09- Implementing Secure Network Designs

Ahmed Sultan
Senior Technical Instructor
ahmedsultan.me/about

Outlines

9.1- Implement Secure Network Designs

9.2- Implement Secure Switching and Routing

9.3- Implement Secure Wireless Infrastructure

9.4- Implement Load Balancers

Labs

Lab 13: Implementing a Secure Network Design

9.1- Implement Secure Network Designs

9.2- Implement Secure Switching and Routing

9.3- Implement Secure Wireless Infrastructure

9.4- Implement Load Balancers

SECURE NETWORK DESIGNS

- A secure network design provisions the assets and services.
- Weaknesses in the network architecture make it more susceptible to undetected intrusions or to catastrophic service failures.
- Typical weaknesses include:
  - ✓ Single points of failure—a "pinch point" relying on a single hardware server or appliance or network channel.
  - ✓ Lack of documentation and change control—network segments, appliances, and services might be added without proper change control procedures, leading to a lack of visibility into how the network is constituted.
  - ✓ Overdependence on perimeter security—if the network architecture is "**flat**" (that is, if any host can contact any other host), penetrating the network edge gives the attacker freedom of movement.

NETWORK APPLIANCES

- A number of network appliances are involved in provisioning a network architecture:

  ✓ Switches—forward frames between nodes in a cabled network, Switches work at **layer 2** of the OSI model and make forwarding decisions based on the hardware or Media Access Control (MAC) address of attached nodes, Switches can establish network segments that either map directly to the underlying cabling or to logical segments, created in the switch configuration as virtual LANs (**VLANs**).

  ✓ Wireless access points—provide a bridge between a cabled network and wireless clients, or stations, Access points work at **layer 2** of the OSI model.

NETWORK APPLIANCES (cont.)

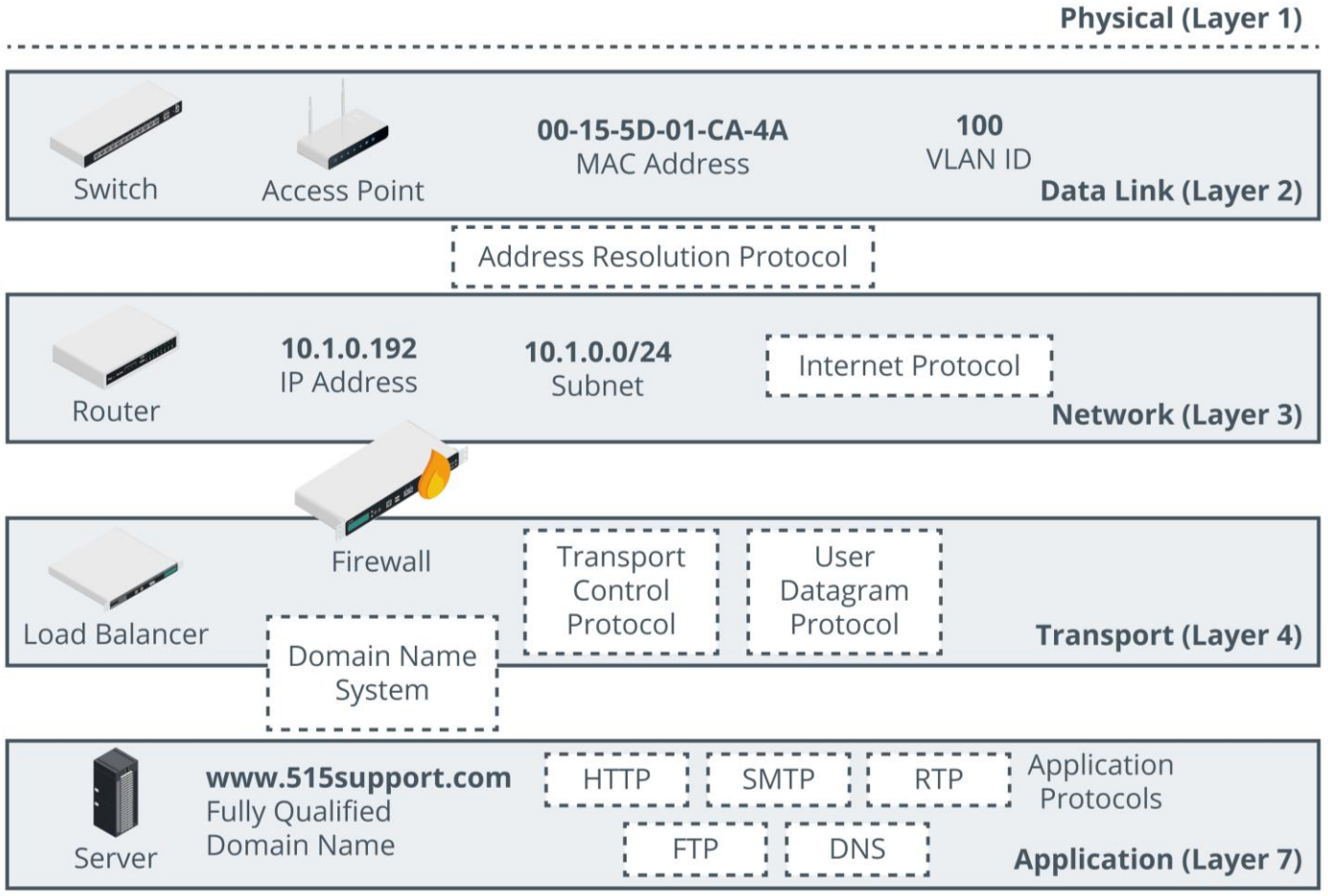
- A number of network appliances are involved in provisioning a network architecture (cont.)

