CompTIA Network+ Exam N10-008

Lesson 14

Supporting and Troubleshooting Secure Networks

Objectives

- Compare and contrast security appliances
- Troubleshoot service and security issues

Lesson 14

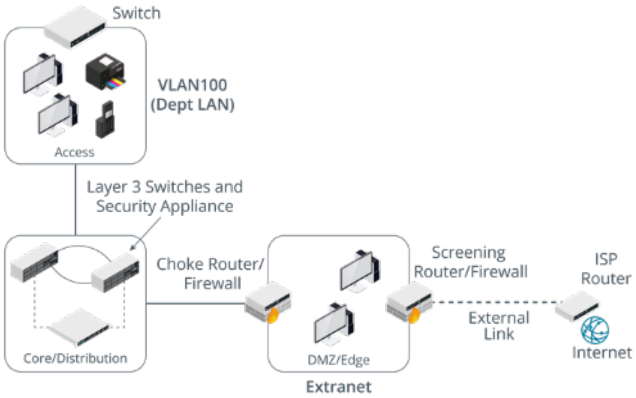
Topic 14A

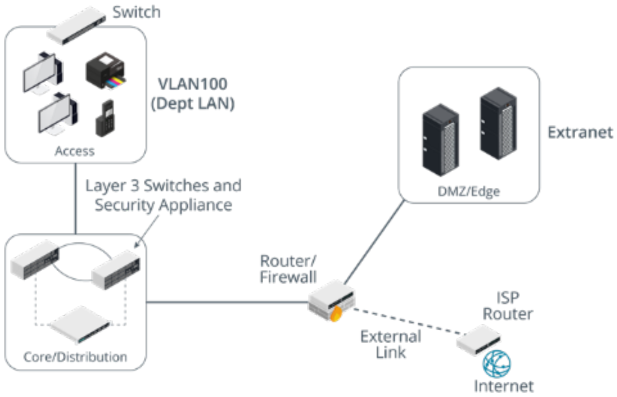
Compare and Contrast Security Appliances

Network Segmentation Enforcement

- Segmentation creates boundaries for network traffic
- Traffic between segments can be filtered
- Network security zones
    - Internet-facing versus internal
    - Perimeter network

Screened Subnets

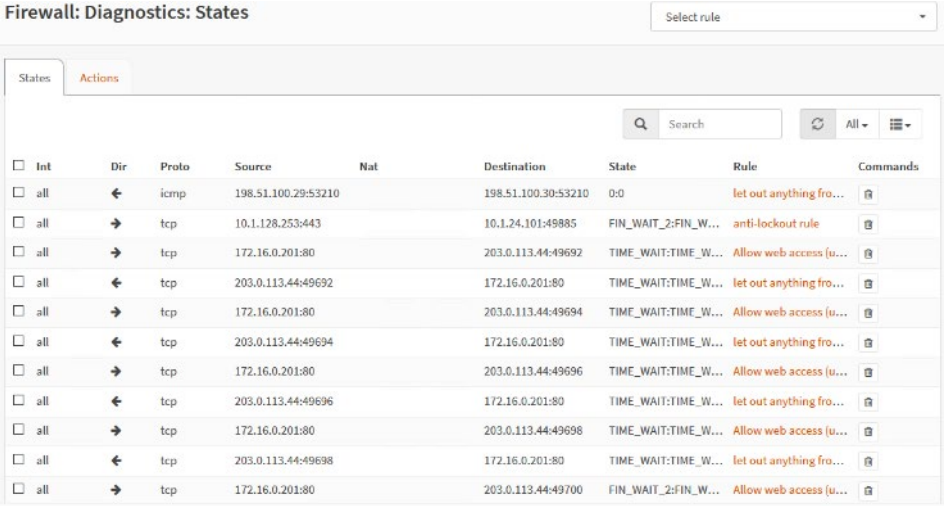




- Different security configurations for public and private gateways
- Screening firewall on the public interface
- Choke firewall on the internal interface
- Triple homed firewall configuration

