Technologies for Monitoring and Managing (1 of 6)

- Port Security
  - Threat actors who access a network device through an unprotected port can reconfigure the device to their advantage
  - **Route security** is the trust of packets sent through a router
    - False route information can be injected or altered by weak port security
  - **Broadcast storm prevention** can be accomplished by loop prevention
    - Loop prevention uses the IEEE 802.1d standard *spanning-tree protocol (STP)*
    - STP uses an algorithm that creates a hierarchical tree layout that spans the entire network

Technologies for Monitoring and Managing (2 of 6)

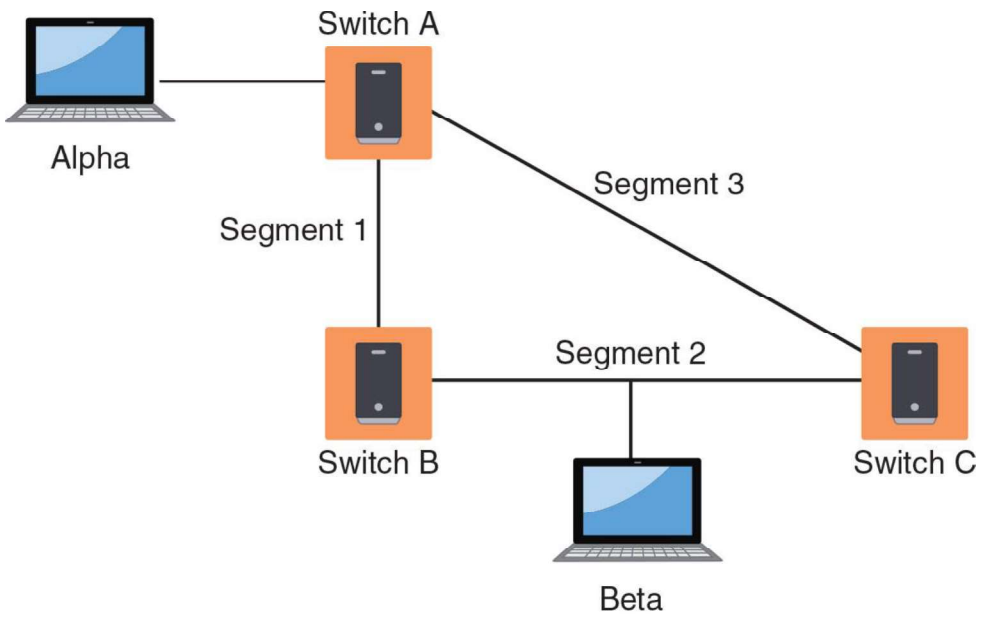

Figure 9-9 Broadcast storm

Figure 9-9 Broadcast storm

Technologies for Monitoring and Managing (3 of 6)

- Packet Capture and Analysis
  - Analyzing packets helps to monitor network performance and reveal cybersecurity incidents
  - Monitoring traffic on switches can be done in two ways:
    - A **separate port TAP** (test access point) can be installed
    - **Port mirroring** (also called **port spanning**) allows the administrator to configure the switch to copy traffic on some or all ports to a designated monitoring port on the switch
- Monitoring Services
  - An external third-party monitoring service can be used to provide additional resources to assist an organization in its cybersecurity defenses

Technologies for Monitoring and Managing (4 of 6)

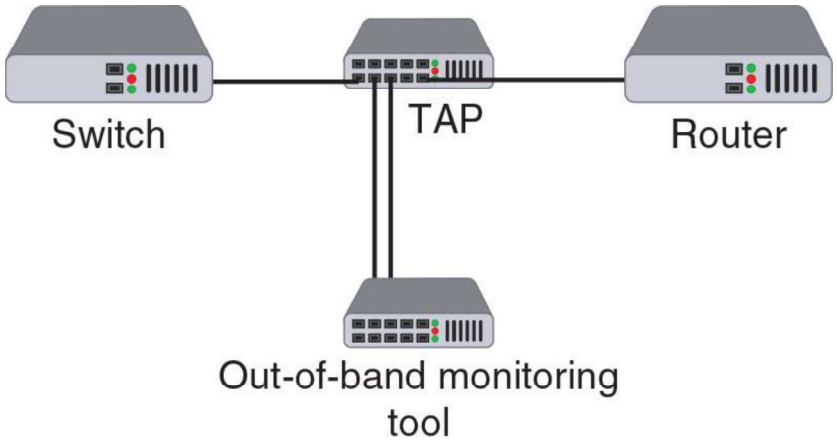

Figure 9-10 Port TAP

Figure 9-10 Port TAP

Technologies for Monitoring and Managing (5 of 6)

