Lesson 9

Implementing Secure Network Designs

CompTIA®

Topic 9A

Implement Secure Network Designs

Syllabus Objectives Covered

- 3.3 Given a scenario, implement secure network designs

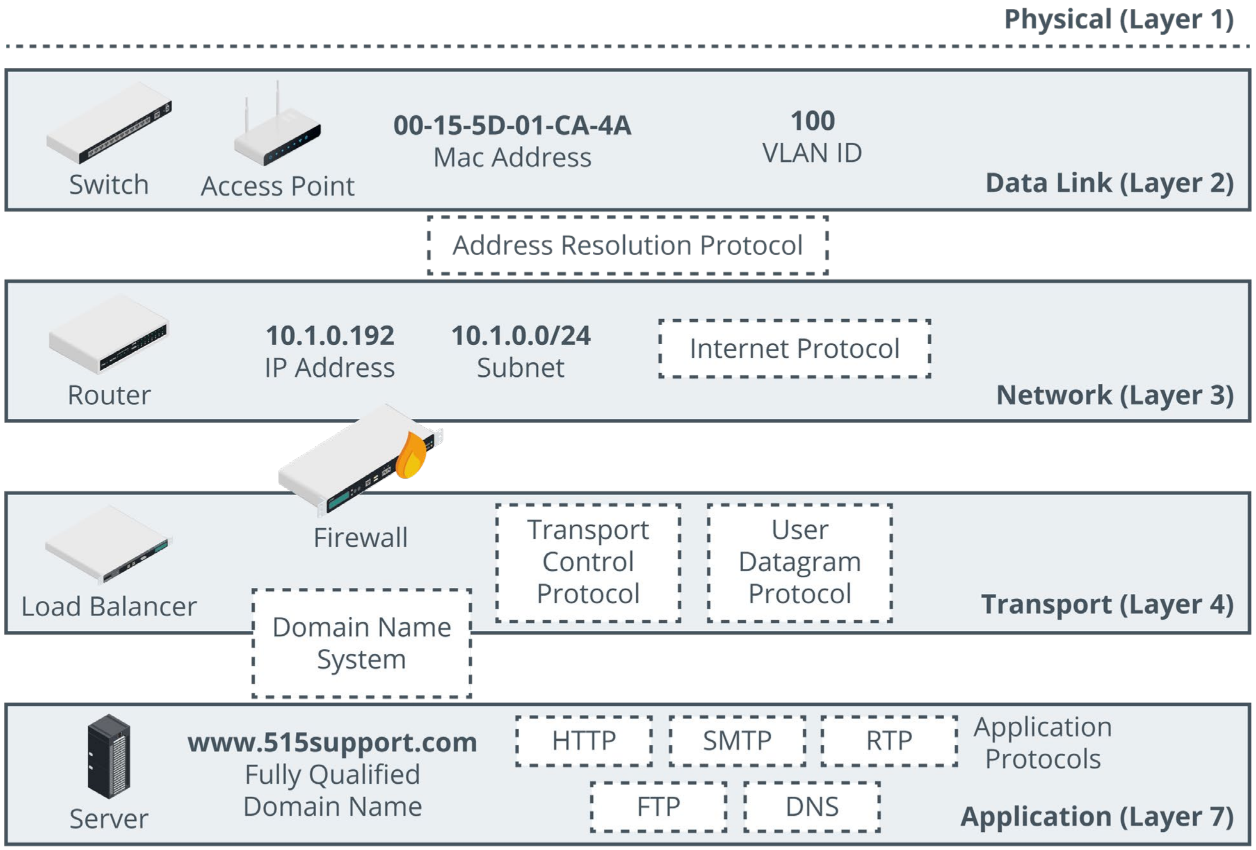
Secure Network Designs

- What problems arise from weaknesses in the network design/architecture?
  - Single points of failure
  - Complex dependencies
  - Availability over confidentiality and integrity
  - Lack of documentation and change control
  - Overdependence on perimeter security
- Best practice design and architecture guides
  - Cisco's SAFE Architecture
  - Places in the Network

Business Workflows and Network Architecture

- Corporate network
  - Access
  - Email mailbox server
  - Mail transfer server
- Segmentation
- Data flows and access controls

Network Appliances



Physical (Layer 1)

Switch

Access Point

00-15-5D-01-CA-4A
Mac Address

100
VLAN ID

Data Link (Layer 2)

Address Resolution Protocol

Router

10.1.0.192
IP Address

10.1.0.0/24
Subnet

Internet Protocol

Network (Layer 3)

Firewall

Load Balancer

Transport Control Protocol

User Datagram Protocol

Transport (Layer 4)

Domain Name System

Server

www.515support.com
Fully Qualified Domain Name

HTTP

SMTP

RTP

Application Protocols

FTP

DNS

Application (Layer 7)

Images © 123rf.com.

Routing and Switching Protocols

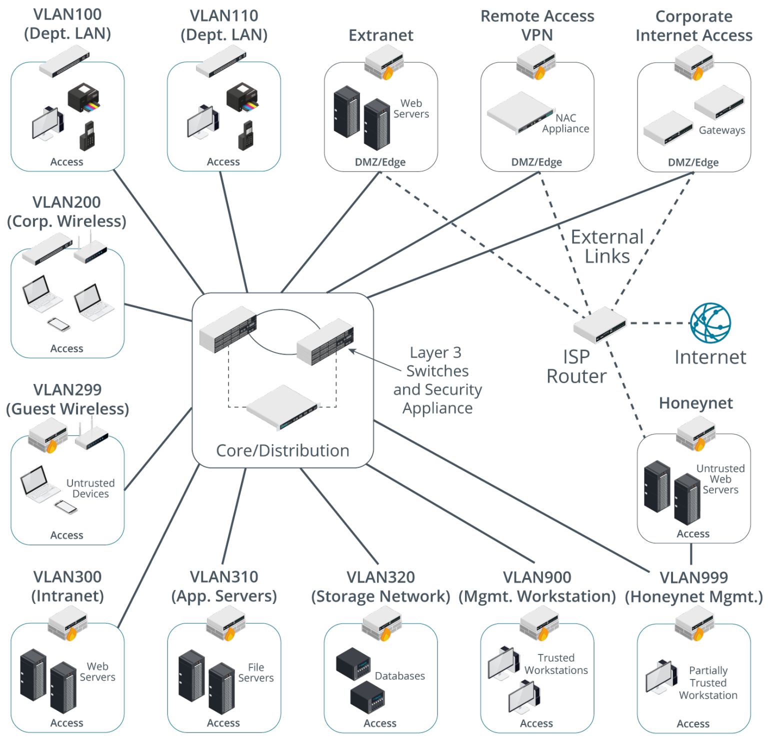
- Forwarding
  - Layer 2 forwarding
  - Layer 3 forwarding
- Address Resolution Protocol (ARP)
  - Map IP addresses to MAC addresses
- Internet Protocol (IP)
  - IPv4 and IPv6
  - Network prefix/subnet mask
- Routing protocols
  - Communicate routing table updates

Network Segmentation

- Network segment
  - Nodes can communicate at layer 2
  - Broadcast domain
- Implementing network segments
  - Separate unmanaged switches
  - Configure virtual LANs (VLANs) on managed switches
- Layer 3 subnets
  - Map subnets to VLANs