Firewall Uses and Types

- Packet filtering firewalls
  - Access control list (ACL) with accept or deny rules
  - Layer 3 (+ TCP/UDP port number) only
  - IP source/destination, IP protocol type, source/destination port
- Stateful inspection firewalls
  - Layer 4
    - Monitor connection state
  - Layer 7
    - Inspect application protocol packet contents

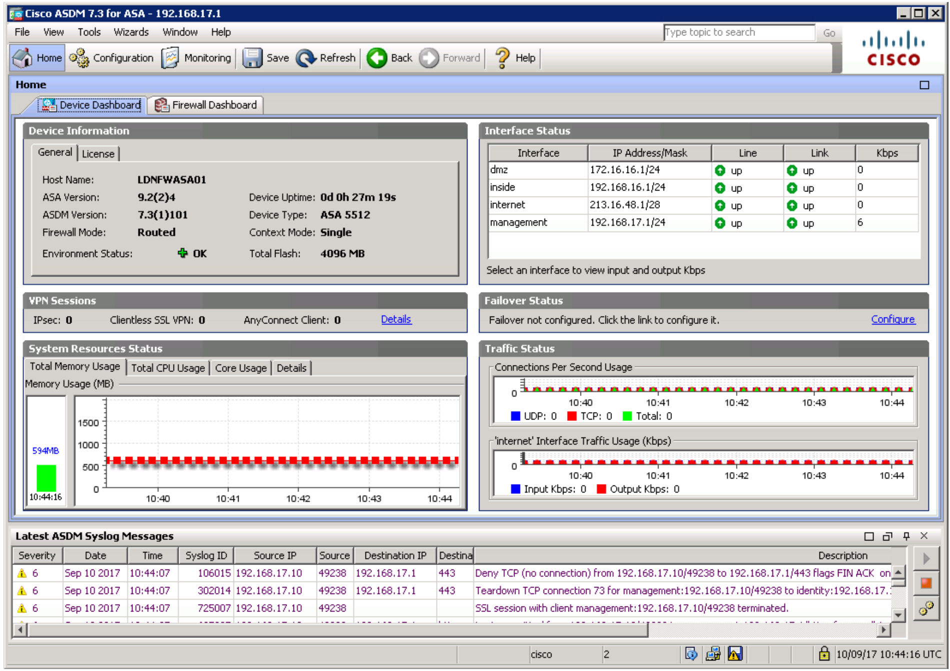


Firewall: Diagnostics: States

☐	Int	Dir	Proto	Source	Nat	Destination	State	Rule	Commands
☐	all	←	icmp	198.51.100.29:53210		198.51.100.30:53210	0:0	let out anything fro...	🗑
☐	all	→	tcp	10.1.128.253:443		10.1.24.101:49885	FIN_WAIT_2:FIN_W...	anti-lockout rule	🗑
☐	all	→	tcp	172.16.0.201:80		203.0.113.44:49692	TIME_WAIT:TIME_W...	Allow web access (u...	🗑
☐	all	←	tcp	203.0.113.44:49692		172.16.0.201:80	TIME_WAIT:TIME_W...	let out anything fro...	🗑
☐	all	→	tcp	172.16.0.201:80		203.0.113.44:49694	TIME_WAIT:TIME_W...	Allow web access (u...	🗑
☐	all	←	tcp	203.0.113.44:49694		172.16.0.201:80	TIME_WAIT:TIME_W...	let out anything fro...	🗑
☐	all	→	tcp	172.16.0.201:80		203.0.113.44:49696	TIME_WAIT:TIME_W...	Allow web access (u...	🗑
☐	all	←	tcp	203.0.113.44:49696		172.16.0.201:80	TIME_WAIT:TIME_W...	let out anything fro...	🗑
☐	all	→	tcp	172.16.0.201:80		203.0.113.44:49698	TIME_WAIT:TIME_W...	Allow web access (u...	🗑
☐	all	←	tcp	203.0.113.44:49698		172.16.0.201:80	TIME_WAIT:TIME_W...	let out anything fro...	🗑
☐	all	→	tcp	172.16.0.201:80		203.0.113.44:49700	FIN_WAIT_2:FIN_W...	Allow web access (u...	🗑

Firewall Selection and Placement

- Placement
  - Perimeter versus internal versus host
  - Load
- Appliance firewall
  - Routed versus layer 2
- Router firewall
  - Enterprise versus SOHO