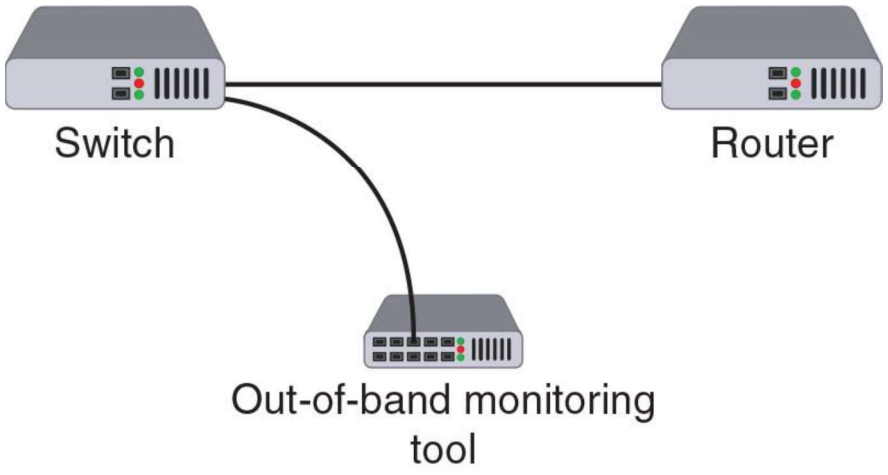

Figure 9-11 Port mirroring

Figure 9-11 Port Mirroring

Technologies for Monitoring and Managing (6 of 6)

- File Integrity Monitors
  - **File integrity monitors** examine files to see if they have changed
  - File integrity monitors are used for detecting malware as well as maintaining compliance with industry-specific regulations
- Quality of Service (QoS)
  - **QoS** is a set of network technologies used to guarantee its ability to dependably serve network resources and high-priority applications to endpoints
  - A network administrator can assign the order in which packets are handled and the amount of bandwidth given to an application or traffic flow (called **traffic shaping**)
  - Almost all firewalls today recognize QoS settings

Design Technologies (1 of 7)

- Network Segmentation
  - Examples of network segmentation include virtual LANs and a demilitarized zone
  - Zero trust is a strategic initiative about networks that is designed to prevent successful attacks
    - It attempts to eliminate the concept of trust from an organization's network architecture
  - Zero trust requires that networks be segmented
  - A network can be segmented by separating devices into logical groups by creating a **virtual LAN (VLAN)**
  - VLANs can be isolated so that sensitive data is transported only to members of the VLAN

Design Technologies (2 of 7)

- Network Segmentation (continued)
  - A *demilitarized zone (DMZ)* is a separate network located outside secure network perimeter
  - Untrusted outside users can access DMZ but cannot enter the secure network
  - A common approach to configuring a DMZ is to use a **jump box** (sometimes called a *jump server* or *jump host*)
    - A jump box is a minimally configured administrator server that connects two dissimilar security zones while providing tightly restricted access between them

Design Technologies (3 of 7)

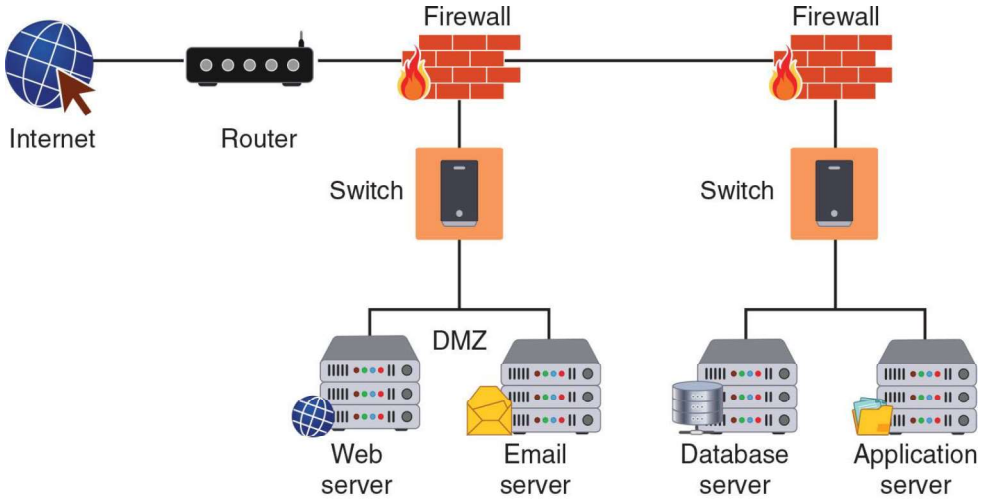

Figure 9-12 DMZ with two firewalls

Figure 9-12 DMZ with two firewalls

Design Technologies (4 of 7)