Network Topology and Zones

- Physical and logical topologies
- Zones represent isolated segments for hosts that have the same security requirement
- Traffic between zones is subject to filtering by a firewall
- Main zone types
  - Intranet (private)
  - Extranet
  - Internet (public)
- Enterprise architecture zones
  - Access blocks representing host groups

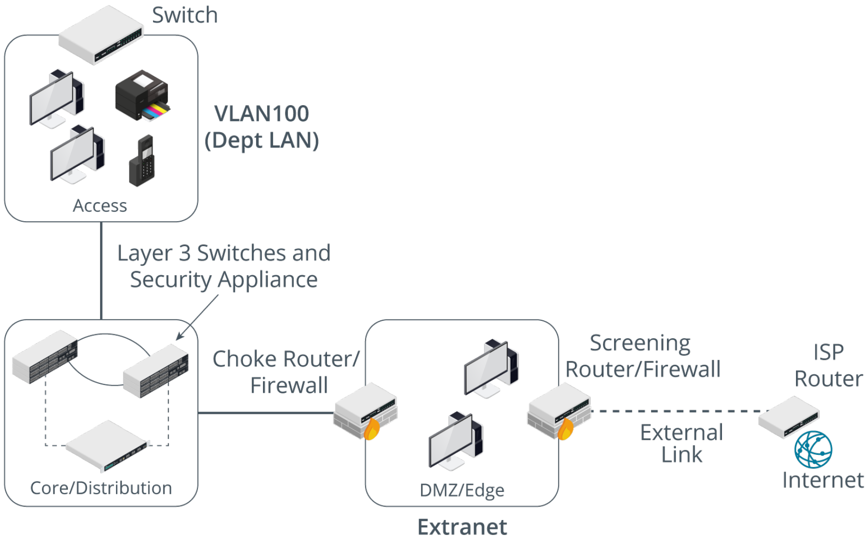


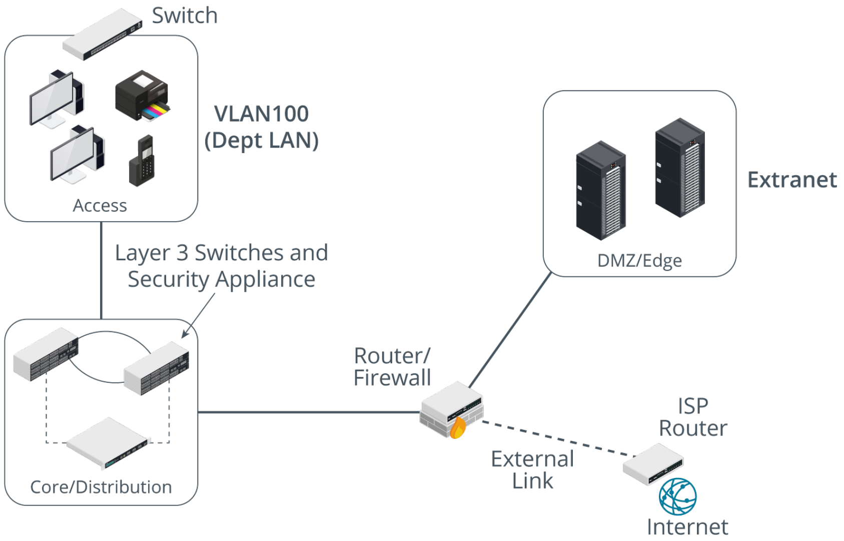
Images © 123rf.com.

Demilitarized Zones

- Demilitarized zones (DMZs) isolate hosts that are Internet-facing
- Communications through the DMZ should not be allowed
- Ideally use proxies to rebuild packets for forwarding
- Bastion hosts
  - Not fully trusted by internal network
  - Run minimal services
  - Do not store local network account credentials
- Using different types of DMZ for different functions

Demilitarized Zone Topologies

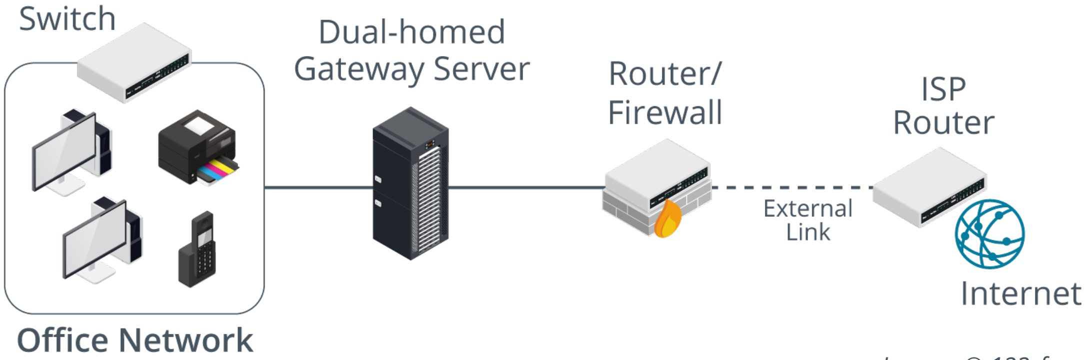




Images © 123rf.com.

Screened Host

- Screened host
  - Local network screened by a single firewall
- “SOHO DMZ”
  - SOHO router configuration option
  - Host configured to accept connections from the Internet



Images © 123rf.com.

Implications of IPv6

- Enabled by default configuration issues
  - Risks of unmanaged configurations
  - IPv6-specific attack vectors
- Map IPv6 address space to appropriate security zones
- Configure IPv6 firewall rules
- Typically no need for address translation

Other Secure Network Design Considerations

- Data center and cloud design requirements
- East-west traffic
  - North-south traffic enters and leaves data center
  - East-west traffic is between servers within the data center
  - Problem for security inspection and filtering
- Zero trust
  - Do not rely on perimeter security
  - Continuous/context-based authentication
  - Microsegmentation
    - Single host zones

Topic 9B

Implement Secure Switching and Routing

Syllabus Objectives Covered

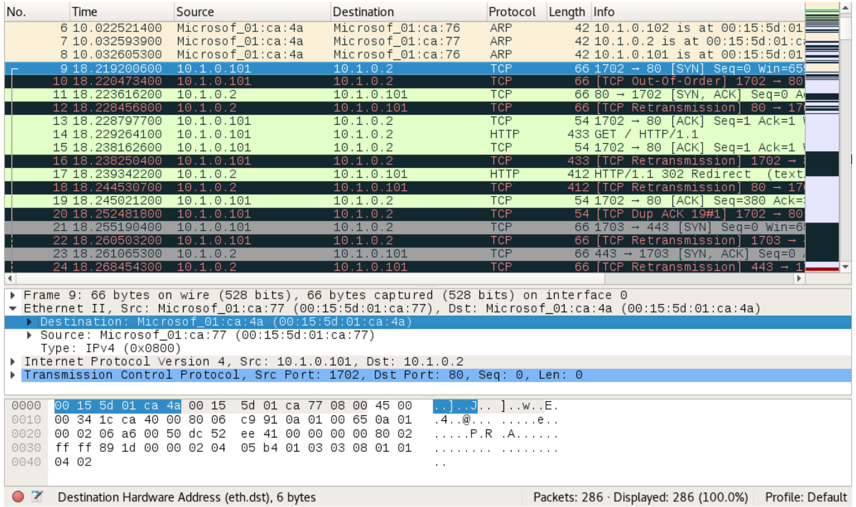
- 1.4 Given a scenario, analyze potential indicators associated with network attacks
- 3.1 Given a scenario, implement secure protocols
    - Routing and switching only
- 3.3 Given a scenario, implement secure network designs

