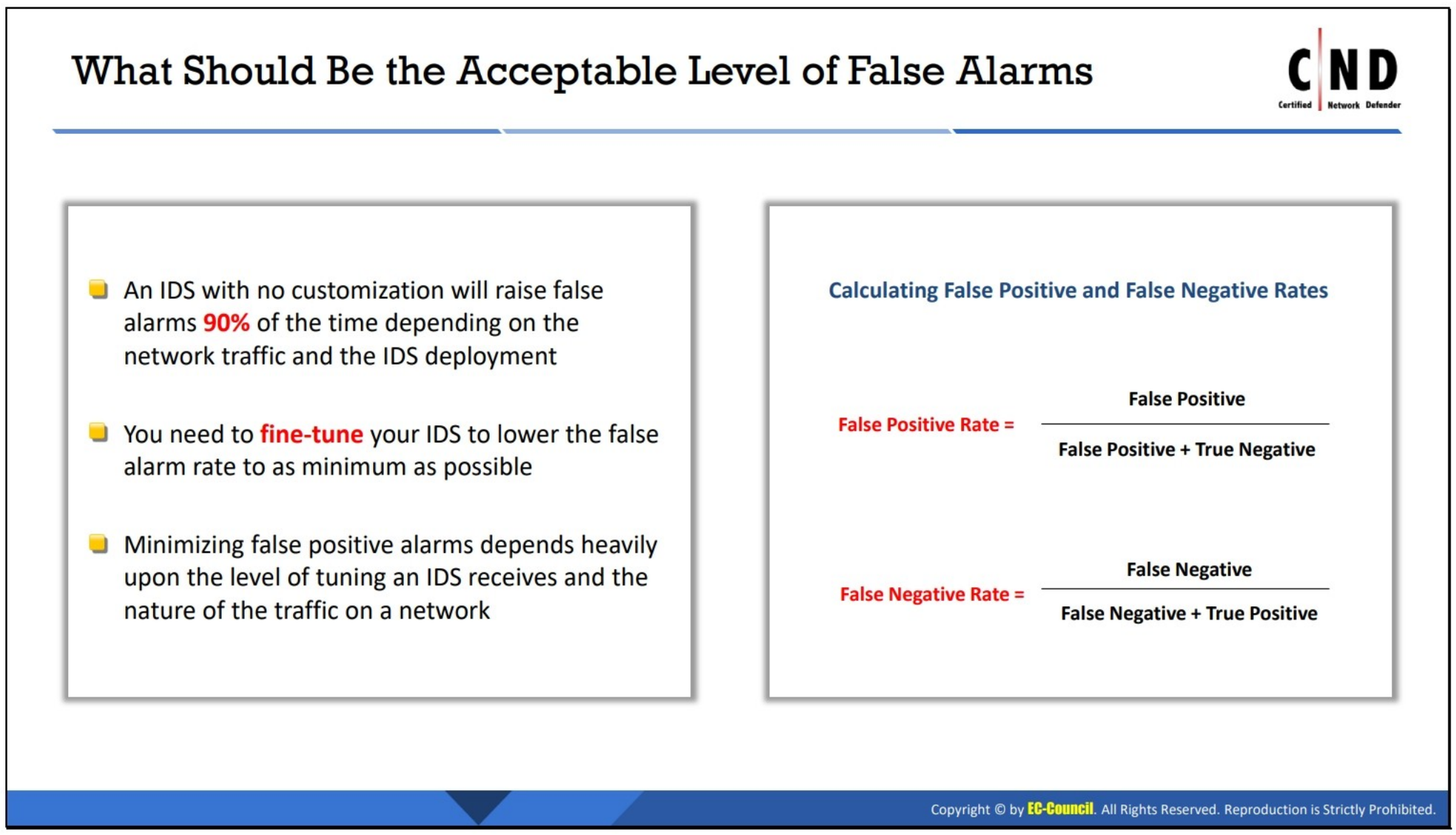
True Negative (No Attack - No Alert)

A true negative is a condition occurring when an IDS identifies an activity as acceptable behavior and the activity is actually acceptable. A true negative involves successfully ignoring acceptable behavior. It is not harmful as the IDS is performing as expected.

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

https://t.me/learningnets

Technet24



What Should Be the Acceptable Level of False Alarms

If the number of intrusions in a network is low, compared to network usage, the rate of false alarms will be high. It is important to keep the false positive rate as minimal as possible. At times an IDS will ignore half of the network traffic; therefore, tuning is not the only option. An effective implementation of an IDS inspects both incoming and outgoing traffic for anomalies. Based on the organization's network tolerance toward false positives, network defender can setup a threshold level for the IDS.

The number of false alarms depends on two phases, as described below.

1. The detection phase: To bring false alarms down to acceptable levels, administrators enhance the configuration of the IDS and change the detection approach methods. The higher the detection rate and accuracy, the lower the amount of false alarms will be. Techniques such as data mining and data clustering reduce the amount of false alarms.
2. The alert processing phase: Alert processing studies the cause of false alarms, recognizes the high amount, and uses case scenarios to subsequently provide a coherent response to the alarm. Alert processing techniques such as statistical filtering and fuzzy alert aggregation help identify the sequences for false alarms, filters them, and later discards them from the system.

Based on the organization's network tolerance, network defender can reduce false alarms by raising the threshold level of the IDS. The threshold level depends on two statistics called sensitivity and specificity. Sensitivity represents the legitimacy of alerts detected by the IDS. Specificity filters the accuracy of the alerts detected by the IDS.

The false positive and false negative rates are calculated using the formulas listed below. These formulas help fine-tune the IDS solution with reduced rates.

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

https://t.me/learningnets

False Positive Rate

- False positive rate = false positive/(false positive + true negative).

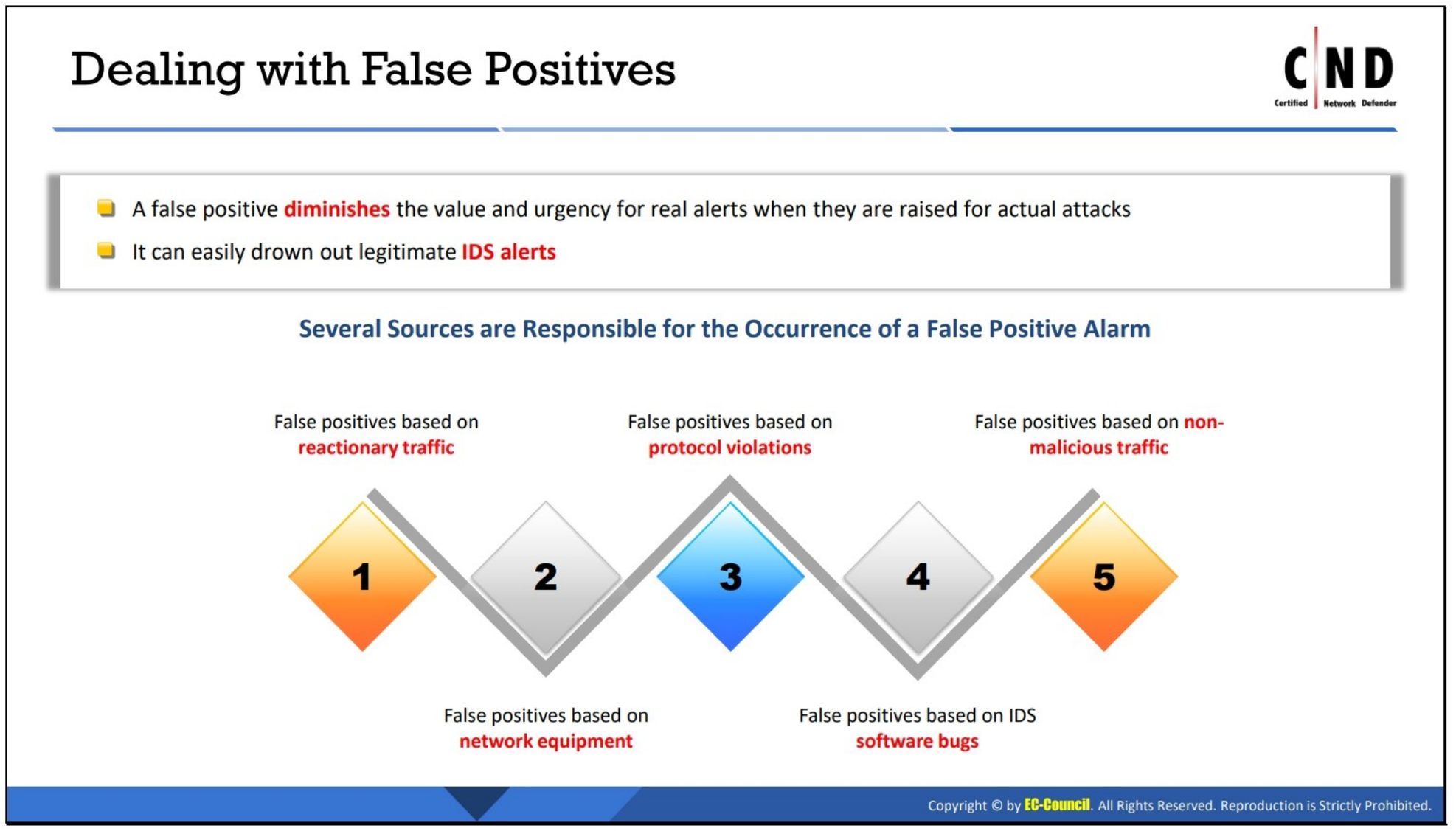
False Negative Rate

- False negative rate = false negative/(false negative + true positive).

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

https://t.me/learningnets

Technet24



Dealing with False Positives

In a false positive alarm an IDS raises an alarm on a non-malicious event. Evidently, they have the potential to cause chaos in the organization. They nullify the urgency and value of the real alerts, leading to laxity in case of an actual security situation.

Causes of False Positive Alarms

- A network traffic false alarm: A network traffic false alarm triggers when a non-malicious traffic event occurs. A great example of this would be an IDS triggering an alarm when the packets do not reach the destination due to network device failure.
- A network device alarm: An IDS triggers a network device alarm when the device generates unknown or odd packets, for example, by a load balancer.
- An alarm caused by an incorrect software script: If poorly written software generates odd or unknown packets, an IDS will trigger a false positive alarm.
- Alarms caused by an IDS bug: A software bug in an IDS will raise an alarm for no reason.

Reducing False Positive Alarms

To reduce false positive alarms it is important to understand the weakness of the device. Implementing effective countermeasures can help reduce the occurrence of false positive alarms.

- Differentiating alerts: Administrators should distinguish the important priority alerts against the less important ones. One of the methods used is to verify the alerts with an alert triggered earlier. For example, a specific signature triggering an alert at regular intervals can be termed as an important alert. For future reference, the administrator

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

https://t.me/learningnets

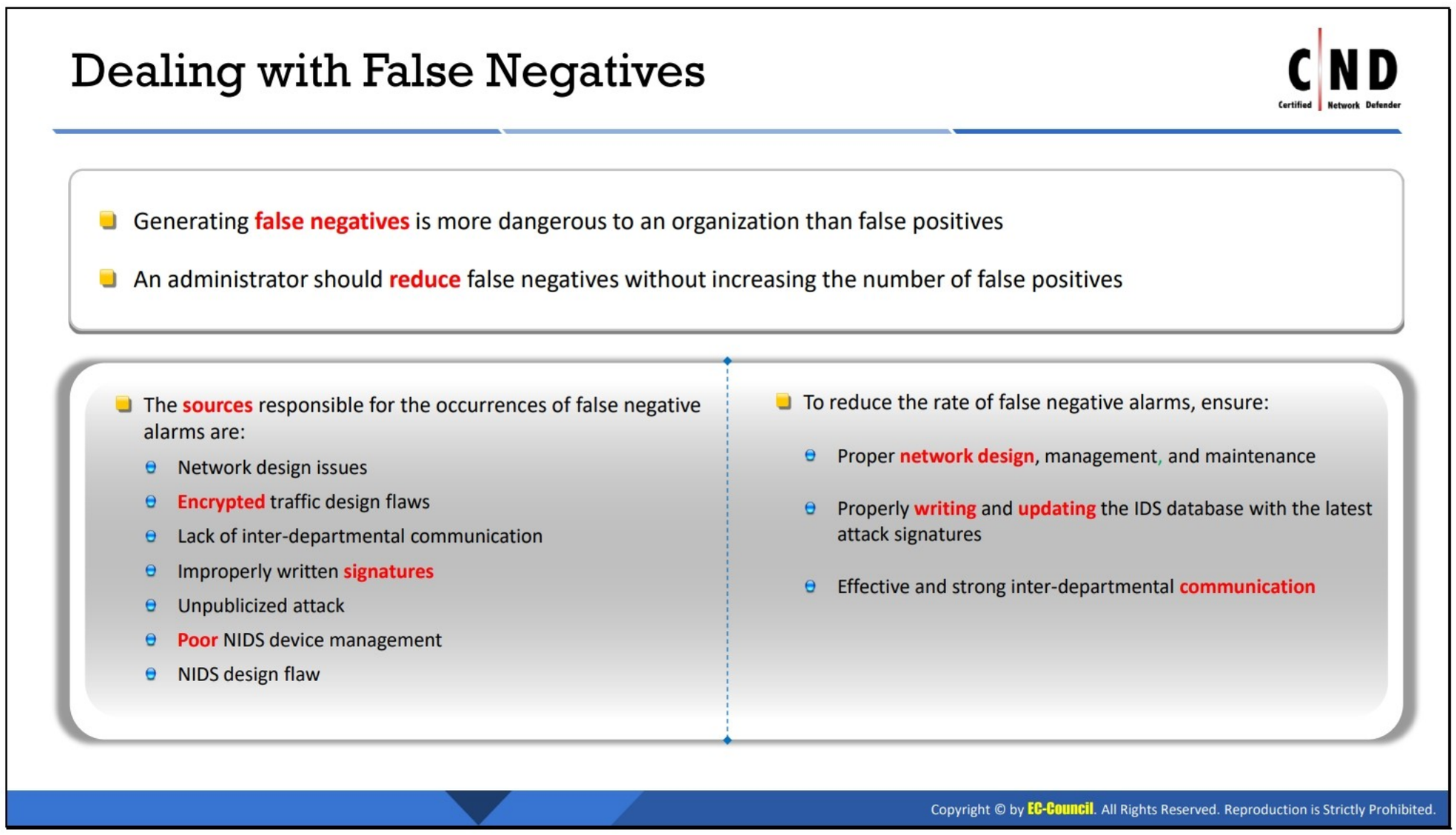
can maintain a log of these alerts. They can also classify the alerts based on the attack behavior. For instance, classification may be done based on normal behavior, intrusion behavior, and suspicious behavior occurring in the network.

- Setting thresholds on alerts: A single intrusion can create multiple alerts with generic features. Setting thresholds for alerts helps to reduce the number of alerts related to the same attack.

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

https://t.me/learningnets

Technet24



Dealing with False Negatives

A false negative is a more complex issue than a false positive. In a false negative, the IDS does not detect a legitimate attack on the network.

Some of the causes behind generation of false negative alarms are listed below.

- Network setup issue: Network flaws involving improper port spanning on switches and network traffic imbalance. Failure of NIDS devices to detect incoming and outgoing network traffic due to multiple entry points is one of the causes of a false negative alert. Improper configuration of an IDS will also raise a false negative alert.
- Encrypted traffic design flaws: An IDS is not capable of detecting intrusions when they are encapsulated in encrypted traffic, as it is not possible to match encrypted traffic to signatures. It is advisable to place an IDS behind a VPN termination with SSL encryption.
- Misleading signatures: If the signatures are not correctly written, they can mislead in determination of attacks. Vendors cannot create signatures of those attacks of which they are not aware. Occasionally even the tools are incapable of determining the legitimate signatures.

Dealing with False Negative Alarms

To reduce false negative alerts, it is important to understand them as well as any implementation issues with the device. Some effective ways to deal with false negative alerts are listed below.

- Appropriate network design: The primary requirement for minimizing a false negative alert is to setup a proper network design. The network design should be parallel to the security policies of the organization.

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

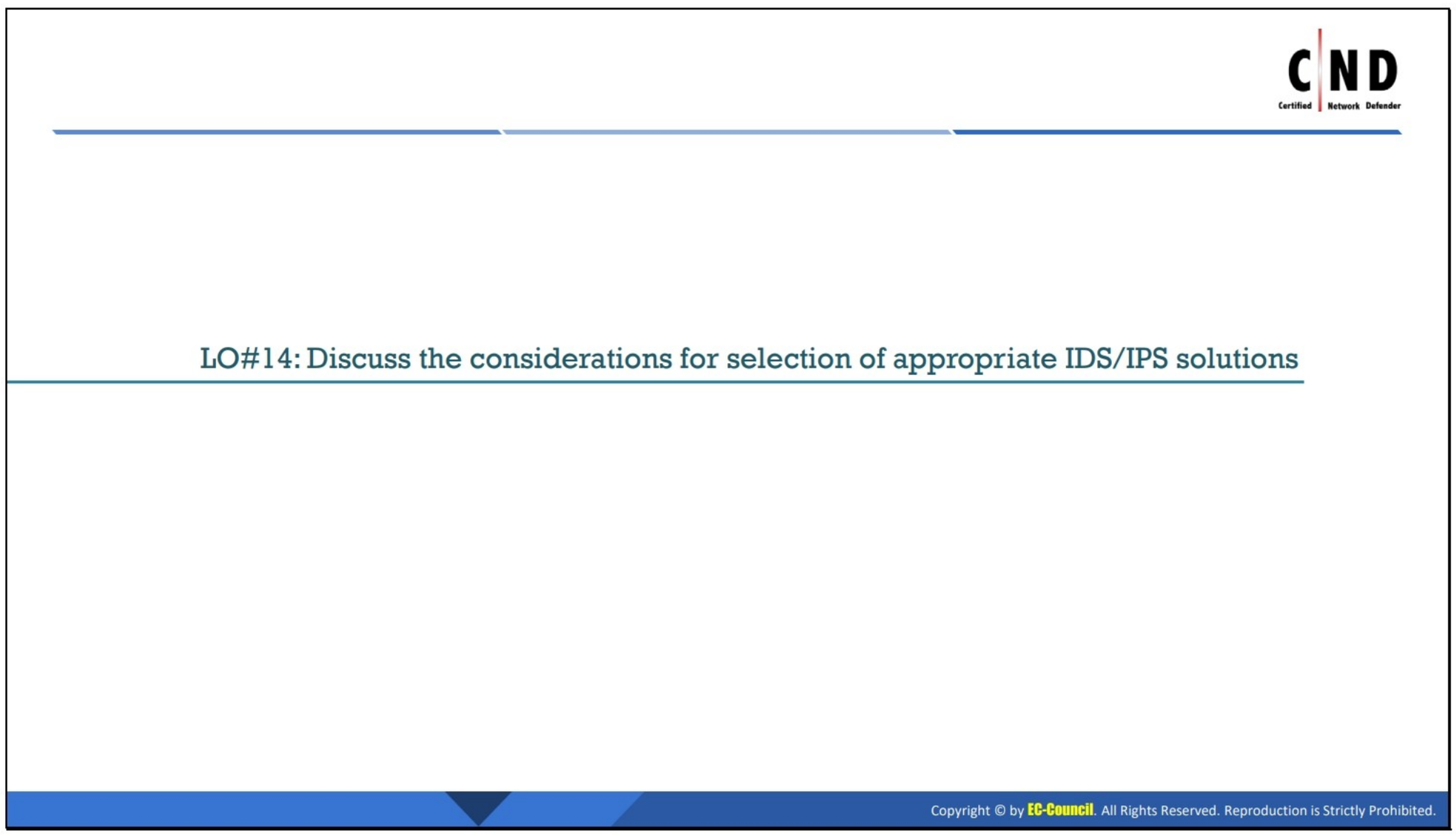
https://t.me/learningnets

- Proper placement of an IDS: The proper placement of an IDS is behind the firewall. Such a placement will raise alerts against port scans, automated scans, and DoS attacks. The IDS should also be configured to detect illegitimate signatures.
- Network analysis: Active network analysis and monitoring will minimize the number of false negative alerts. For this, network defenders can utilize various network analysis tools or utilities. The IDS should also be configured to nullify false negative alerts from triggering the rules set on it.
- Inclusion of additional data: False alerts can be reduced by including additional data about the network in the security event. The additional information includes information about the organization's assets, users, networks, and network device sources. Inclusion of this additional data can be through automated or manual processes.

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

https://t.me/learningnets

Technet24

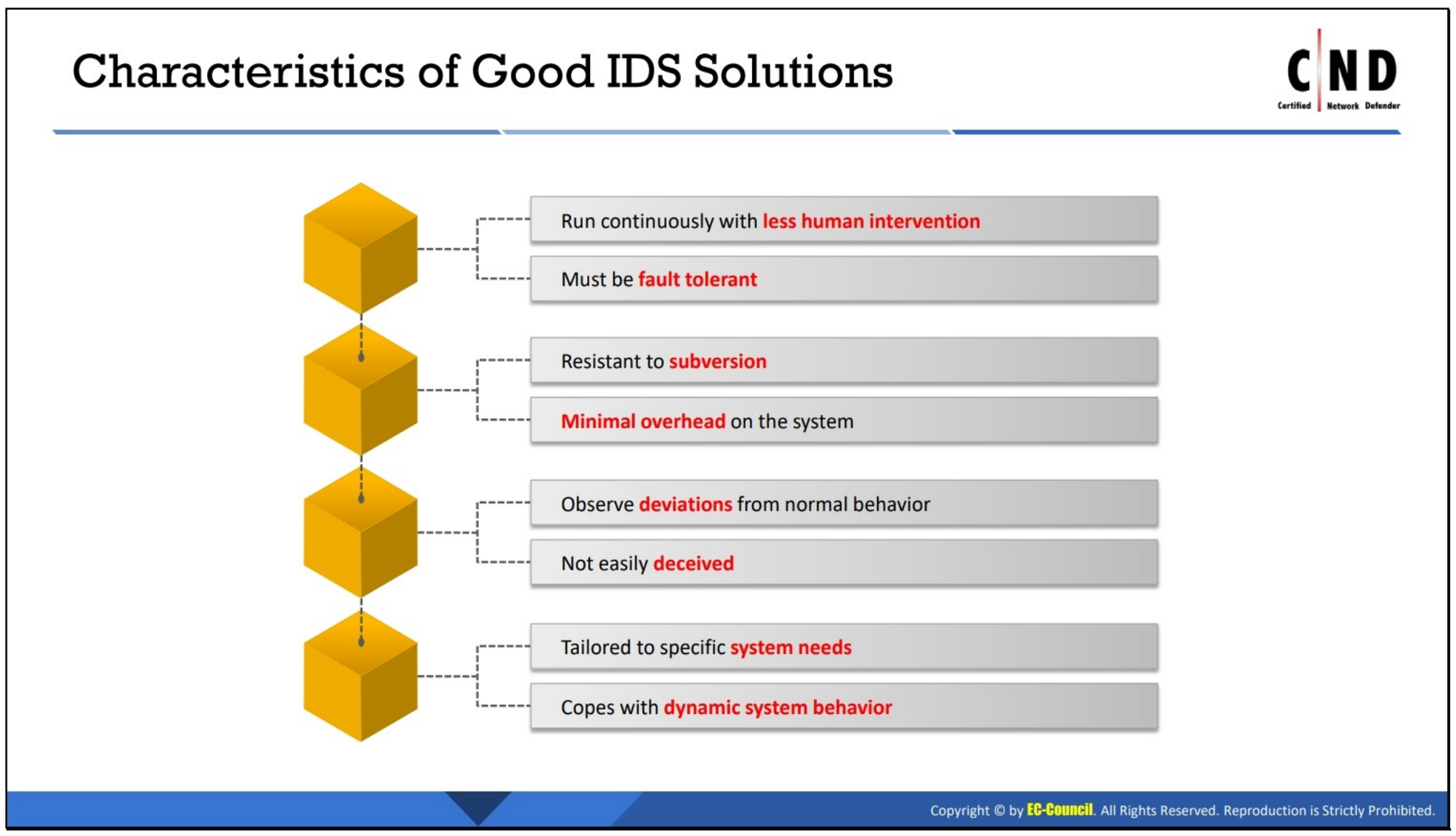


LO#14: Considerations for Selection of Appropriate IDS/IPS Solutions

This section explains how to select appropriate IDS/IPS solutions for effective protection.

