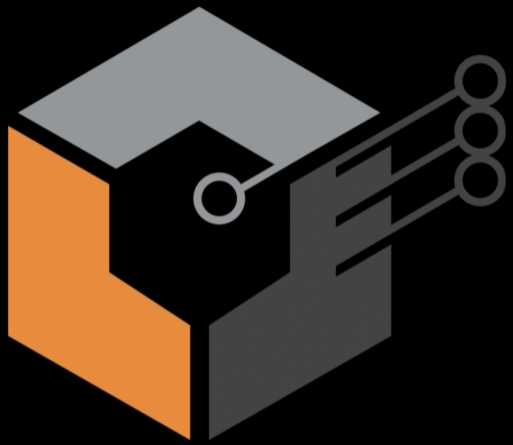
F5 101 Exam Preparation

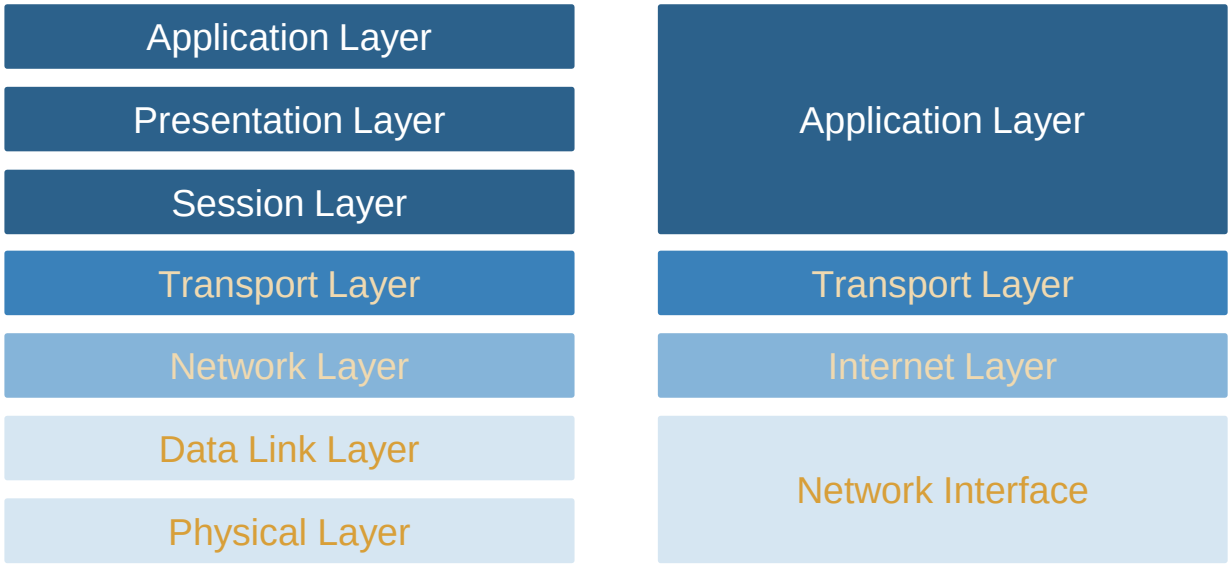
Application and Security Technologies



ZURIEN

www.zurien.com

OSI Model vs TCP/IP Model



Application Layer / Session, Presentation and Application

Application Layer

- Exchange data between programs from source to destination server
- High Level API, including resource sharing, remote file access
- Closest to end User

Presentation Layer

- Formatting data at the source device for the receiving device
- Establishes context between application-layer entities
- Responsible for compressing and encrypting/decrypting data

Session Layer

- Create and maintain dialogs between two host
- Establish and terminates the connection between local and remote application
- Manages communication sessions

HTTP

Application Layer

- Domain Name System (DNS) – TCP and UDP 53
- BOOTP (superseded by DHCP)

  Dynamic Host Configuration Protocol (DHCP)

  – UDP Client 68, Server 67
- Simple Mail Transport Protocol (SMTP) – TCP 25
- Post Office Protocol (POP3) – TCP 110
- Internet Message Access Protocol (IMAP) – TCP 993
- Simple Network Management Protocol (SNMP) – TCP 161, SNMP Traps 162
- Network Time Protocol (NTP) – UDP and TCP 123

HTTP

Application Layer

- File Transfer Protocol (FTP) – TCP 20 and 21
- Trivial FTP (TFTP) – UDP 69
- Telnet – TCP 23
- Secure Shell (SSH) – TCP 22

  SSH File Transfer (SFTP)

  Secure Copy (SCP)
- Hypertext Transfer Protocol (HTTP) – TCP 80
- Hypertext Transfer Protocol Secure (HTTPS) – TCP 443