Man-in-the-Middle and Layer 2 Attacks

- Man-in-the-Middle (MitM) attacks
  - Threat actor can intercept and modify communications
  - On-path attack
  - Snooping
  - Spoofing
- MAC address cloning/spoofing
  - Media Access Control (MAC) hardware interface address
  - Easy to change for a different value

ARP Poisoning and MAC Flooding Attacks

- Address Resolution Protocol (ARP) poisoning
    - Broadcasting unsolicited ARP replies to poison the cache of local hosts with spoofed MAC address
    - Attacker usually tries to masquerade as default gateway
- MAC flooding
    - Overwhelm switch memory to trigger unicast flooding
    - Facilitates sniffing



No.	Time	Source	Destination	Protocol	Length	Info
6	10.022521400	Microsof_01:ca:4a	Microsof_01:ca:76	ARP	42	10.1.0.102 is at 00:15:5d:01
7	10.032593900	Microsof_01:ca:4a	Microsof_01:ca:77	ARP	42	10.1.0.2 is at 00:15:5d:01:c
8	10.032605300	Microsof_01:ca:4a	Microsof_01:ca:76	ARP	42	10.1.0.101 is at 00:15:5d:01
9	18.219200600	10.1.0.101	10.1.0.2	TCP	66	1702 → 80 [SYN] Seq=0 Win=65
10	18.220473400	10.1.0.101	10.1.0.2	TCP	66	[TCP Out-Of-Order] 1702 → 80
11	18.223616200	10.1.0.2	10.1.0.101	TCP	66	80 → 1702 [SYN, ACK] Seq=0 A
12	18.228456800	10.1.0.2	10.1.0.101	TCP	66	[TCP Retransmission] 80 → 17
13	18.228797700	10.1.0.101	10.1.0.2	TCP	54	1702 → 80 [ACK] Seq=1 Ack=1
14	18.229264100	10.1.0.101	10.1.0.2	HTTP	433	GET / HTTP/1.1
15	18.238162600	10.1.0.101	10.1.0.2	TCP	54	1702 → 80 [ACK] Seq=1 Ack=1
16	18.238250400	10.1.0.101	10.1.0.2	TCP	433	[TCP Retransmission] 1702 →
17	18.239342200	10.1.0.2	10.1.0.101	HTTP	412	HTTP/1.1 302 Redirect (text
18	18.244530700	10.1.0.2	10.1.0.101	TCP	412	[TCP Retransmission] 80 → 17
19	18.245021200	10.1.0.101	10.1.0.2	TCP	54	1702 → 80 [ACK] Seq=380 Ack=
20	18.252481800	10.1.0.101	10.1.0.2	TCP	54	[TCP Dup ACK 19#1] 1702 → 80
21	18.255190400	10.1.0.101	10.1.0.2	TCP	66	1703 → 443 [SYN] Seq=0 Win=6
22	18.260503200	10.1.0.101	10.1.0.2	TCP	66	[TCP Retransmission] 1703 →
23	18.261065300	10.1.0.2	10.1.0.101	TCP	66	443 → 1703 [SYN, ACK] Seq=0
24	18.268454300	10.1.0.2	10.1.0.101	TCP	66	[TCP Retransmission] 443 → 1

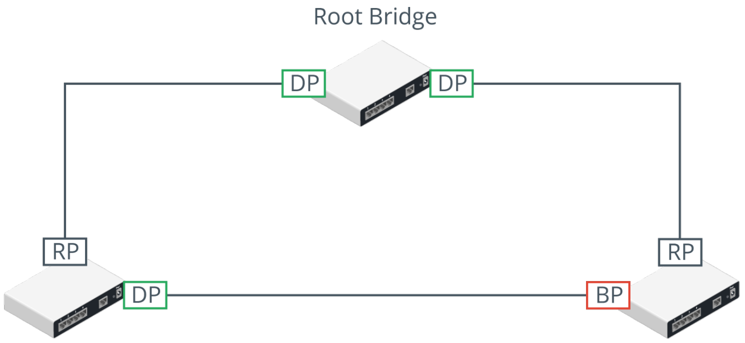
```
▸ Frame 9: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
▾ Ethernet II, Src: Microsof_01:ca:77 (00:15:5d:01:ca:77), Dst: Microsof_01:ca:4a (00:15:5d:01:ca:4a)
   ▸ Destination: Microsof_01:ca:4a (00:15:5d:01:ca:4a)
   ▸ Source: Microsof_01:ca:77 (00:15:5d:01:ca:77)
     Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 10.1.0.101, Dst: 10.1.0.2
▸ Transmission Control Protocol, Src Port: 1702, Dst Port: 80, Seq: 0, Len: 0
```

```
0000  00 15 5d 01 ca 4a 00 15  5d 01 ca 77 08 00 45 00   ..]..J.. ]..w..E.
0010  00 34 1c ca 40 00 80 06  c9 91 0a 01 00 65 0a 01   .4..@... .....e..
0020  00 02 06 a6 00 50 dc 52  ee 41 00 00 00 00 80 02   .....P.R .A......
0030  ff ff 89 1d 00 00 02 04  05 b4 01 03 03 08 01 01   ........ ........
0040  04 02                                              ..
```

Destination Hardware Address (eth.dst), 6 bytes   Packets: 286 · Displayed: 286 (100.0%)   Profile: Default

Screenshot used with permission from wireshark.org.

Loop Prevention

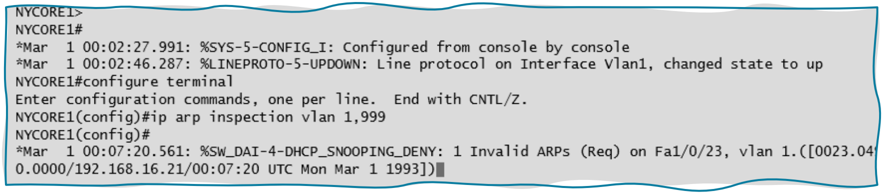


Images © 123RF.com.

- Spanning Tree Protocol (STP)
- Broadcast storm prevention
  - Broadcast and flooded unicast getting amplified as it loops continually around network
  - Storm control if STP has failed
- Bridge Protocol Data Unit (BPDU) guard
  - Configure switches to defeat attempts to engineer a loop
  - Portfast setting configured for access ports
  - BPDU guard disables port if STP traffic is detected

Physical Port Security and MAC Filtering

- Physical port security
  - Secure switch hardware
  - Physically disconnect unused ports
  - Disable unused ports via management interface
- MAC address limiting and filtering
  - Configure permitted MACs
  - Limit number of MAC changes
- DHCP snooping
  - Dynamic ARP inspection