Certified Network Defender 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 network defender 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 an network defender 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.

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

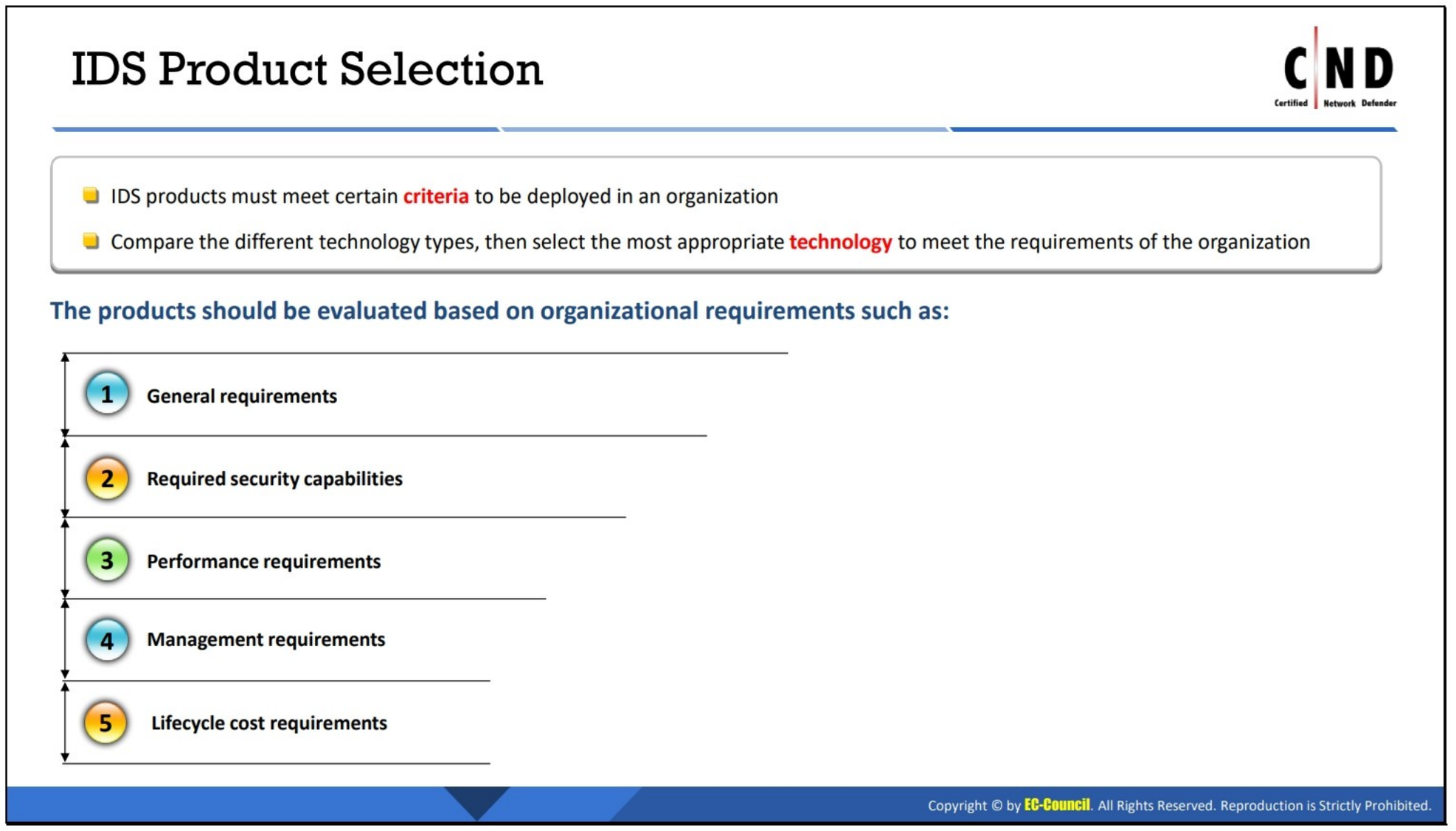
https://t.me/learningnets

Technet24

- 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 network defender 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 network defender when analyzing vulnerabilities and rectifying them.
- 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.
- The configuration of an IDS should be such that it does not cause overheads in the network or system.

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

https://t.me/learningnets



IDS Product Selection

The selection of any IDS product depends on whether it meets certain requirements. The selection process consists of assessing the four aspects of IDS technologies: security capabilities, performance, management, and lifecycle costs.

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

https://t.me/learningnets

Technet24

IDS Product Selection: General Requirements

- Evaluate the general requirements the IDS products will have to meet post deployment
- Size of an organization also modifies the number of IDS products needed

System and Network Environments

An organization's characteristics such as system and network environments should be evaluated and examined if the selected IDS/IPS is compatible with them and if the capabilities include **event monitoring**

Consider the following characteristics:

- Technical specifications of the IT environment
- Technical specifications of the existing security protections

Goals and Objectives

An organization should decide whether a particular IDS solution satisfies their technical, operational, **business goals**, and objectives behind the reason for implementing an IDS

Consider the following questions while articulating goals and objectives:

- Which type of threats does an IDS/IPS protect against?
- Will an IDS/IPS be able to monitor activities against acceptable use, violations, non-security reasons, etc.?

Security and Other IT Policies

Review the current security and IT policies and evaluate whether a certain IDS will offer the specified protection to meet an organization's policies

Consider the following points when selecting and IDS product:

- Policy goals
- Reasonable use policies
- Policy violations and consequences

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

IDS Product Selection: General Requirements (Cont'd)

External Requirements:

- Security-specific requirements
- Security audit requirements
- System accreditation requirements
- Standards and law enforcement, incident investigation, incident response requirements
- Purchase products previously evaluated through an independent process
- Cryptography requirements

Resource Constraints:

- An organization should consider **constraints** that add extra costs to implement IDS/IPS features
- **Consider the following constraints:**
  - The budget required to purchase, deploy, administer, and maintain the IDS/IPS hardware, software, and infrastructure
  - The staff needed to monitor and maintain an IDS

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

IDS Product Selection: General Requirements

An organization needs to have a clear baseline of the requirements for an IDS product. Each IDS solution may differ in features and services. An organization needs to determine which IDS product will suit their requirements the best. 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

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

https://t.me/learningnets

method of detecting anomalies and the process of connecting to other components that decide if the product can satisfy the company's requirements.

The selection of an IDS depends on the general requirements listed below:

System and Network Environments

The network defender should be able to select the IDS product according to the requirements of the organization and its network configuration. In addition, the selected IDS product should be able to detect and log events of interest that the organization wants to evaluate and examine. Consider the characteristics listed below.

- Technical specifications of the IT environment
- Technical specifications of the existing security protections

Goals and Objectives

The network defender must evaluate their product against technical-, operational-, and business-related goals and objectives. Consider the characteristics listed below.

- Which type of threats will the IDS monitor?
- Will it monitor acceptable use violations?

Security and Other IT Policies

The network defender should review their security policies prior to selecting the IDS product. Consider the characteristics listed below.

- Policy goals
- Reasonable use policies
- Consequences of no compliance with policies

External Requirements

If the organization is supposed to undergo a review by other organizations, an network defender will need to assess whether they can review the IDS implementation in their organization.

- Security-specific requirements help in the investigation of security violation incidents.
- Audit requirements are specific functions an IDS must support.
- System accreditation requirements help network defender address the accreditation authority's requirements.
- An IDS must support law enforcement investigations and the resolution of security incident requirements.
- Purchase products previously evaluated through an independent process requirement.

Resource Constraints

network defenders should also consider their adequacy in terms of system or personnel to handle the IDS feature that they are thinking of implementing. Expenses on additional IDS features will

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

https://t.me/learningnets

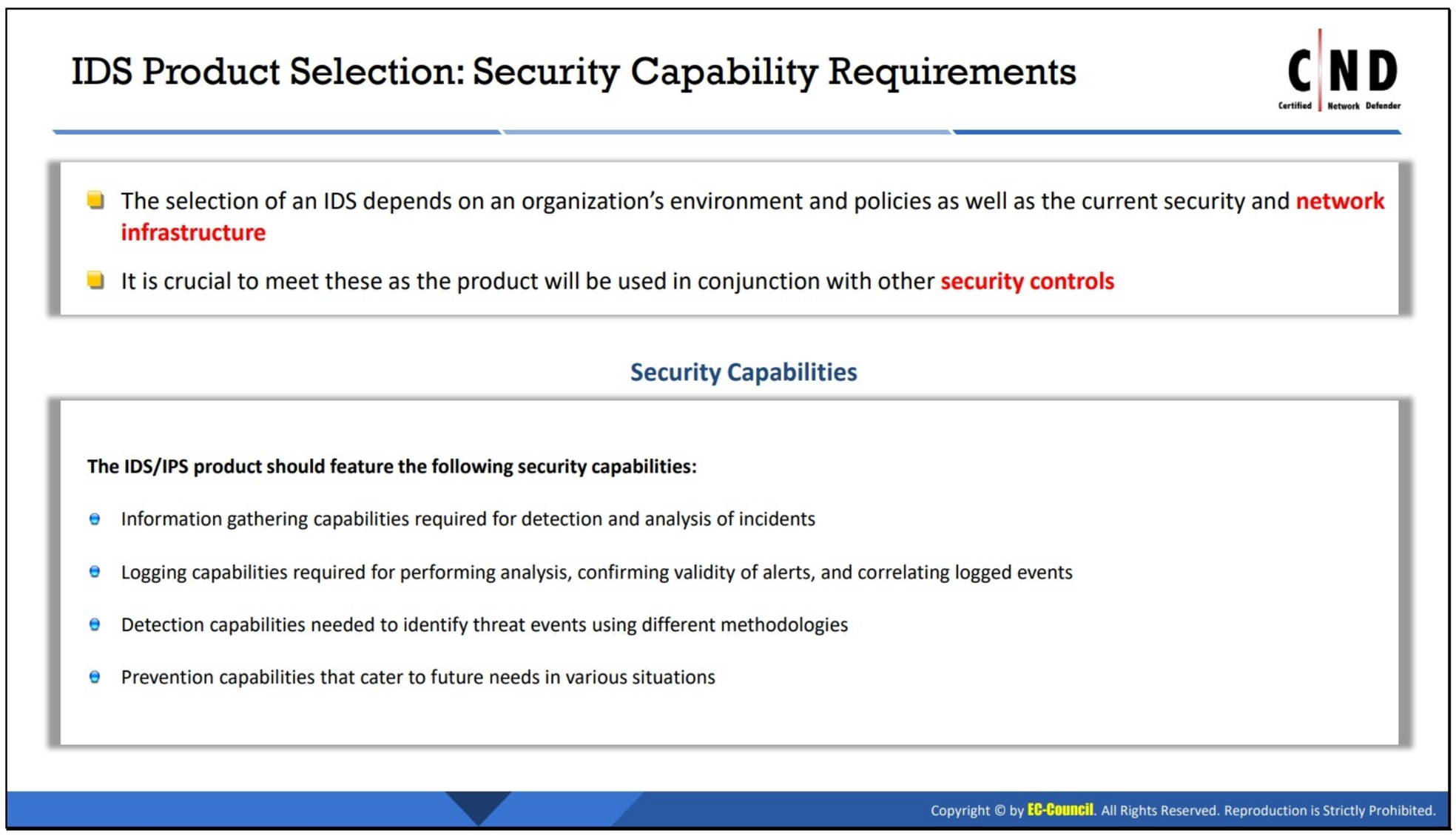
Technet24

be in vain if the organizations do not have enough resources to handle them. Specifically, consider the following constraints:

- The budget for purchasing, implementing, and maintaining IDS hardware, software, and structure.
- The staff needed to monitor and maintain an IDS.

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

https://t.me/learningnets



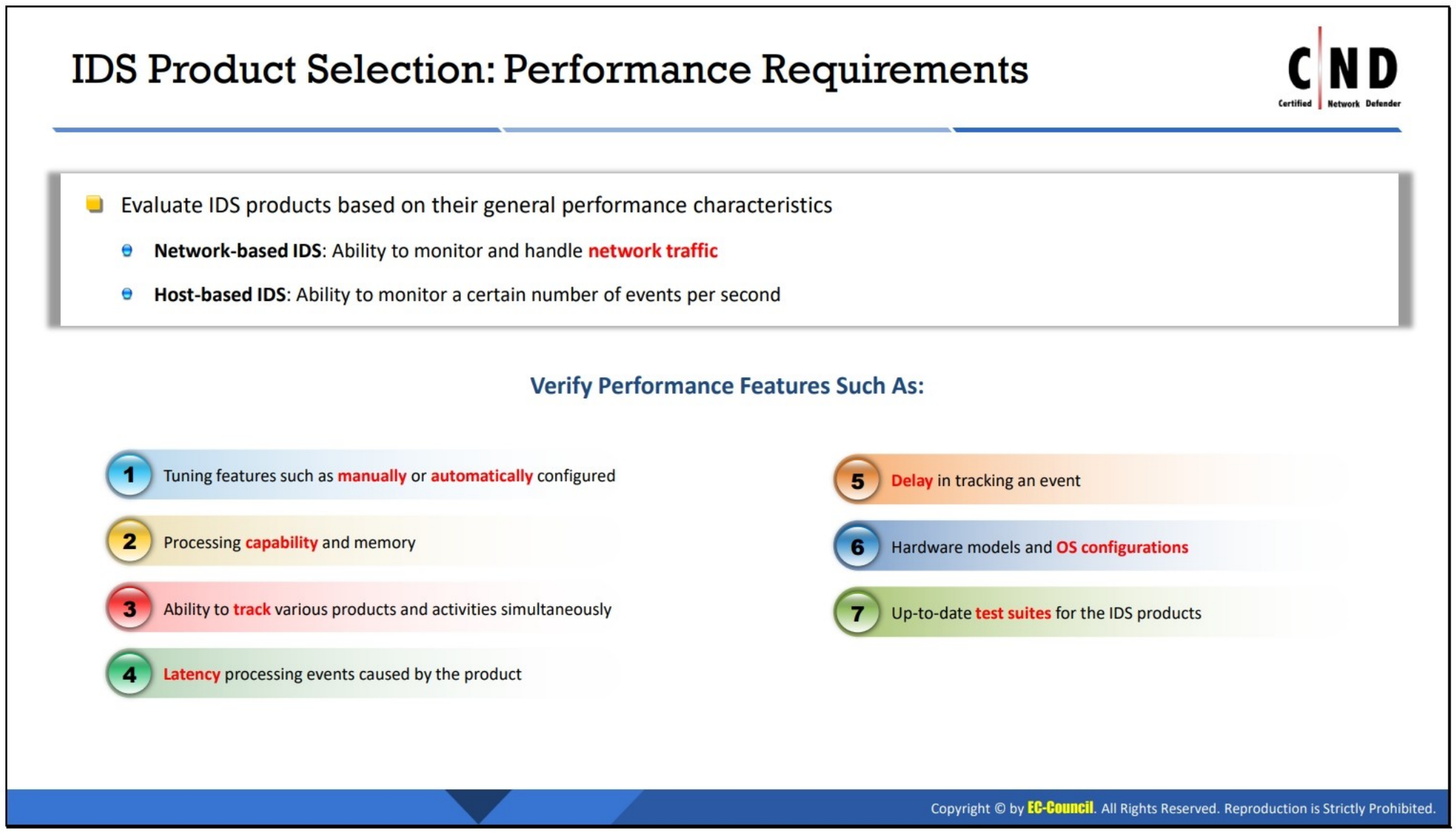
IDS Product Selection: Security Capability Requirements

In addition to defining general requirements, the network defenders needs to define a specialized set of requirements. Organizations should evaluate IDS security capability requirements as a baseline for creating a specific set of criteria. This is done by taking their environment, security policies, and network infrastructure into consideration. 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 an network defender 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.

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

https://t.me/learningnets

Technet24



IDS Product Selection: Performance Requirements

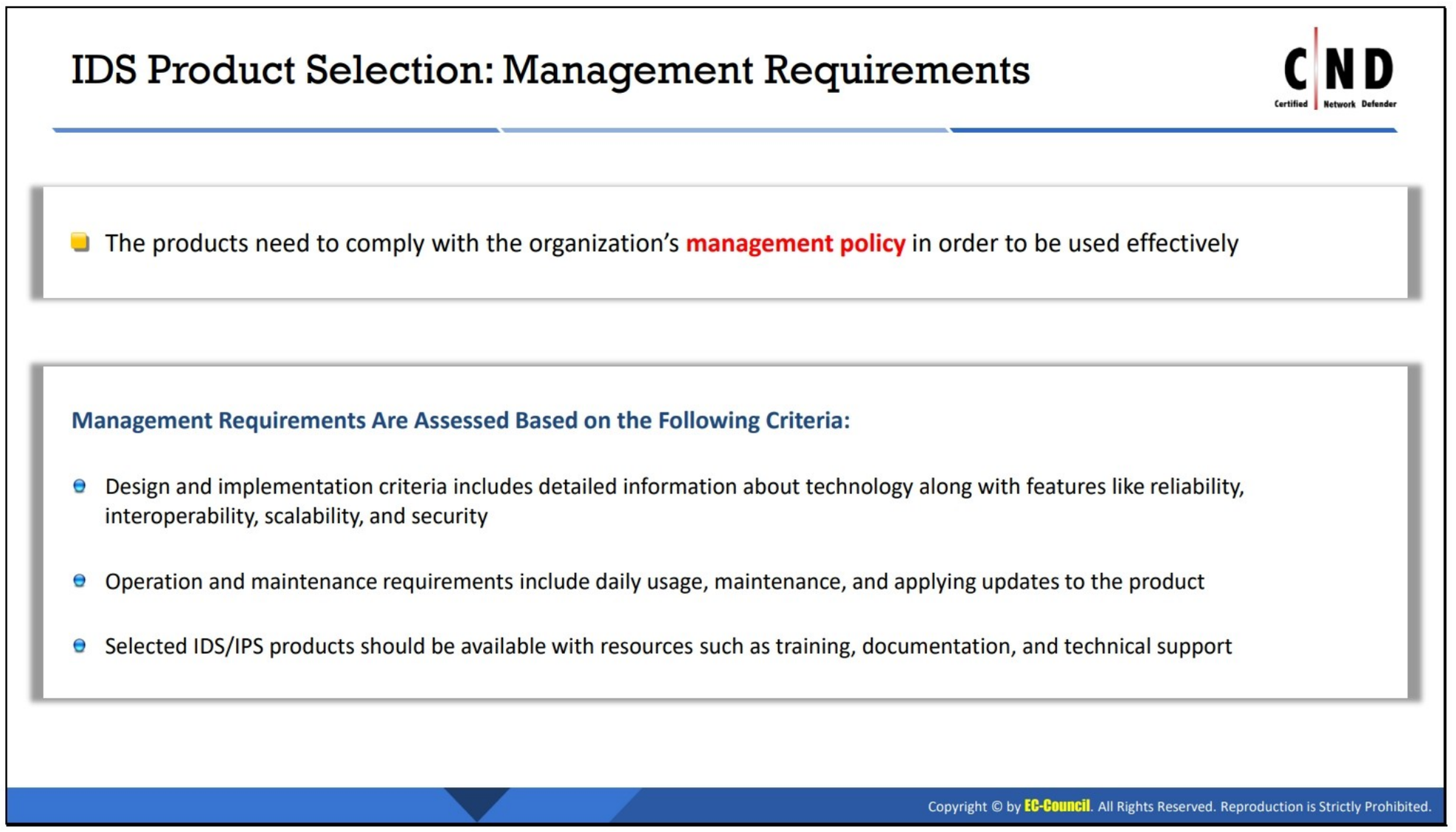
Network defenders should evaluate an IDS product's general performance characteristics by assessing its capacity to handle the network traffic or packet monitoring capabilities for NIDS and event monitoring capabilities for HIDS.