HTTP

- TCP Based Application Layer
- Client-Server listening on port 80
- URL – Uniform Resource Locator
- Connectionless
- Stateless
- Client Side – Web Browser
- Server Side – Web Server

HTTP

Web Server

- Apache, NGINX or IIS
- HTML
- Linux, Apache, MySQL, PHP (LAMP)
- JavaScript

HTTP

HTTP REQUEST

▼General

Request URL: http://172.16.20.1/

Request Method: GET

Status Code: 200 OK

Remote Address: 172.16.20.1:80

Referrer Policy: no-referrer-when-downgrade

▼Request Headers view parsed

```
GET / HTTP/1.1
Host: 172.16.20.1
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.61 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

Header Summary:

Cookies

Accept-xxx

Content-Type

Content-Length

User-Agent

Referrer

HTTP METHODS

- GET – Retrieves data from the Server
- POST – Submit data to the Server
- PUT – Update data already on the Server
- DELETE – Deletes data from the Server

HTTP RESONSE

HTTP

HTTP Status Codes

1xx: Informational

Request received / processing

2xx: Success

Successfully Received, understood and accepted

3xx: Redirect

Further action must be taken / Redirect

4xx: Client Error

Request does not have what it needs

5xx: Server Error

Server failed to fulfil a valid request

200 - OK

201 – OK Created

301 – Moved to new URL

304 – Not modified (Cached version)

400 – Bad Request

401 – Unauthorized

404 – Not Found

500 – Internal Server Error

TLS/SSL

Hypertext Transfer Protocol Secure (HTTPS)

- Design to increase privacy in the internet from web applications
- Primary goal is to make known attacks (Man-in-the-Middle) increasingly difficult
- Used to be only found in Banking, Retail sites (or any website with payment transactions)
- Need to purchase Secured Socket Layer (SSL) certificate

Security Socket Layer (SSL)

- standard technology that provide secured connectivity between two systems
- SSL Certificate is a small data files that digitally bind a cryptographic key to an organization's details
- application protocol independent and can be used with many different applications

Transport Layer Security (TLS)

- Transport Layer Security (TLS) is an updated and more secured version of SSL

TLS/SSL

Digital Certificates / Public Key Certificate / Identity Certificate

- Electronic document used to proved the ownership of a public key
- information about the identity of its owner (called the subject), and the digital signature of an entity that has verified the certificate's contents (called the issuer)
- If the signature is valid, and the software examining the certificate trusts the issuer (CA), then it can use that key to communicate securely with the certificate's subject

Certificate Authority (CA)

- Is a third-party entity that issues digital certificate
