

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

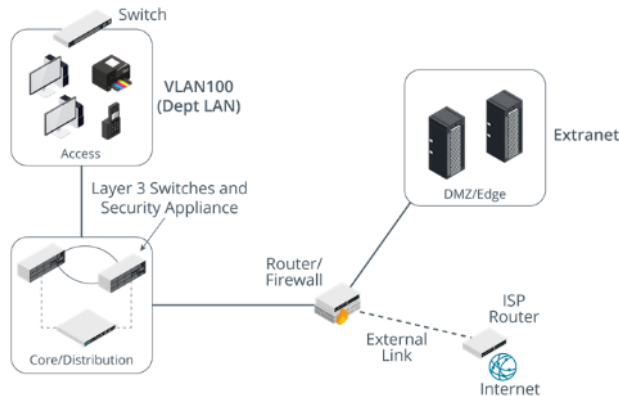
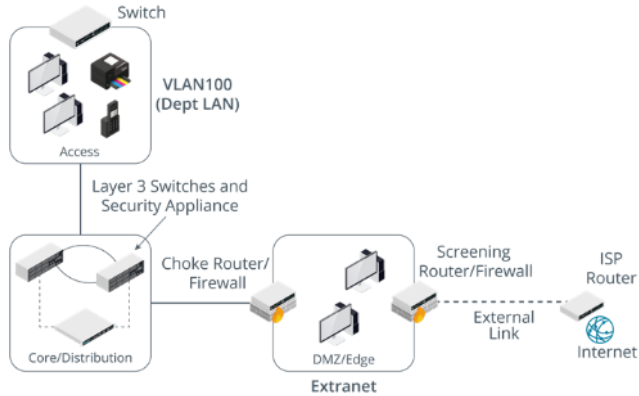
# Topic 14A

## 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

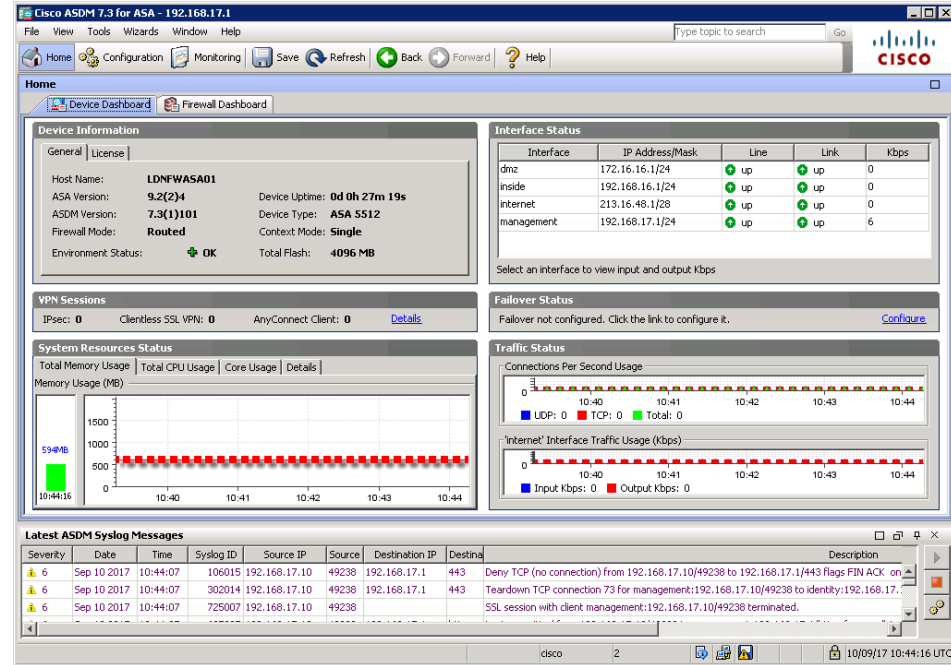
- Packet filtering firewalls
  - Access control list (ACL) with accept or deny rules
  - Layer 3 (+ TCP/UDP port number) only
  - IP source/destination, IP protocol type, source/destination port
- Stateful inspection firewalls
  - Layer 4
    - Monitor connection state
  - Layer 7
    - Inspect application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