Device Information

Host Name: **LDNFWASA01**
ASA Version: **9.2(2)4** Device Uptime: **0d 0h 27m 19s**
ASDM Version: **7.3(1)101** Device Type: **ASA 5512**
Firewall Mode: **Routed** Context Mode: **Single**
Environment Status: ✚ **OK** Total Flash: **4096 MB**

Interface Status

Interface	IP Address/Mask	Line	Link	Kbps
dmz	172.16.16.1/24	up	up	0
inside	192.168.16.1/24	up	up	0
internet	213.16.48.1/28	up	up	0
management	192.168.17.1/24	up	up	6

Select an interface to view input and output Kbps

VPN Sessions

IPsec: **0** Clientless SSL VPN: **0** AnyConnect Client: **0** Details

Failover Status

Failover not configured. Click the link to configure it. Configure

System Resources Status

Traffic Status

🟦 UDP: 0 🟥 TCP: 0 🟩 Total: 0

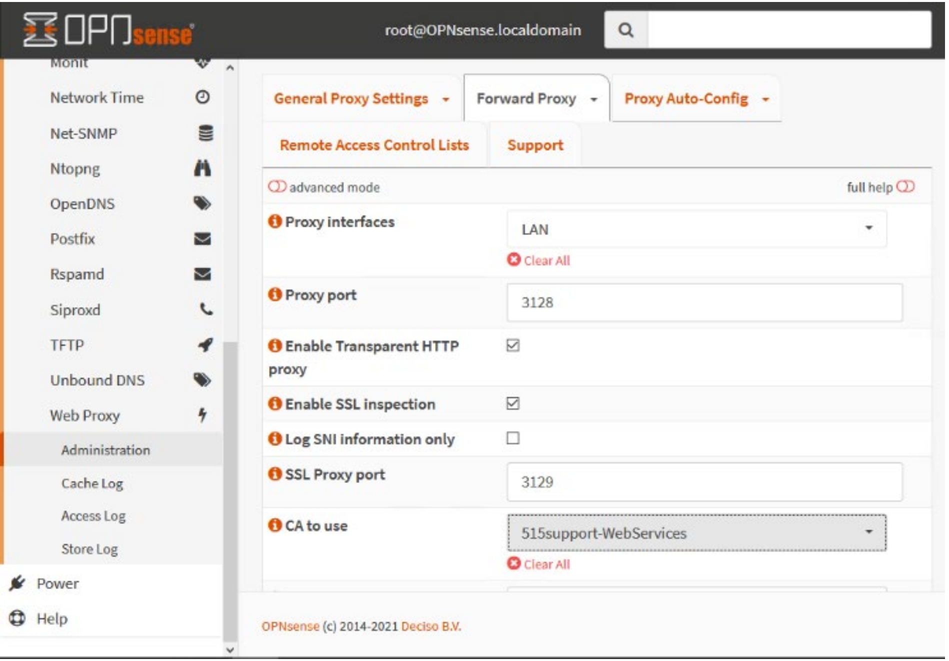
🟦 Input Kbps: 0 🟥 Output Kbps: 0

Latest ASDM Syslog Messages

Severity	Date	Time	Syslog ID	Source IP	Source	Destination IP	Destina	Description
⚠ 6	Sep 10 2017	10:44:07	106015	192.168.17.10	49238	192.168.17.1	443	Deny TCP (no connection) from 192.168.17.10/49238 to 192.168.17.1/443 flags FIN ACK on
⚠ 6	Sep 10 2017	10:44:07	302014	192.168.17.10	49238	192.168.17.1	443	Teardown TCP connection 73 for management:192.168.17.10/49238 to identity:192.168.17.
⚠ 6	Sep 10 2017	10:44:07	725007	192.168.17.10	49238			SSL session with client management:192.168.17.10/49238 terminated.

