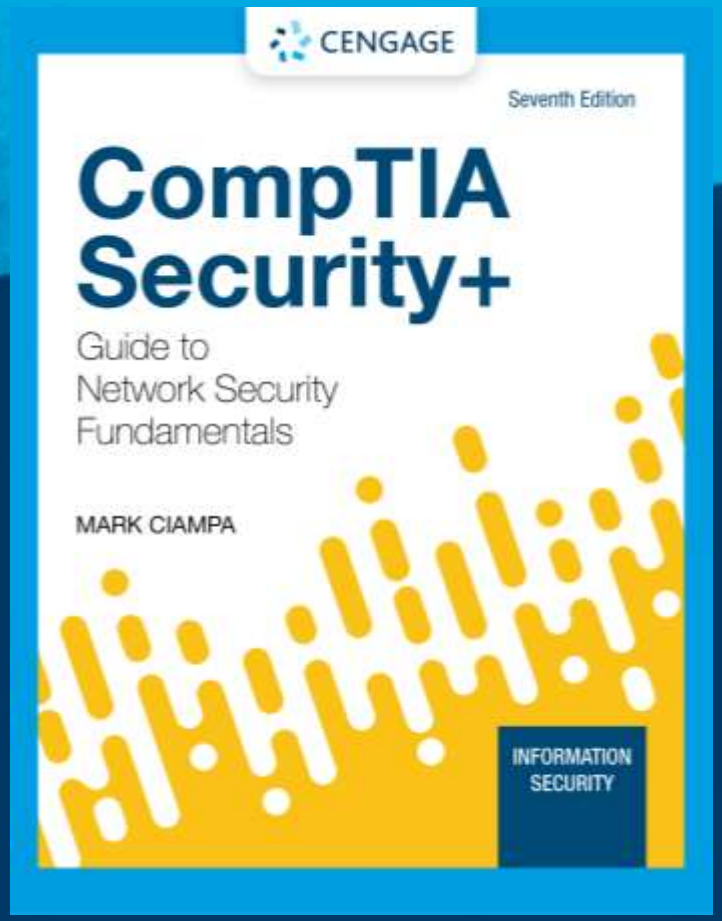

CompTIA Security+ Guide to Network Security Fundamentals, 7th Edition

Module 9: Network Security Appliances and Technologies

CENGAGE

Module Objectives

By the end of this module, you should be able to:

1. List the different types of network security appliances and how they can be used

2. Describe network security technologies

Security Appliances

- Security can be achieved through appliances that directly address security and by using the security features in standard networking devices
- Using both standard networking devices and security appliances can result in a layered security approach
- Appliances include:
  - Firewalls
  - Proxy servers
  - Deception instruments
  - Intrusion detection and prevention systems
  - Network hardware security models

Firewalls (1 of 6)

- To use firewalls effectively, you must understand the function of firewalls and know the different types of firewalls and specialized firewall appliances
- Firewall Functions
  - A firewall uses bidirectional inspection to examine outgoing and incoming packets
  - The actions are based on specific criteria or rules (called *rule-based firewalls*)
  - A more flexible type of firewall is a *policy-based firewall* which allows more generic statements instead of specific rules
  - Firewalls can also apply **content/URL filtering**

Firewalls (2 of 6)

Source: BullGuard

Figure 9-1 Content/URL filtering

Firewalls (3 of 6)

- Firewall Categories
  - *Stateful vs. stateless*
  - *Open source vs. proprietary*
  - *Hardware vs. software*
  - *Host vs. appliance vs. virtual*

Firewalls (4 of 6)

Used with permissions from Microsoft

Figure 9-3 Windows host-based firewall

CENGAGE

Firewalls (5 of 6)