- Trusted both by the subject (owner) of the certificate and by the party relying upon the certificate.
- Certificate format is specified by the X.509 standard

TLS/SSL

Transport Layer Security (TLS)

- cryptographic protocols designed to provide communications security over a computer network
- also used on other applications such as email, instant messaging, and voice over IP (VoIP) etc
- Most of the time called by its older name Secure Sockets Layer (SSL)
- notable for being a part of HTTPS, a protocol for securely browsing the web
- certificate's subject is typically a computer or organization

Virtual Private Network (VPN)

IPSec VPN

- Secure communication over an unsecured medium
- Secured protocol suite for IP communications
- IETF Standard that provides data confidentiality, authentication and integrity
- Authenticates and encrypts the packets of data
- Uses cryptographic security services to protect communications over IP

Benefits

- Cost
- Scalability
- Flexibility
- Security

Virtual Private Network (VPN)

Types of VPN

- Secured VPN (IPsec, SSL VPN)
- Trusted VPN (MPLS VPN)
- Hybrid (Combination of both)

Note: Generic Routing Encapsulation (GRE) is not a VPN but just a tunnel. Though, you may enable IPsec to encrypt traffic that is sent thru the tunnel

VPN Deployment

- Site-to-Site
- Remote Access

IPsec Protocols

- Authentication Header (AH)
- Encapsulating Security Payload (ESP)

Virtual Private Network (VPN)

Site-site IPsec VPN

- Uses Ipsec VPN to replace dedicated WAN link
- Creates a dedicated tunnel per VPN concentrators
- Not scalable
- Not ideal for teleworkers

Remote Access VPNs

- Uses Ipsec or SSL/TLS from user laptop to VPN concentrators
- Client based or Clientless
- More flexible
- ideal for teleworkers

Virtual Private Network (VPN)

Authentication

- Validate Identity
- Attackers will not be able to spoof servers

Privacy

- Encrypts and decrypt data
- Attackers will not be able to View data

Integrity

- Uses hashing algorithm to detect if message has been changed
- Attackers will not be able to modify data undetected

Domain Name Service (DNS)

Domain Nae System (DNS)

- Maps host name to IP address
- www.f5.com → 104.219.111.168
- Easier to remember names than numbers

Root Name Server

192.33.4.12

.com Name Server

100.1.1.1

Local DNS

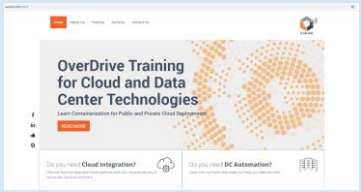
Data Center

Name Server

128.199.206.240

Web Application

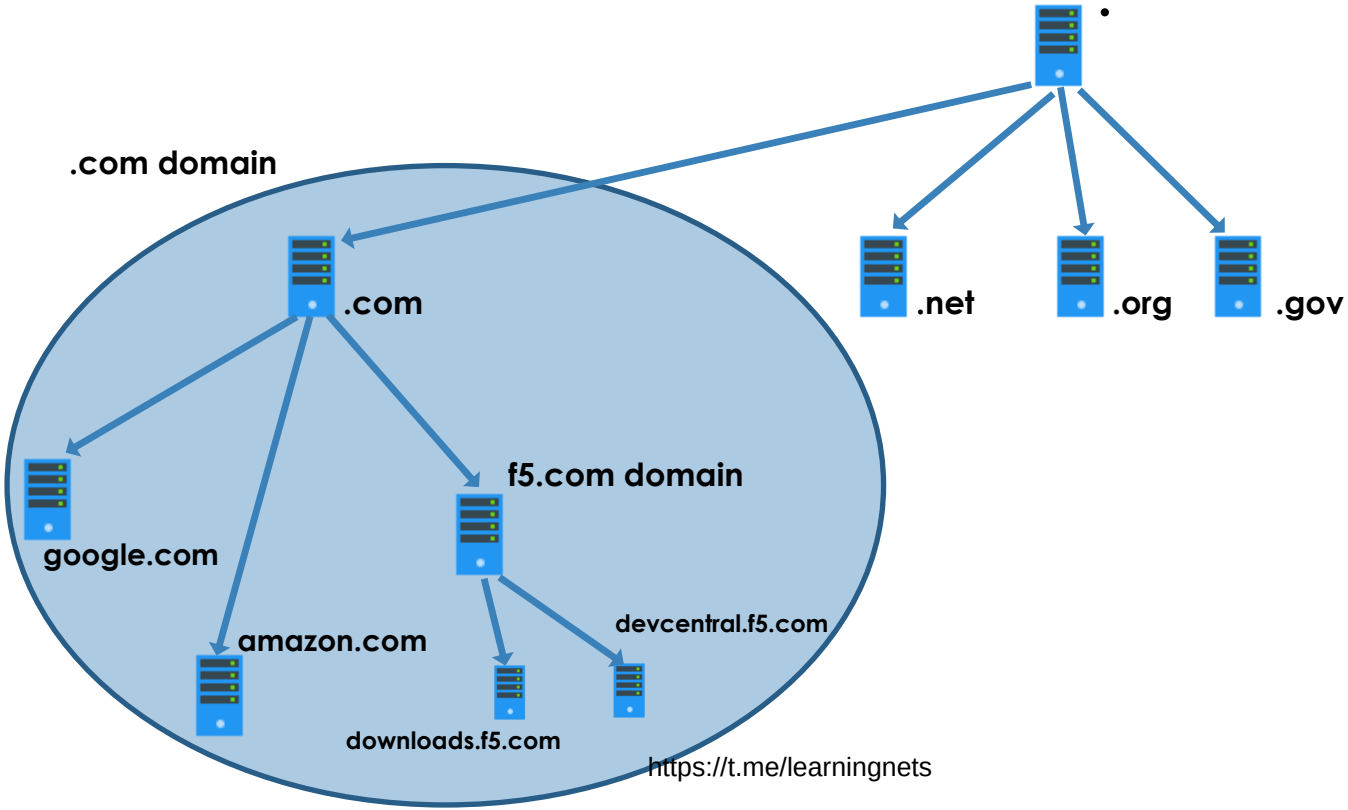
128.199.224.58



http://zurien.com

Domain Name Service (DNS)

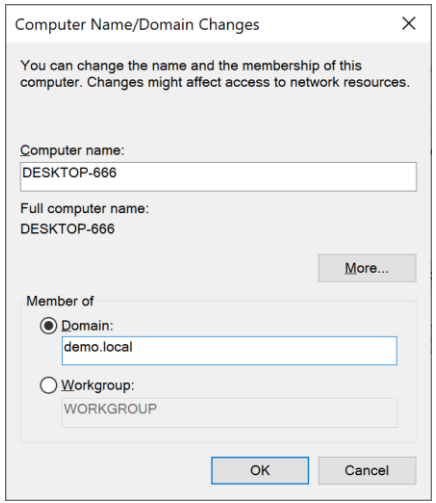
Domains and Zones



Domain Name Service (DNS)

How Critical DNS

- Since we as humans prefer to use names
- Its also common to integrate our servers and devices using names
- It must be redundant and protected