cisco 2 10/09/17 10:44:16 UTC

Proxy Servers



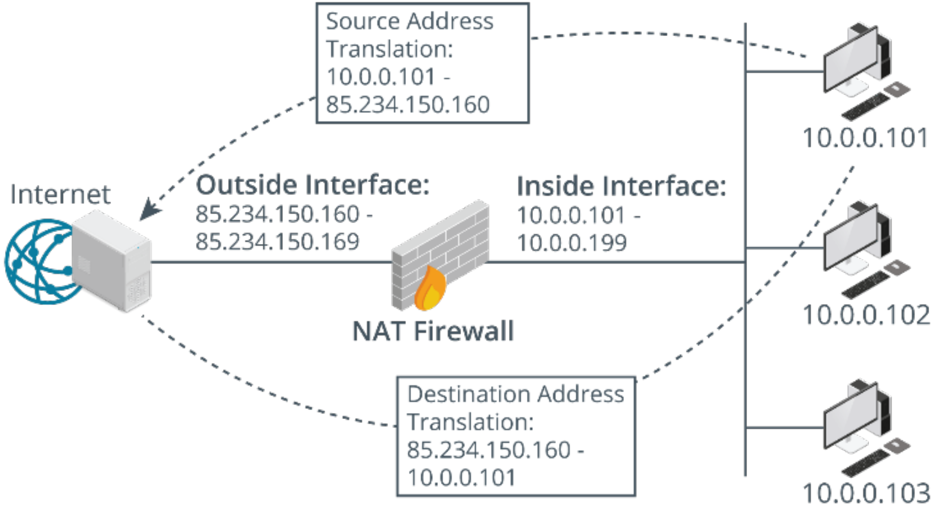
Proxy interfaces	LAN
Proxy port	3128
Enable Transparent HTTP proxy	☑
Enable SSL inspection	☑
Log SNI information only	☐
SSL Proxy port	3129
CA to use	515support-WebServices

OPNsense (c) 2014-2021 Deciso B.V.

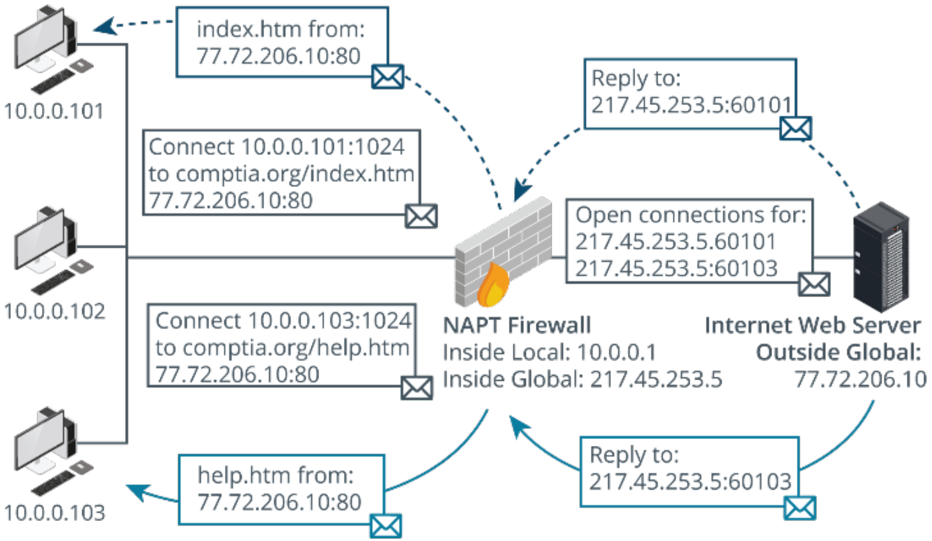
- Outbound proxy completes requests on behalf of clients
- Application-specific versus multipurpose
- Caching
- Non-transparent versus transparent
- Reverse proxies

Network Address Translation

- Mapping between internal private IP ranges and public IP addresses
- Static NAT versus dynamic NAT


Source Address Translation: 10.0.0.101 - 85.234.150.160
Internet
Outside Interface: 85.234.150.160 - 85.234.150.169
Inside Interface: 10.0.0.101 - 10.0.0.199
NAT Firewall
Destination Address Translation: 85.234.150.160 - 10.0.0.101
10.0.0.101
10.0.0.102
10.0.0.103