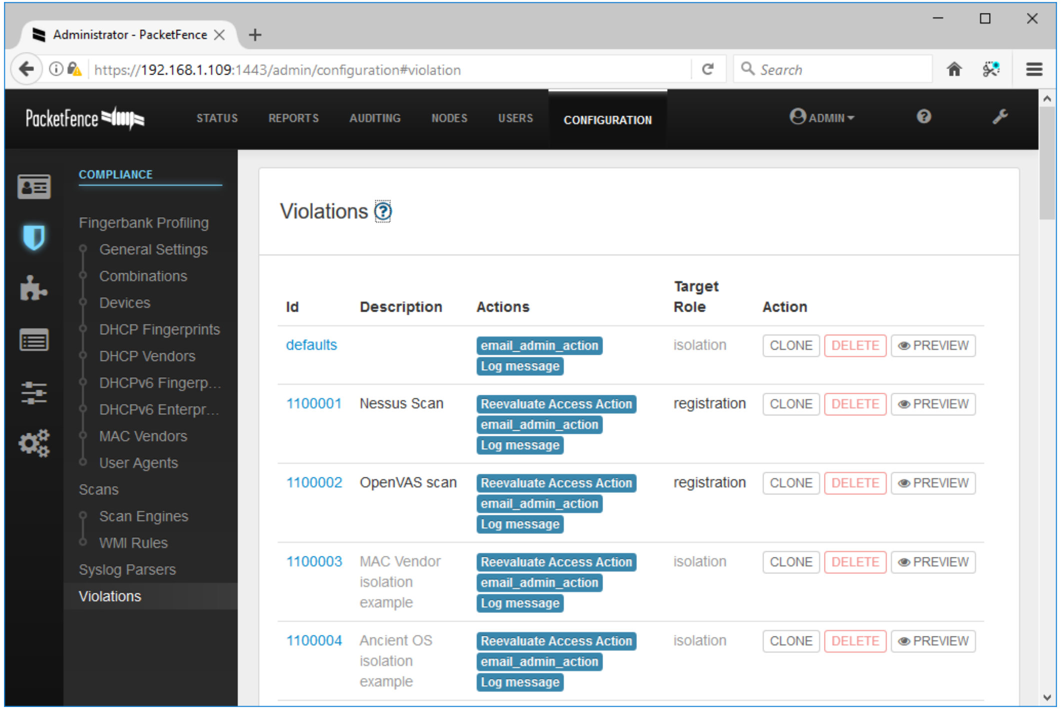


```
NYCORE1>
NYCORE1#
*Mar  1 00:02:27.991: %SYS-5-CONFIG_I: Configured from console by console
*Mar  1 00:02:46.287: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
NYCORE1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
NYCORE1(config)#ip arp inspection vlan 1,999
NYCORE1(config)#
*Mar  1 00:07:20.561: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa1/0/23, vlan 1.([0023.04
0.0000/192.168.16.21/00:07:20 UTC Mon Mar 1 1993])
```

Network Access Control

- Endpoint security/defense in depth
- IEEE 802.1X/port-based network access control (PNAC)
- Can also enforce health policy
- Posture assessment
  - Agent-based
    - Persistent versus non-persistent
  - Agentless
    - Scanning software
    - Device polling

Screenshot used with permission from packetfence.org.

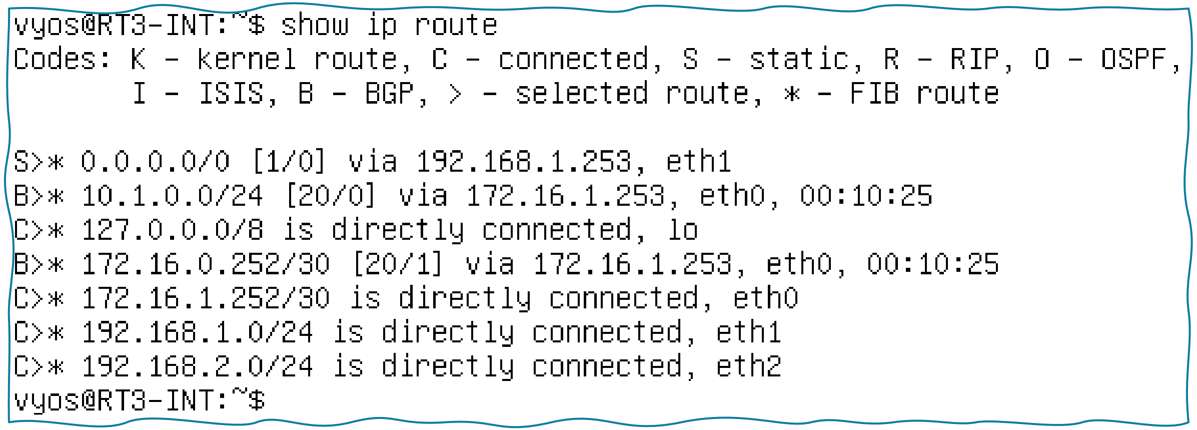


Violations

Id	Description	Actions	Target Role	Action
defaults		email_admin_action Log message	isolation	CLONE DELETE PREVIEW
1100001	Nessus Scan	Reevaluate Access Action email_admin_action Log message	registration	CLONE DELETE PREVIEW
1100002	OpenVAS scan	Reevaluate Access Action email_admin_action Log message	registration	CLONE DELETE PREVIEW
1100003	MAC Vendor isolation example	Reevaluate Access Action email_admin_action Log message	isolation	CLONE DELETE PREVIEW
1100004	Ancient OS isolation example	Reevaluate Access Action email_admin_action Log message	isolation	CLONE DELETE PREVIEW

Route Security

- Sources of routing table updates
- Preventing route injection
- Source routing
- Patch management and router appliance hardening



```
vyos@RT3-INT:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

S>* 0.0.0.0/0 [1/0] via 192.168.1.253, eth1
B>* 10.1.0.0/24 [20/0] via 172.16.1.253, eth0, 00:10:25
C>* 127.0.0.0/8 is directly connected, lo
B>* 172.16.0.252/30 [20/1] via 172.16.1.253, eth0, 00:10:25
C>* 172.16.1.252/30 is directly connected, eth0
C>* 192.168.1.0/24 is directly connected, eth1
C>* 192.168.2.0/24 is directly connected, eth2
vyos@RT3-INT:~$
```

Lesson 9C

Implement Secure Wireless Infrastructure

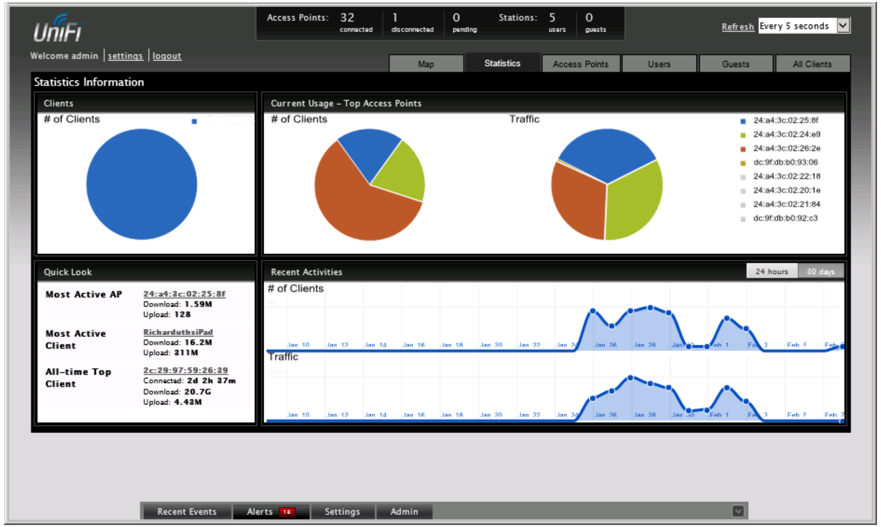
Syllabus Objectives Covered

- 1.4 Given a scenario, analyze potential indicators associated with network attacks
- 3.4 Given a scenario, install and configure wireless security settings