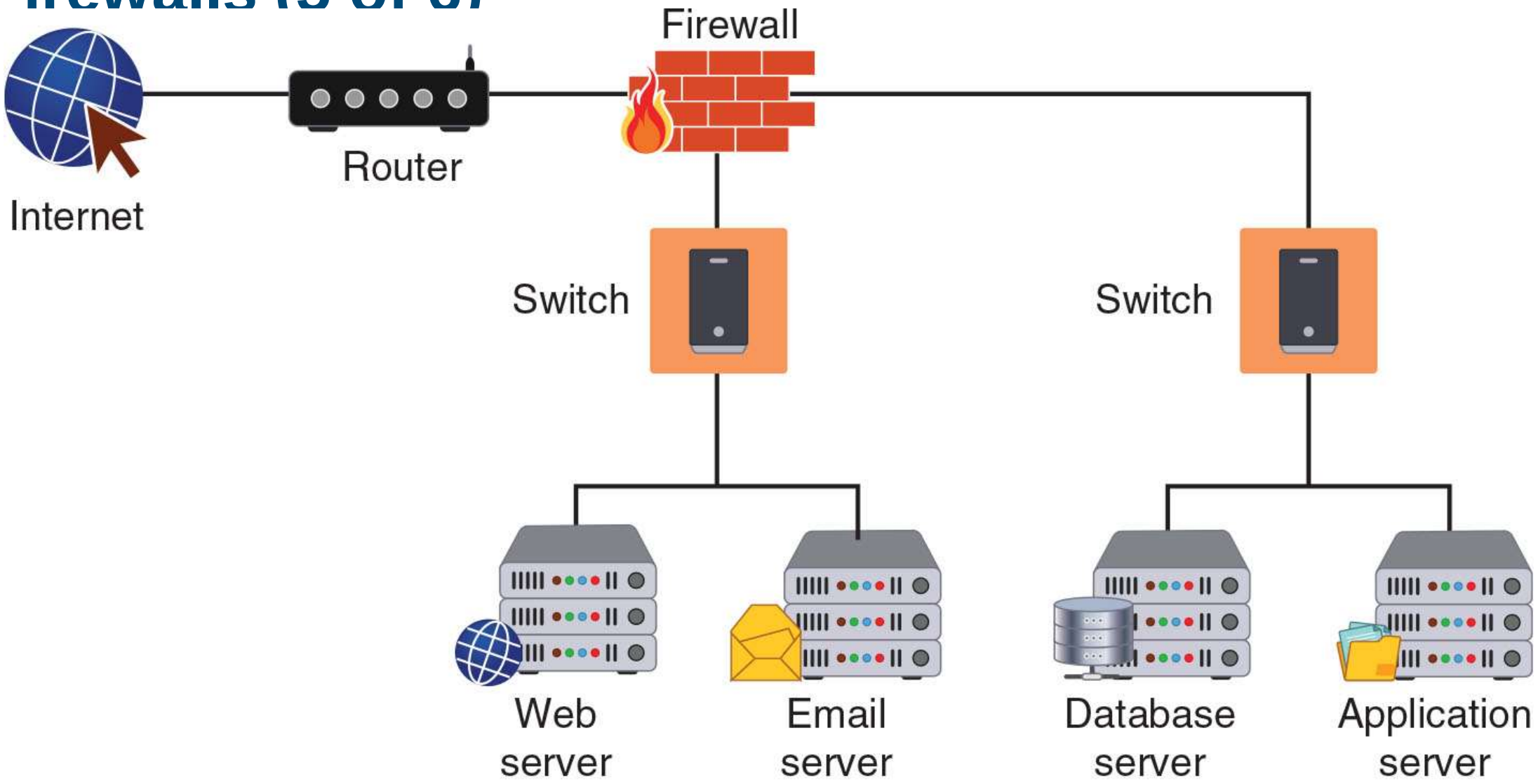

Figure 9-4 Appliance firewall

Firewalls (6 of 6)

- Specialized Firewall Appliances
  - *Web application firewall*
  - *Network address translation gateway*
    - Network address translation (NAT) is a technique that allows private IP addresses to be used on the public internet
  - *Next generation firewall*
  - *Unified threat management (UTM)*
    - UTM is a device that combines several security functions such as packet filtering, antispam, antiphishing, antispyware, encryption, intrusion protection, and web filtering

Proxy Servers (1 of 2)

- Proxies are devices that act as substitutes on behalf of the primary device
- A **forward proxy** is a computer or an application that intercepts user requests from the internal secure network and processes the requests on behalf of the user
- A **reverse proxy** routes requests coming from an external network to the correct internal server
- A proxy server can provide a degree of protection
  - It can look for malware by intercepting it before it reaches the internal endpoint
  - It can hide the IP address of endpoints inside the secure network so that only the proxy server's IP address is used on the open Internet

Proxy Servers (2 of 2)