Verify the performance features that are listed below:

- Tuning features of an IDS, as its performance is dependent on product configuration and tuning
- Processing capability and memory
- Ability to track various product state activities simultaneously
- Latency of processing events caused by the product
- Delay in tracking an event
- Hardware models and OS configurations
- Up-to-date test suites for the IDS products

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

https://t.me/learningnets



IDS Product Selection: Management Requirements

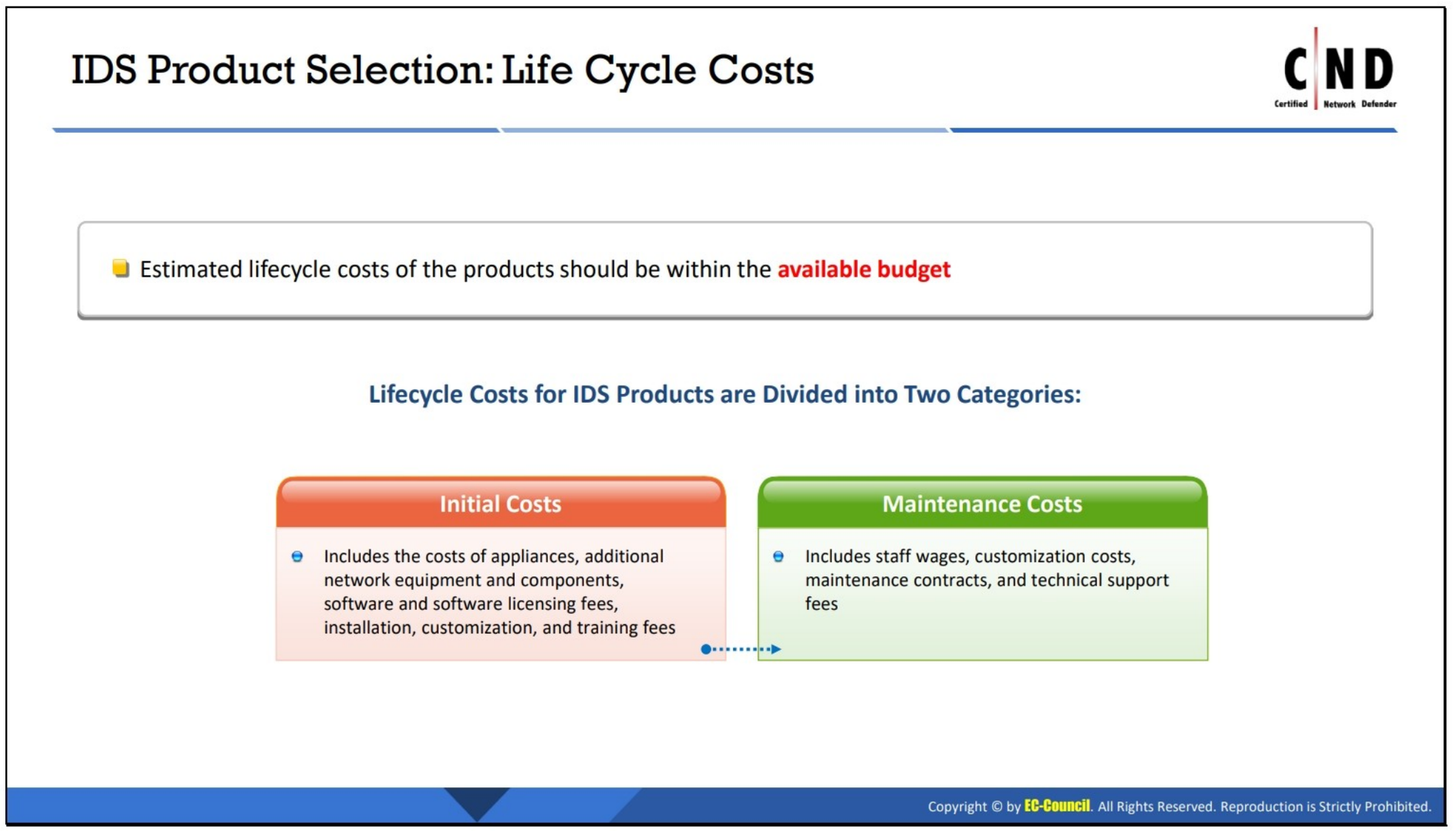
The products need to comply with the organization's management policy in order to offer better performance. If the product does not comply with the company's policy, it would be difficult to handle and make it work effectively. Some examples of management requirements for an IDS are listed below:

- Design and implementation criteria, including detailed information about the technology type used in the product along with features such as reliability, interoperability, scalability, and security
- Operation and maintenance requirements, including daily usage, maintenance, and applying updates to the product
- Better interoperability, which refers to the process of offering effective performance while working in combination with existing systems
- Resources such as training, documentation, and technical support
- Scalability, so that the company would be able to increase or decrease the product quantity to meet future requirements

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

https://t.me/learningnets

Technet24



IDS Product Selection: Life Cycle 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 liable to dominate the situation. Lifecycle costs of the IDS products include the following categories.

Initial Costs

The initial cost is the starting point for all IDS product calculations. Its components are listed below.

- Cost for deploying hardware or software tools: It involves the cost of network devices, IDS load balancers, and software tools such as reporting tools, database software, etc.
- Installation and configuration costs: This cost includes internal or external labor for fixing systems and network devices or for installing network or system accessories.
- Cost of application customization: This type of cost involves the programmers or developers who develop scripts or applications for maintaining the security.
- Cost for training and awareness: It involves the cost for training and its awareness among the administrators.

Maintenance Costs

Usually organizations do not have a standard for measuring maintenance costs, which results in different costs within the same organization. The various components of maintenance costs are listed below.

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

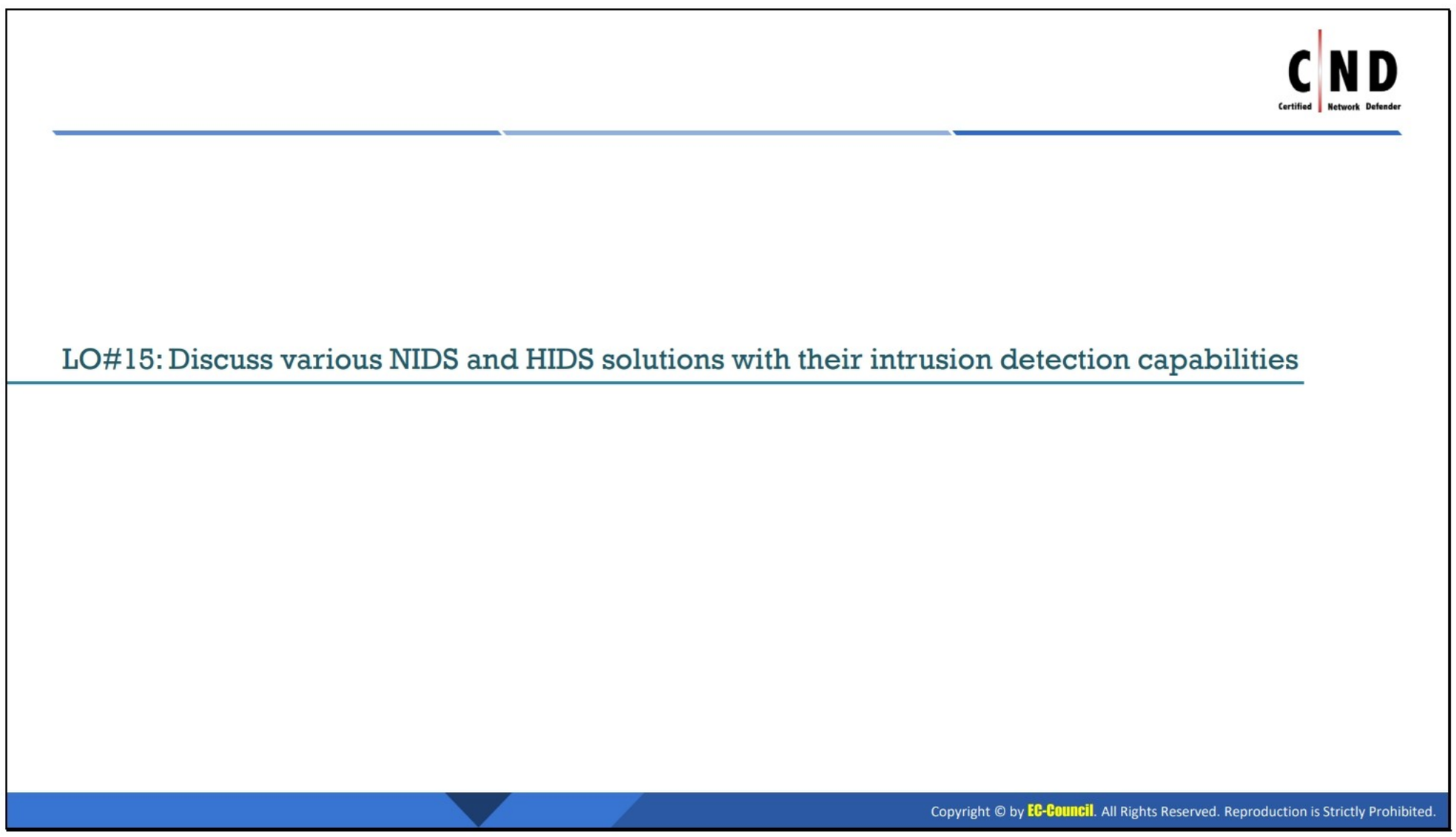
https://t.me/learningnets

- Cost of labor: Cost of labor includes the cost of staff handling the IDS solutions and the administration.
- Cost of technical support: Costs associated with organizations using external technical support from third-party services.
- Cost of professional services: Technical support vendors that do not provide IDS solution services fall under professional services.

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

https://t.me/learningnets

Technet24

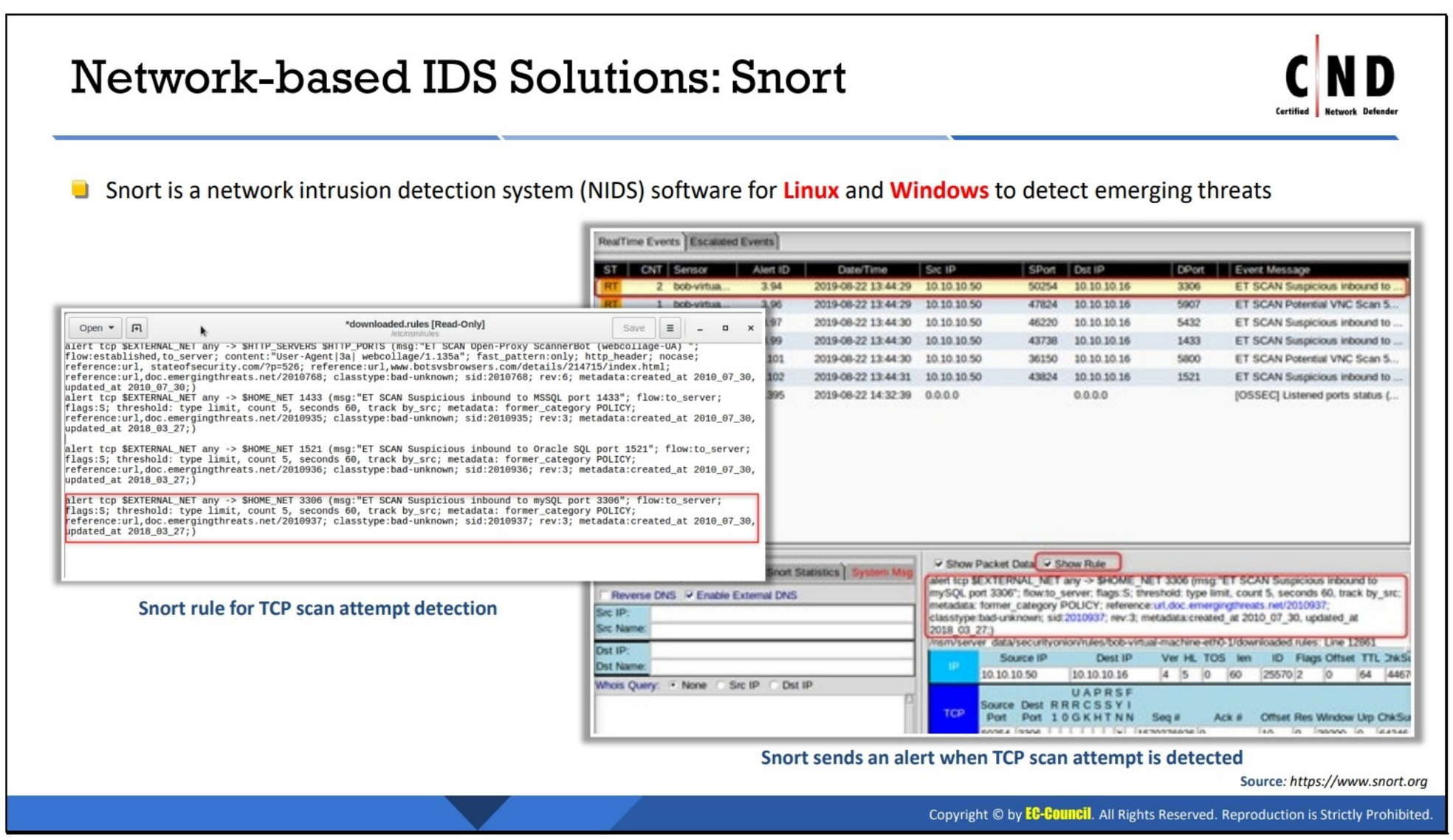


LO#15: NIDS and HIDS Solutions with Their Intrusion Detection Capabilities

This section describes various NIDS and HIDS solutions along with their intrusion detection capabilities.

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

https://t.me/learningnets



Network-based IDS Solutions: Snort

Snort

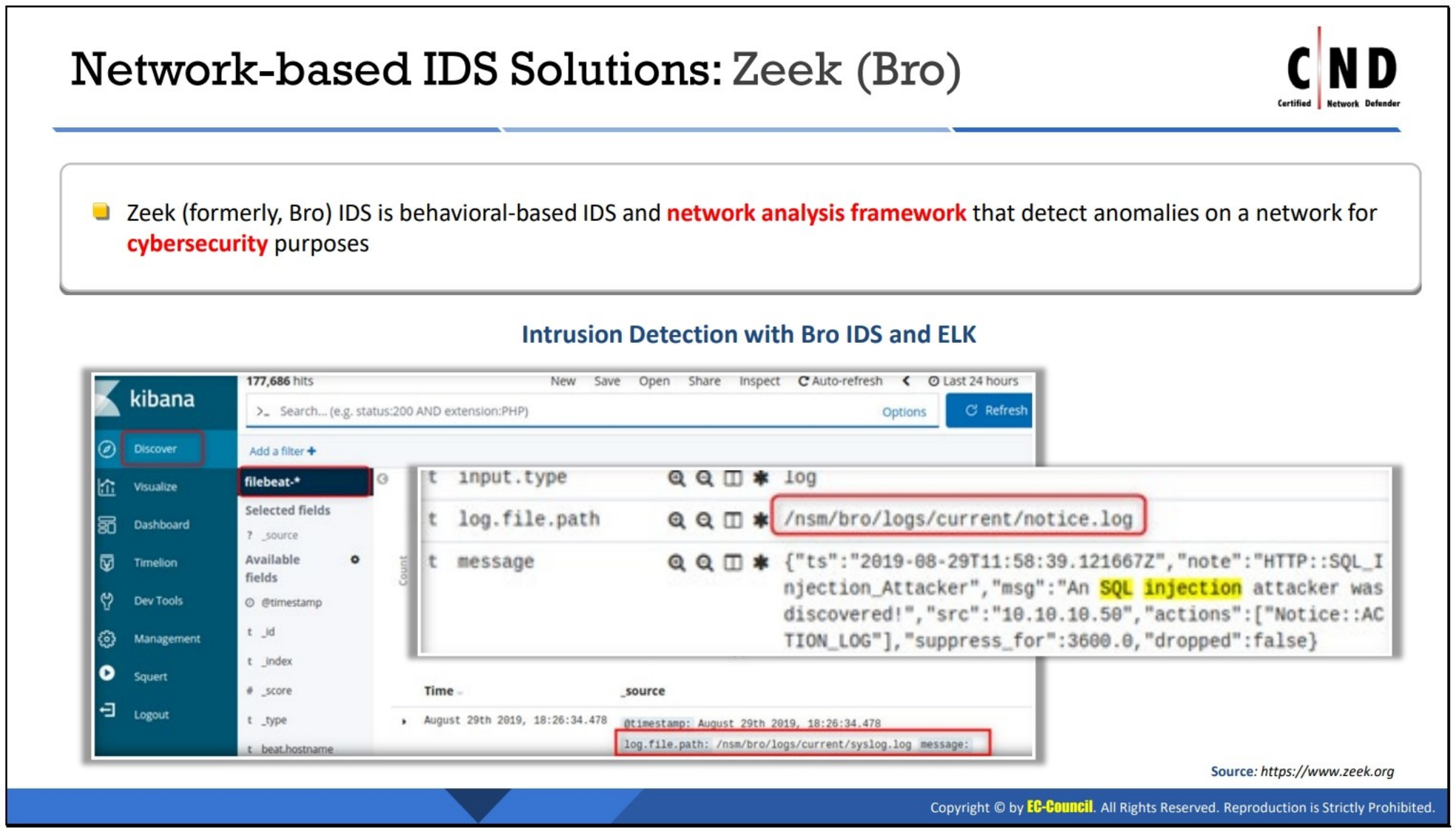
Source: https://www.snort.org

Snort is an open-source NIDS software for Linux and Windows to detect emerging threats. It is capable of real-time traffic analysis and packet logging on IP networks, protocol analysis, content searching, and matching against a ruleset defined by the user. The program will do an action based on what has been identified. It uses a rule-based language combining signature, protocol, and anomaly inspection methods to identify malicious activity. It can also be used to identify DoS attacks, OS fingerprinting attempts, buffer overflows, semantic URL attacks, stealth port scans, server message block probes, CGI attacks, and SMB probes.

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

https://t.me/learningnets

Technet24



Network-based IDS Solutions: Zeek (Bro)

Zeek

Source: https://www.zeek.org

Zeek (formerly, Bro) is a behavioral-based IDS and network analysis framework that can detect anomalies in a network for cybersecurity purposes. Zeek analyses general network traffic while focusing on network security monitoring.

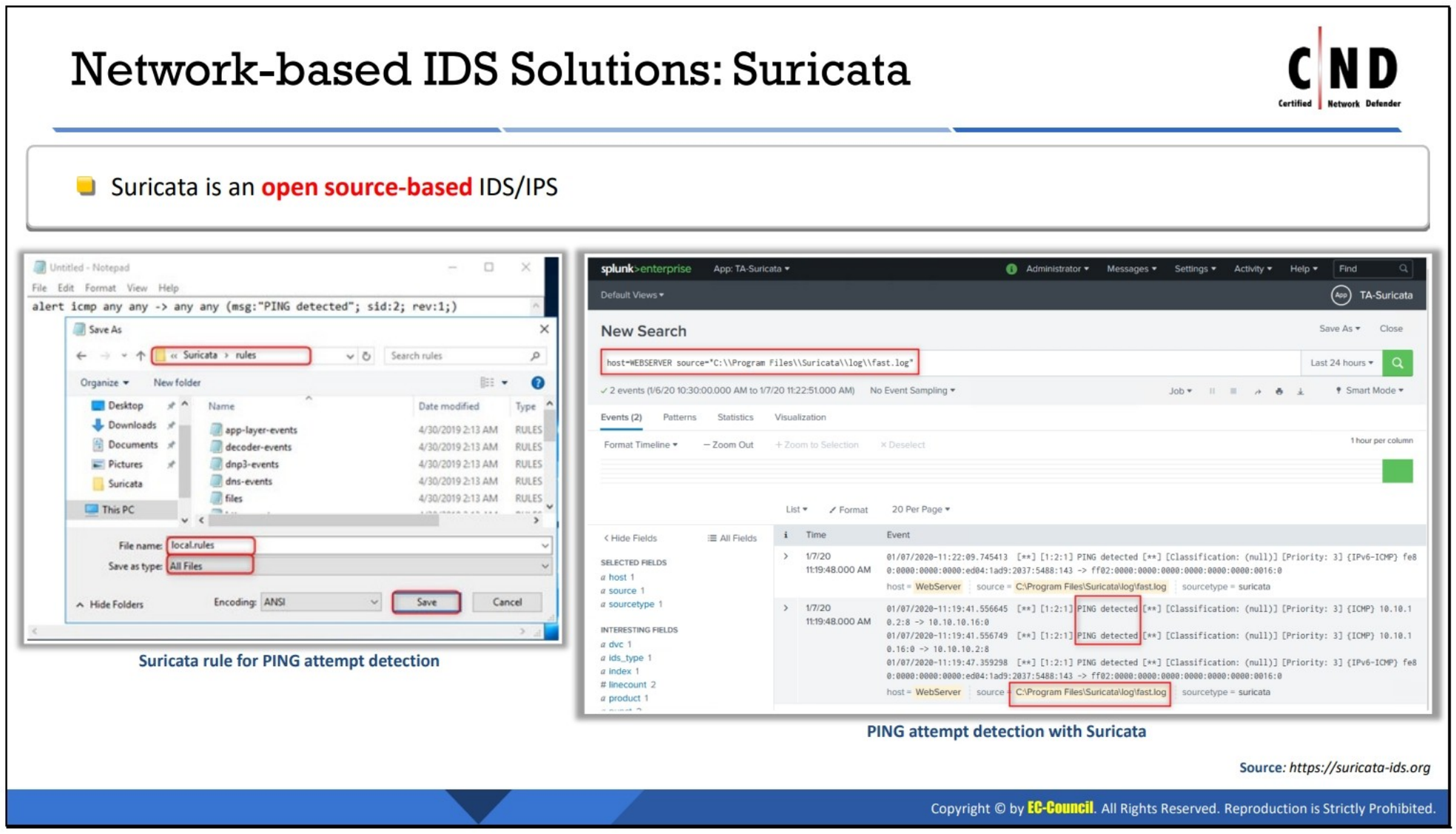
Features:

- It is not restricted to any particular detection approach and does not rely on traditional signatures.
- It targets high-performance networks and is used operationally at a variety of large sites.
- It comprehensively logs what it sees and provides a high-level archive of a network's activity.
- It comes with analyzers for many protocols, enabling high-level semantic analysis at the application layer.
- It keeps extensive application-layer state about the network it monitors.
- Its domain-specific scripting language enables site-specific monitoring policies.

To monitor and analyze the generated logs from Zeek IDS we can integrate it with various SIEM solutions. Zeek logs can be integrated with ELK stack to analyze and visualize the data. Configuring the Zeek's notification framework is useful for alerting, which can notify if a suspicious network activity exists but its scope is limited. Tools such as X-Pack, Logz.io, etc., can be used for generating alerts for any suspicious activity.

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

https://t.me/learningnets



Network-based IDS Solutions: Suricata

Suricata

Source: https://suricata-ids.org

The Suricata engine is capable of real-time intrusion detection, inline intrusion prevention, network security monitoring (NSM), and offline pcap processing.