Wireless Network Installation Considerations

- Ensure maximum availability from legitimate access points
- Wireless access point (WAP) placement
  - Service set identifier (SSID) and basic service set identifier (BSSID)
  - Frequency bands and channels
  - Co-channel interference (CCI)
  - Adjacent channel interference (ACI)
- Site surveys and heat maps
  - Architectural plan
  - Wi-Fi analyzer
  - Heat map plots signal strength from high (red) to low (green/blue)
  - Channel layout shows overlapping usage

Controller and Access Point Security



Access Points: 32 connected | 1 disconnected | 0 pending

Stations: 5 users | 0 guests

Refresh: Every 5 seconds

Most Active AP: 24:a4:3c:02:25:8f
Download: 1.59M
Upload: 128

Most Active Client: RicharduthsiPad
Download: 16.2M
Upload: 311M

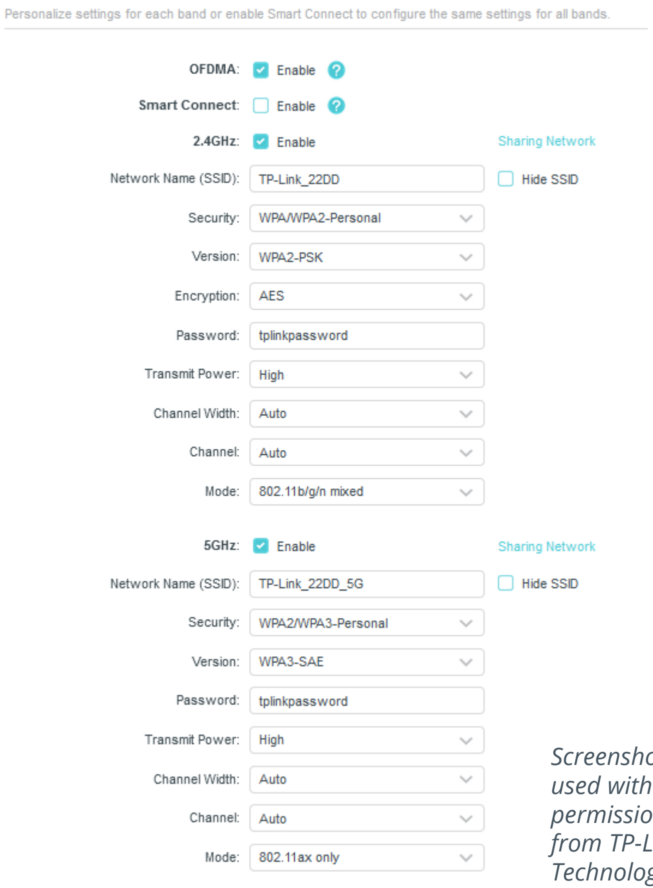
All-time Top Client: 2c:29:97:59:26:39
Connected: 2d 2h 37m
Download: 20.7G
Upload: 4.43M

Screenshot used with permission from Ubiquiti Networks.

- Configuration of multi-WAP WLANs
- Hardware and software controllers
- Fat versus thin WAPs
- Physical security and management interfaces

Wi-Fi Protected Access

- WPA (v1)
  - RC4 with Temporal Key Integrity Protocol (TKIP)
- Wi-Fi protected access 2 (WPA2)
  - Advanced Encryption Standard (AES) replaces RC4
  - Counter Mode with Cipher Block Chaining Message Authentication Code (CBC-MAC) Protocol (CCMP) replaces TKIP
  - Also enables enterprise authentication options
- Wi-Fi protected access 3 (WPA3)
  - Simultaneous Authentication of Equals (SAE)
  - Enhanced Open
  - Updated cryptography
  - Management protection frames



Personalize settings for each band or enable Smart Connect to configure the same settings for all bands.

OFDMA: ☑ Enable

Smart Connect: ☐ Enable

2.4GHz: ☑ Enable   Sharing Network

Network Name (SSID): TP-Link_22DD   ☐ Hide SSID

Security: WPA/WPA2-Personal

Version: WPA2-PSK

Encryption: AES

Password: tplinkpassword

Transmit Power: High

Channel Width: Auto

Channel: Auto

Mode: 802.11b/g/n mixed

5GHz: ☑ Enable   Sharing Network

Network Name (SSID): TP-Link_22DD_5G   ☐ Hide SSID

Security: WPA2/WPA3-Personal

Version: WPA3-SAE

Password: tplinkpassword

Transmit Power: High

Channel Width: Auto

Channel: Auto

Mode: 802.11ax only

Screenshot used with permission from TP-Link Technologies.

Wi-Fi Authentication Methods

- WPA2 pre-shared key authentication
  - Passphrase used to generate a pairwise master key (PMK)
  - 4-way handshake
  - PMK is used to derive session keys
- WPA3 personal authentication
  - Password Authenticated Key Exchange (PAKE)
  - Simultaneous Authentication of Equals (SAE) protocol replaces the 4-way handshake
  - Dragonfly handshake

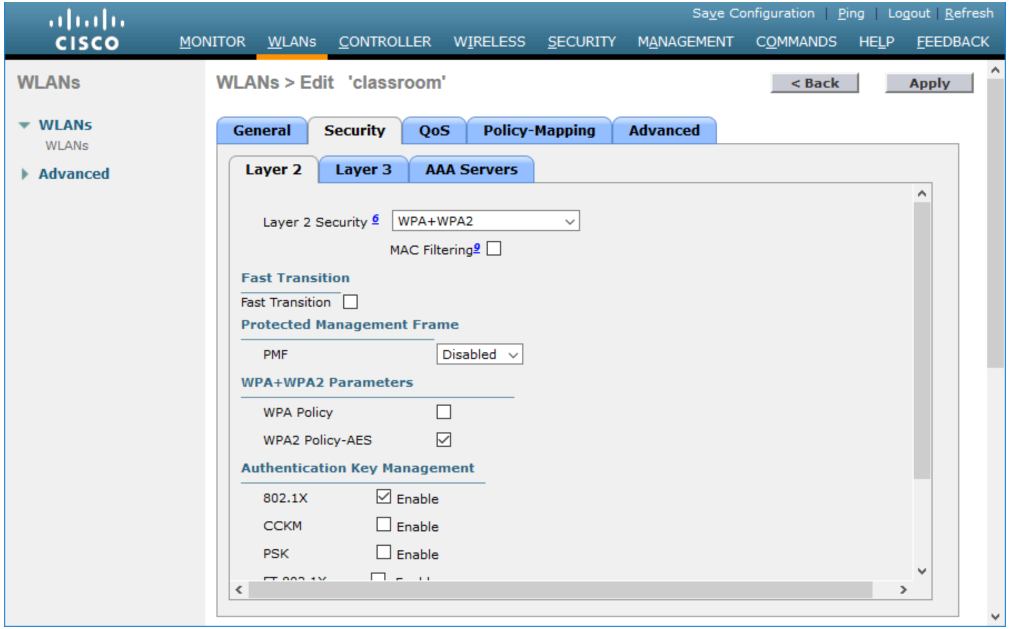
Wi-Fi Protected Setup (WPS)

- Pushbutton or passcode autoconfiguration of access points and clients
- Brute-force vulnerability in passcode algorithm
- Access point may support lockout to mitigate
- Make sure access point firmware is up-to-date
- EasyConnect and Device Provisioning Protocol (DPP)