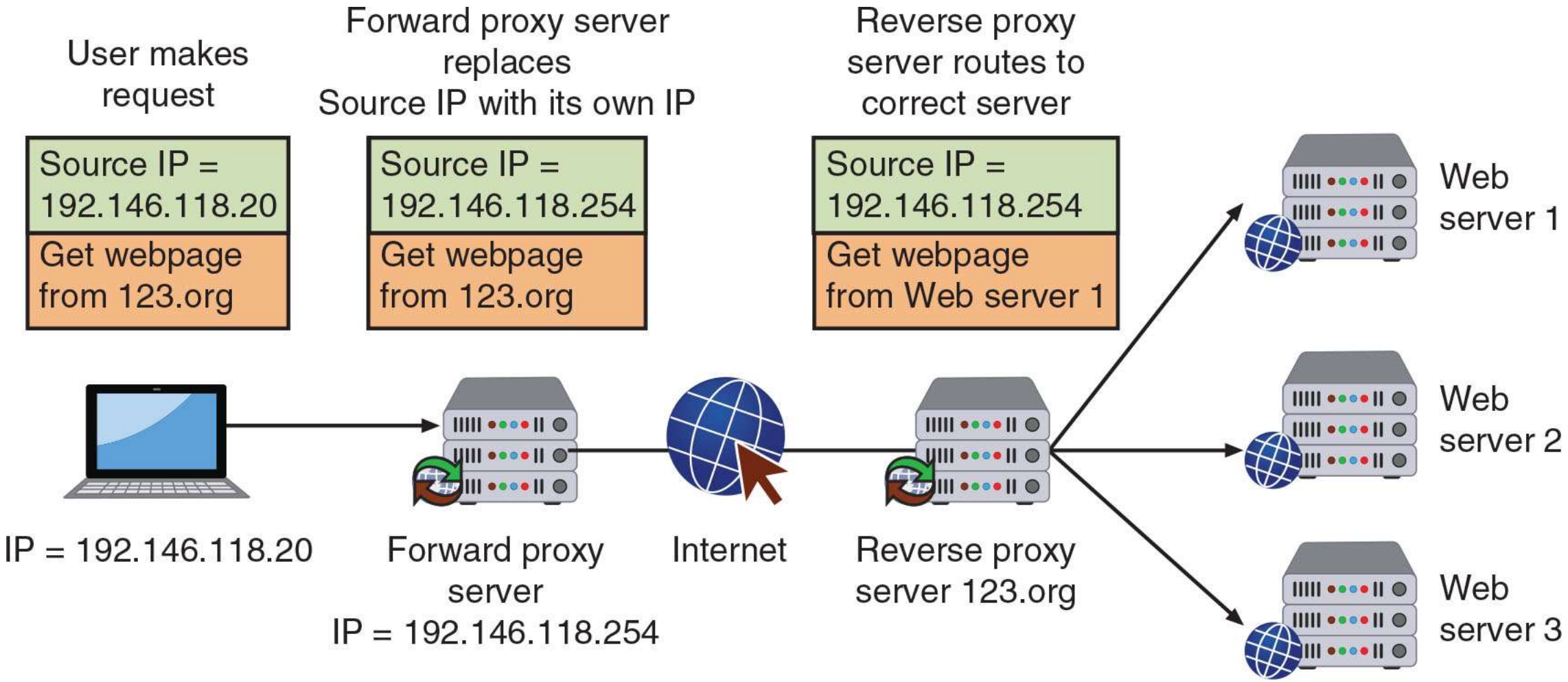

Figure 9-5 Forward and reverse proxy servers

Deception Instruments (1 of 3)

- Deception can be used as a security defense
  - By directing threat actors away from a valuable asset to something that has little or no value
- Network deception can involve creating and using honeypots and sinkholes
- Honeypots
  - A **honeypot** is a computer located in an area with limited security that serves as “bait” to threat actors
  - Two goals of using a honeypot:
    - *Deflect*
    - *Discover*

Deception Instruments (2 of 3)