Firewall: Diagnostics: States

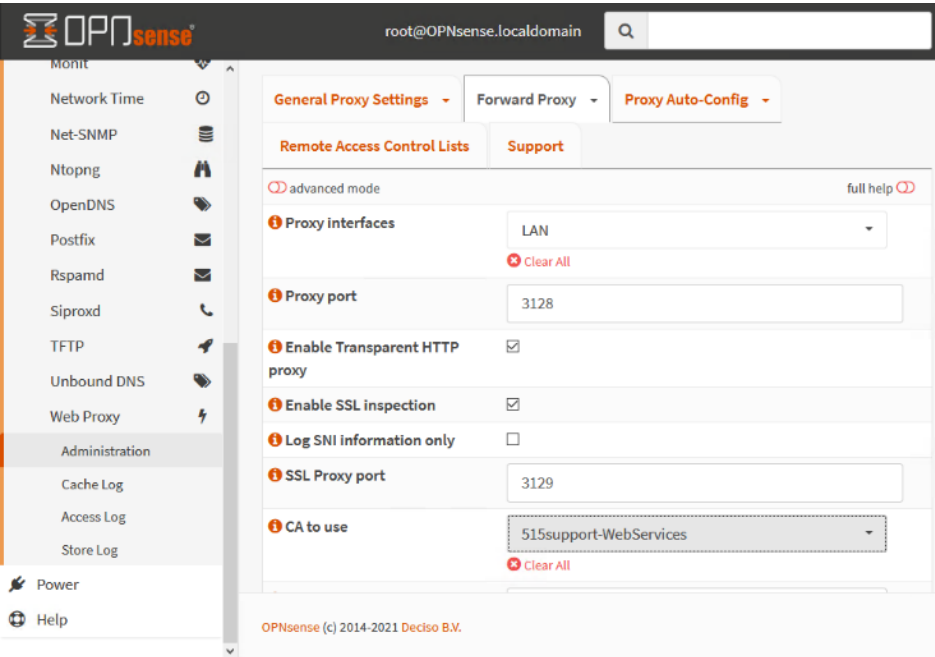
Firewall: Diagnostics: States									Select rule
States									
Actions									
Q Search									All
Int	Dir	Proto	Source	Nat	Destination	State	Rule	Commands	
<input type="checkbox"/>	all	←	icmp	198.51.100.29:53210	198.51.100.30:53210	0:0	let out anything fro...		
<input type="checkbox"/>	all	→	tcp	10.1.128.253:443	10.1.24.101:49885	FIN_WAIT_2:FIN_W...	anti-lockout rule		
<input type="checkbox"/>	all	→	tcp	172.16.0.201:80	203.0.113.44:49692	TIME_WAIT:TIME_W...	Allow web access (u...		
<input type="checkbox"/>	all	←	tcp	203.0.113.44:49692	172.16.0.201:80	TIME_WAIT:TIME_W...	let out anything fro...		
<input type="checkbox"/>	all	→	tcp	172.16.0.201:80	203.0.113.44:49694	TIME_WAIT:TIME_W...	Allow web access (u...		
<input type="checkbox"/>	all	←	tcp	203.0.113.44:49694	172.16.0.201:80	TIME_WAIT:TIME_W...	let out anything fro...		
<input type="checkbox"/>	all	→	tcp	172.16.0.201:80	203.0.113.44:49696	TIME_WAIT:TIME_W...	Allow web access (u...		
<input type="checkbox"/>	all	←	tcp	203.0.113.44:49696	172.16.0.201:80	TIME_WAIT:TIME_W...	let out anything fro...		
<input type="checkbox"/>	all	→	tcp	172.16.0.201:80	203.0.113.44:49698	TIME_WAIT:TIME_W...	Allow web access (u...		
<input type="checkbox"/>	all	←	tcp	203.0.113.44:49698	172.16.0.201:80	TIME_WAIT:TIME_W...	let out anything fro...		
<input type="checkbox"/>	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