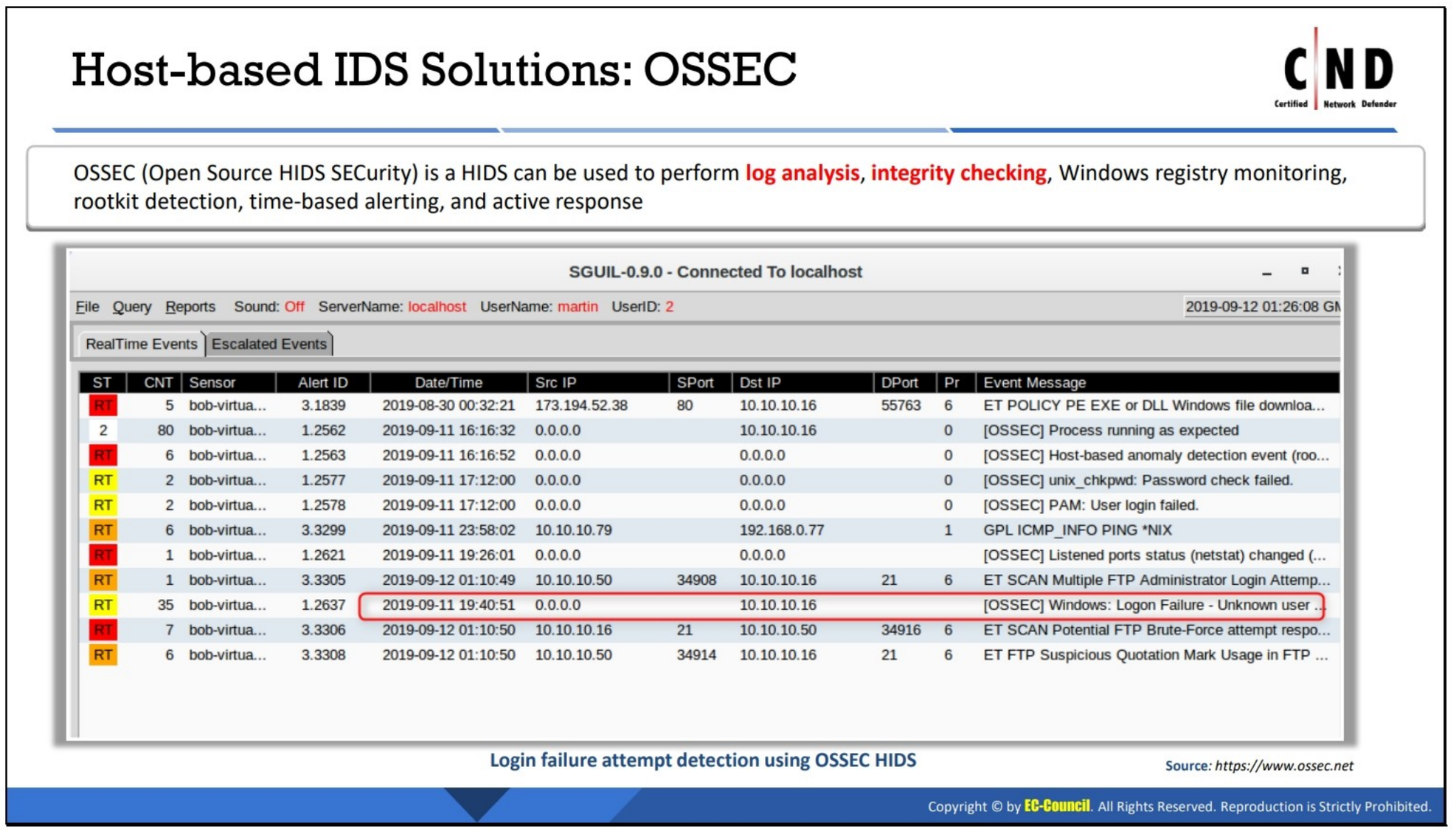
Features:

- A single Suricata instance can inspect multi-gigabit traffic.
- It automatically detects protocols such as HTTP on any port and applies the proper detection and logging logic. The full pcap capture support allows easy analysis.
- It provides Lua scripting—advanced analysis and functionality for detecting things not possible within the ruleset syntax.
- It offers industry-standard logging output, "Eve," allowing for easy integration with Logstash and similar tools.
- Suricata supports standard input output formats such as YAML and JSON, which can be easily integrated with various SIEM tools such as Splunk, Logstash/Elasticsearch, Kibana, etc.

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

https://t.me/learningnets

Technet24



Host-based IDS Solutions: OSSEC

OSSEC

Source: https://www.ossec.net

OSSEC (Open Source HIDS SECurity) is a HIDS can be used to perform log analysis, integrity checking, Windows registry monitoring, rootkit detection, time-based alerting, and active response. OSSEC offers extensive configuration options, adding custom alert rules, and writing scripts to take action when alerts occur.

Features:

- Log-based intrusion detection (LIDs)
- Rootkit and malware detection
- Active response through firewall policies, integration with 3rd parties such as CDNs and support portals, as well as self-healing actions
- File integrity monitoring (FIM), in which changes to the system are detected

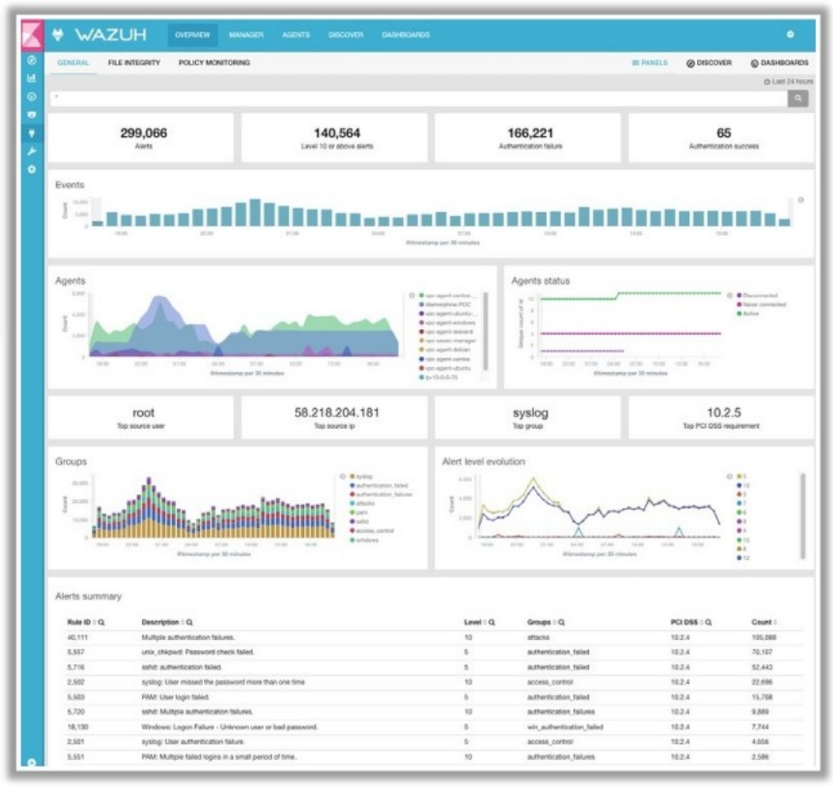
Logs and events generated from OSSEC can be monitored using tools such as Suricata, AlienVault USM, etc.

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

https://t.me/learningnets

Host-based IDS Solutions: Wazuh

- Wazuh is a host-based intrusion detection system. It performs **log analysis**, **integrity checking**, Windows registry monitoring, rootkit detection, time-based alerting, and active response
- Wazuh was born as a **fork of OSSEC HIDS**



Source: https://wazuh.com

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

Host-based IDS Solutions: Wazuh

Wazuh

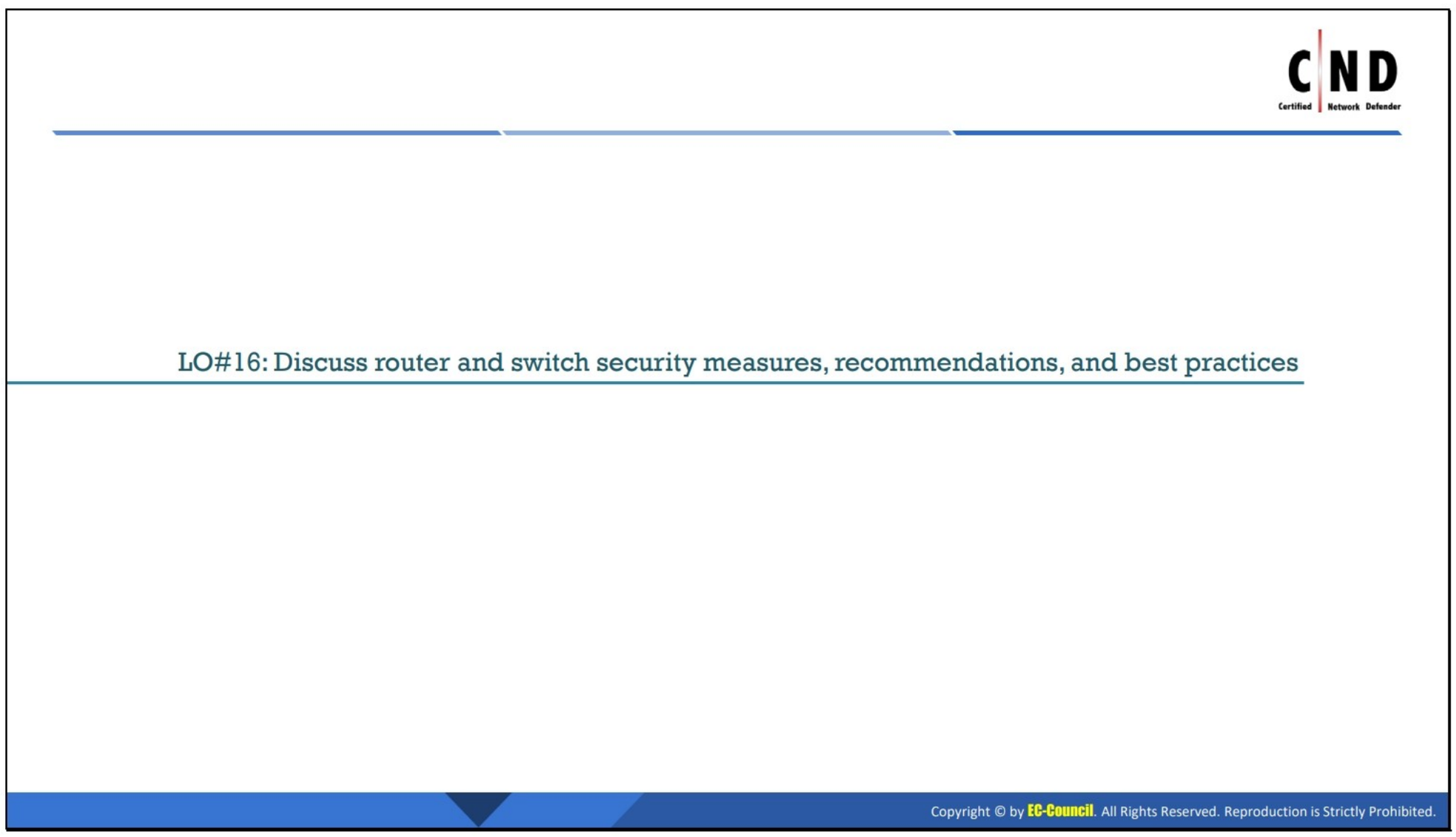
Source: https://wazuh.com/

Wazuh is a host-based IDS that performs log analysis, integrity checking, Windows registry monitoring, rootkit detection, time-based alerting, and active response. It was born as a fork of OSSEC HIDS. Wazuh agent runs at the host level, combining anomaly and signature-based technologies to detect intrusions or software misuse. It can also be used to monitor user activities, assess system configuration, and detect vulnerabilities.

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

https://t.me/learningnets

Technet24

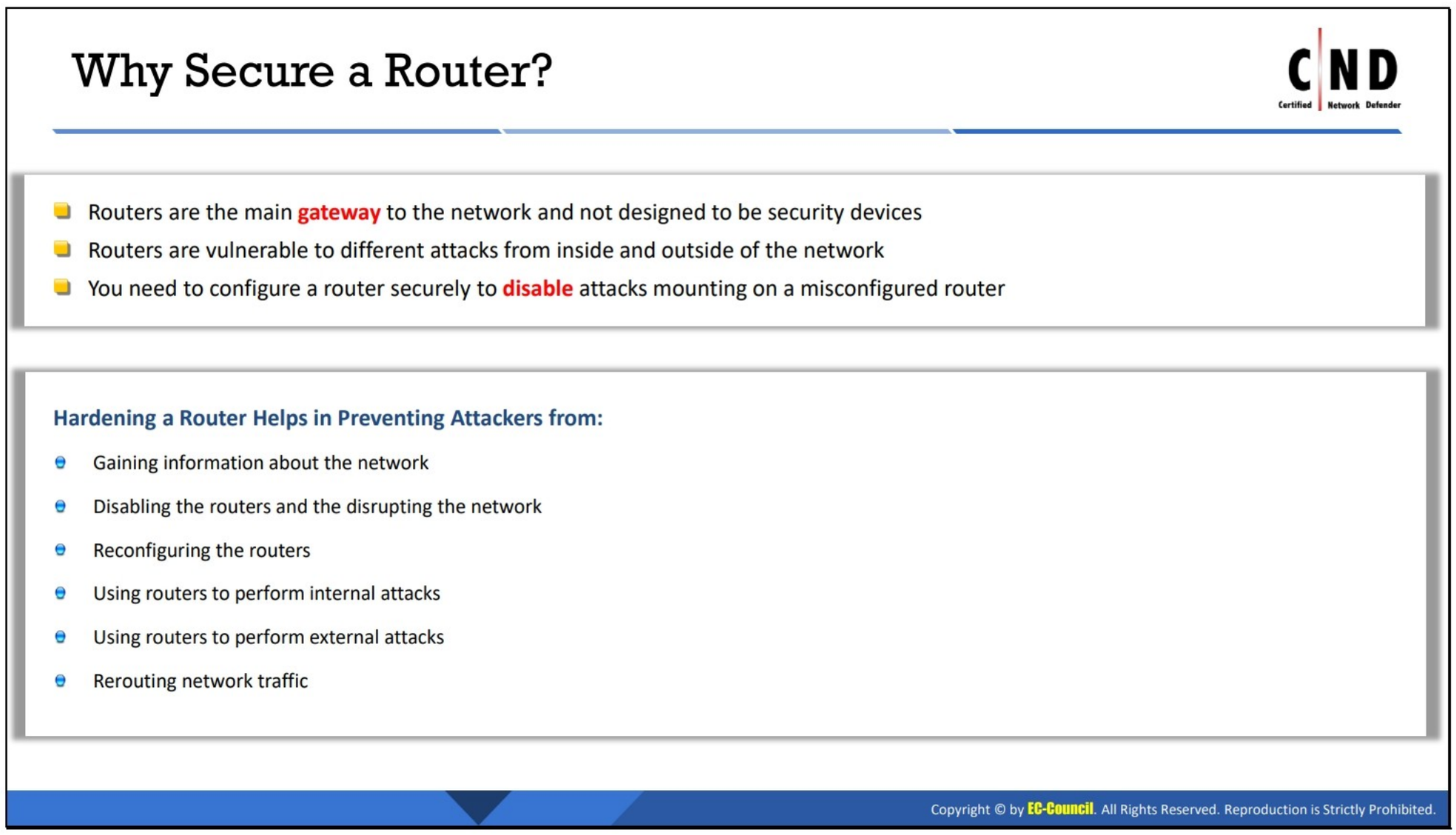


LO#16: Router and Switch Security Measures, Recommendations, and Best Practices

This section describes the various security recommendations and best practices for router and switch security.

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

https://t.me/learningnets



Why Secure a Router?

Routers are the main gateway to the network and not designed to be security devices. Routers are vulnerable to different attacks from inside and outside of the network. You need to configure a router securely to disable attacks mounting on a misconfigured router

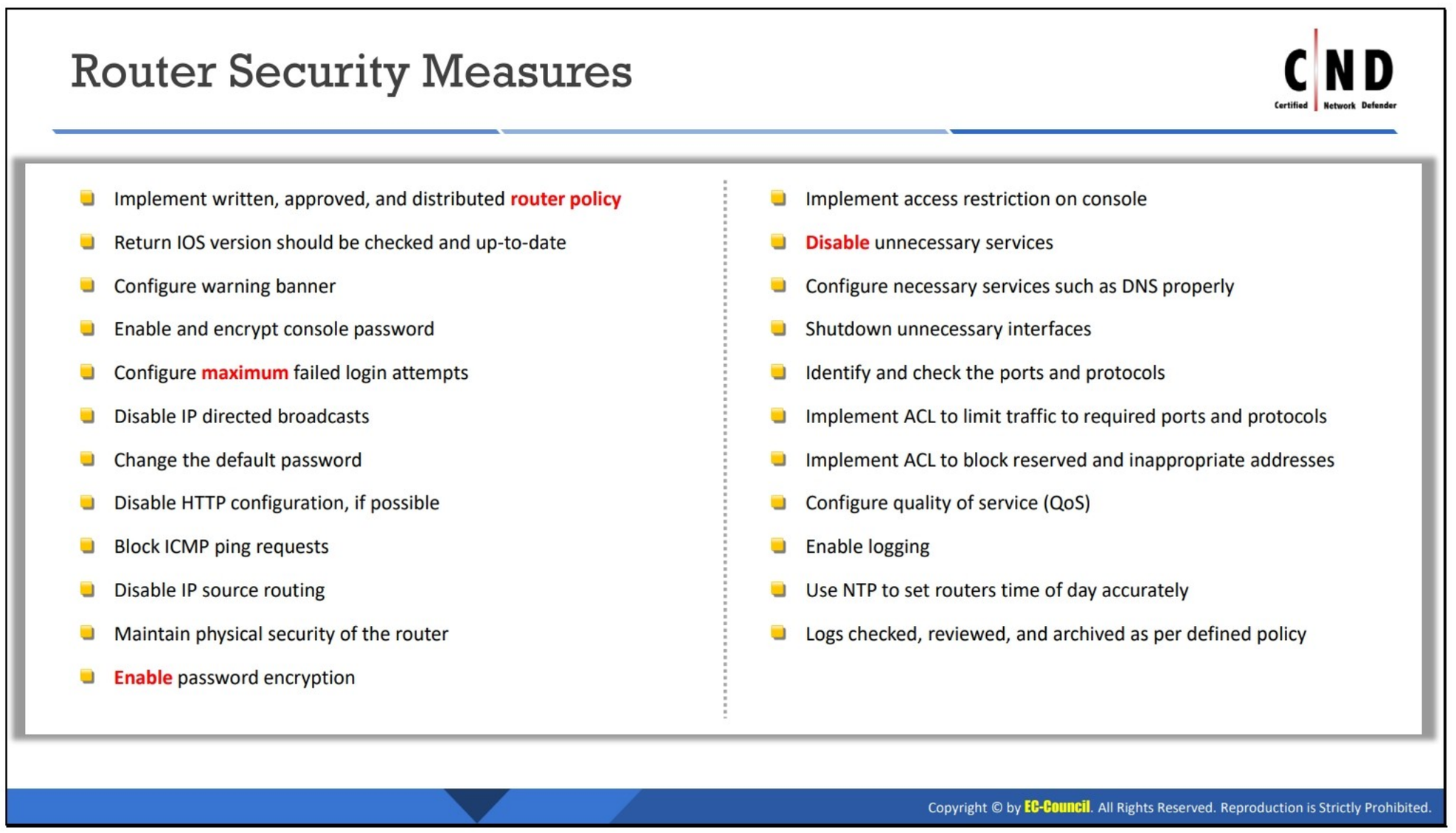
Hardening a Router Helps in Preventing Attackers from:

- Gaining information about the network
- Disabling the routers and the disrupting the network
- Reconfiguring the routers
- Using routers to perform internal attacks
- Using routers to perform external attacks
- Rerouting network traffic

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

https://t.me/learningnets

Technet24



Router Security Measures

The following are recommended best practices for enhancing the security of a router:

- Change the default password: Most users do not change the default password of the router after installation. This is the same thing as giving a key to attackers so they can easily log in to your router.
- Deactivate IP directed broadcasts: Enabling IP directed broadcasts would allow attackers to send ICMP ECHO requests to another user broadcast address, using a spoofed address. The broadcast network responds to the ECHO request thereby affecting the working of all hosts in the network.
- Deactivate the HTTP configuration: Enabling the HTTP protocol for routers sends clear text traffic.
- Restrict ICMP ping requests: Accepting ping requests enables attackers to guess the active hosts and thereby scan the network without the original user's knowledge.
- Disable IP source routing: Enabling this routing feature allows attackers to identify the path taken by the packet. This give user the ability to sniff packets from the network.
- Identify the need for packet filtering: Filtering of packets depends on the needs of the organization. The filtering mechanism helps identify whether to permit or block traffic.
- Create ingress and egress address-filtering policies: Creating policies for verifying the inbound and outbound traffic based on an IP address increases the security of the router.
- Maintain physical security of the router: It is mandatory to maintain physical security of the router as inappropriate placement of routers allows attackers to sniff and have direct access to the device.

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

https://t.me/learningnets

- Review the security logs: Appropriate review of the security logs will provide detailed information regarding what attacks, if any, have been launched against the router. It also provides a detailed description of the router. Reviewing logs of the router provides an overall idea regarding the status of the network too.