  - ✓ Routers— forward packets around an internetwork, making forwarding decisions based on IP addresses, Routers work at layer 3 of the OSI model, Routers can apply logical IP subnet addresses to segments within a network.

  - ✓ Firewalls— apply an access control list (ACL) to filter traffic passing in or out of a network segment, Firewalls can work at layer 3 of the OSI model or higher.

  - ✓ Load balancers—distribute traffic between network segments or servers to optimize performance, Load balancers can work at layer 4 of the OSI model or higher.

NETWORK APPLIANCES (cont.)



ROUTING AND SWITCHING PROTOCOLS

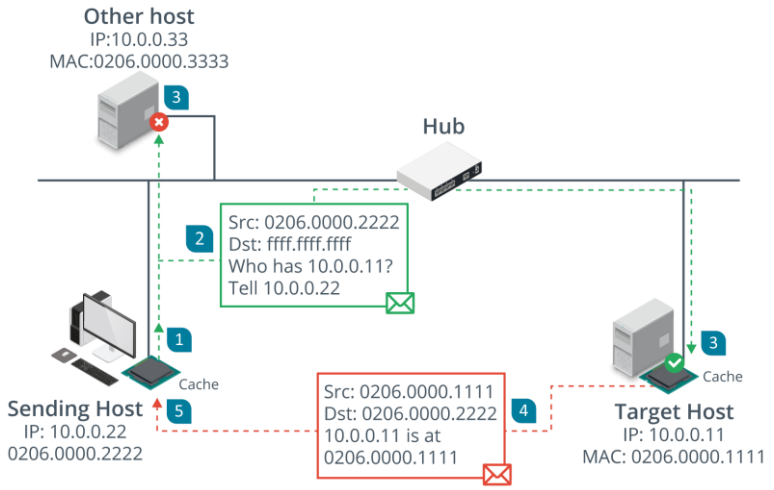
- The basic function of a network is to forward traffic from one node to another.
- A number of routing and switching protocols are used to implement forwarding.
- The forwarding function takes place at two different layers:
  - ✓ Layer 2 forwarding occurs between nodes on the same local network segment that are all in the same broadcast domain, At layer 2, a broadcast domain is either all the nodes connected to the same physical unmanaged switch, or all the nodes within a virtual LAN (VLAN) configured on one or more managed switches, At layer 2, each node is identified by the network interface's hardware or **Media Access Control (MAC) address**, A MAC address is a 48-bit value written in hexadecimal notation, such as 00-15-5D-F4-83-48.

ROUTING AND SWITCHING PROTOCOLS (cont.)

- The forwarding function takes place at two different layers (cont.)
  - ✓ Layer 3 forwarding, or routing, occurs between both logically and physically defined networks, A single network divided into multiple logical broadcast domains is said to be subnetted, Multiple networks joined by routers form an internetwork, At layer 3, nodes are identified by an Internet Protocol (IP) address.

ROUTING AND SWITCHING PROTOCOLS (cont.)

- Address Resolution Protocol (ARP)
  - ✓ The Address Resolution Protocol (ARP) maps a network interface's hardware (MAC) address to an IP address.
  - ✓ Normally a device that needs to send a packet to an IP address but does not know the receiving device's MAC address broadcasts an ARP Request packet, and the device with the matching IP responds with an ARP Reply.



ROUTING AND SWITCHING PROTOCOLS (cont.)

- Internet Protocol (IP)
  - ✓ IP provides the addressing mechanism for logical networks and subnets.
  - ✓ A **32-bit IPv4** address is written in dotted decimal notation, with either a network suffix or subnet mask to divide the address into network ID and host ID portions.
  - ✓ For example, in the IP address **172.16.1.101/16**, the /16 suffix indicates that the first half of the address (172.16.0.0) is the network ID, while the remainder uniquely identifies a host on that network.
  - ✓ This /16 suffix can also be written as a subnet mask in the form **255.255.0.0.**
  - ✓ Networks also use **128-bit IPv6** addressing.
  - ✓ IPv6 addresses are written using hex notation in the general format: **2001:db8::abc:0:def0:1234**.
  - ✓ In IPv6, the last 64-bits are fixed as the host's interface ID. The first 64-bits contain network information in a set hierarchy.