# Proxy Servers

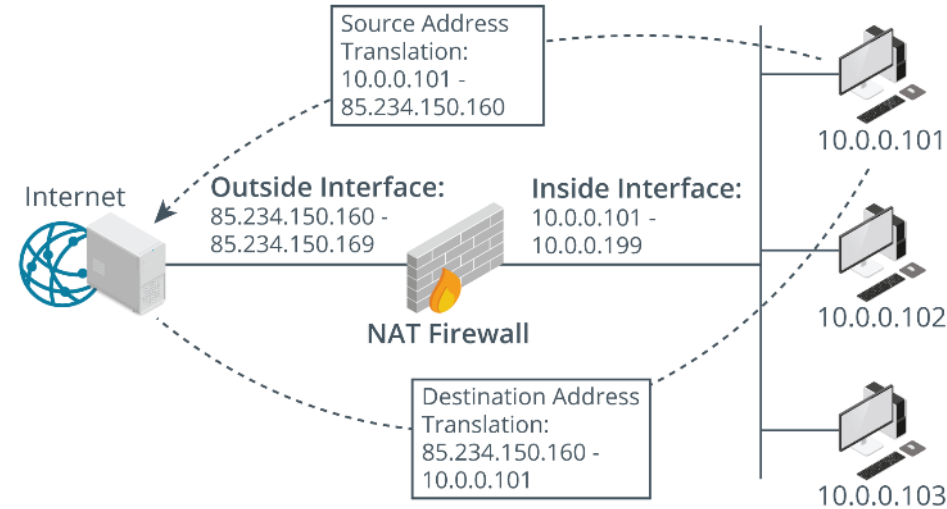


- Outbound proxy completes requests on behalf of clients
- Application-specific versus multipurpose
- Caching
- Non-transparent versus transparent
- Reverse proxies