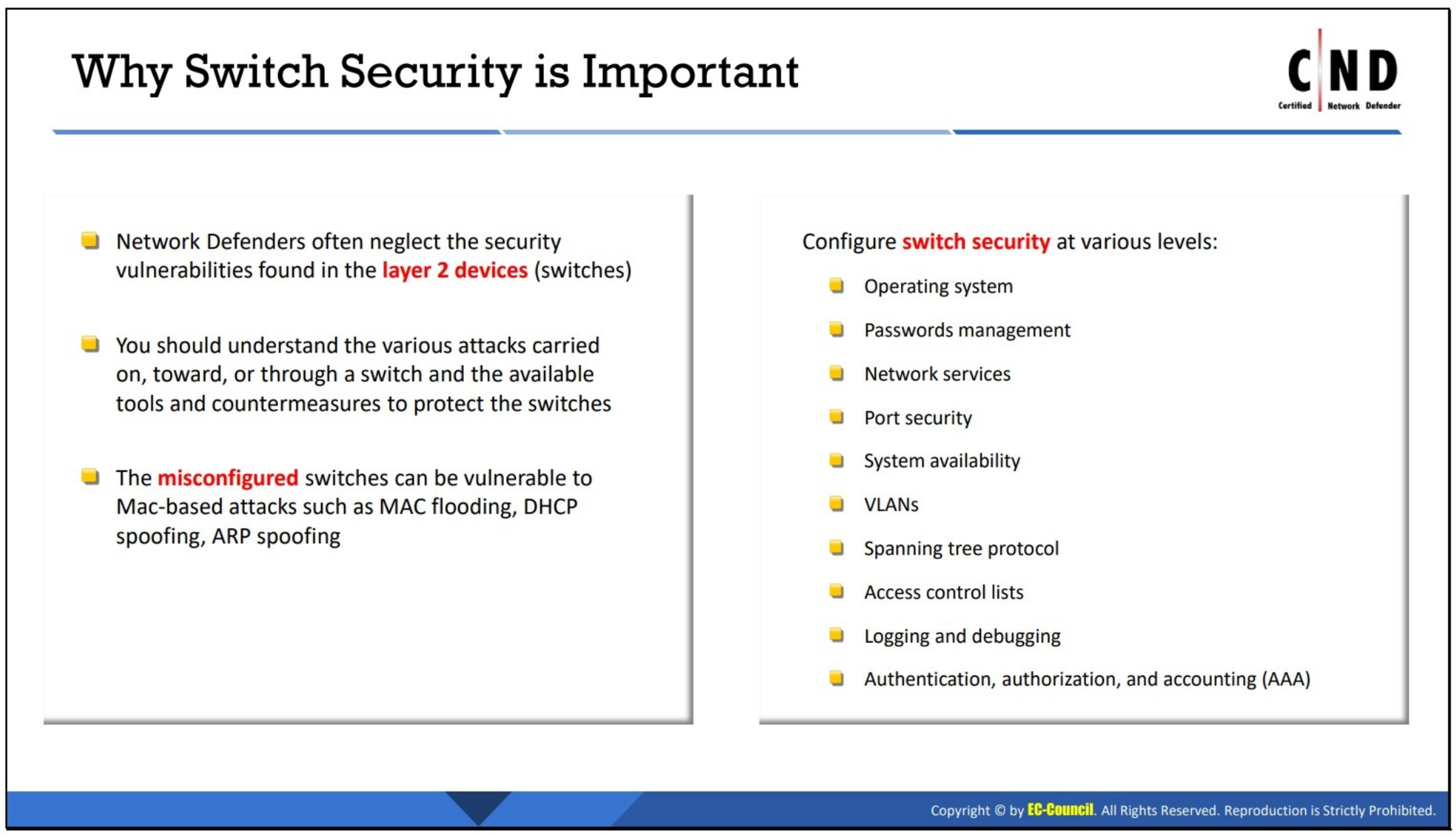
In addition to the above recommendations, implement the following best practices to harden router security:

- Disable unnecessary router interfaces.
- Disable unnecessary services.
- Disable unnecessary management protocols.
- Disable address resolution protocol (ARP) and proxy ARP.

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

https://t.me/learningnets

Technet24



Why Switch Security is Important

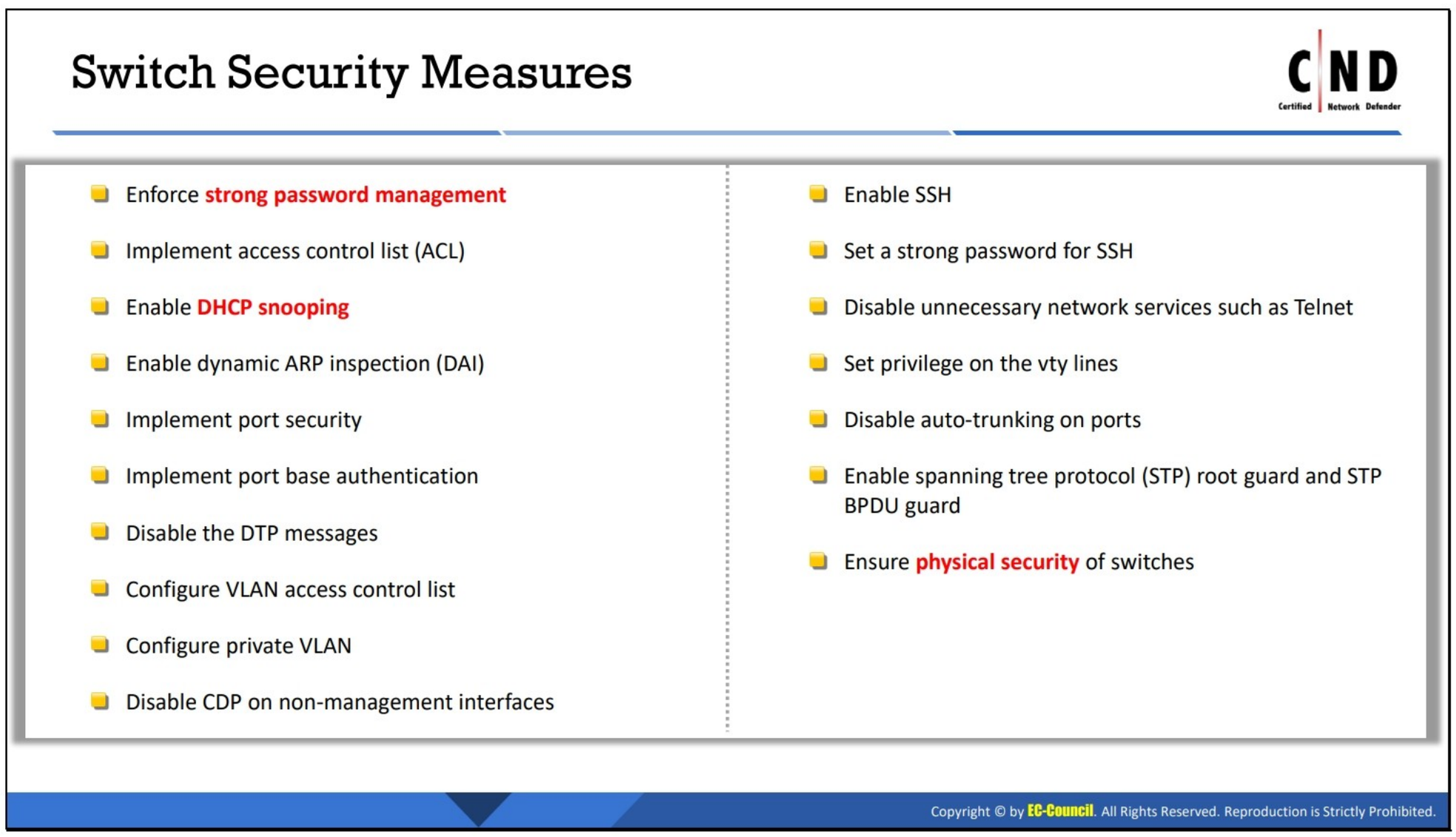
Network Defenders often neglect the security vulnerabilities found in the layer 2 devices (switches). You should understand the various attacks carried on, toward, or through a switch and the available tools and countermeasures to protect the switches. The misconfigured switches can be vulnerable to Mac-based attacks such as MAC flooding, DHCP spoofing, ARP spoofing

Configure switch security at various levels:

- Operating system
- Passwords management
- Network services
- Port security
- System availability
- VLANs
- Spanning tree protocol
- Access control lists
- Logging and debugging
- Authentication, authorization, and accounting (AAA)

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

https://t.me/learningnets



Switch Security Measures

The best way to manage switch security is by using port-level security. Port-level security limits the number of MAC addresses connected to a device. The three different methods of connecting MAC addresses to a port are described below.

- Statically: This allows only a single MAC address to be connected to a port.
- Dynamically: These are present by default in the content–addressable memory.
- Sticky: A MAC address given to a specific port. This MAC address can be lost if not saved during reboot.

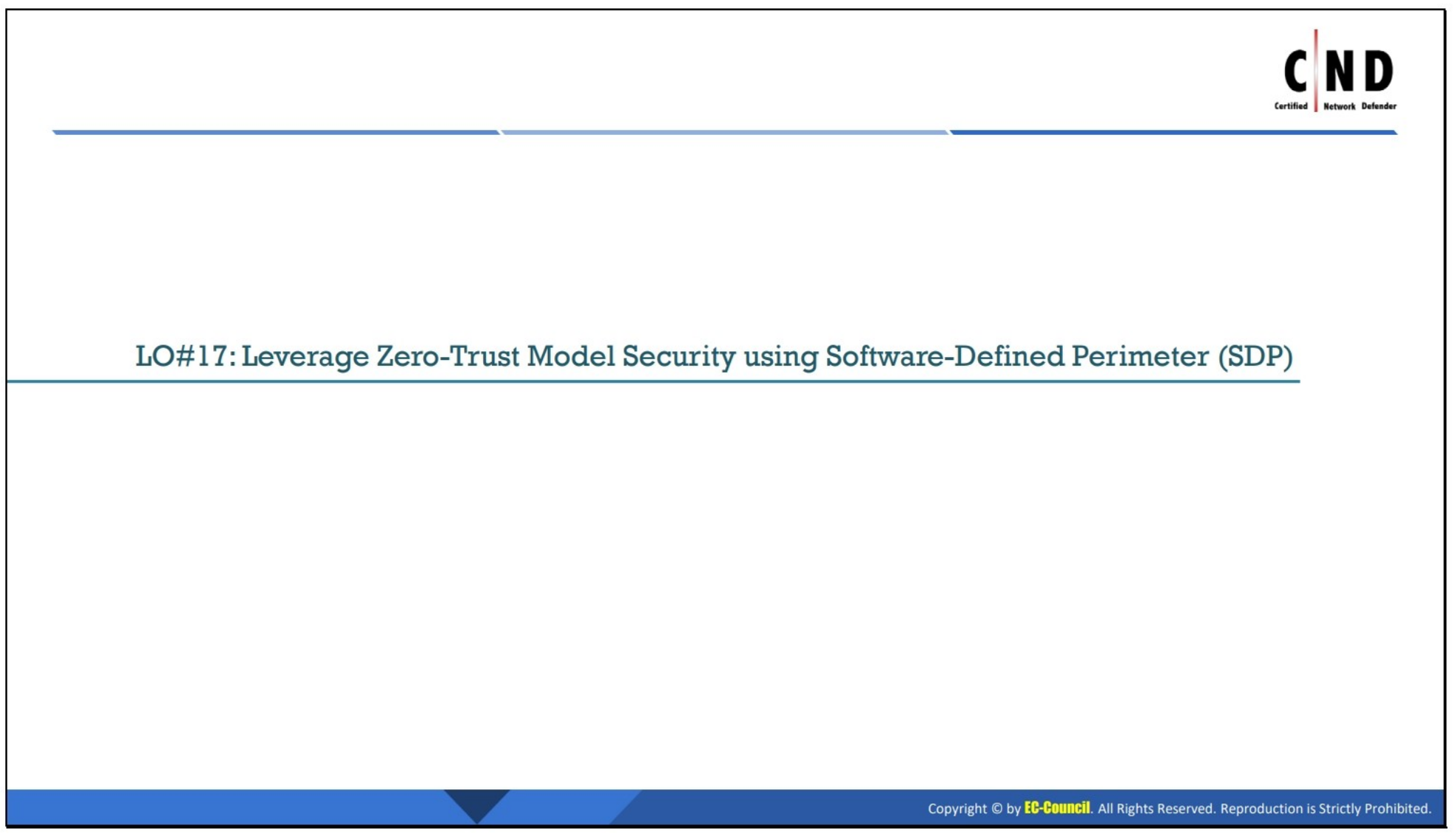
Some additional switch security best practices are listed below:

- Create a strong password.
- Create time-out sessions and user access rights.
- Disable auto-trunking on ports and activate port security for MAC addresses in order to control access.
- Deactivate all ports that are not in use and assign them an unused VLAN number.
- Control the number of VLANs that can pass over a trunk.
- Maximize the use of access control lists.
- Review all security logs of the switch
- Implement the principle of authentication, authorization, and accounting (AAA) for local and remote access to the switch.
- Keep the switch configuration file offline and control access to it.

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

https://t.me/learningnets

Technet24

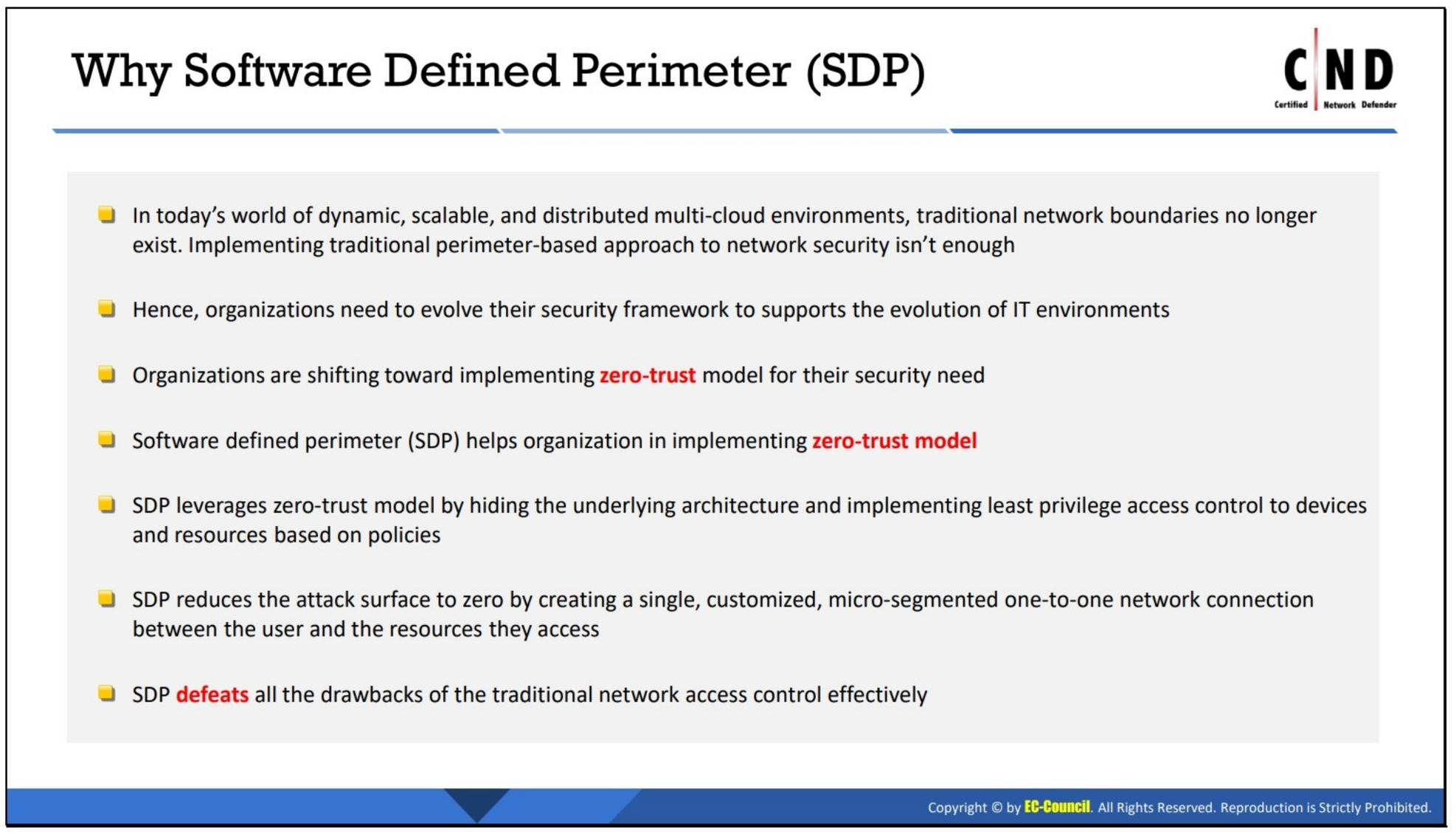


LO#17: Leverage Zero-Trust Model Security using Software-Defined Perimeter (SDP)

This section describes the role of software-defined perimeter (SDP) in an organization's network security.

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

https://t.me/learningnets



Why Software Defined Perimeter (SDP)

In today's world of dynamic, scalable, and distributed multi-cloud environments, traditional network boundaries no longer exist. Implementing a traditional perimeter-based approach to network security is not enough. The traditional perimeter model is not identity-centric and allows anyone to access the resources.

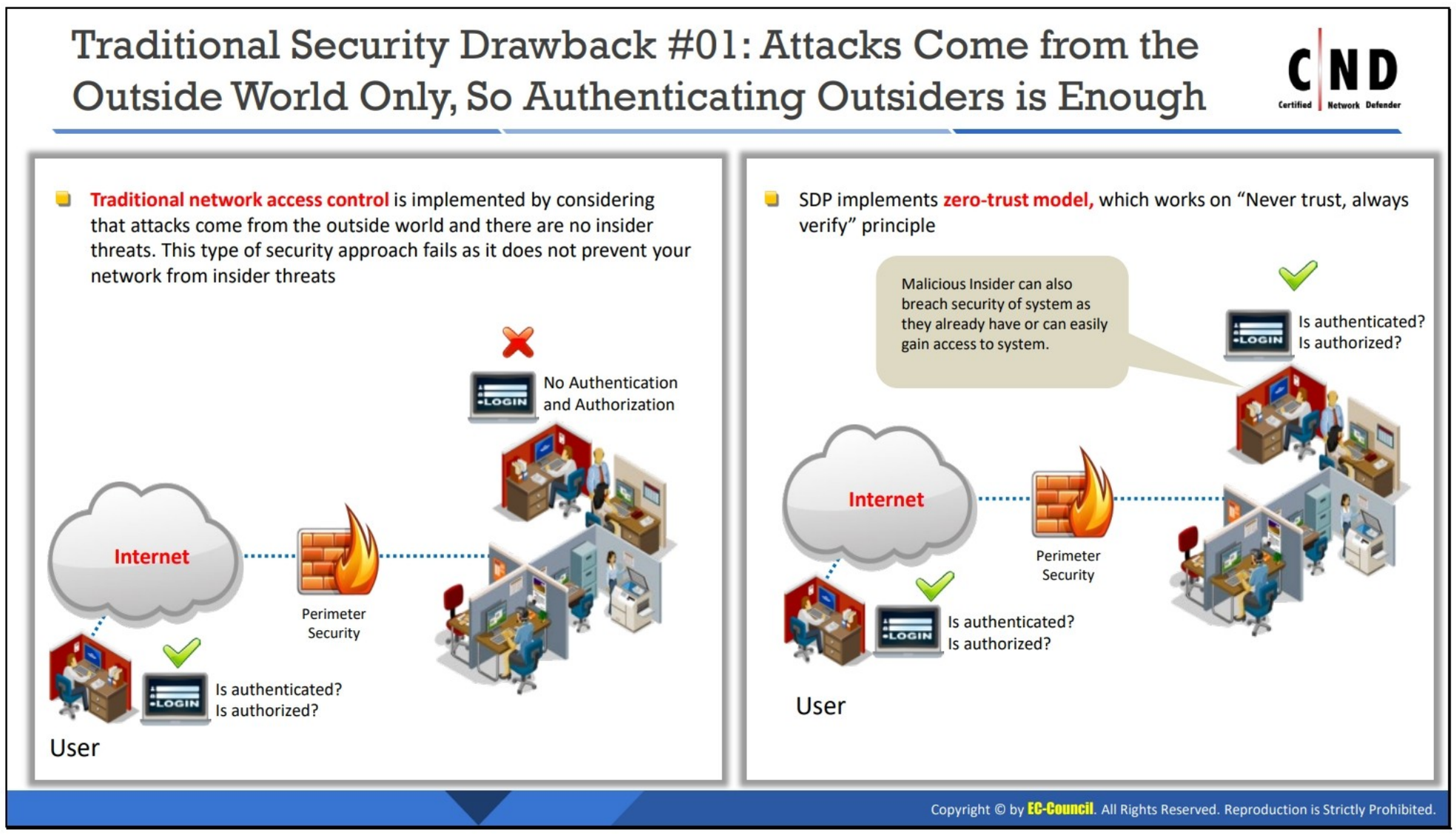
The cloud application infrastructure is vulnerable to various network attacks and the traditional perimeter defense techniques fails to safeguard it. The adversary can easily gain access to the devices inside the perimeter and target the application infrastructure; as the number of devices increases inside the perimeter, the vulnerabilities also increase simultaneously. Traditional networking tools also cannot keep up with the pace of the business and are difficult to manage the security of the network. The traditional network security approach does not provide network segmentation, fine-grained user access control, traffic visibility, on-premises security, Wi-Fi security, etc. Hence, organizations need to evolve their security framework to support the evolution of IT environments.

Presently, organizations are shifting toward the zero-trust model for their security needs. SDP helps the organization in implementing the zero-trust model. SDP leverages the zero-trust model by hiding the underlying architecture and implementing least privilege access control to devices and resources based on policies. SDP reduces the attack surface to zero by creating a single, customized, micro-segmented one-to-one network connection between the user and the resources they access. Therefore, SDP defeats all the drawbacks of the traditional network access control effectively.