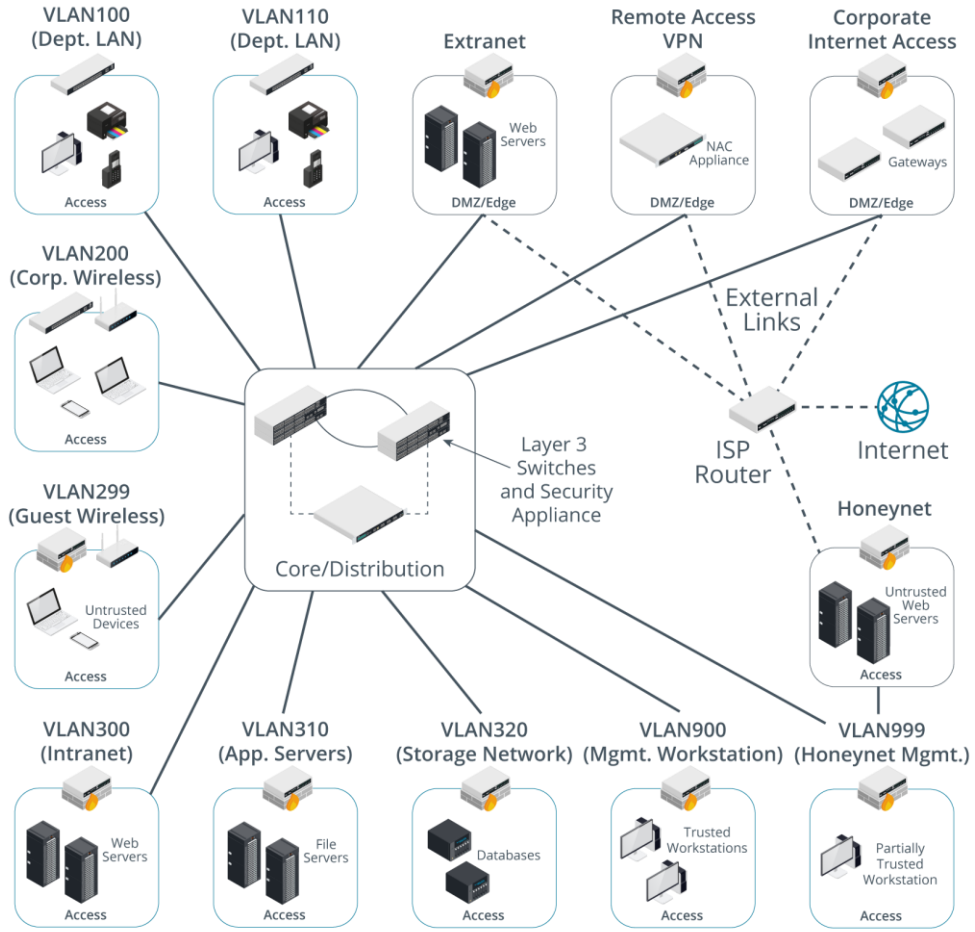
NETWORK TOPOLOGY AND ZONES

- A **topology** is a description of how a computer network is physically or logically organized.
- The logical and physical network topology should be analyzed to identify points of vulnerability and to ensure that the goals of confidentiality, integrity, and availability are met by the design.
- The main building block of a security topology is the **zone**.
- A **zone** is an area of the network where the security configuration is the same for all hosts within it.
- Traffic between zones should be strictly controlled using a security device, typically a firewall.

NETWORK TOPOLOGY AND ZONES (cont.)

- Dividing a campus network or data center into zones implies that each zone has a different security configuration.
- The main zones are as follows:
  - ✓ Intranet (private network)—this is a network of trusted hosts owned and controlled by the organization, Within the intranet, there may be sub-zones for different host groups, such as servers, employee workstations, VoIP handsets, and management workstations.
  - ✓ Extranet—this is a network of semi-trusted hosts, typically representing business partners, suppliers, or customers, Hosts must authenticate to join the extranet.
  - ✓ Internet/guest—this is a zone permitting anonymous access (or perhaps a mix of anonymous and authenticated access) by untrusted hosts over the Internet.

NETWORK TOPOLOGY AND ZONES (cont.)