```
server 0.ubuntu.pool.ntp.org
server 1.ubuntu.pool.ntp.org
```

zurien.com

Network Time Protocol (NTP)

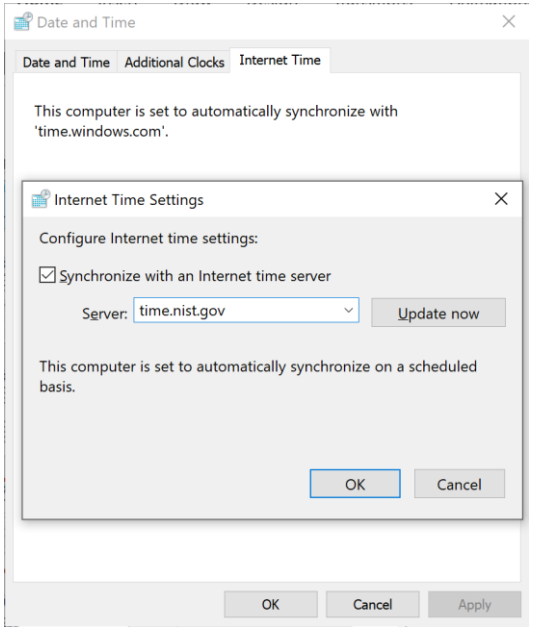
Network Time Protocol (NTP)

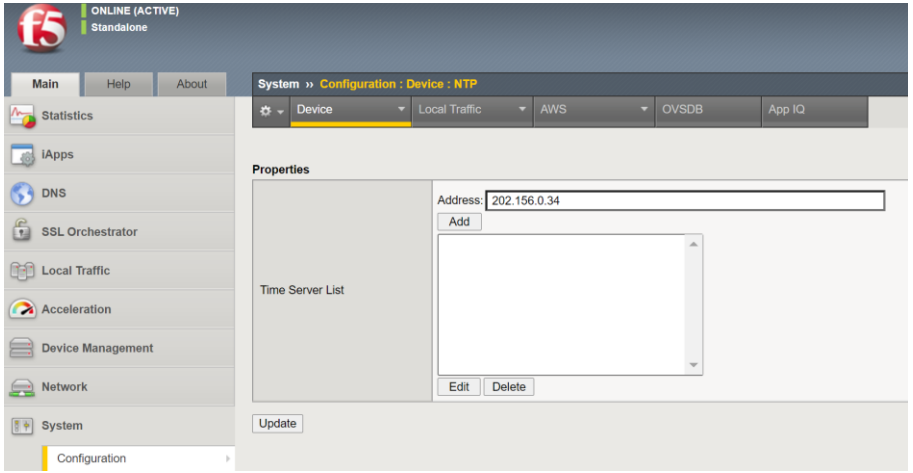
- is network protocol for time synchronization
- client-server model, send and receives timestamps using UDP port 123
- Allows to get the correct time from internal or external time source – local, master, GPS

Why use NTP?

- Correct time allows the tracking of many events in the network in the correct order
- Better management, troubleshooting and forensic
- Time synchronization is critical for Digital Certificates
- Time synchronization is a requirement for some Device integration
- Time Synchronization is required by Law

Network Time Protocol (NTP) Configuration



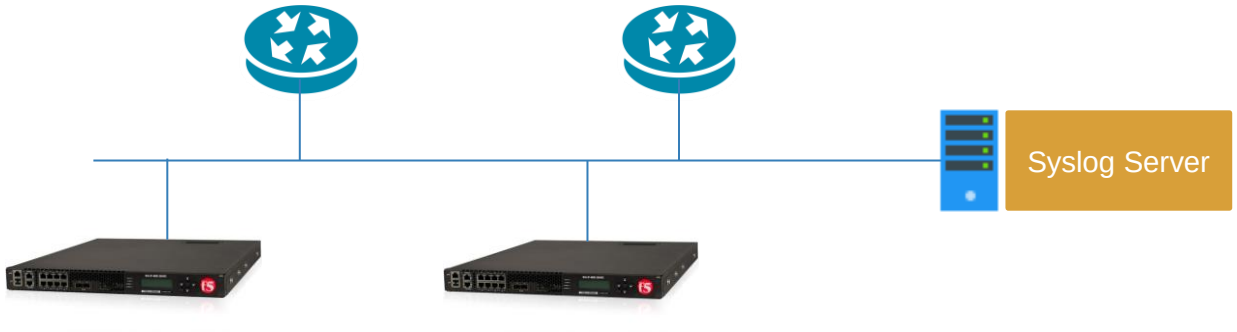