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

https://t.me/learningnets

Technet24



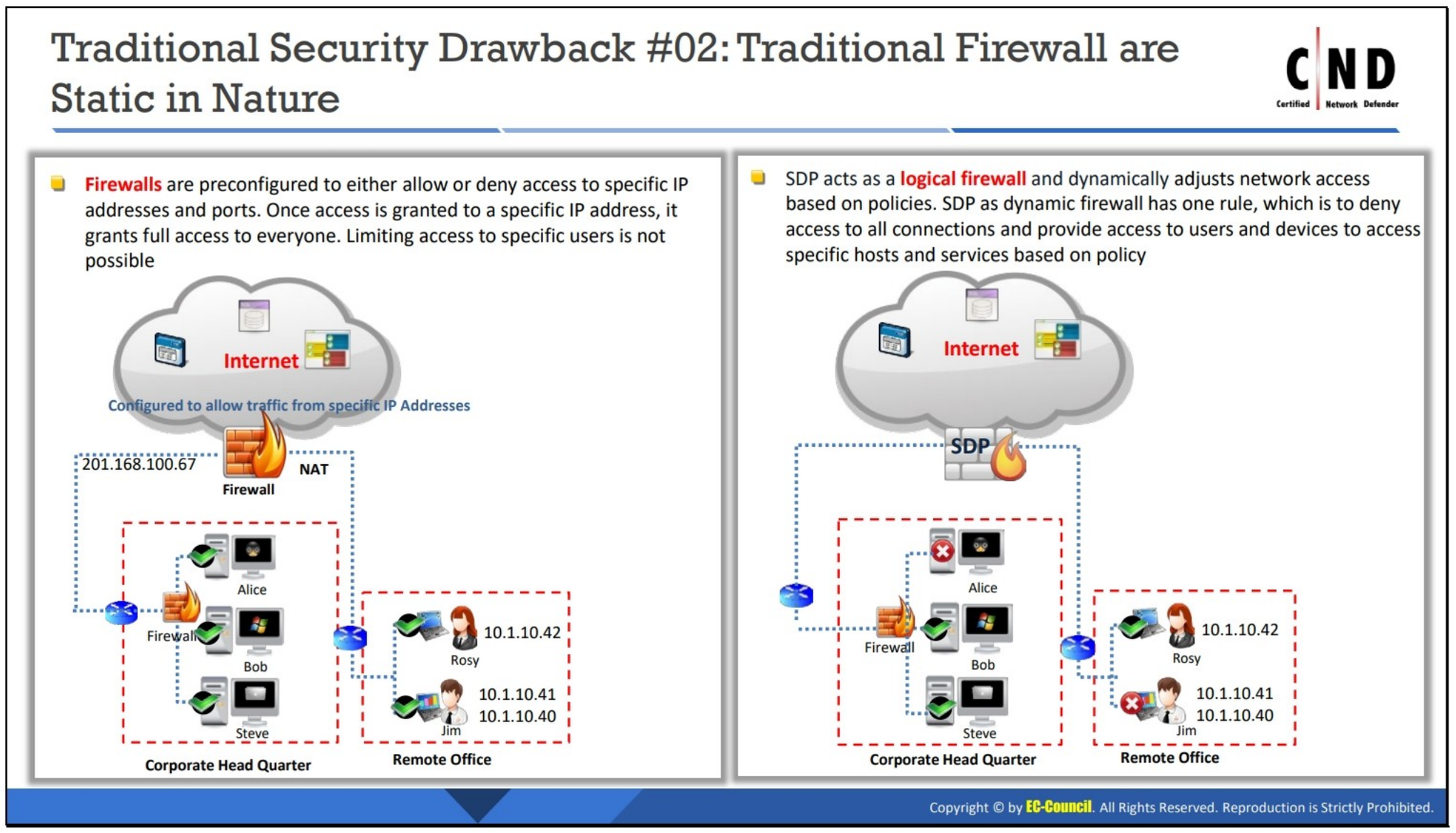
Traditional Security Drawback #01: Attacks Come from the Outside World Only, So Authenticating Outsiders is Enough

Traditional network access control focuses mainly on external threats without paying much attention to the insider threats emerging inside the organization. In the traditional network model, the external user requires authentication and authorization for gaining access to the resources and once the user is authenticated he gains access to the all the network resources. Hence, if an external attacker is able gain access to the network, it becomes easy to access confidential data or privileged accounts.

SDP implements the zero-trust model, which works on principle of "never trust and always verify." In SDP, after obtaining access, the user can only use the resources as per the access policy. Both the external user and the internal user require authentication and authorization for gaining access to the resources or sensitive information. If there is an insider threat, then the access is limited to a small slice of data and the rest of the resources are safeguarded. The transferring of data is completely controlled and protected. The data usage per user is strictly monitored and reported, so that if there is an instance of a data breach, then it will be easily found and mitigated quickly. SDP limits the extent of damage caused by an attacker. The SDP system policies allow users access to only those specific resources that are required for their business function and hide the rest.

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

https://t.me/learningnets



Traditional Security Drawback #02: Traditional Firewall are Static in Nature

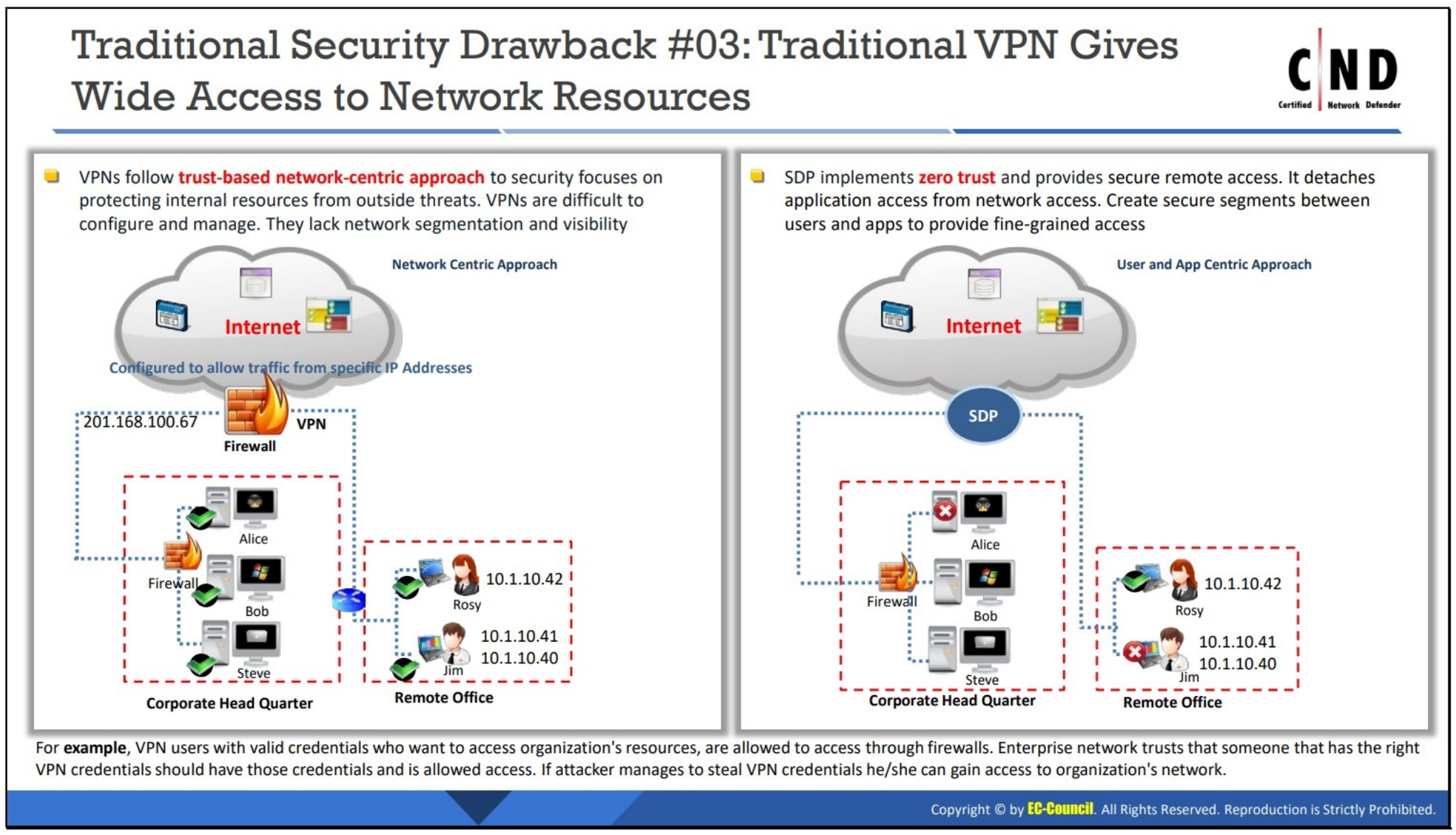
Traditional firewalls are preconfigured to either allow or deny access to specific IP addresses and ports. The static nature of the firewalls and pre-configuration of rules in the traditional model make firewalls difficult to manage in a large organization. Traditional firewalls block or allow access to the users based on preconfigured rules. Therefore, a misconfigured firewall wall becomes a threat to the security of the entire network. Once access is granted to a specific IP address, it grants fully accessible to everyone. As multiple users have network access to various systems, compliance becomes more difficult. Moreover, limiting access to specific users is not possible in traditional firewalls.

SDP acts as a logical firewall and dynamically adjusts network access based on policies. Contrary to traditional firewalls, which have numerous rules, dynamic firewalls have only one rule that is to deny all connections. SDP implements dynamic firewall rule policy on the gateway by adding or removing policy that allows only authorized user to access the protected resources. Therefore, a dynamic firewall allows only authenticated users to access protected resources and hence plays a key role in preventing lateral movement attacks.

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

https://t.me/learningnets

Technet24



Traditional Security Drawback #03: Traditional VPN Gives Wide Access to Network Resources

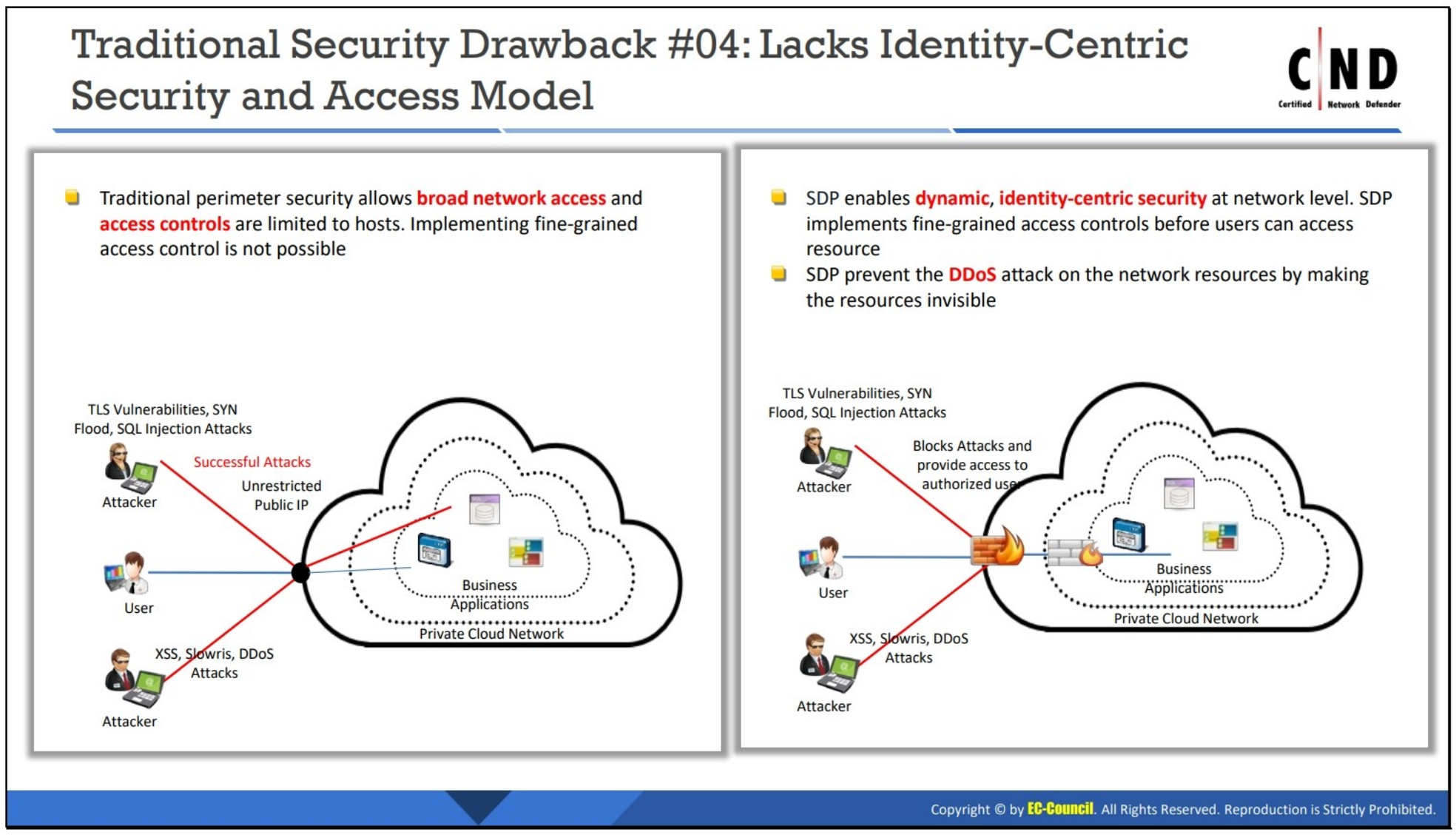
VPNs follow a trust-based network-centric approach with security focuses for protecting internal resources from outside threats. VPNs are difficult to configure and manage. Traditional VPNs give a wide access to network resources, and they are not cloud-friendly. The key security risks of VPNs include theft of credentials and excessive access. VPNs also lack network segmentation and traffic visibility; therefore, they are not appropriate for dynamic networks.

As SDP implements the zero-trust model and provides secure remote access, it detaches application access from network access and creates secure segments between users and applications to provide fine-grained access. SDP is installed and managed with ease. It is also cloud-friendly and integrated easily with the cloud. It delivers all the features of a VPN and also overcomes many of its disadvantages. SDP blocks all the ports, encrypts the traffic, and prevents attacks through the Internet. It implements multifactor authentication (MFA) before allowing user access to any resource; this helps mitigate lateral movement attacks by insiders. SDP implements multiple levels of access control, which enhances application and data security over network.

For example, if VPN users with valid credentials want to access the organization's resources and can access through firewalls, the enterprise network allows access to the user by trusting that the right VPN credential belongs to an authorized user. If an attacker is able to steal VPN credentials, then they can easily gain access to the enterprise network.

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

https://t.me/learningnets



Traditional Security Drawback #04: Lacks Identity-Centric Security and Access Model

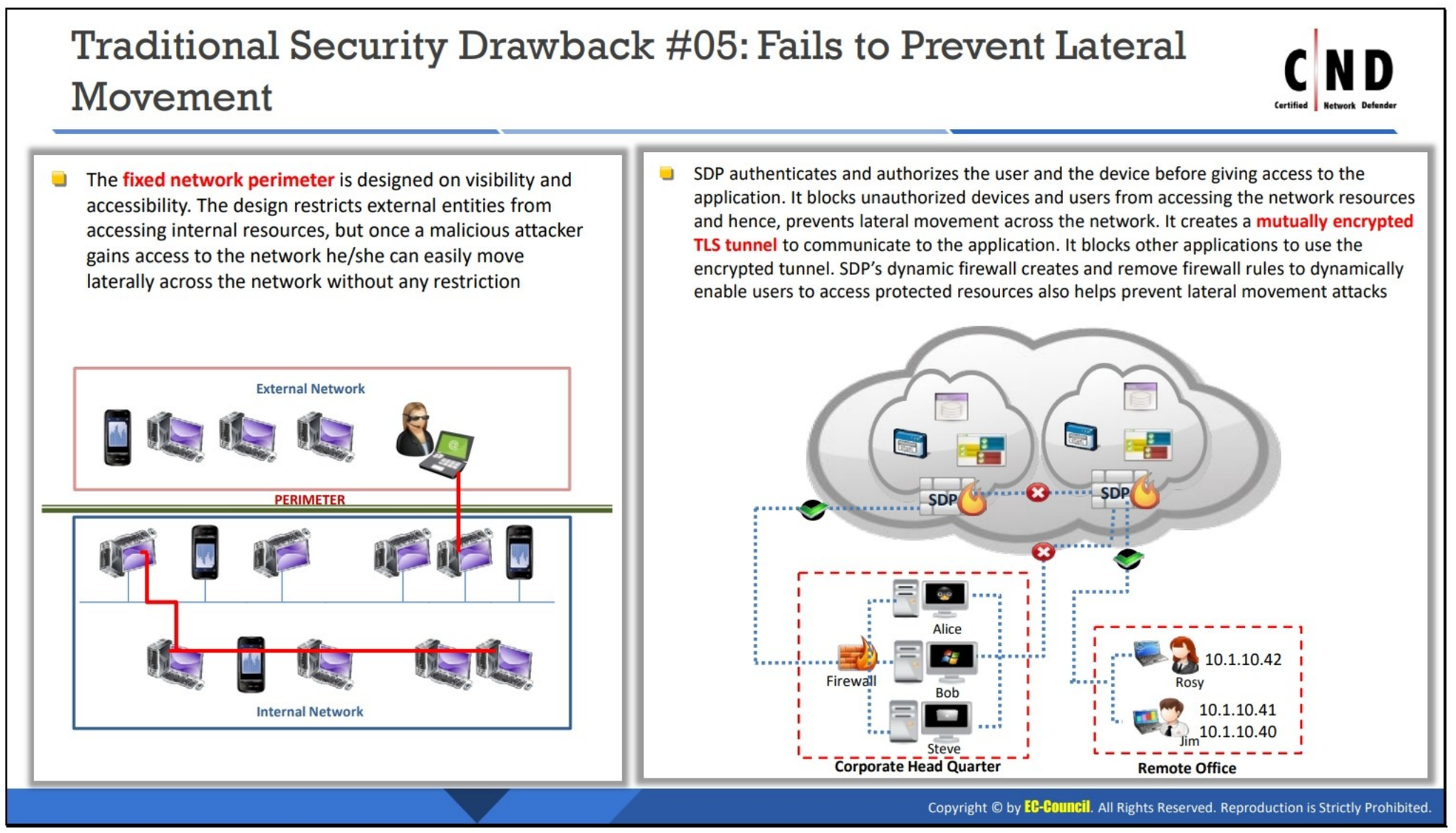
Traditional perimeter security allows broad network access, and access controls are limited to hosts. Therefore, it is not possible to implement fine-grained access control. Managing access by IP address and port is not enough to access cloud resources. The network security group (security rules that allow or deny network traffic to resources) cannot identify users and grant full access to everyone to all resources. This enables malicious users, attackers, or malware to travel from the premises to the cloud network. Network security groups need to be updated regularly because users access the cloud from multiple devices, and IP addresses are dynamically assigned and changes regularly; thus, failing to update the security groups leaves the network vulnerable to various attacks.

SDP enables dynamic, identity-centric security at the network level. SDP's identity-centric approach implements micro-segmentation and fine-grained access control that allows the user to gain access to specific resource(s) securely**.** SDP enables isolation of the network, which hides other resources on the network. Hence, by making the resources invisible SDP safeguards against DDoS attack on the network. It detects new server instances and based on its metadata (tags) automatically grants the user access to required resources. SDP's need-to-know model hides DNS information, internal IP addresses, or visible ports of the internal network infrastructure. SDP safeguards against network-based attacks such as server scanning, DoS, SQL injection, OS and application's vulnerability exploits, man-in-the-middle (MITM), pass-the-hash (PtH), pass-the-ticket (PtT), and other attacks by unauthorized users.

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

https://t.me/learningnets

Technet24



Traditional Security Drawback #05: Fails to Prevent Lateral Movement

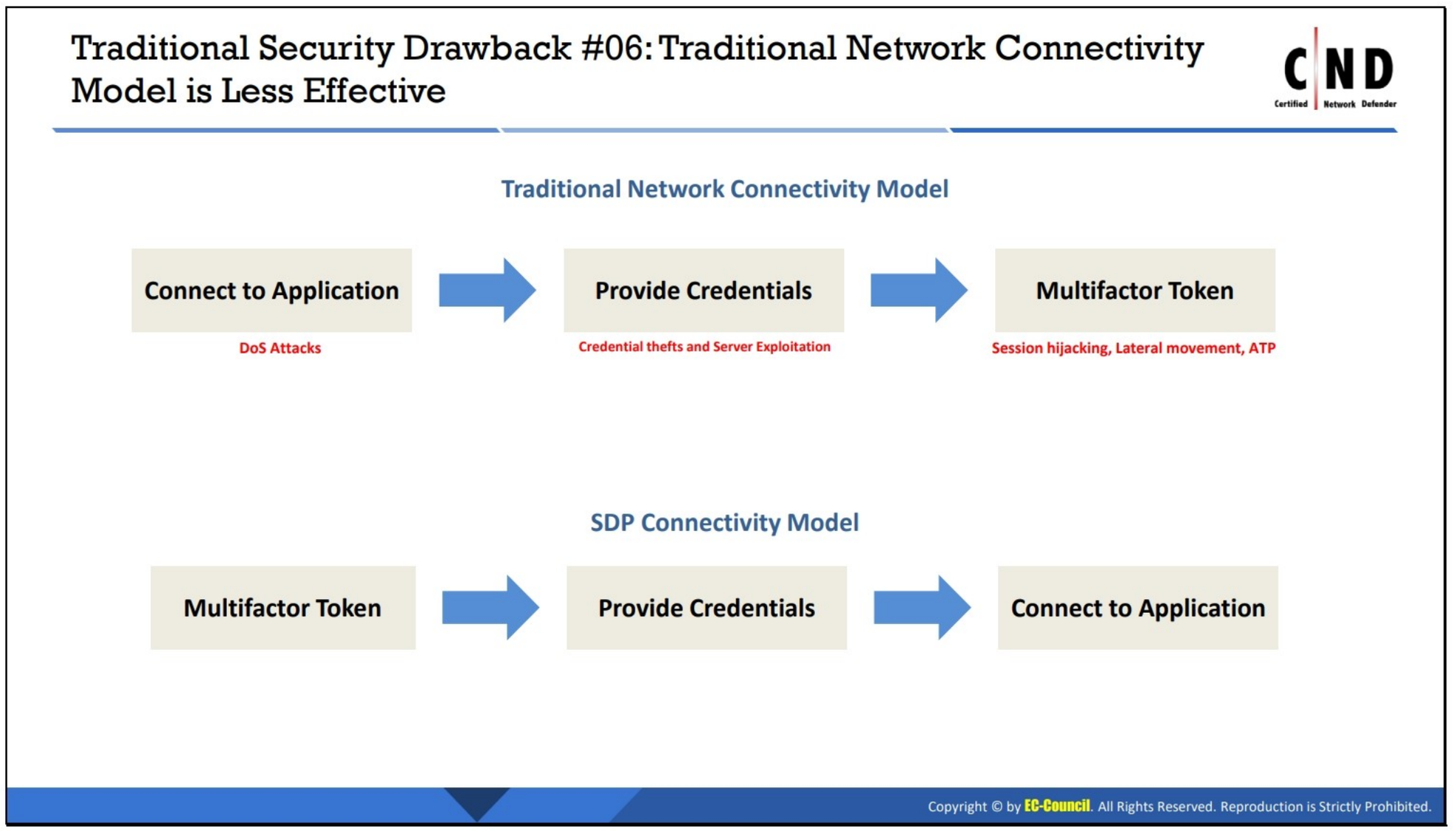
An adversary targets sensitive information available in the enterprise network and gains access by compromising one computer in the internal network and moves ahead laterally to obtain the target information. The traditional network perimeter is designed on visibility and accessibility. The design restricts external entities from accessing internal resources, but once a malicious attacker gains access to the network, they can easily move laterally across the network without any restriction. PtH and PtT attacks target the user login credentials through various techniques and use the captured credentials for authentication. The adversary, after gaining access to the internal network, uses these techniques to execute a lateral movement attack.