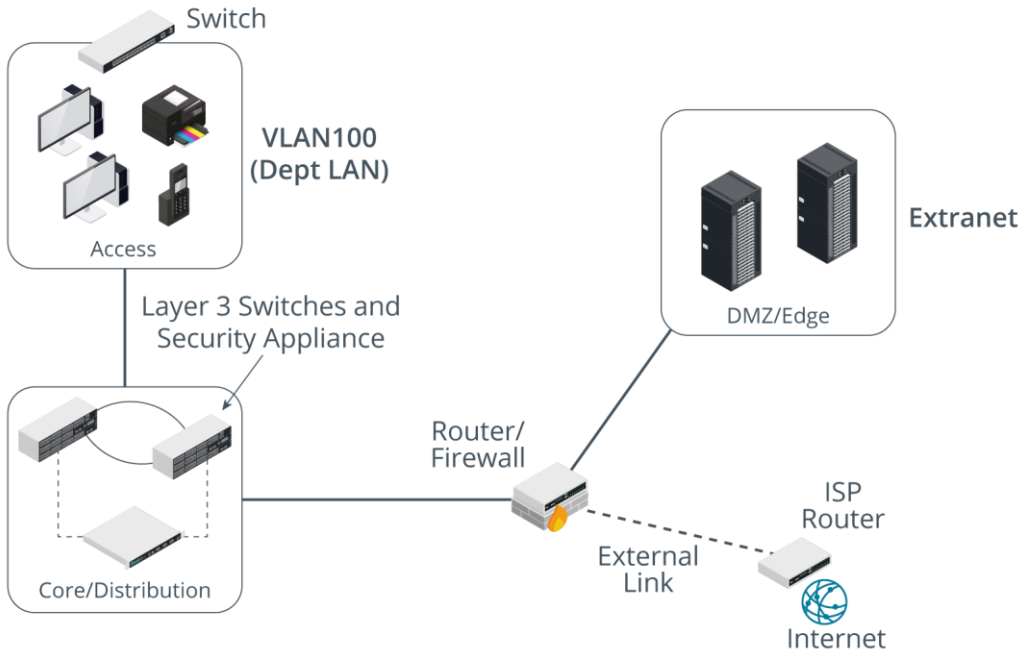


DEMILITARIZED ZONES (DMZ)

- A **DMZ** is also referred to as a perimeter or edge network.
- The basic principle of a DMZ is that traffic cannot pass directly through it.
- A **DMZ** enables external clients to access data on private systems, such as web servers, without compromising the security of the internal network as a whole.
- If communication is required between hosts on either side of a DMZ, a host within the DMZ acts as a **proxy**.
- For example, if an intranet host requests a connection with a web server on the Internet, a proxy in the DMZ takes the request and checks it.
- If the request is valid, it retransmits it to the destination.
- External hosts have no idea about what (if anything) is behind the DMZ.

DEMILITARIZED ZONES (DMZ) (cont.)

- A **DMZ** can be established using one **router/firewall** appliance with three network interfaces.
- One interface is the public one, another is the DMZ, and the third connects to the LAN.



9.1- Implement Secure Network Designs

9.2- Implement Secure Switching and Routing

9.3- Implement Secure Wireless Infrastructure

9.4- Implement Load Balancers

MAN-IN-THE-MIDDLE AND LAYER 2 ATTACKS

- Man-in-the-Middle/On-Path Attacks
  - ✓ Attackers can take advantage of the lack of security in low-level data link protocols to perform man-in-the-middle **(MitM)** attacks.
  - ✓ A **MitM** or on-path attack is where the threat actor gains a position between two hosts, and transparently captures, monitors, and relays all communication between the hosts.
  - ✓ An on-path attack could also be used to covertly modify the traffic.
  - ✓ For example, a **MitM** host could present a workstation with a spoofed website form, to try to capture the user credential.
  - ✓ Another common on-path attack spoofs responses to DNS queries, redirecting users to spoofed websites.
  - ✓ On-path attacks can be defeated using mutual authentication, where both hosts exchange secure credentials, but at layer 2 it is not always possible to put these controls in place.

MAN-IN-THE-MIDDLE AND LAYER 2 ATTACKS (cont.)

- MAC Cloning
  - ✓ **MAC cloning**, or **MAC address spoofing**, changes the hardware address configured on an adapter interface or asserts the use of an arbitrary MAC address.
  - ✓ While a unique MAC address is assigned to each network interface by the vendor at the factory, it is simple to override it in software via OS commands, alterations to the network driver configuration, or using packet crafting software.
  - ✓ This can lead to a variety of issues when investigating security incidents or when depending on MAC addresses as part of a security control, as the presented address of the device may not be reliable.

MAN-IN-THE-MIDDLE AND LAYER 2 ATTACKS (cont.)

- MAC Flooding Attacks
  - ✓ **MAC flooding** is used to attack a switch.
  - ✓ The intention of the attacker is to exhaust the memory used to store the switch's MAC address table.
  - ✓ The switch uses the MAC address table to determine which port to use to forward unicast traffic to its correct destination.
  - ✓ Overwhelming the table can cause the switch to stop trying to apply MAC-based forwarding and flood unicast traffic out of all ports, working as a hub.
  - ✓ This makes sniffing network traffic easier for the threat actor.