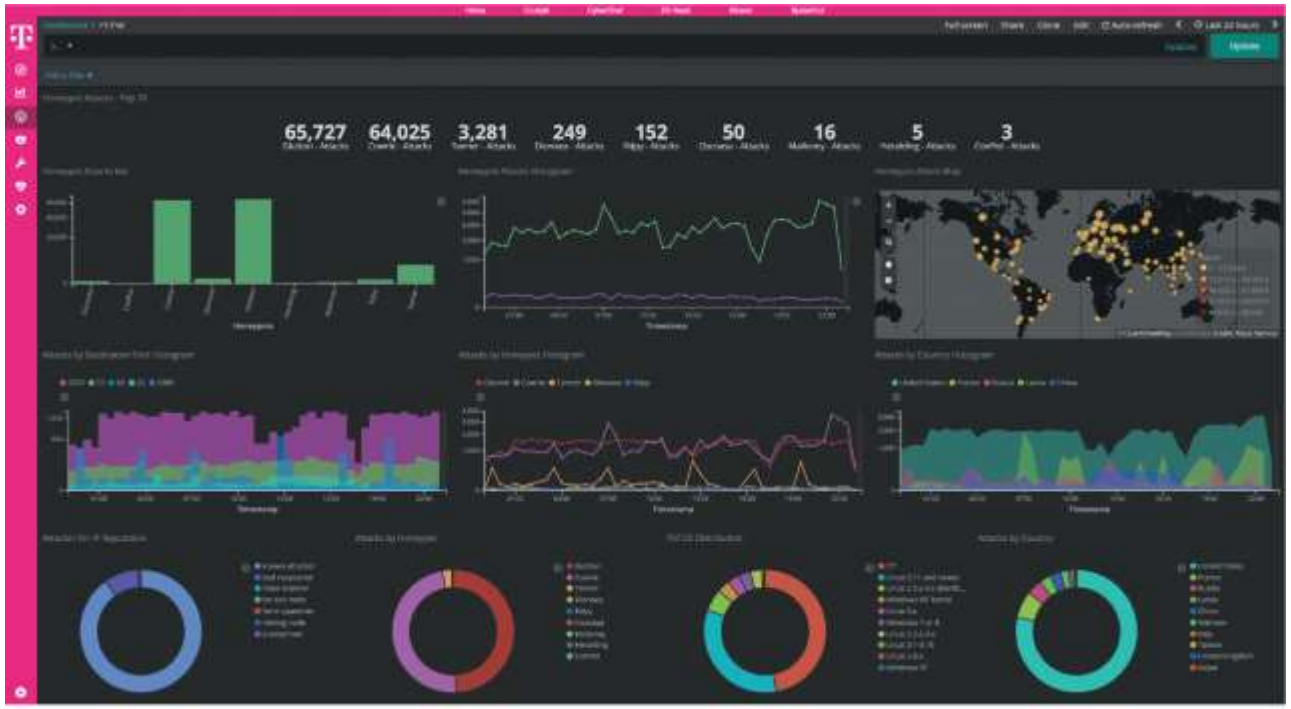

Figure 9-6 Honeypot dashboard

Figure 9-6 Honeypot dashboard

Deception Instruments (3 of 3)

- Honeypots (continued)
  - Different types of honeypots:
    - A *low-interaction honeypot* may only contain a login prompt
    - A *high-interaction honeypot* is designed for capturing more information from the threat actor
      - This type of honeypot can collect information from threat actors about attack techniques or the particular information they are seeking from the organization
  - A **honeynet** is a network of honeypots set up with intentional vulnerabilities
- Sinkholes
  - A **sinkhole** is a "bottomless pit" designed to steer unwanted traffic away from its intended destination to another device
    - The goal is to deceive the threat actor into thinking the attack was successful

Intrusion Detection and Prevention Systems (1 of 3)

- An *intrusion detection system (IDS)* can detect an attack as it occurs
- An *intrusion prevention system (IPS)* attempts to block the attack
- **Inline system** is connected directly to the network and monitors the flow of data as it occurs
- A **passive system** is connected to a port on a switch, which receives a copy of network traffic
- IDS systems can be managed in different ways:
  - In-band management is through the network itself by using network protocols and tools
  - Out-of-band management is using an independent and dedicated channel to reach the device

Intrusion Detection and Prevention Systems (2 of 3)

- Monitoring Methodologies
  - **Anomaly-based monitoring** compares current detected behavior with baseline
  - **Signature-based monitoring** looks for well-known attack signature patterns
  - **Behavior-based monitoring** detects abnormal actions by processes or programs
    - Alerts user who decides whether to allow or block activity
  - **Heuristic monitoring** uses experience-based techniques
    - Attempts to answer the question “Will this do something harmful if it is allowed to execute?”