SDP authenticates and authorizes the user and the device before giving access to the application. It prevents lateral movement attacks by granting access to the user only to authorized assets, which was a major flaw in traditional security mechanisms. An enterprise can implement SDP to separate high-value applications from other applications. Hence, unauthorized users would not be able to detect the protected application, which mitigates against lateral movement attack.

After authenticating and authorizing the user and the device, SDP creates an encrypted TLS tunnel to safeguard the application and allow secure communication. The dynamic firewall also plays a major role in preventing lateral movement attacks by tethering users to devices. It allows users to access specific resources by regulating firewall rules.

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

https://t.me/learningnets



Traditional Security Drawback #06: Traditional Network Connectivity Model is Less Effective

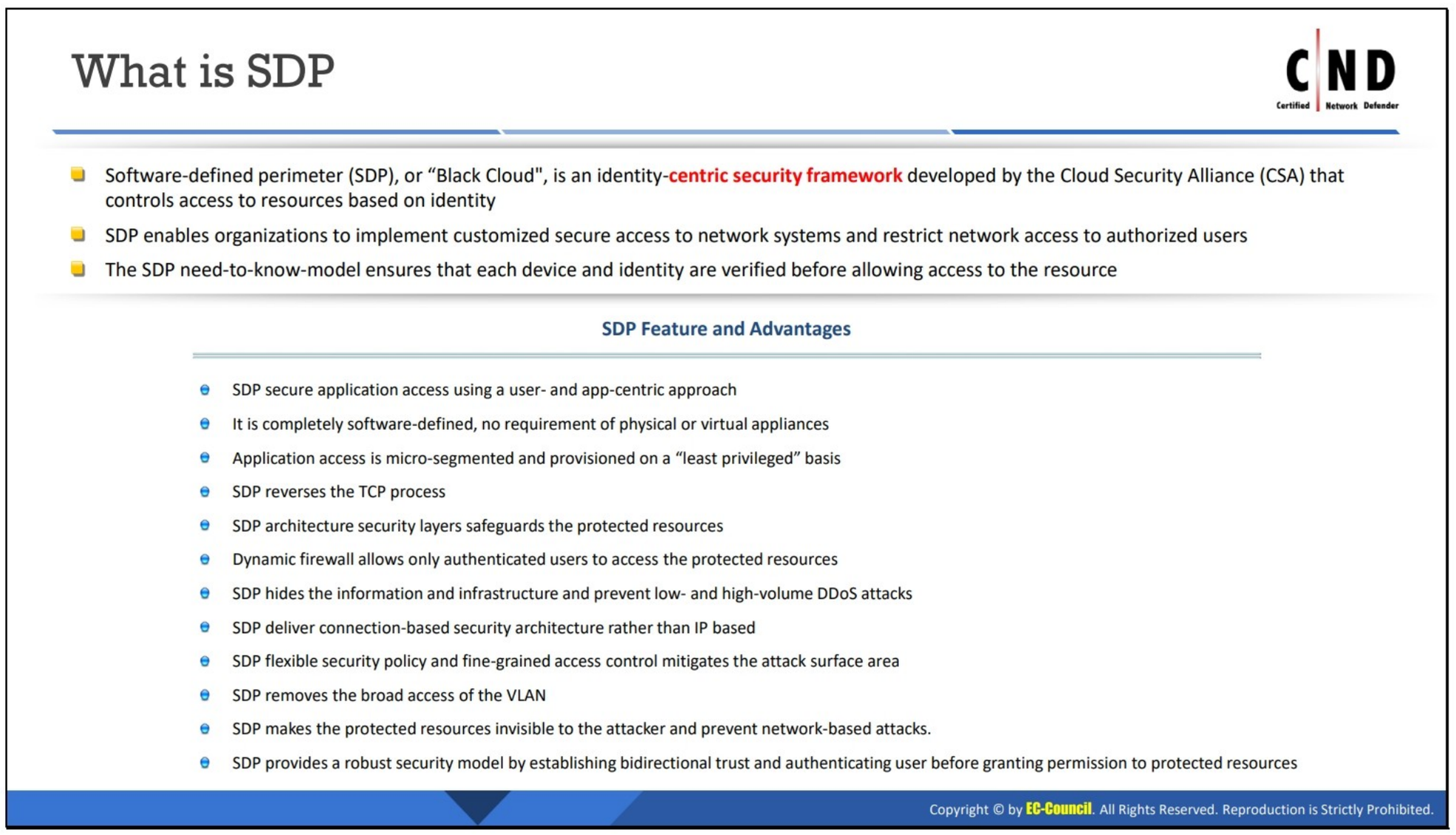
In the traditional network connectivity model, the user connects to the application, provides credentials, the application authenticates the user with a multifactor token. This model is vulnerable to many attacks. As this model allows anyone to connect to the application, it is especially vulnerable to DoS attacks. An attacker can execute a DoS attack and block the network resources by simply trying to connecting to the network resources. This model is also open to various brute-force attack techniques to gain credential access. Once an attacker gains credentials, they can easily perform various server exploits, session hijacking, and lateral movement attack.

SDP connectivity's model is also called as a "need-to-know model" as it hides all the resources from unauthorized users and it verifies the device or identity before granting access to the network. SDP components only respond to requests that are authenticated and authorized. SDP connectivity model implements connection-based security architecture rather than an IP-based one. Access policy based on IP address cannot provide identity-focused security. SDP determines who can connect to what type of services. If the user did not meet the level of trust, then SDP would not provide access to the protected resources. This model helps mitigate against network scanning attacks, DoS attacks, application attacks such as SQL injection and XSS attacks, MITM attacks, and PtH and PtT attacks.

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

https://t.me/learningnets

Technet24



What is SDP

SDP, or "Black Cloud" developed by the Cloud Security Alliance (CSA), is a network security model that is identity-centric and only allows access to authorized users. It establishes 1:1 network connection between the user and the resources they access. SDP restricts network access and verifies the device and identity before granting access to the network. Thus, it reduces the attack surface area by creating a single, customized, micro-segmented network for individual users, devices, sessions, etc.

In SDP, the endpoints should authenticate and be authorized first before gaining access to servers, and then the connections between the requesting systems and application infrastructure are encrypted. The on-premises and remote users can gain access to the on-premises and remote resources through the secure access control platform provided by SDP. SDP's need-to-know model ensures that each device and identity is verified before allowing access to the resource.

The three main pillars of the software-defined perimeter are listed below.

- Zero trust: It utilizes micro-segmentation and applies the principle of least privilege to the network, thereby minimizing the attack surface.
- Identify centric: It relies and functions on the user's identity but not their IP address.
- Built for the cloud: It can operate on cloud networks and can provide scalable security.

SDP Features and Advantages

- SDP secures application access using a user and app-centric approach.
- It is completely software-defined and there is no requirement of physical or virtual devices.

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

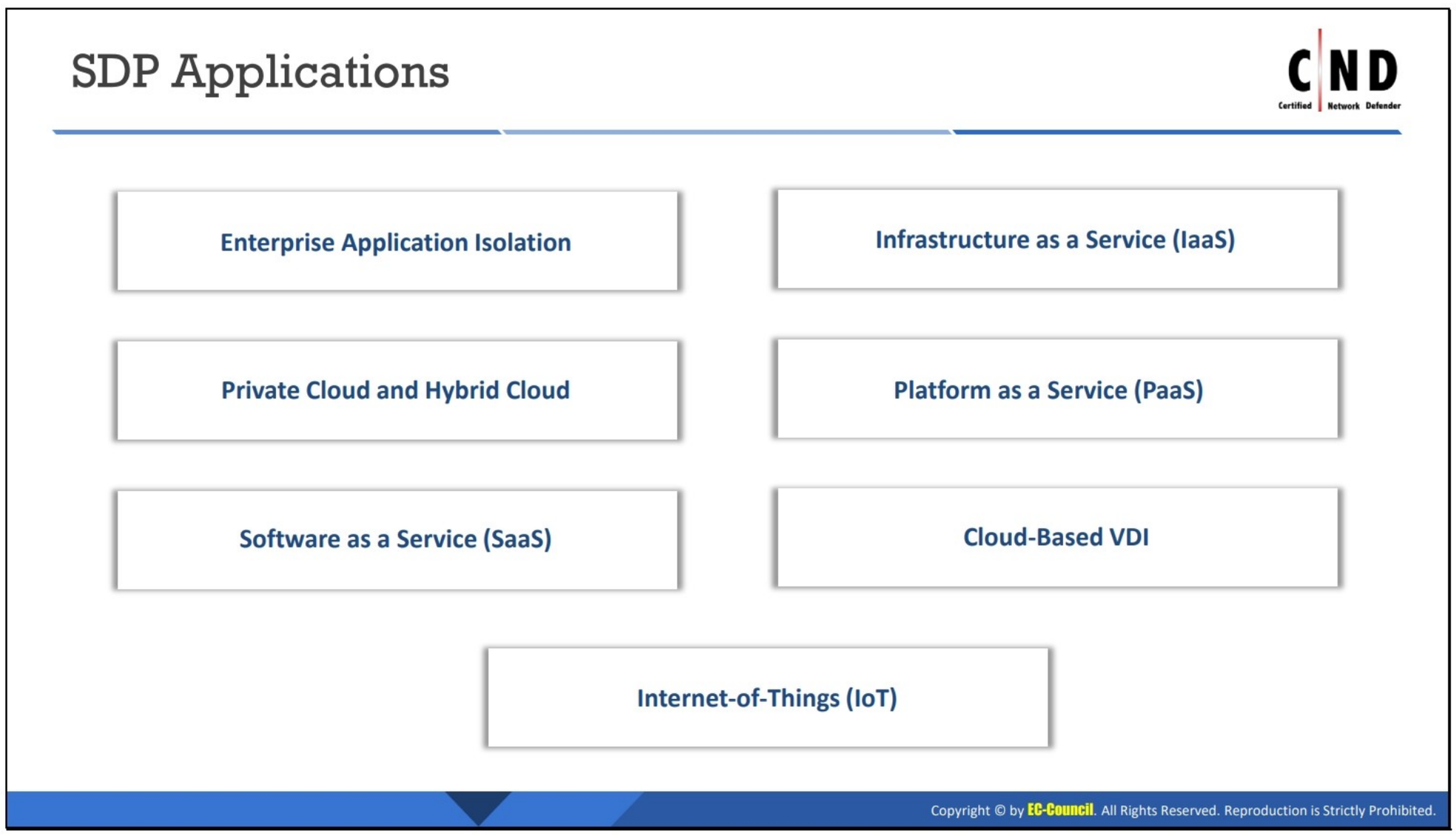
https://t.me/learningnets

- The access to the application is micro-segmented and based on the principle of least privileged.
- SDP is the inverse of TCP. In TCP, the user initiates a connecting phase, authentication phase, and then the data pass stage; this is completely reversed in SDP.
- SDP architecture security layers safeguard protected resources
- The dynamic firewall allows only authenticated users to access protected resources.
- SDP hides information and infrastructure. It makes the controller and gateways invisible and prevents low-volume as well as high-volume DDoS attacks. SDP components would not respond to any request until and unless it is authenticated and authorized; only then it allows the good packets to pass through.
- SDP delivers connection-based security architecture rather than an IP-based one. Access policy based on IP address would not provide identity-focused security. SDP determines who can connect to what type of services. If the user did not meet the level of trust, then SDP would not provide access to the protected resources. SDP prevents lateral movement attack by granting access to the user only to authorized assets, which was unnoticed in traditional security mechanisms.
- SDP's flexible security policy and fine-grained access control mitigates the attack surface area.
- VLANs have a wide attack surface area; SDP overcomes this by removing the broad access provided by VLANs.
- SDP makes the protected resources invisible to the attacker and prevents network-based attacks. It establishes bidirectional trust, between client and SDP services and application and SDP services. Once the trust is established, then SDP moves toward authentication. After successful authentication, SDP connects the user to the application.

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

https://t.me/learningnets

Technet24



SDP Applications

The common applications of SDP are listed below.

- Enterprise application isolation: As explained earlier, with SDP, an organization can separate high-value applications from other applications. By doing this, unauthorized users would not be able to detect the protected application; hence, organizations can be protected from lateral movement attack.
- Private cloud and hybrid cloud: As SDP is software-based, it can be easily integrated into the private cloud to maximize cloud environment flexibility and elasticity. Apart from this, the enterprise can utilize SDP to secure and obscure public cloud instances.
- Software as a Service (SaaS): SaaS services are safeguarded by SDP. The software services accepts hosts and the users who wanted to connect to these services are the initiating hosts. With this application of SDP, the SaaS services can be utilized globally without any security concerns.
- Infrastructure as a Service (IaaS): IaaS vendors provide SDP-as-a-Service as secure and safe to the users. Thus, the users will benefit from the agility and cost savings of IaaS while at the same time mitigating exposure to various threats.
- Platform as a Service (PaaS): PaaS vendors can include SDP in their service to minimize network-based attacks.
- Cloud-based VDI: VDIs are located in an elastic cloud. Implementation of a VDI user accessing servers in the enterprise network is not only challenging but prone to security vulnerabilities. However, use of SDP resolves this by providing simpler user interaction and granular access.

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

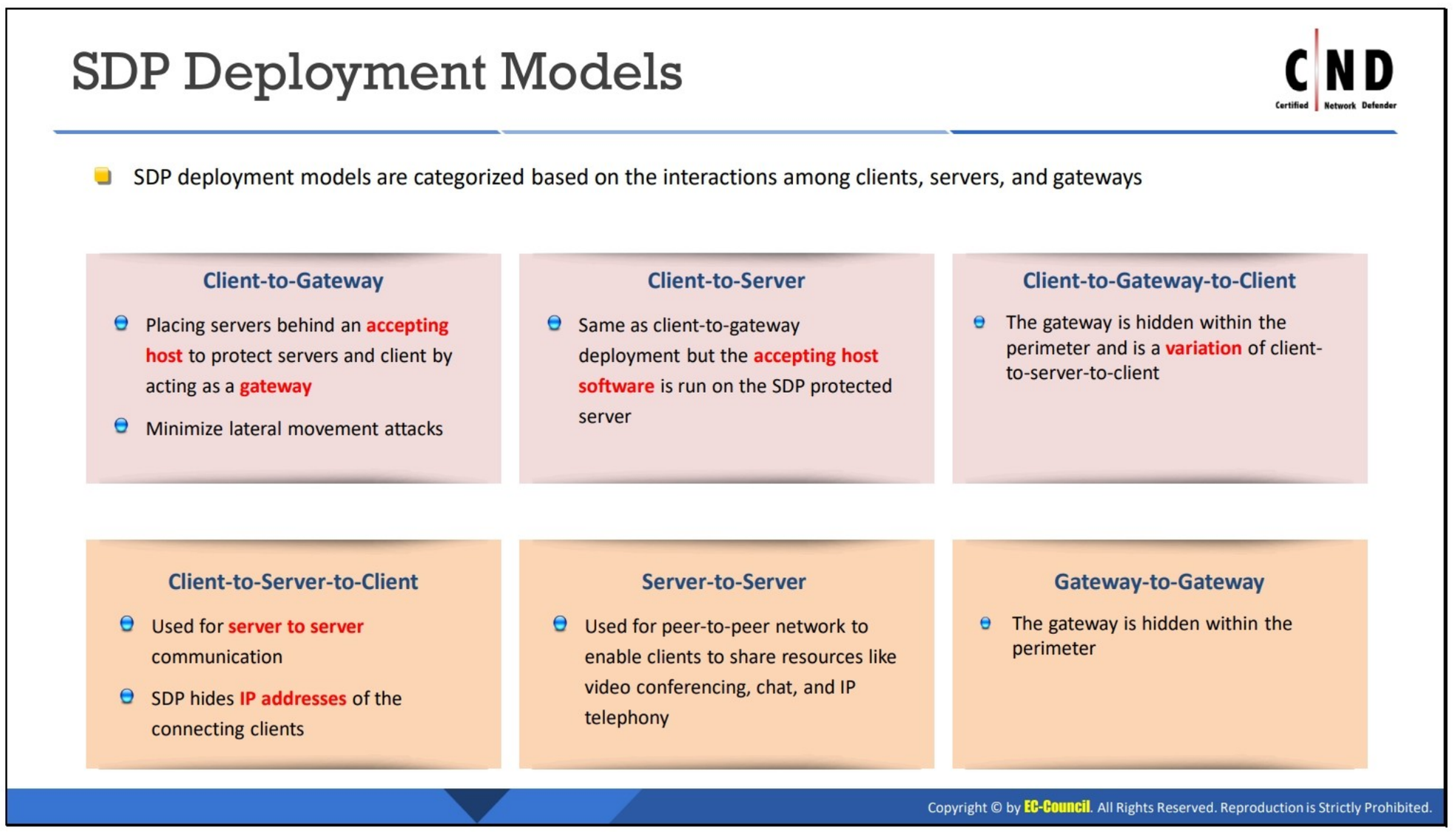
https://t.me/learningnets

- Internet-of-things (IoT): Numerous new IoT devices are connected to the Internet every day. The backend application of these IoT devices not only manages the data but also extracts information from these devices and acts as the custodian of sensitive information. SDPs can obscure the servers and their interactions on the Internet, thereby improving security as well as uptime.

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

https://t.me/learningnets

Technet24



SDP Deployment Models

SDP deployment models are categorized based on the interactions among clients, servers, and gateways. The various SDP deployment models are listed below:

- **Client-to-gateway:** In client-to-gateway SDP deployment, single or multiple servers are protected by the gateway present between the clients and the servers. This helps in preventing lateral movement in the network. Apart from this, client-to-gateway SDP implementation is applied on the Internet to separate the protected server from an unauthorized user and minimize attacks such as DDoS, SQL injection, XSS, CSRF, etc.
- **Client-to-server:** The benefits and features of client-to-server deployment are same as client-to-gateway deployment, except instead of the gateway the server that is being protected runs the software. The selection of client-to-server and the client-to-gateway implementation is performed based on topological factors such as load balancing methodology, the elasticity of servers, etc.
- **Server-to-server:** In this type of SDP deployment, all the APIs on the Internet are safeguarded from unauthorized hosts. For example, the server that initiates the REST call is the initiating SDP host and the server that offers the REST service will be the accepting SDP host. Server-to-server SDP implementation reduces the load on the services and minimizes the number of attacks.
- **Client-to-server-to-client:** This type of SDP deployment believes in establishing the peer-to-peer relationship between the clients, which can be utilized by applications such as IP telephone, chatting, and video conferencing. In client-to-server-to-client implementation, SDP obscures the IP addresses of the clients.

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

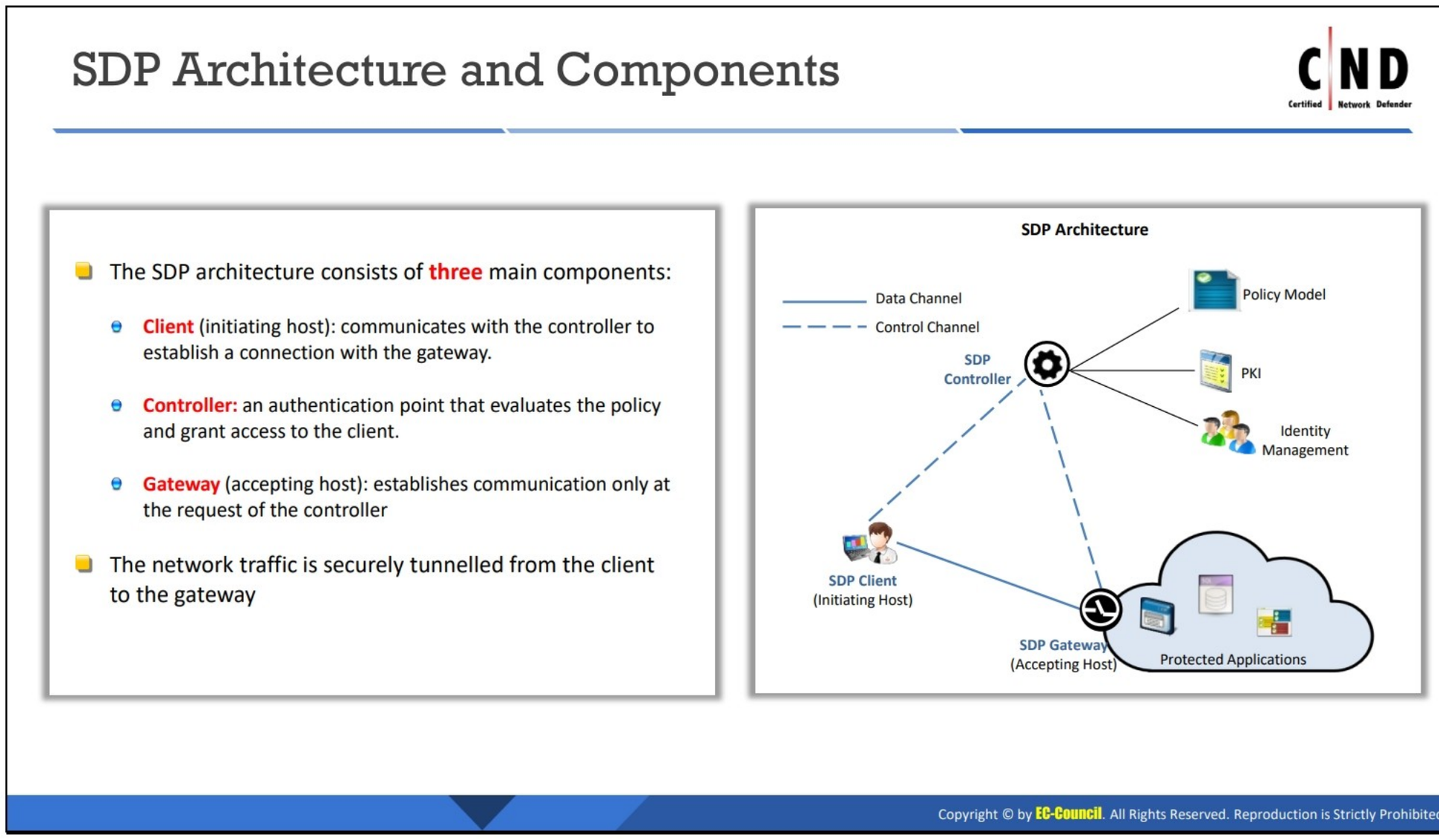
https://t.me/learningnets

- **Client-to-gateway-to-client:** In this type of SDP deployment, the gateway is hidden within the perimeter and is a variation of client-to-server-to-client. It supports peer-to-peer network protocols that need clients to connect directly to one another while enforcing access policies.
- **Gateway-to-gateway:** This type of SDP deployment model is competent for certain IoT environments. The gateway is hidden within the perimeter.