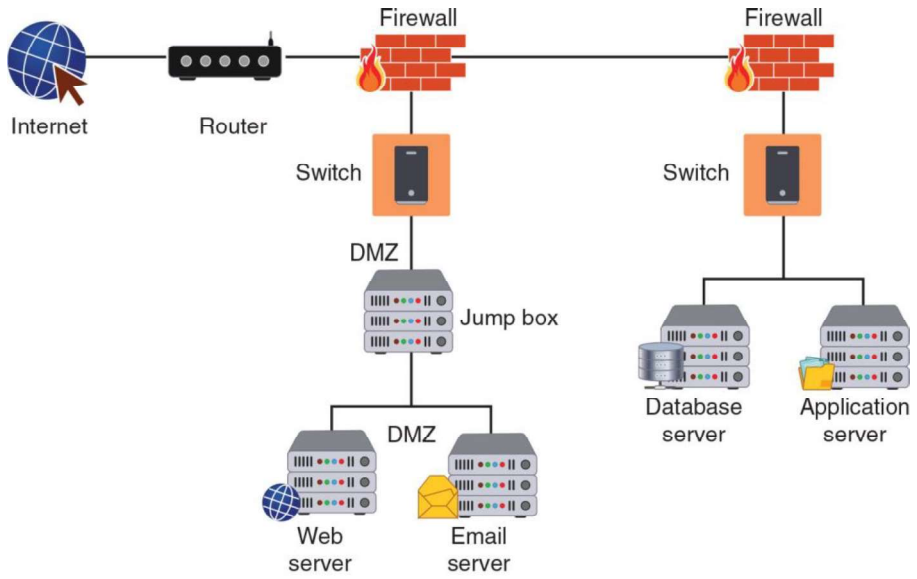

Figure 9-13 Jump box

Figure 9-13 Jump box

Design Technologies (5 of 7)

- Load Balancing
  - **Load balancing** is a technology that can help to evenly distribute work across a network and can allocate requests among multiple devices
  - Advantages of load-balancing technology:
    - Reduces probability of overloading a single server
    - Optimizes bandwidth of network computers
  - Load balancing is achieved through software or hardware device (*load balancer*)
  - Different scheduling protocols used in load balancers:
    - *Round-robin*
    - *Affinity*

Design Technologies (6 of 7)

- Load Balancing (continued)
  - When multiple load balancers are used together, they can be placed in different configurations that include:
    - In an **active-passive configuration**, the primary load balancer distributes the network traffic to the most suitable server, while the secondary load balancer operates in a "listening mode"
    - In an **active-active configuration**, all load balancers are always active
  - Load balancing can also support session **persistence**, which is a process in which a load balancer creates a link between an endpoint and a specific network server for the duration of a session
    - This can help improve the user experience and optimize network resource usage

Design Technologies (7 of 7)

- Load Balancing (continued)
  - Security advantages of using a load balancer:
    - They can detect and stop attacks directed at a server or application
    - Can also detect and prevent protocol attacks
    - Some load balancers can hide HTTP error pages or remove server identification headers from HTTP responses, denying attackers additional information about the internal network

Knowledge Check Activity 2

What type of access technology routes some traffic over a secure VPN while other traffic accesses the Internet directly without going through the VPN?

a. Split tunnel
b. Site-site VPN
c. Router ACL
d. Full tunnel

Knowledge Check Activity 2: Answer

What type of access technology routes some traffic over a secure VPN while other traffic accesses the Internet directly without going through the VPN?

Answer: a. Split tunnel

A split tunnel routes only some traffic over the secure VPN while other traffic directly accesses the Internet (this helps preserve bandwidth).

Self-Assessment

Consider the network security appliances and technologies you have studied in this module. Based on what you know now, if you could pick only one network security appliance and one security technology you could deploy on a network you were managing, which would they be and why?

Summary (1 of 2)

- A computer firewall is designed to limit the spread of malware
- Stateless packet filtering on a firewall looks at a packet and permits or denies it based solely on the firewall rules
  - Stateful packet filtering uses both the firewall rules and the state of the connection
- There are several specialized firewall appliances: a web application firewall (WAF), a next generation firewall (NGFW), unified threat management (UTM) device
- A forward proxy is a computer or program that intercepts user requests from the internal network and processes these requests on behalf of the user
- A honeypot is a computer located in an area with limited security that serves as “bait” to threat actors
- An intrusion detection system (IDS) can detect an attack as it occurs, an intrusion prevention system (IPS) attempts to block the attack

Summary (2 of 2)

- A network hardware security module is a special trusted network computer that performs cryptographic operations such as key management, key exchange, onboard random number generation, key storage facility, and symmetric and asymmetric encryption
- An access control list (ACL) contains rules that administer the availability of digital assets by granting or denying access to the assets
- Network access control (NAC) examines the current state of an endpoint before it can connect to the network
- Data loss prevention (DLP) is a system of security tools used to recognize and identify data critical to the organization and ensure that it is protected
- Broadcast storm prevention can be accomplished by loop prevention, which uses the IEEE 802.1d standard spanning-tree protocol (STP)