Port Address Translation



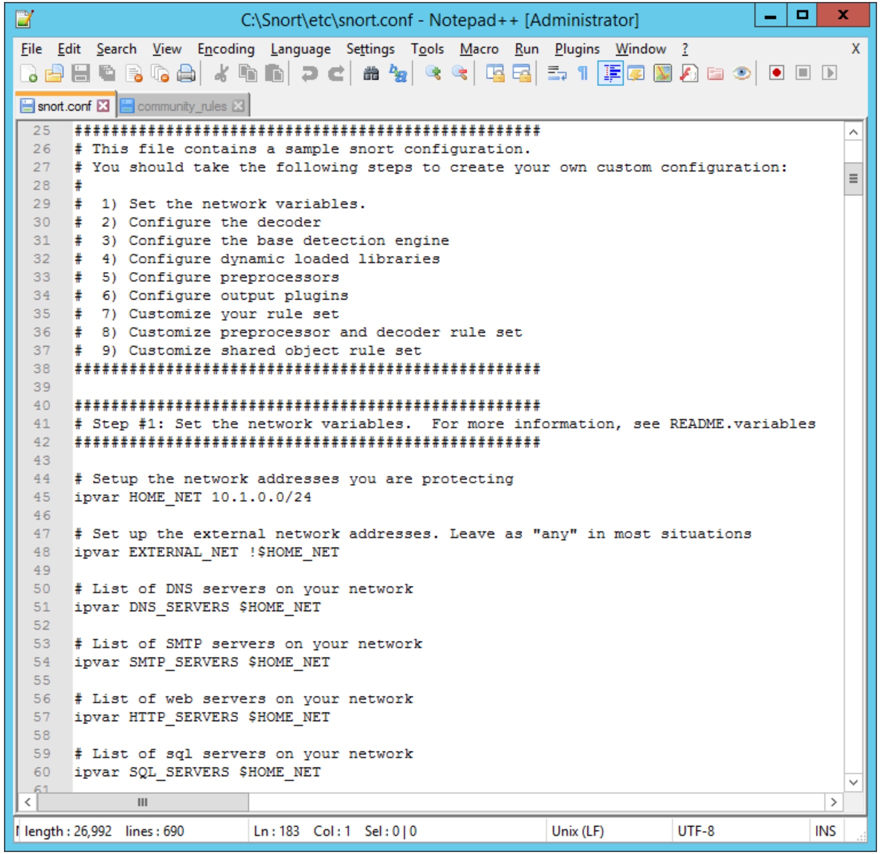
- Network Address Port Translation (NAPT) or NAT overloading
- Router is configured with single public IP address
- Maps client connections using ephemeral ports

Defense in Depth

- Focus away from perimeter security
- Network access control
- Honeypots
- Separation of duties

Intrusion Detection and Prevention Systems

- Intrusion detection system (IDS)
  - Sniff traffic to match signatures of suspicious packets/flows
  - Passive detection
- Intrusion prevention system (IPS)
  - Can block traffic
- Standalone versus integrated with firewall


C:\Snort\etc\snort.conf - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
snort.conf
community_rules
length : 26,992 lines : 690
Ln : 183 Col : 1 Sel : 0 | 0
Unix (LF)
UTF-8
INS

```
###################################################
# This file contains a sample snort configuration.
# You should take the following steps to create your own custom configuration:
#
#  1) Set the network variables.
#  2) Configure the decoder
#  3) Configure the base detection engine
#  4) Configure dynamic loaded libraries
#  5) Configure preprocessors
#  6) Configure output plugins
#  7) Customize your rule set
#  8) Customize preprocessor and decoder rule set
#  9) Customize shared object rule set
###################################################

###################################################
# Step #1: Set the network variables.  For more information, see README.variables
###################################################

# Setup the network addresses you are protecting
ipvar HOME_NET 10.1.0.0/24

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET !$HOME_NET

# List of DNS servers on your network
ipvar DNS_SERVERS $HOME_NET

# List of SMTP servers on your network
ipvar SMTP_SERVERS $HOME_NET

# List of web servers on your network
ipvar HTTP_SERVERS $HOME_NET

# List of sql servers on your network
ipvar SQL_SERVERS $HOME_NET
```