Open Authentication and Captive Portals

- Use an access point without authentication (or encryption)
- Secondary authentication via captive portal or splash page
- Everything sent over link can be snooped
- Use secure protocols for confidential data (HTTPS, Secure IMAP, FTPS)
- Use a Virtual Private Network (VPN) to create a secure tunnel
- Wi-Fi Enhanced Open

Enterprise/IEEE 802.1X Authentication



WLANs > Edit 'classroom'

Layer 2 Security [6] WPA+WPA2

MAC Filtering[9] ☐

Fast Transition

Fast Transition ☐

Protected Management Frame

PMF Disabled

WPA+WPA2 Parameters

WPA Policy ☐

WPA2 Policy-AES ☑

Authentication Key Management

802.1X ☑ Enable

CCKM ☐ Enable

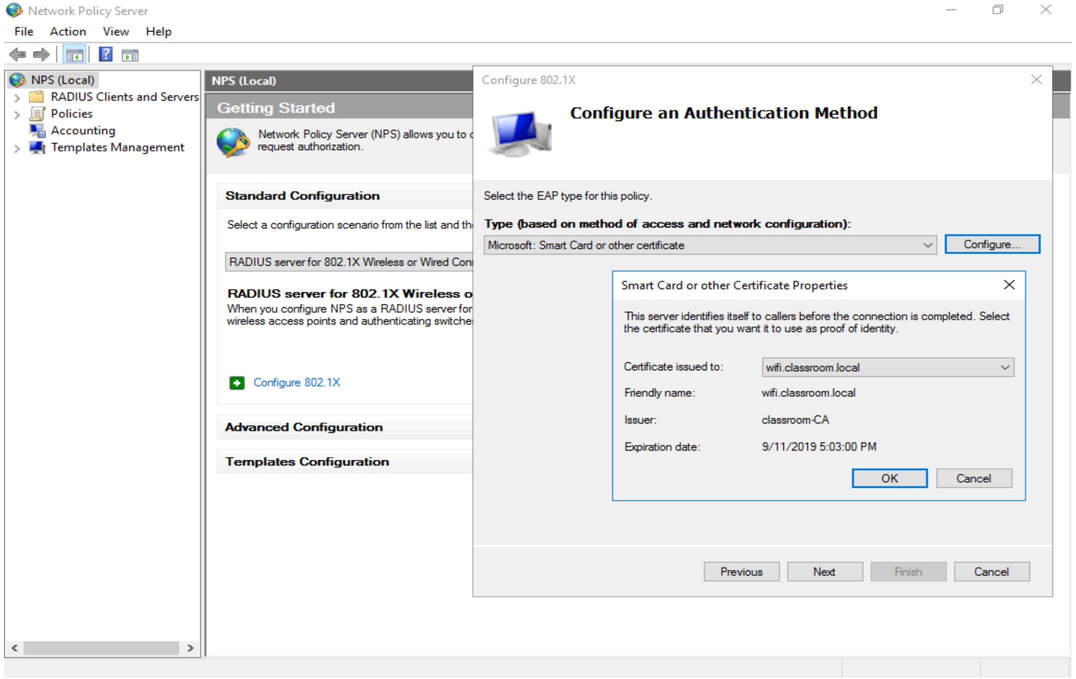
PSK ☐ Enable

Screenshot used with permission from Cisco.

- Extensible Authentication Protocol (EAP) over Wireless (EAPoW)
- Network directory authorization via RADIUS or TACACS+
- User credential is used to generate session encryption key

Extensible Authentication Protocol

- Designed to provide for interoperable security devices and software
- EAP-TLS
  - Transport Layer Security (TLS) to authenticate via device certificates/smart cards
  - Both server and supplicant must have certificates
  - Mutual authentication



Network Policy Server (NPS) allows you to c
request authorization.

Standard Configuration

Select a configuration scenario from the list and th

RADIUS server for 802.1X Wireless or Wired Con

RADIUS server for 802.1X Wireless o

When you configure NPS as a RADIUS server for
wireless access points and authenticating switche

Configure 802.1X

Advanced Configuration

Templates Configuration

Configure 802.1X

Configure an Authentication Method

Select the EAP type for this policy.

Type (based on method of access and network configuration):

Microsoft: Smart Card or other certificate

Configure...

Smart Card or other Certificate Properties

This server identifies itself to callers before the connection is completed. Select the certificate that you want it to use as proof of identity.

Certificate issued to: wifi.classroom.local

Friendly name: wifi.classroom.local

Issuer: classroom-CA

Expiration date: 9/11/2019 5:03:00 PM

Screenshot used with permission from Microsoft.

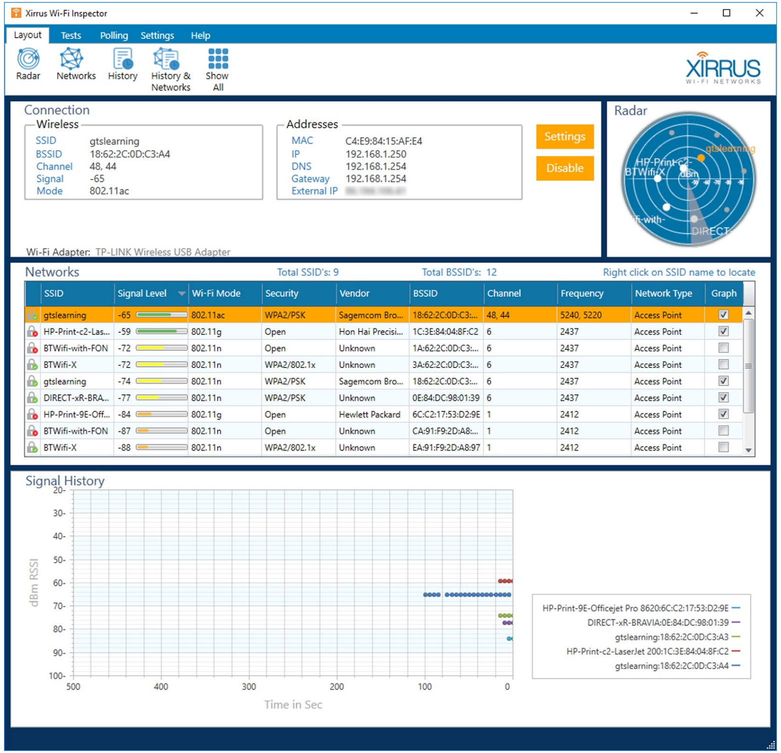
PEAP, EAP-TTLS, and EAP-FAST

- Secure tunneling for user credentials
- Protected EAP (PEAP)
  - Password authentication through a TLS-protected tunnel
  - Server certificate only
  - PEAPv0 (EAP-MSCHAPv2)
  - PEAPv1 (EAP-GTC)
- EAP with Tunneled TLS (EAP-TTLS)
  - Similar to PEAP but with more flexibility on inner authentication method
- EAP with Flexible Authentication via Secure Tunneling (EAP-FAST)
  - Cisco alternative to PEAP that can be set up without certificate infrastructure

RADIUS Federation

- Federated identity solution
- Mesh network for RADIUS servers operated by different institutions
- Eduroam

Rogue Access Points and Evil Twins



Connection

Wireless

SSID gtslearning
BSSID 18:62:2C:0D:C3:A4
Channel 48, 44
Signal -65
Mode 802.11ac

Addresses

MAC C4:E9:84:15:AF:E4
IP 192.168.1.250
DNS 192.168.1.254
Gateway 192.168.1.254
External IP [redacted]