```
server 0.ubuntu.pool.ntp.org
server 1.ubuntu.pool.ntp.org
```

Syslog

Syslog

- standard for message logging, listens to UDP 514
- allows separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them
- Each message is labeled with a facility code, indicating the software type generating the message, and assigned a severity level.
- When operating over a network, syslog uses a client-server architecture where a syslog server listens for logs messages coming from clients.



Syslog

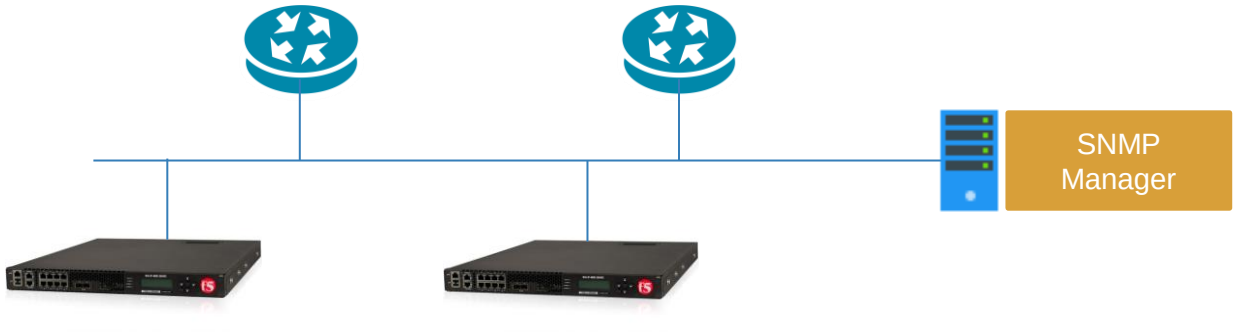
Log Information Levels

Emergency	System Failures
Alert	Serious errors; administrator intervention
Critical	Hardware / System failures
Error	Non-critical but possibility important
Warning	Logged for review
Notice	Useful; can typically be ignored
Informational	Useful; can be ignored
Debug	Troubleshooting

Simple Network Management Protocol

Simple Network Management Protocol (SNMP)

- protocol for collecting and organizing information about managed devices on IP networks. Listens to UDP 161, 162
- Can also modify information to change device behavior. RO and RW access privileges
- support cable modems, routers, switches, servers, workstations, printers, and more



Simple Network Management Protocol

Protocol Versions

- **SNMPv1**

  initial implementation, poor in security

- **SNMPv2c**

  revises version 1 and includes improvements in the areas of performance, security and communications.

  still a very common deployment

  uses community strings to authenticated to SNMP server

- **SNMPv3**

  makes no changes to the protocol aside from the addition of cryptographic security

  security aspect is addressed by offering both strong authentication and data encryption for privacy

  implements User-based Security Model (USM)

Simple Network Management Protocol

Communication Mechanism for SNMP User-based Security Model

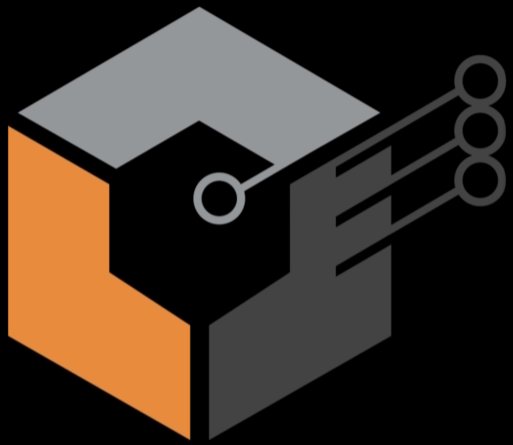
- Communication without authentication and privacy (NoAuthNoPriv).
- Communication with authentication and without privacy (AuthNoPriv).
- Communication with authentication and privacy (AuthPriv).

Available Authentication and Privacy Protocols

- MD5, SHA, HMAC-SHA-2
- DES, 3DES, AES

F5 101 Exam Preparation

Application and Security Technologies



ZURIEN

www.zurien.com