Intrusion Detection and Prevention Systems (3 of 3)

- A network intrusion detection system (NIDS) watches for attacks on the network
  - NIDS sensors installed on firewalls and routers gather information and report back to central device
- A network intrusion prevention system (NIPS) monitors to detect malicious activities and also attempts to stop them

Network Hardware Security Modules

- A *hardware security module (HSM)* is a removable external cryptographic device
- For endpoints, an HSM is typically a USB device, an expansion card, or a device that connects directly to a computer through a port
- A **network hardware security module** performs cryptographic operations such as key management, key exchange, onboard random number generation, key storage facility, and accelerated symmetric and asymmetric encryption

Configuration Management

- It is essential that security appliances be properly configured
- Basic configuration management tools include:
  - *Secure baseline configurations*
  - *Standard naming conventions*
  - *Defined Internet Protocol schema*
  - *Diagrams*

Knowledge Check Activity 1

Which of the following network security devices is a computer that is purposely located in an area with limited security to attract threat actors?

a. Forward proxy

b. Honeypot

c. Inline system

d. Behavior monitor

Knowledge Check Activity 1: Answer

Which of the following network security devices is a computer that is purposely located in an area with limited security to attract threat actors?

Answer: b. Honeypot

A honeypot is a computer located in an area with limited security that serves as "bait" to threat actors. Its purpose is to deflect and discover threats.

Security Technologies

- There are general security technologies that can provide a defense
- Some of these technologies can be found in both standard networking devices (switches and routers) and specialized security appliances
- Categories of security technologies include:
  - Access technologies
  - Monitoring and managing technologies
  - Design technologies

Access Technologies (1 of 7)

- Access Control List (ACL)
  - An **access control list (ACL)** contains rules that administer the availability of digital assets by granting or denying access to the assets
  - Two types of ACLS include:
    - *Filesystem ACLs* filter access to files and directories on an endpoint by telling the OS who can access the device and what privileges they are allowed
    - *Networking ACLs* filter access to a network
      - Often found on routers
  - Router ACLs can be used on external routers to restrict vulnerable protocols and limit traffic from entering the network
  - Internal router ACLs are often configured with explicit *allow* and *deny* statements for specific addresses and protocol services

Access Technologies (2 of 7)

- Virtual Private Network (VPN)
  - A **VPN** is a security technology that enables authorized users to use an unsecured public network (the Internet) as if it were a secure private network
  - Two common types of VPNs:
    - A **remote access VPN**
    - A **site-to-site VPN**
  - A **full tunnel** sends all traffic to the VPN concentrator and protects it
  - A **split tunnel** routes only some traffic over the secure VPN while other traffic directly accesses the Internet (this helps preserve bandwidth)
  - The most common protocols used for VPNs are IPsec and SSL

Access Technologies (3 of 7)

- Network Access Control (NAC)
  - **NAC** examines the current state of a system or network device before it can connect to the network
  - Any device that does not meet a specified set of criteria can connect only to a "quarantine" network where the security deficiencies are corrected
  - NAC uses software "agents" to gather information and report back (called host agent health checks)
  - An agent may be a *permanent* NAC agent or a *dissolvable* NAC agent that disappears after reporting information to the NAC
  - The NAC technology can be embedded within a Microsoft Windows Active Directory (AD) domain controller
    - NAC uses AD to scan the device (called **agentless NAC**)

Access Technologies (4 of 7)