Wi-Fi Adapter: TP-LINK Wireless USB Adapter

Networks   Total SSID's: 9   Total BSSID's: 12   Right click on SSID name to locate

SSID	Signal Level	Wi-Fi Mode	Security	Vendor	BSSID	Channel	Frequency	Network Type	Graph
gtslearning	-65	802.11ac	WPA2/PSK	Sagemcom Bro...	18:62:2C:0D:C3:...	48, 44	5240, 5220	Access Point	☑
HP-Print-c2-Las...	-59	802.11g	Open	Hon Hai Precisi...	1C:3E:84:04:8F:C2	6	2437	Access Point	☑
BTWifi-with-FON	-72	802.11n	Open	Unknown	1A:62:2C:0D:C3:...	6	2437	Access Point	☐
BTWifi-X	-72	802.11n	WPA2/802.1x	Unknown	3A:62:2C:0D:C3:...	6	2437	Access Point	☐
gtslearning	-74	802.11n	WPA2/PSK	Sagemcom Bro...	18:62:2C:0D:C3:...	6	2437	Access Point	☑
DIRECT-xR-BRA...	-77	802.11n	WPA2/PSK	Unknown	0E:84:DC:98:01:39	6	2437	Access Point	☑
HP-Print-9E-Off...	-84	802.11g	Open	Hewlett Packard	6C:C2:17:53:D2:9E	1	2412	Access Point	☑
BTWifi-with-FON	-87	802.11n	Open	Unknown	CA:91:F9:2D:A8:...	1	2412	Access Point	☐
BTWifi-X	-88	802.11n	WPA2/802.1x	Unknown	EA:91:F9:2D:A8:97	1	2412	Access Point	☐

Signal History

20-
30-
40-
50-
60-
70-
80-
90-
100-
dBm RSSI
500
400
300
200
100
0
Time in Sec
HP-Print-9E-Officejet Pro 8620:6C:C2:17:53:D2:9E
DIRECT-xR-BRAVIA:0E:84:DC:98:01:39
gtslearning:18:62:2C:0D:C3:A3
HP-Print-c2-LaserJet 200:1C:3E:84:04:8F:C2
gtslearning:18:62:2C:0D:C3:A4

Screenshot used with permission from Xirrus.

- Rogue access point
  - Troubleshooting access point misconfiguration
  - Disable unused devices and interfaces
- Evil twin
  - Masquerade as legitimate AP
  - Use similar SSID
  - Capture authentication information
- Wi-Fi analyzers

Disassociation and Replay Attacks

- Deauthentication attack
  - Attacker sends spoofed deauth packet
  - DoS and assists other attacks
- Disassociation attack
  - Similar but just causes station to disassociate
- Configure Management Frame Protection (MFP/802.11w)
- Initialization vector (IV) attack
  - Generate packets to strip IV
  - KRACK/key reinstallation

Jamming Attacks

- Environmental versus malicious interference
- Jamming attacks
  - Denial of service
  - Promote evil twin
- Use spectrum analyzer to locate source

| |

Topic 9D

Implement Load Balancers

Syllabus Objectives Covered

- 1.4 Given a scenario, analyze potential indicators associated with network attacks
- 3.3 Given a scenario, implement secure network designs

Distributed Denial of Service (DDoS)

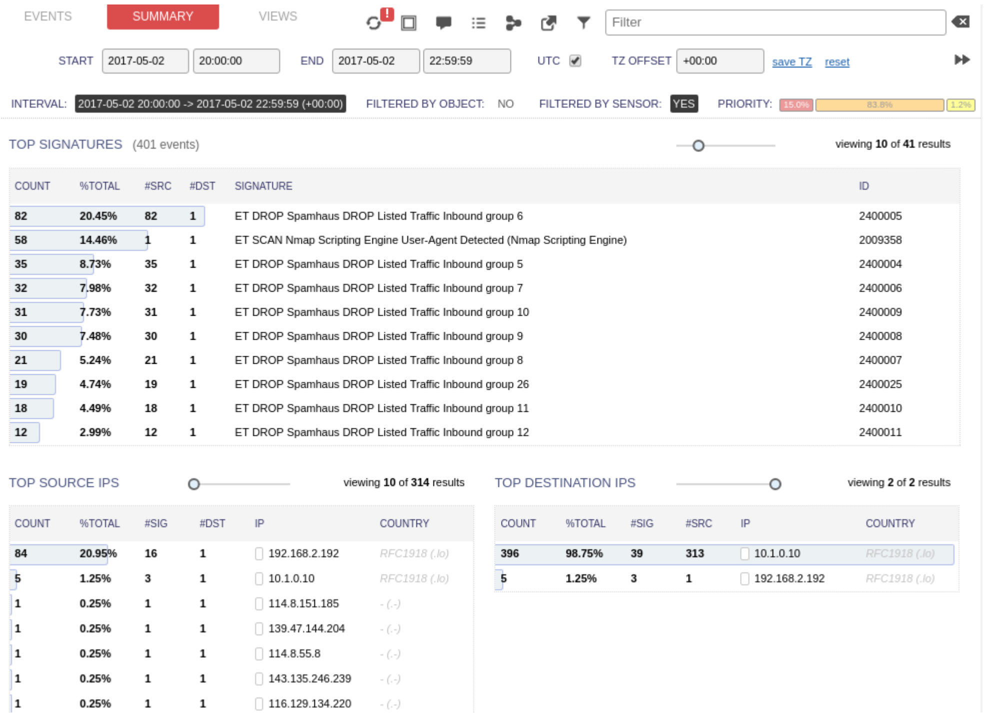
- Leverage bandwidth from compromised hosts/networks
  - Handlers form a command and control (C&C) network
  - Compromised hosts installed with bots that can run automated scripts
  - Co-ordinated by the C&C network as a botnet
- Overwhelm with superior bandwidth (number of bots)
- Consume resources with spoof session requests (SYN flood)

Amplification, Application, and OT Attacks

- Distributed Reflection DoS (DRDoS)
- Amplified SYN flood
  - Spoof victim's IP address and attempt to open connections with multiple servers
  - Those servers direct their SYN/ACK responses to the victim
- Application attacks
  - Bogus DNS/NTP queries
  - Direct responses at victim
  - Queries can be constructed to generate large response packets
- Operational technology (OT) networks
  - DoS against embedded systems
  - Can be more vulnerable to miscrafted packets than computing hosts

Distributed Denial of Service Attack Mitigation

- Attacks use spoofed addresses, making them hard to block
- Drop traffic to protect other hosts in the routing domain
    - Access control list (ACL)
    - remotely triggered blackhole (RTBH)
    - Sinkhole routing
- Cloud DDoS mitigation services



START 2017-05-02 20:00:00 END 2017-05-02 22:59:59 UTC ☑ TZ OFFSET +00:00 save TZ reset

INTERVAL: 2017-05-02 20:00:00 -> 2017-05-02 22:59:59 (+00:00) FILTERED BY OBJECT: NO FILTERED BY SENSOR: YES PRIORITY: 15.0% 83.8% 1.2%