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

https://t.me/learningnets

Technet24



SDP Architecture and Components

SDP architecture has three main components:

- Client (initiating host): It runs on every user's device. The client communicates with the controller to establish a connection with the gateway. Before granting permission, the controller may request hardware or software inventory information from the client.
- Controller: It is an authentication point that evaluates the policy and grant access to the user. The client and the gateway that could communicate will be determined by the controller and send the information to the external authentication services (attestation, geo-location, identity services, etc.).
- Gateway (accepting host): It safeguards the system resources. The network traffic from the client moves through an encrypted tunnel and reaches the gateway where it is decrypted and sent to the protected resources. The gateway establishes communication only at the request of the controller.

After successful authentication from the controller, the network traffic is securely tunneled from the client to the gateway.

The client generates a hash-based message authentication code (HMAC)-based one-time password utilizing the single-packet authorization (SPA) technique and sends this to the controller and gateway as the first network packet to establish a communication setup; this is also utilized for gateway-controller connection setup. The invalid packets sent through an invalid client are rejected by the controller and the gateway, which prevent any connection with unauthorized users or devices. This allows a safer deployment of SDP services and minimizes the impact of a DDoS attack.

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

https://t.me/learningnets

In the SDP connectivity model, the user authenticates with a multifactor token, provides credentials, and then connects to the application.

SDP Architecture Workflow

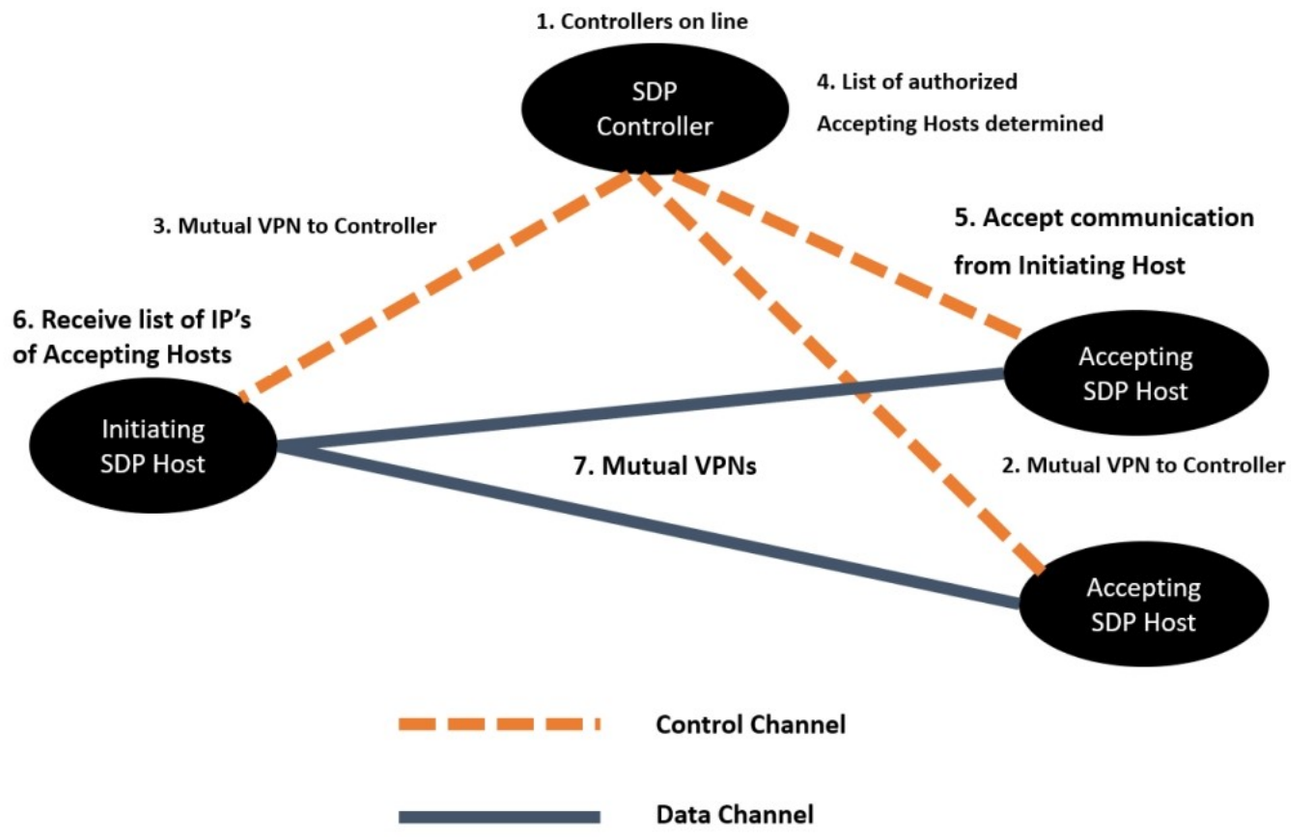


Figure 4.4: SDP Architecture Workflow

SDP architecture has the following workflow:

- The controller comes online and connects to the required authentication and authorization services such as public key infrastructure (PKI), MFA, device fingerprinting, etc.
- Single or multiple gateways come online, which connect(s) and authenticate(s) to the controller. The gateways do not communicate directly with any clients.
- The client connects and authenticates with the controller.
- After successful authentication, the controller determines the list of gateways authorized to communicate with the client.
- The controller instructs the gateway to communicate with the client and implement the set encryption policies.
- The list of authorized gateways is provided to the client by the controller as well as optional encryption policies.
- The client starts a mutual VPN connection to the authorized gateway.

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

https://t.me/learningnets

Technet24

SDP Advantages Over Traditional Network Access Control

	Traditional Network Access Control (NAC)	Software-Defined Perimeter (SDP)
Reduced Attack Surface	• All the applications are assigned to VLANs with all-or-nothing user access • Third-party access management is difficult • VPN is required for remote user access • Infrastructure changes are not easy to manage • If an anomaly is detected, then the device is quarantined	• Every user and every application will have fine-grained access control. All the unauthorized applications or ports are concealed • Third-party access management is simple and secure based on policy • VPN is replaced securely • Infrastructure changes are automatically adjusted • If an anomaly is detected in SDP, the response is flexible
Private and Public Cloud Adoption	• Virtual machines have VLAN assignment. The services on the machines have all-or-nothing access • Traditional NAC is not designed for policy-based, dynamic assignment of servers • The VLAN cannot be extended to IaaS	• The newly created servers in IaaS and private cloud are dynamically detected • Designed for policy-based, dynamic server access control • Unified control of access to IaaS, physical, and private cloud environments

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

SDP Advantages Over Traditional Network Access Control (Cont'd)

	Traditional Network Access Control (NAC)	Software-Defined Perimeter (SDP)
BYOD Enabled	• The devices are visible on the network • Profile validation through device attributes • Authentication through 802.1X integration • The devices that are assigned to the VLANs have coarse-grained control	• The devices having access to network resources are visible • Devices and user validation is through dynamic attributes • Authentication through identity system integration • In the assigned perimeter, fine-grained control of the user access
Streamlined Compliance	• Before accessing the network, the user and devices have to validate – the users not having authorization will be blocked.	• The user and devices are validated before accessing the resources (unauthorized users are unable to access the resources)
	• Partial automation of compliance reporting	• Complete visibility of user history and access permission, not just by IP address
	• For mapping users and IP address activity, it requires consolidation and unification with SIEMs	• It is user-centric, the segmentation is simplified by the descriptive policy
	• All-or-nothing policies for VLAN access	• Audit scope is reduced through fine grained network access control

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

SDP Advantages Over Traditional Network Access Control

Listed below are the key differences between traditional network access control and SDP access control.

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

https://t.me/learningnets

Reducing the Attack Surface

In traditional network access control, to reduce the attack surface, all the applications are assigned to VLANs with all-or-nothing user access. Third-party access management is not easy, and a VPN is required for remote user access. Moreover, infrastructure changes are difficult to manage and, if any anomaly is detected, the device needs to be quarantined. Whereas in a software-defined network, every user and every application will have fine-grained access control, the unauthorized applications or ports are concealed, third-party access management is simple and secure, VPN is securely replaced, infrastructure changes are automatically adjusted, and there is flexibility in response to the detected anomaly.

Accelerating Cloud Adoption (Private and Public)

For public and private cloud services, the VMs have VLAN assignment and the services have all-or-nothing access in traditional NAC. Traditional NAC is not designed for policy-based, dynamic assignment of servers and the VLAN cannot be extended to IaaS. Whereas in a software-defined network the newly created servers in IaaS and public cloud are dynamically detected and the services have controlled access. SDP was designed for policy-based, dynamic server access control, and there is unified control of access to IaaS, physical, and private cloud environments.

Enabling BYOD (Bring Your Own Device)

If an organization enables BYOD in traditional network access control (NAC), the devices that are connected to the network are visible, the profile is validated through device attributes, authentication will be performed through 802.1X integration, and the BYOD devices assigned to the VLAN will have coarse-grained control. Whereas if an organization enables BYOD with SDP access control, then the devices gaining access to the network resources are visible, the device and user validation is executed through dynamic attributes, identity system integration will perform the authentication, and the user will have fine-grained access control in the assigned perimeter.

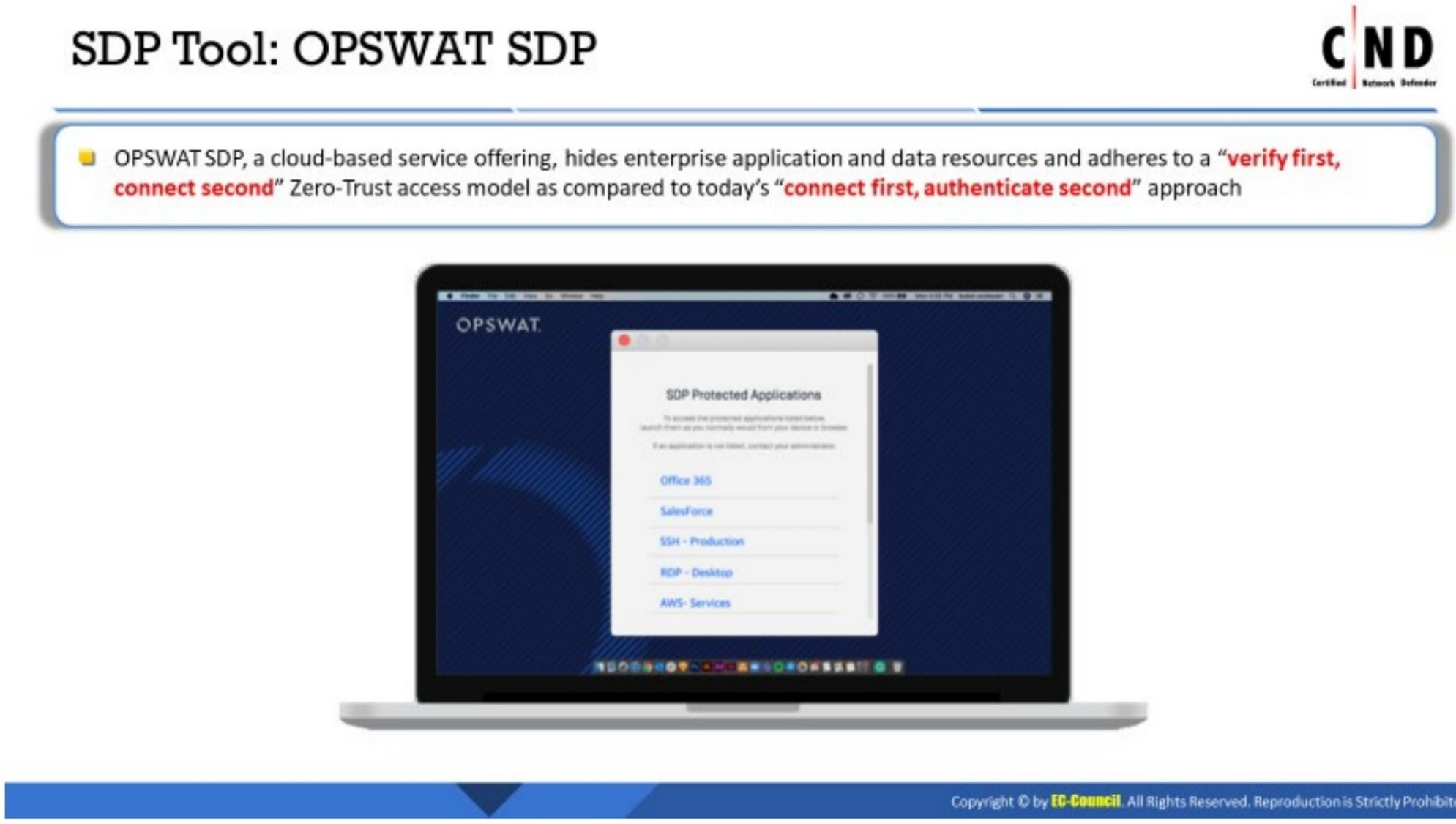
Streamlining Compliance

In traditional NAC, to streamline compliance, the users and devices should be validated before gaining access to the network; the users not having authorization will be blocked. In addition, there is partial automation of compliance reporting and mapping users, and IP address activity requires consolidation and unification with SIEMs and all-or-nothing policies for VLAN access. Whereas to streamline compliance in SDP, the user and devices should be validated before accessing the resources, users not having authorization are unable to access the resources, and there is complete visibility of user history and access permission. SDP is user-centric, the segmentation is simplified by the descriptive policy, and the audit scope is reduced through fine-grained network access control.

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

https://t.me/learningnets

Technet24



SDP Tool: OPSWAT SDP

Source: https://www.opswat.com

OPSWAT SDP, a cloud-based service offering, hides enterprise application and data resources and adheres to a "**verify first, connect second**" Zero-Trust access model as compared to today's "**connect first, authenticate second**" approach.

Protect data with mutual TLS encryption both within the perimeter and beyond, ensuring the required secure access. This security system protects against credential theft, connection hijacking and data loss, and common attacks such as DDOS, Man-in-the-Middle and more. SDP enables greater security based on an application-session only (least-privileged) zero-trust access model.

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

https://t.me/learningnets

Additional SDP Tools / Solutions

Some additional SDP tools/solutions are listed below:

Open Source SDP

Source: www.waverleylabs.com

Open Source SDP reduces risk and secures critical cloud-based applications and infrastructures. This security model has been tested and proven to stop all forms of network attacks including credential theft, denial of service, and server exploitation.

Absolute ZTNA

Source: www.absolute.com

Absolute ZTNA makes applications invisible to unsanctioned users, ensuring organization is safe from intruders or high-risk connections. It allows controlling access to the web, as well as private and public cloud applications based on risk and compliance requirements associated with a multitude of contextual factors like time of day, user, device's security posture, geolocation, network connection, etc.

Perimeter 81

Source: www.perimeter81.com

Perimeter 81 provides client and endpoint protection, identity and access management, OS and application-level security, all while encrypting traffic with mutual TLS encryption. It offers complete visibility, precise segmentation, highly scalable solution, user-centric experience, and simple transition to cloud environments.

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

https://t.me/learningnets

Technet24

Cisco Software-Defined Access (SDA)

Source: www.cisco.com

Cisco Software-Defined Access (SDA) helps streamline the process of providing access to users and devices while mitigating the increased risk of unknown IoT devices. By using network infrastructure and telemetry to inform and enforce security, SD-Access can deliver unrivaled zero-trust workplace capabilities for IoT endpoints and managed user devices while helping ensure continuous trusted access.

Netmotion SDP

Source: www.safe-t.com

Safe-t supports total flexibility, grants full network segmentation, prevents attacks before they happen, and supports any type of user. Safe-T's secure file access (SFA) reduces insider threats by transforming the standard network drives into secure, encrypted, and access-controlled drives.

AppGate SDP

Source: www.appgate.com

AppGate SDP is a full-featured network security platform that embodies the core principles of zero trust. It provides financial institutions with multilayered security against all forms of online fraud, across every stage of the attack cycle.

GoodAccess

Source: www.goodaccess.com

GoodAccess allows defining an organization's network with identity-based network access to face modern online threats with confidence. With GoodAccess' software-defined perimeter, the organization's infrastructure becomes invisible to the outside world, whether it resides in your LAN, datacenter, or cloud.

Wandera

Source: https://www.wandera.com/

Wandera is a real-time security in the network, blocking zero-day threats at source. Its cloud-based SDP creates secure isolated connections for each application. Its fast and resilient tunneling and encryption protocols deliver enterprise grade security.

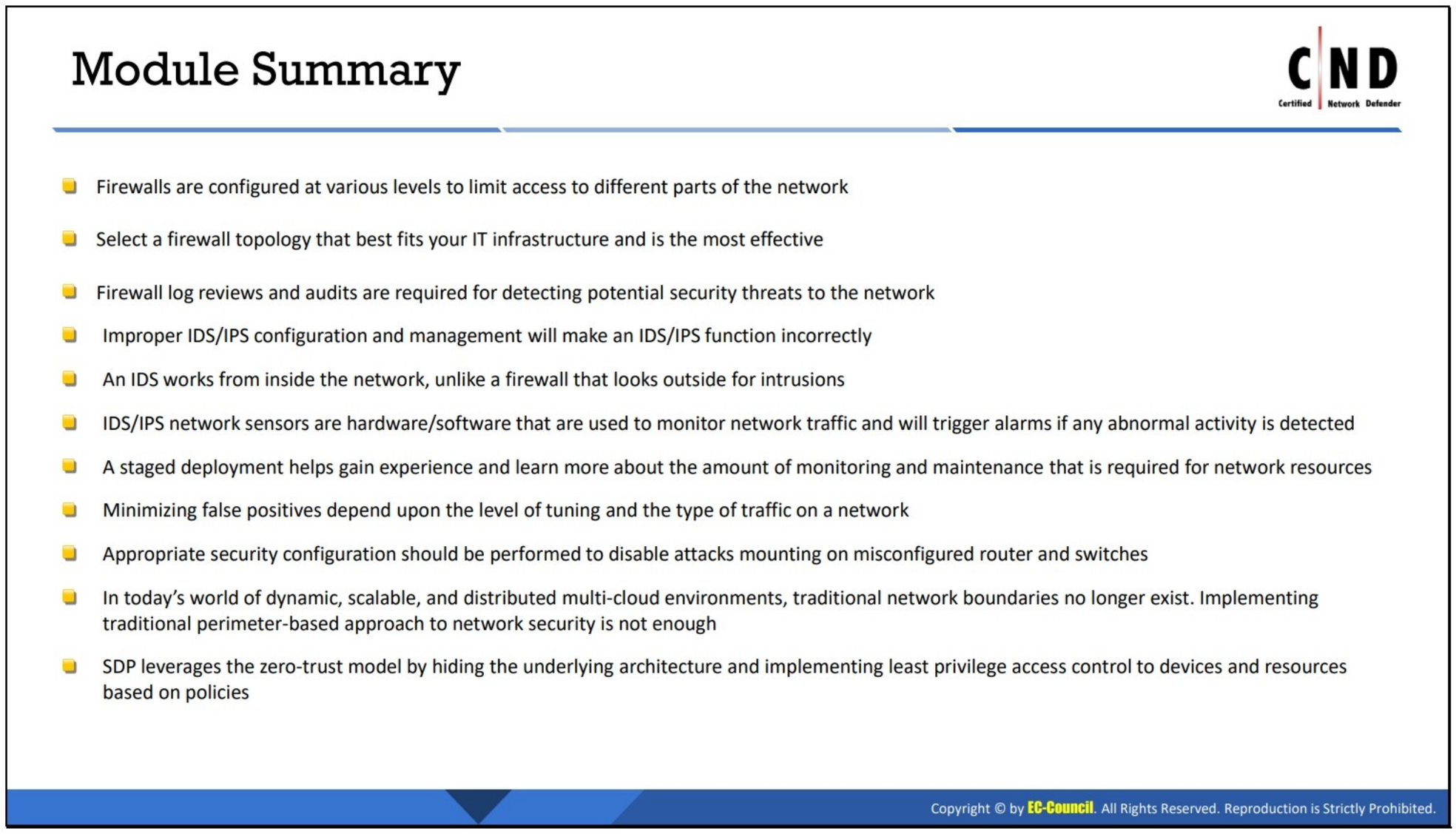
Netmotion SDP

Source: www.Netmotionsoftware.com

NetMotion SDP provides a more intelligent way to deliver secure remote access, protecting users and resources while improving the experience of working remotely. Its features included are full visibility outside the corporate perimeter, continuous risk assessments, using multiple data points to power access policies, restricting access to enterprise resources, etc.

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

https://t.me/learningnets



Module Summary

In this module, you have learned the various security configurations, best practices, and recommendations for network security perimeter devices such as firewalls, IDSs, routers, and switches.

The key highlighted points in this module are listed below:

- Firewalls are configured at various levels to limit access to different parts of the network.
- Select a firewall topology that best fits with your IT infrastructure and is the most effective.
- Firewall log reviews and audits are required to detect potential security threats to the network.
- Improper IDS/IPS configuration and management will make an IDS/IPS function incorrectly.
- An IDS works from inside the network, unlike a firewall that looks outside for intrusions.
- IDS/IPS network sensors are hardware/software that are used to monitor network traffic and will trigger alarms if any abnormal activity is detected.
- A staged deployment helps gain experience and learn more about the amount of monitoring and maintenance that is required for network resources.
- Minimizing false positives depends upon the level of tuning and the type of traffic on a network.
- Appropriate security configuration should be performed to disable attacks mounting on misconfigured router and switches.
- In today's world of dynamic, scalable, and distributed multi-cloud environments, traditional network boundaries no longer exist. Implementing traditional perimeter-based approach to network security is not enough.
- SDP leverages the zero-trust model by hiding the underlying architecture and implementing least privilege access control to devices and resources based on policies.

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

https://t.me/learningnets

Technet24