PHYSICAL PORT SECURITY AND MAC FILTERING

- Because of the risks, access to the physical switch ports and switch hardware should be restricted to authorized staff, using a secure server room and/or lockable hardware cabinets.
- MAC Filtering and MAC Limiting
  - ✓ Configuring MAC filtering on a switch means defining which MAC addresses are allowed to connect to a particular port.
  - ✓ This can be done by creating a list of valid MAC addresses or by specifying a limit to the number of permitted addresses.
  - ✓ For example, if port security is enabled with a maximum of two MAC addresses, the switch will record the first two MACs to connect to that port, but then drop any traffic from machines with different MAC addresses that try to connect. (cisco.com/c/en/us/td/docs/ios/lanswitch/command/reference/lsw_book/lsw_m1.html).

NETWORK ACCESS CONTROL

- Endpoint security is a set of security procedures and technologies designed to restrict network access at a device level.
- Endpoint security contrasts with the focus on perimeter security established by topologies such as DMZ and technologies such as firewalls.
- Endpoint security does not replace these but adds defense in depth.
- The **IEEE 802.1X** standard defines a port-based network access control (PNAC) mechanism.
- **PNAC** means that the switch uses an AAA server to authenticate the attached device before activating the port.

ROUTE SECURITY

- A successful attack against route security enables the attacker to redirect traffic from its intended destination.
- On the Internet, this may allow the threat actor to herd users to spoofed websites.
- Routes between networks and subnets can be configured manually, but most routers automatically discover routes by communicating with each other.
- Dynamic routers exchange information about routes using routing protocols.
- It is important that this traffic be separated from channels used for other types of data.

ROUTE SECURITY (cont.)

```
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 [20/1] 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:~$
```

9.1- Implement Secure Network Designs

9.2- Implement Secure Switching and Routing

9.3- Implement Secure Wireless Infrastructure

9.4- Implement Load Balancers

WIRELESS NETWORK INSTALLATION

- Most organizations have both a wired and a wireless network for employees to access while on the move within their facilities.
- An infrastructure-based wireless network comprises one or more wireless **access points**, each connected to a wired network.
- The access points forward traffic to and from the wired switched network.
- Each **WAP** is identified by its MAC address, also referred to as its **basic service set identifier (BSSID)**.
- Each wireless network is identified by its name, or **service set identifier (SSID)**.

WIRELESS NETWORK INSTALLATION (cont.)

- Wireless networks can operate in either the 2.4 GHz or 5 GHz radio band.
- Each radio band is divided into a number of channels, and each **WAP** must be configured to use a specific channel.
- Site Surveys and Heat Maps
  - ✓ The coverage and interference factors mean that WAPs must be positioned and configured so that the whole area is covered, but that they overlap as little as possible.
  - ✓ A site survey is used to measure signal strength and channel usage throughout the area to cover.
  - ✓ A site survey starts with an architectural map of the site, with features that can cause background interference marked.
  - ✓ These features include solid walls, reflective surfaces, motors, microwave ovens, and so on. The survey is performed with a Wi-Fi-enabled laptop or mobile device with Wi-Fi analyzer software installed.

CONTROLLER AND ACCESS POINT

- Where a site survey ensures availability, the confidentiality and integrity properties of the network are ensured by configuring authentication and encryption.
- These settings could be configured manually on each **WAP**, but this would be onerous in an enterprise network with tens or hundreds of WAP.
- If access points are individually managed, this can lead to configuration errors and can make it difficult to gain an overall view of the wireless deployment.
- Rather than configure each device individually, enterprise wireless solutions implement **Wireless Controllers** for centralized management and monitoring.
- A controller can be a hardware appliance or a software application run on a server.

CONTROLLER AND ACCESS POINT (cont.)