Review Activity: Security Appliances

- Network Segmentation Enforcement
- Screened Subnets
- Firewall Uses and Types
- Firewall Selection and Placement
- Proxy Servers
- Network Address Translation
- Port Address Translation
- Defense in Depth
- Intrusion Detection and Prevention Systems

Lab Activity

Assisted Lab: Configure a NAT Firewall

- Lab types
  - Assisted labs guide you step-by-step through tasks
  - Applied labs set goals with limited guidance
- Complete lab
  - Submit all items for grading and check each progress box
  - Select “Grade Lab” from final page
- Save lab
  - Select the hamburger menu and select “Save”
  - Save up to two labs in progress for up to 7 days
- Cancel lab without grading
  - Select the hamburger menu and select “End”

Lesson 14

Topic 14B

Troubleshoot Service and Security Issues

DHCP Issues

- Server scope and exhaustion issues
    - Server offline
    - Address pool exhausted
    - No DHCP relay
    - Scopes reconfigured—clients may have “expired” configuration
- Rogue DHCP server issues
    - Accidental deployment
    - Malicious

Name Resolution Issues

- Name resolution methods
  - Verify name resolution sequence
  - Test services with HOSTS
  - Check client's DNS server address configuration
  - Check server availability

- DNS configuration issues
  - Suspect name resolution problem when link test by IP address works
  - Establish scope of problem – single client? subnet?
  - Verify client configuration
    - DNS server and suffix
    - Static assignment or DHCP
  - Use lookup tools to verify resource records on DNS server

VLAN Assignment Issues

- Check configuration on switch
- Check VLAN membership
- Check services available to VLAN
  - Routing
  - DHCP/DHCP relay/IP helper
  - DNS
  - Authentication/network applications

Unresponsive Service and Network Performance Issues

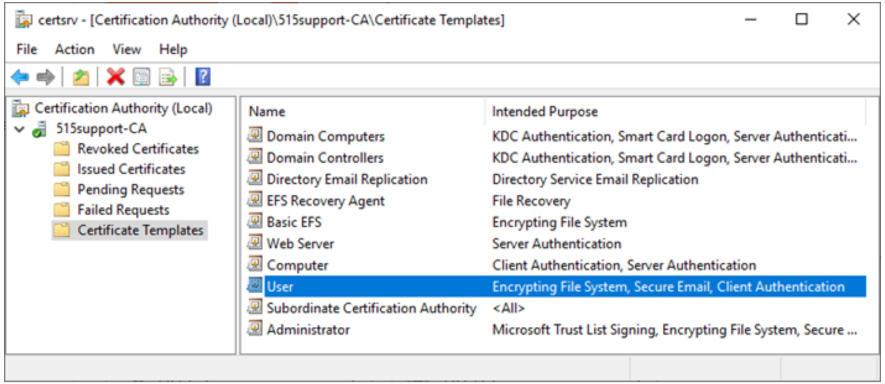
- Verify scope—Is it a client problem or server one?
- Application/OS crash
- Hardware overutilization
- Network congestion
- Broadcast storm
- Denial of service (DoS)

Misconfigured Firewall and ACL Issues

- Authorized application blocked
  - Blocked TCP or UDP port
  - Blocked IP address or network
  - Test from inside and outside firewall
  - Inspect firewall log
- Unauthorized application not blocked

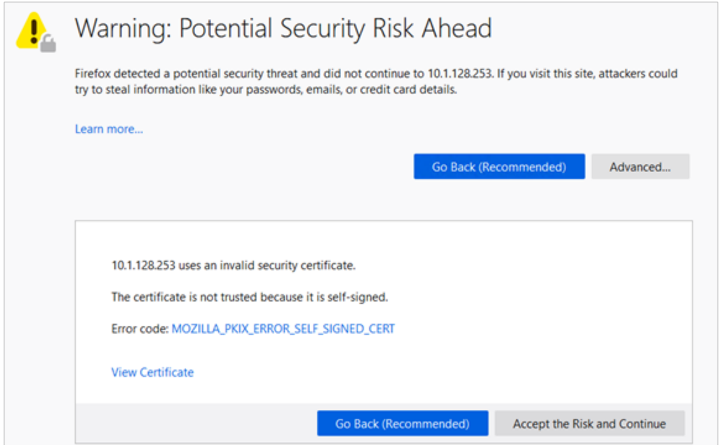
Untrusted Certificate Issues

- Must be a trust relationship with server's CA
- Check root certificates store
  - Apps may use separate trust store
- Self-signed certificates
- Subject name and key usage issues
- Expired and revoked certificates (or CA certificates)
- Time synchronization


certsrv - [Certification Authority (Local)\515support-CA\Certificate Templates]
File
Action
View
Help