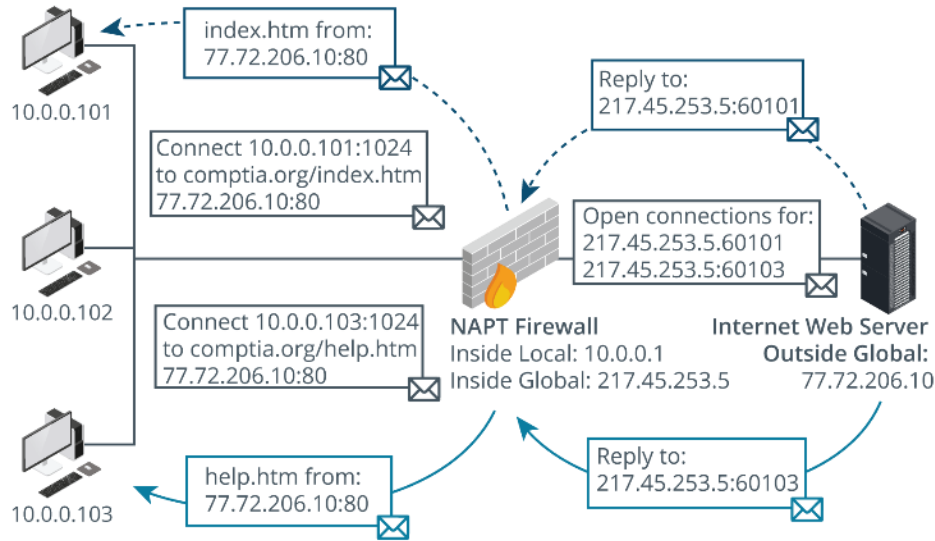


# Network Address Translation

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



# Port Address Translation



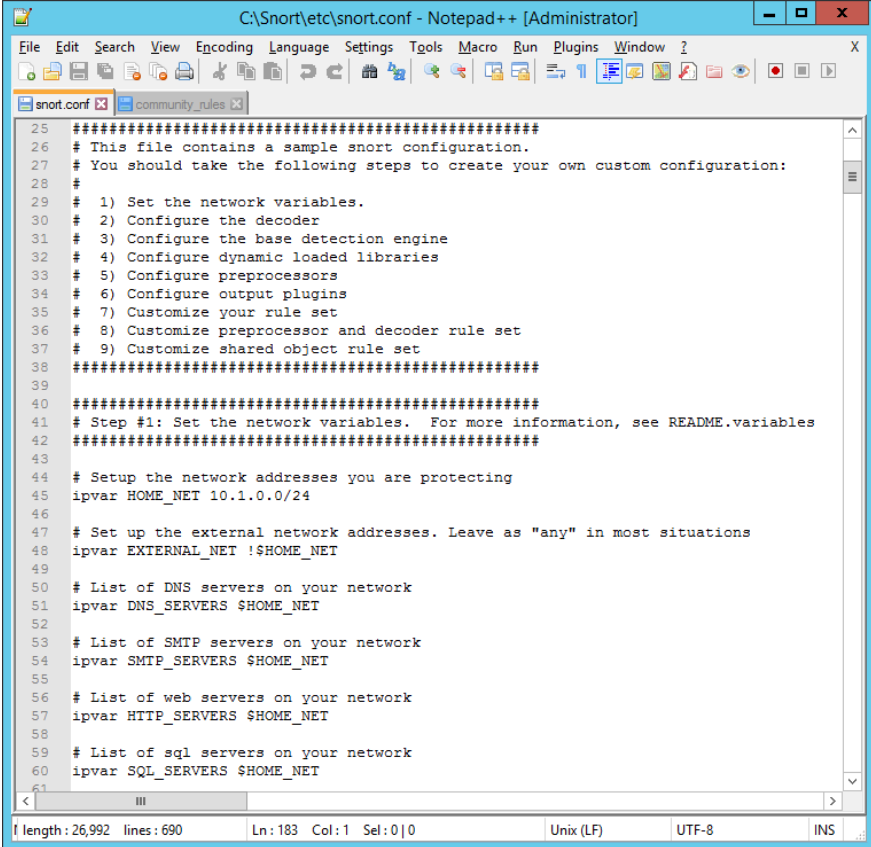
- Network Address Port Translation (NAPT) or NAT overloading
- Router is configured with single public IP address
- Maps client connections using ephemeral ports

# 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



The screenshot shows a Notepad++ window titled "C:\Snort\etc\snort.conf - Notepad++ [Administrator]". The window displays the contents of the snort.conf file, which is a sample configuration for Snort. The text is as follows:


```
25 #####
26 # This file contains a sample snort configuration.
27 # You should take the following steps to create your own custom configuration:
28 #
29 # 1) Set the network variables.
30 # 2) Configure the decoder
31 # 3) Configure the base detection engine
32 # 4) Configure dynamic loaded libraries
33 # 5) Configure preprocessors
34 # 6) Configure output plugins
35 # 7) Customize your rule set
36 # 8) Customize preprocessor and decoder rule set
37 # 9) Customize shared object rule set
38 #####
39
40 #####
41 # Step #1: Set the network variables. For more information, see README.variables
42 #####
43
44 # Setup the network addresses you are protecting
45 ipvar HOME_NET 10.1.0.0/24
46
47 # Set up the external network addresses. Leave as "any" in most situations
48 ipvar EXTERNAL_NET !$HOME_NET
49
50 # List of DNS servers on your network
51 ipvar DNS_SERVERS $HOME_NET
52
53 # List of SMTP servers on your network
54 ipvar SMTP_SERVERS $HOME_NET
55
56 # List of web servers on your network
57 ipvar HTTP_SERVERS $HOME_NET
58
59 # List of sql servers on your network
60 ipvar SQL_SERVERS $HOME_NET
61
```

The status bar at the bottom of the window shows: "length: 26,992 lines: 690", "Ln: 183 Col: 1 Sel: 0 | 0", "Unix (LF)", "UTF-8", and "INS".