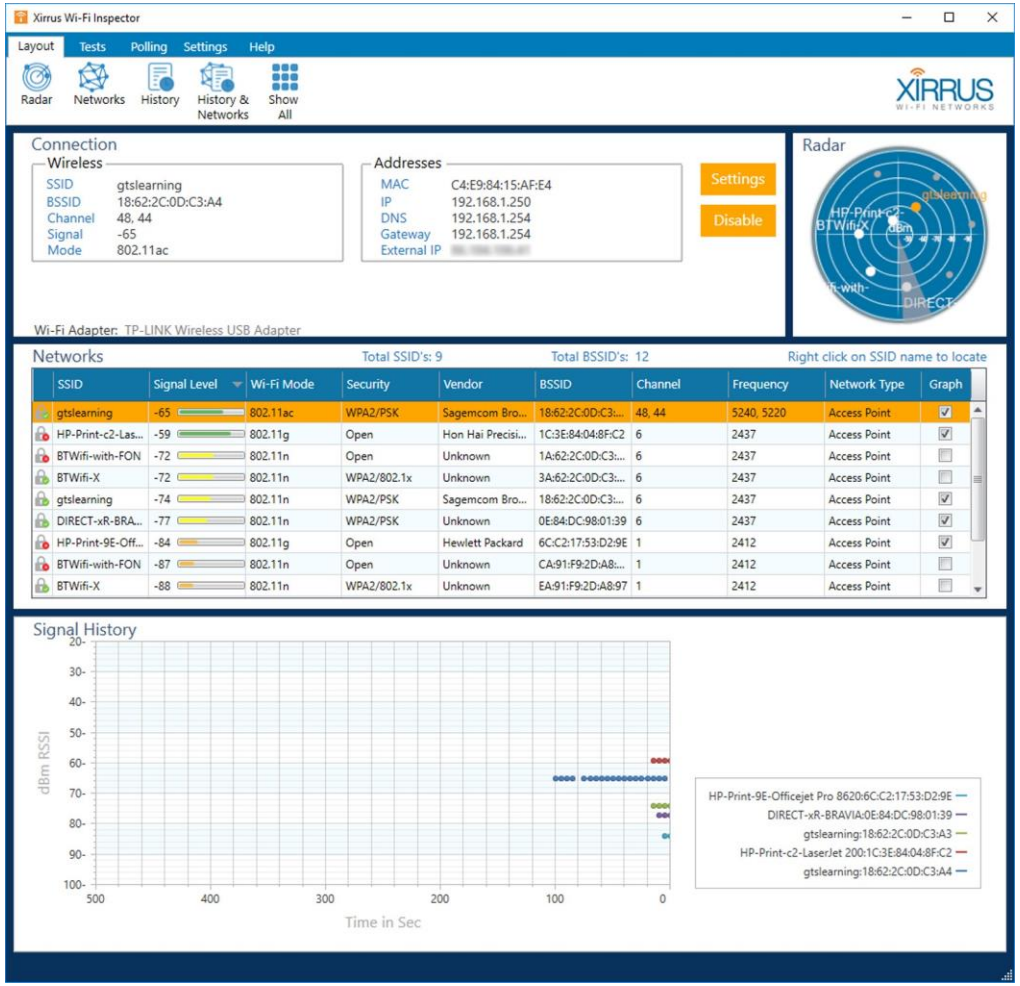
ROGUE ACCESS POINTS AND EVIL TWINS

- A **rogue access point** is one that has been installed on the network without authorization, whether with malicious intent or not.
- It is vital to periodically survey the site to detect rogue WAPs.
- A malicious user can set up such an access point with something as basic as a smartphone with tethering capabilities, and a non-malicious user could enable such an access point by accident.
- If connected to a LAN without security, an unauthorized WAP creates a backdoor through which to attack the network.
- A rogue WAP could also be used to capture user logon attempts, allow **man-in-the-middle attacks**, and allow access to private information.

ROGUE ACCESS POINTS AND EVIL TWINS (cont.)

- A rogue WAP masquerading as a legitimate one is called an **evil twin**.
- An evil twin might just have a similar name (SSID) to the legitimate one, or the attacker might use some DoS technique to overcome the legitimate WAP.
- This attack will not succeed if authentication security is enabled on the WAP, unless the attacker also knows the details of the authentication method.
- However, the evil twin might be able to harvest authentication information from users entering their credentials by mistake.

ROGUE ACCESS POINTS AND EVIL TWINS (cont.)



JAMMING ATTACKS

- A wireless network can be disrupted by interference from other radio sources.
- These are often unintentional, but it is also possible for an attacker to purposefully jam an access point.
- This might be done simply to disrupt services or to position an evil twin on the network with the hope of stealing data.
- A Wi-Fi jamming attack can be performed by setting up a WAP with a stronger signal.
- Wi-Fi jamming devices are also widely available, though they are often illegal to use and sometimes to sell.
- Such devices can be very small, but the attacker still needs to gain fairly close physical proximity to the wireless network.

JAMMING ATTACKS (cont.)

- The only ways to defeat a jamming attack are either to locate the offending radio source and disable it, or to boost the signal from the legitimate equipment.
- WAPs for home and small business use are not often configurable, but the more advanced wireless access points, such as **Cisco's Aironet series**, support configurable power level controls.
- The source of interference can be detected using a spectrum analyzer.
- Unlike a Wi-Fi analyzer, a spectrum analyzer must use a special radio receiver (Wi-Fi adapters filter out anything that isn't a Wi-Fi signal).
- They are usually supplied as handheld units with a directional antenna, so that the exact location of the interference can be pinpointed.