Certification Authority (Local)
- 515support-CA
  - Revoked Certificates
  - Issued Certificates
  - Pending Requests
  - Failed Requests
  - Certificate Templates

Name	Intended Purpose
Domain Computers	KDC Authentication, Smart Card Logon, Server Authenticati...
Domain Controllers	KDC Authentication, Smart Card Logon, Server Authenticati...
Directory Email Replication	Directory Service Email Replication
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
Web Server	Server Authentication
Computer	Client Authentication, Server Authentication
User	Encrypting File System, Secure Email, Client Authentication
Subordinate Certification Authority	<All>
Administrator	Microsoft Trust List Signing, Encrypting File System, Secure ...



Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to 10.1.128.253. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

10.1.128.253 uses an invalid security certificate.

The certificate is not trusted because it is self-signed.

Error code: MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT

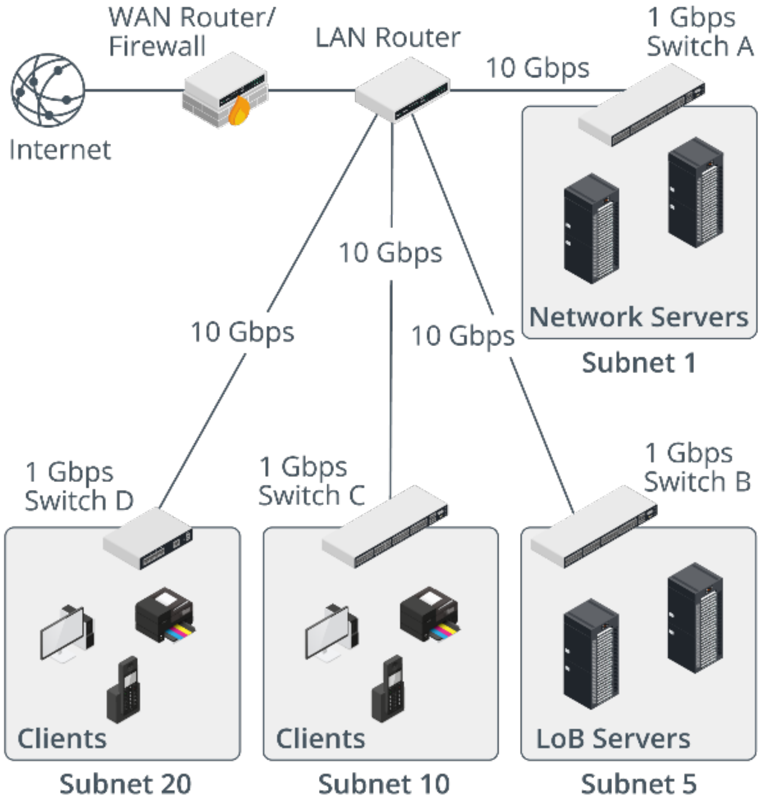
Other Common Issues

- NTP issues
  - Verify accurate time synchronization
- Bring Your Own Device (BYOD) challenges
  - Compatibility support for wide range of employee-selected devices
  - Security issues
  - Enterprise Mobility Management (EMM) and corporate workspaces
- Licensed feature issues
  - Expiry of trial periods
  - Activation failure

Review Activity: Service and Security Issues

- DHCP Issues
- Name Resolution Issues
- VLAN Assignment Issues
- Unresponsive Service and Network Performance Issues
- Misconfigured Firewall and ACL Issues
- Untrusted Certificate Issues
- Other Common Issues

Review Activity: Scenarios in Service and Security Issues



CompTIA Network+ Exam N10-008

Lesson 14

Summary