# 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

## 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

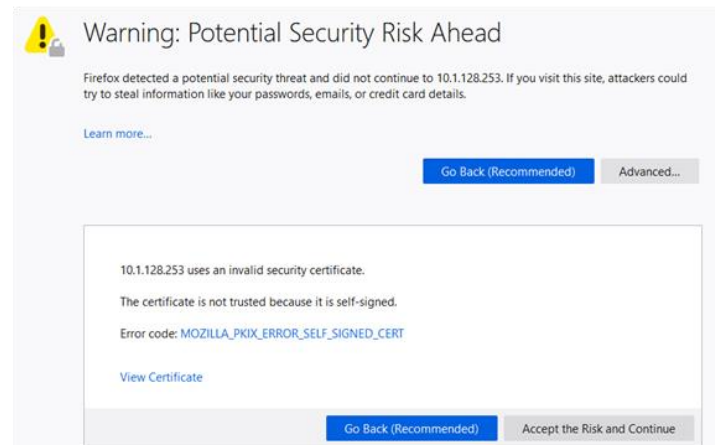
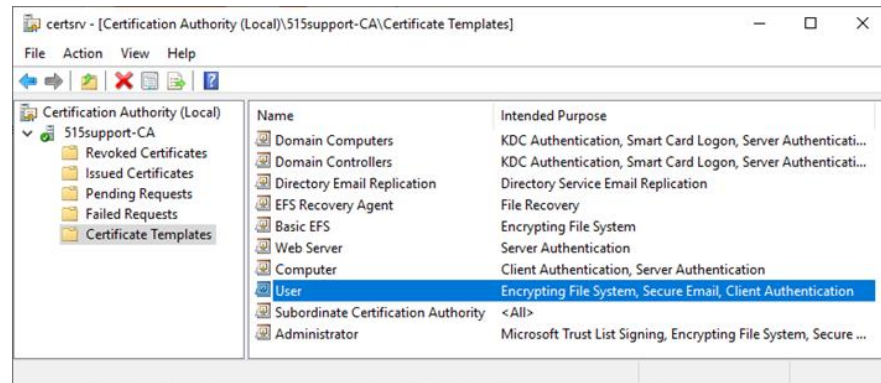
- Verify scope—Is it a client problem or server one?
- Application/OS crash
- Hardware overutilization
- Network congestion
- Broadcast storm
- Denial of service (DoS)

# 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



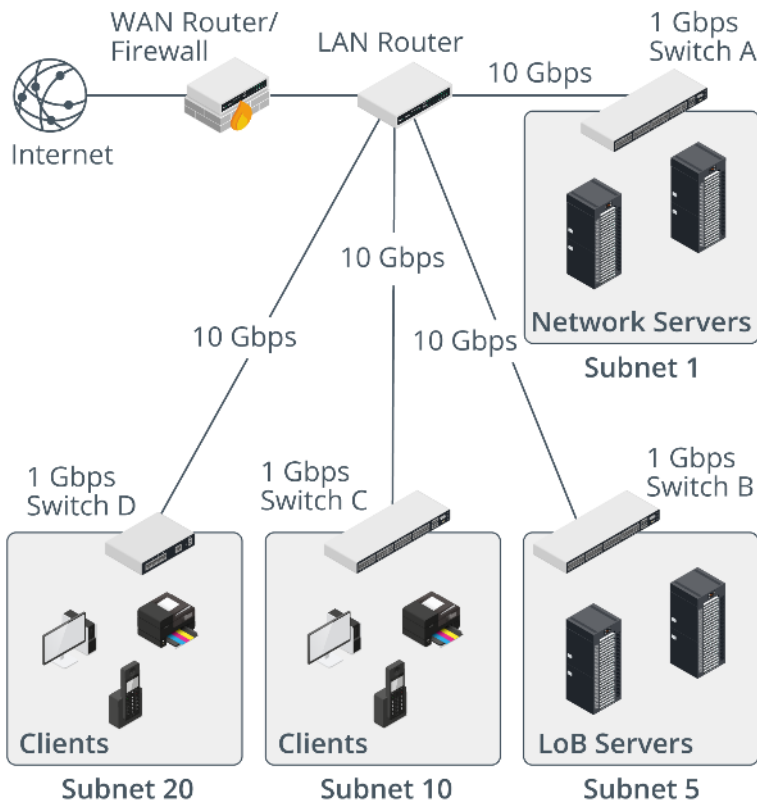
# Other Common Issues

- 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