9.1- Implement Secure Network Designs

9.2- Implement Secure Switching and Routing

9.3- Implement Secure Wireless Infrastructure

9.4- Implement Load Balancers

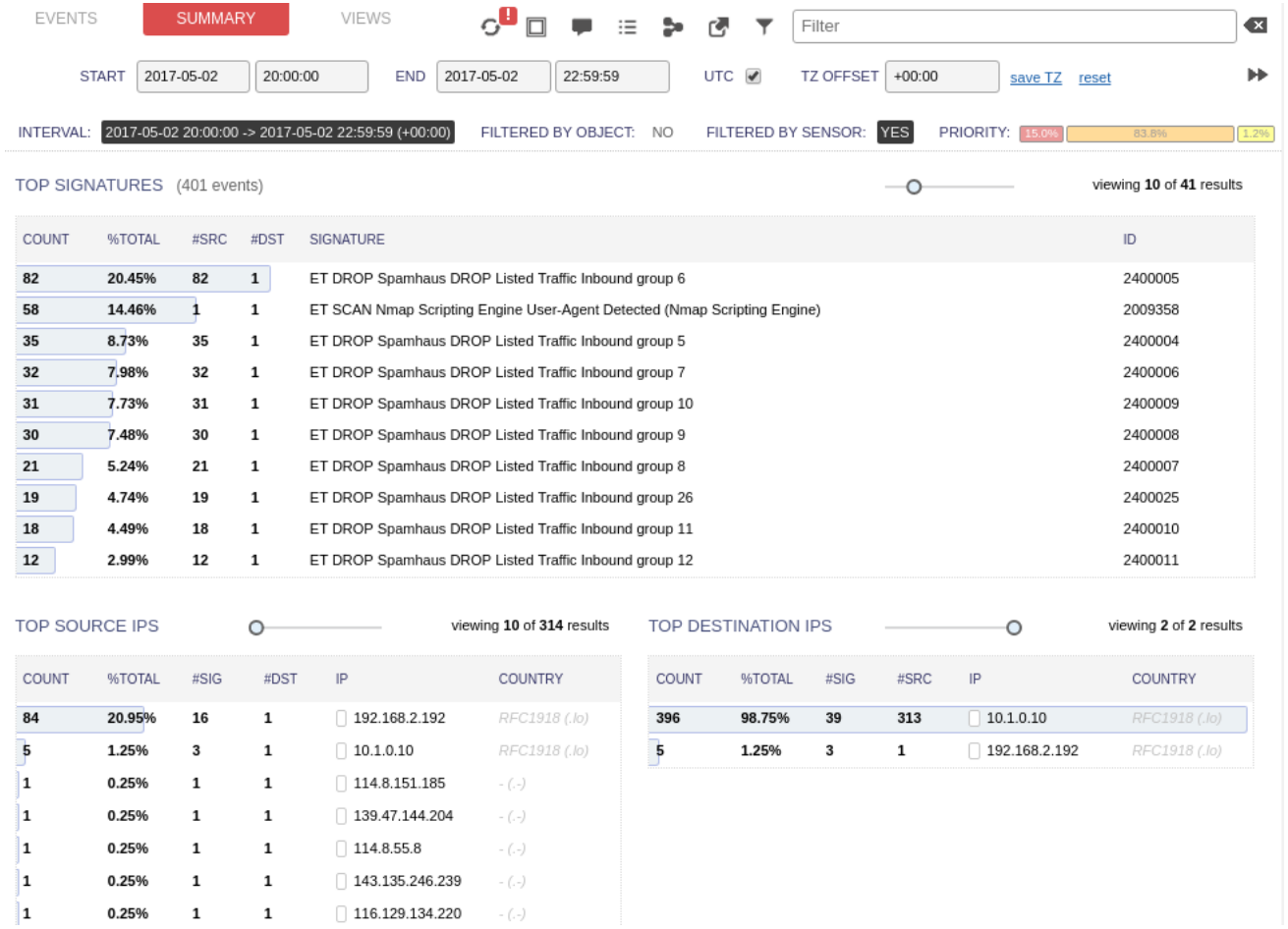
DISTRIBUTED DENIAL OF SERVICE ATTACKS (DDoS)

- Most denial of service (DoS) attacks against websites and gateways are distributed DoS (DDoS).
- This means that the attack is launched from multiple hosts simultaneously.
- Typically, a threat actor will compromise machines to use as handlers in a command and control network.
- The handlers are used to compromise hundreds or thousands or millions of hosts with DoS tools (bots) forming a botnet.
- DDoS attacks simply aim to consume network bandwidth, denying it to legitimate hosts, by using overwhelming numbers of bots.

DDoS ATTACK MITIGATION

- DDoS attacks can be diagnosed by traffic spikes that have no legitimate explanation, but can usually only be counteracted by providing high availability services, such as load balancing.
- In some cases, a stateful firewall can detect a DDoS attack and automatically block the source.
- However, for many of the techniques used in DDoS attacks, the source addresses will be randomly spoofed or launched by bots, making it difficult to detect the source of the attack.

DDoS ATTACK MITIGATION (cont.)