TOP SIGNATURES (401 events) viewing **10** of **41** results

COUNT	%TOTAL	#SRC	#DST	SIGNATURE	ID
82	20.45%	82	1	ET DROP Spamhaus DROP Listed Traffic Inbound group 6	2400005
58	14.46%	1	1	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	2009358
35	8.73%	35	1	ET DROP Spamhaus DROP Listed Traffic Inbound group 5	2400004
32	7.98%	32	1	ET DROP Spamhaus DROP Listed Traffic Inbound group 7	2400006
31	7.73%	31	1	ET DROP Spamhaus DROP Listed Traffic Inbound group 10	2400009
30	7.48%	30	1	ET DROP Spamhaus DROP Listed Traffic Inbound group 9	2400008
21	5.24%	21	1	ET DROP Spamhaus DROP Listed Traffic Inbound group 8	2400007
19	4.74%	19	1	ET DROP Spamhaus DROP Listed Traffic Inbound group 26	2400025
18	4.49%	18	1	ET DROP Spamhaus DROP Listed Traffic Inbound group 11	2400010
12	2.99%	12	1	ET DROP Spamhaus DROP Listed Traffic Inbound group 12	2400011

TOP SOURCE IPS viewing **10** of **314** results

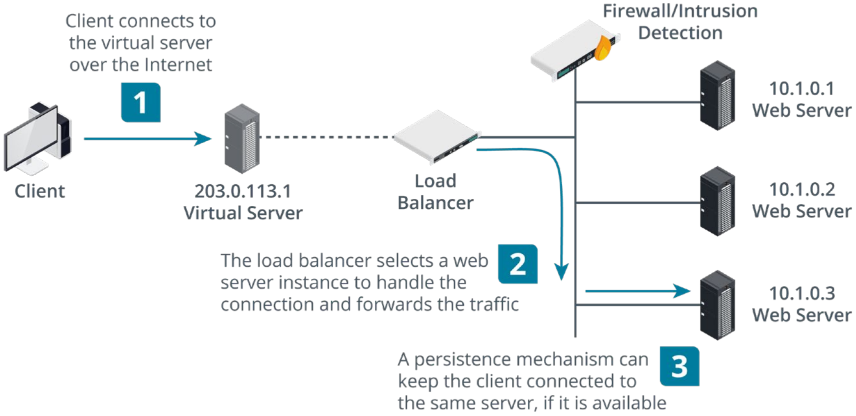
COUNT	%TOTAL	#SIG	#DST	IP	COUNTRY
84	20.95%	16	1	□ 192.168.2.192	RFC1918 (.lo)
5	1.25%	3	1	□ 10.1.0.10	RFC1918 (.lo)
1	0.25%	1	1	□ 114.8.151.185	- (.-)
1	0.25%	1	1	□ 139.47.144.204	- (.-)
1	0.25%	1	1	□ 114.8.55.8	- (.-)
1	0.25%	1	1	□ 143.135.246.239	- (.-)
1	0.25%	1	1	□ 116.129.134.220	- (.-)

TOP DESTINATION IPS viewing **2** of **2** results

COUNT	%TOTAL	#SIG	#SRC	IP	COUNTRY
396	98.75%	39	313	□ 10.1.0.10	RFC1918 (.lo)
5	1.25%	3	1	□ 192.168.2.192	RFC1918 (.lo)

Screenshot used with permission from Security Onion.

Load Balancing

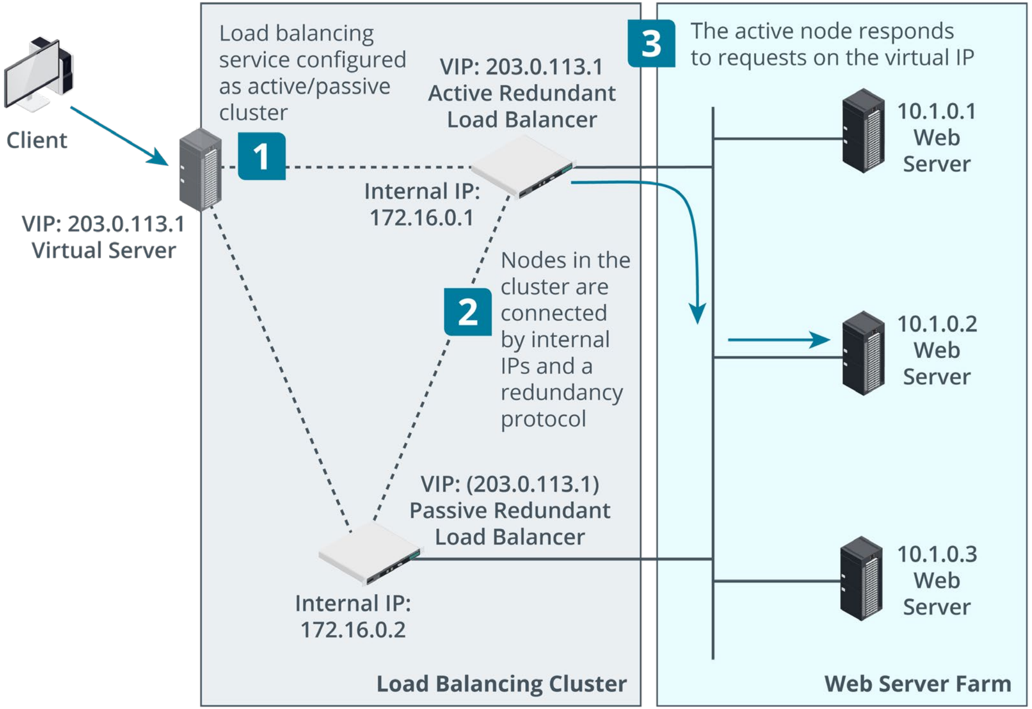

Client connects to the virtual server over the Internet
1
Client
203.0.113.1 Virtual Server
Load Balancer
Firewall/Intrusion Detection
10.1.0.1 Web Server
10.1.0.2 Web Server
10.1.0.3 Web Server
2
The load balancer selects a web server instance to handle the connection and forwards the traffic
3
A persistence mechanism can keep the client connected to the same server, if it is available

Images © 123rf.com.

- Distributes requests across farm or pool of servers (nodes)
  - Layer 4 load balancer
  - Layer 7 load balancer (content switch)
- Scheduling
  - Round robin
  - Fewest existing connections / best response time
  - Weighting
  - Heartbeat and health checks
- Source IP affinity
- Session persistence

Clustering

- Configure nodes for failover
- Virtual IP
  - Common Address Redundancy Protocol (CARP)
- Active/passive versus active/active
- Application clustering
  - Provides stateful fault tolerance


Client
VIP: 203.0.113.1
Virtual Server
1
Load balancing service configured as active/passive cluster
VIP: 203.0.113.1
Active Redundant Load Balancer
Internal IP: 172.16.0.1
2
Nodes in the cluster are connected by internal IPs and a redundancy protocol
VIP: (203.0.113.1)
Passive Redundant Load Balancer
Internal IP: 172.16.0.2
Load Balancing Cluster
3
The active node responds to requests on the virtual IP
10.1.0.1
Web Server
10.1.0.2
Web Server
10.1.0.3
Web Server
Web Server Farm

Images © 123RF.com.

Quality of Service

- Compared to best effort and first in, first out (FIFO)
- Quality of service (QoS) to prioritize traffic with certain characteristics
  - Bandwidth
  - Latency and jitter
- Traffic marking
  - DiffServ and 802.1p
- Traffic policing
- Denial of service and trust boundaries for traffic marking
  - Ensure bandwidth for management and security monitoring traffic

Lesson 9

Summary