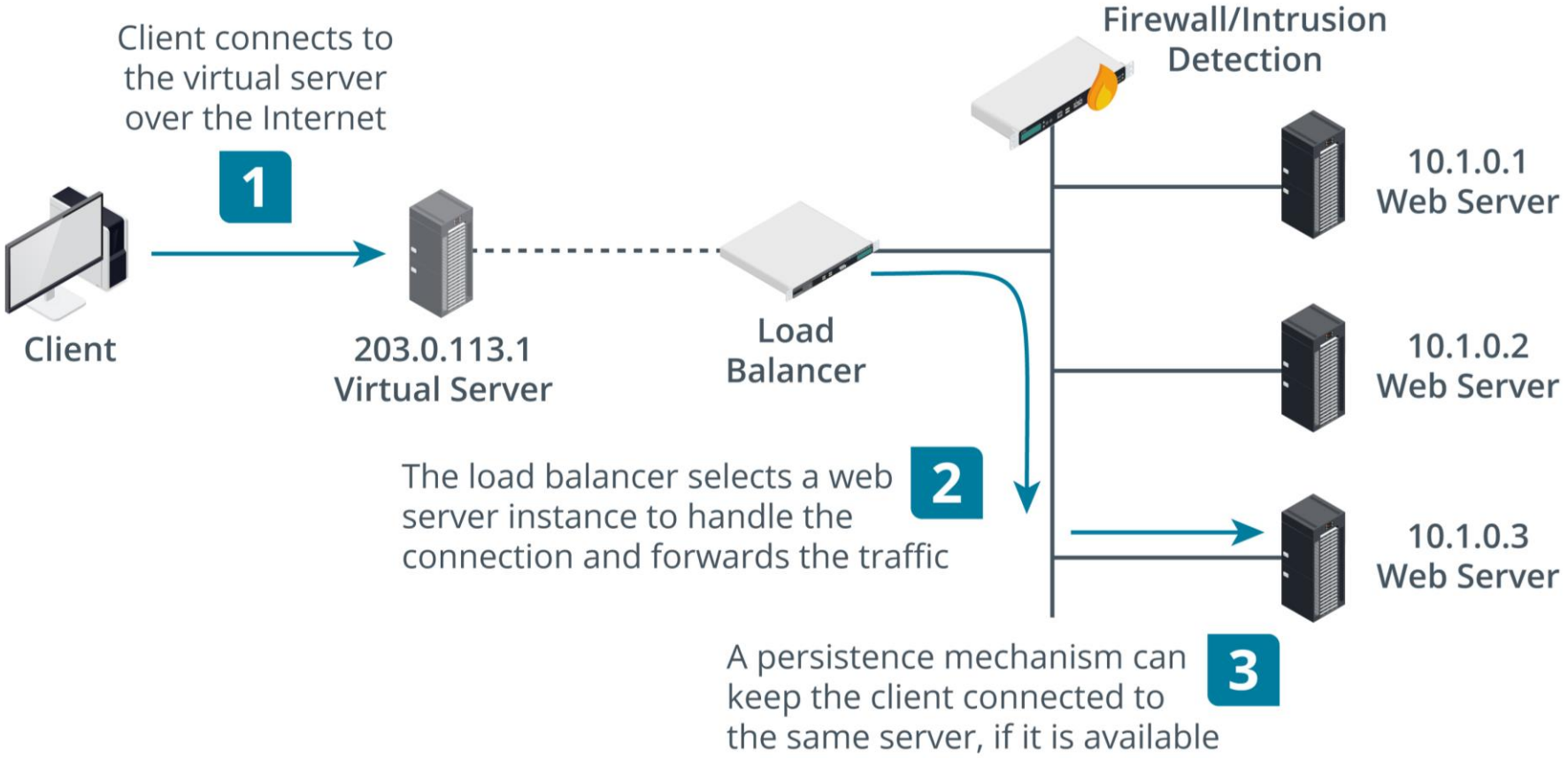
LOAD BALANCING

- A load balancer distributes client requests across available server nodes in a farm or pool.
- This is used to provision services that can scale from light to heavy loads, and to provide mitigation against DDoS attacks.
- A load balancer also provides fault tolerance.
- If there are multiple servers available in a farm, all addressed by a single name/IP address via a load balancer, then if a single server fails, client requests can be routed to another server in the farm.
- You can use a load balancer in any situation where you have multiple servers providing the same function.

LOAD BALANCING (cont.)

- Examples include web servers, front-end email servers, and web conferencing, A/V conferencing, or streaming media servers.
- There are two main types of load balancers:
  - ✓ Layer 4 load balancer—basic load balancers make forwarding decisions on IP address and TCP/UDP port values, working at the transport layer of the OSI model.
  - ✓ Layer 7 load balancer (content switch)—as web applications have become more complex, modern load balancers need to be able to make forwarding decisions based on application-level data, such as a request for a particular URL or data types like video or audio streaming, This requires more complex logic, but the processing power of modern appliances is sufficient to deal with this.

LOAD BALANCING (cont.)



Lab

Lab 13: Implementing a Secure Network Design