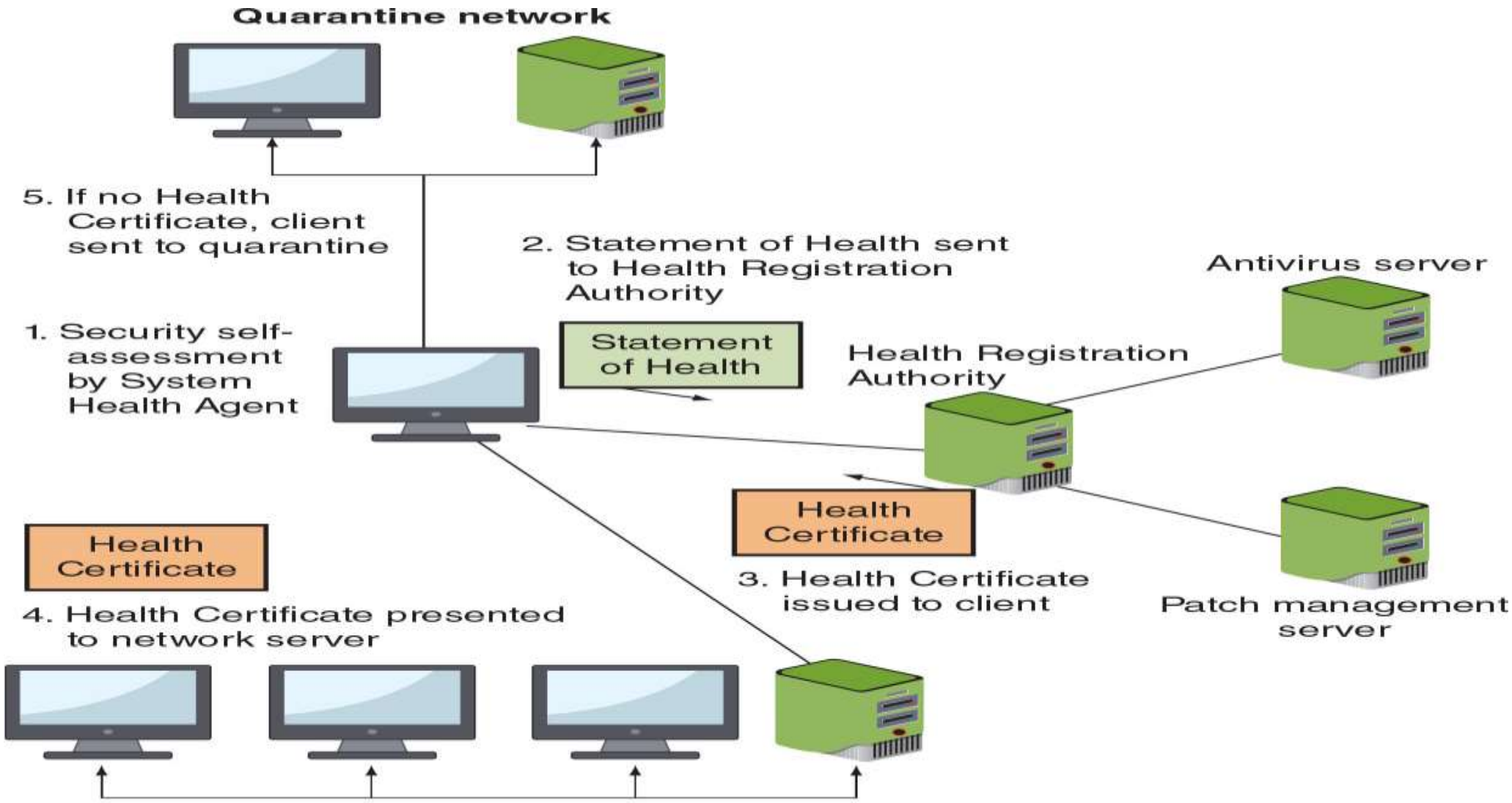

Figure 9-7 Network access control (NAC) process

Access Technologies (5 of 7)

- Data Loss Prevention
  - DLP is considered as rights management, or the authority of the owner of the data to impose restrictions on its use
  - DLP is a system of security tools that is used to recognize and identify data that is critical to the organization
  - Most DLP systems use **content inspection** which is defined as a security analysis of the transaction within its approved context
  - An administrator creates DLP rules based on the data and the policy
  - These rules are loaded into a DLP server
  - When a policy violation is detected by the DLP agent it is reported back to the DLP server

Access Technologies (6 of 7)

- Data Loss Prevention (continued)
  - When a server is notified of a policy violation different actions can be taken:
    - Block the data
    - Redirect it to an individual who can examine the request
    - Quarantine the data until later
    - Alert a supervisor of the request
  - A process called *tokenization* obfuscates sensitive data elements, such as an account number, into a random string of characters (*token*)
    - The original sensitive data element and the token are stored in a database called a *token vault* so that if the actual data element is needed, it can be retrieved as needed
    - Tokenization is illustrated in Figure 9-8 on the following slide

Access Technologies (7 of 7)

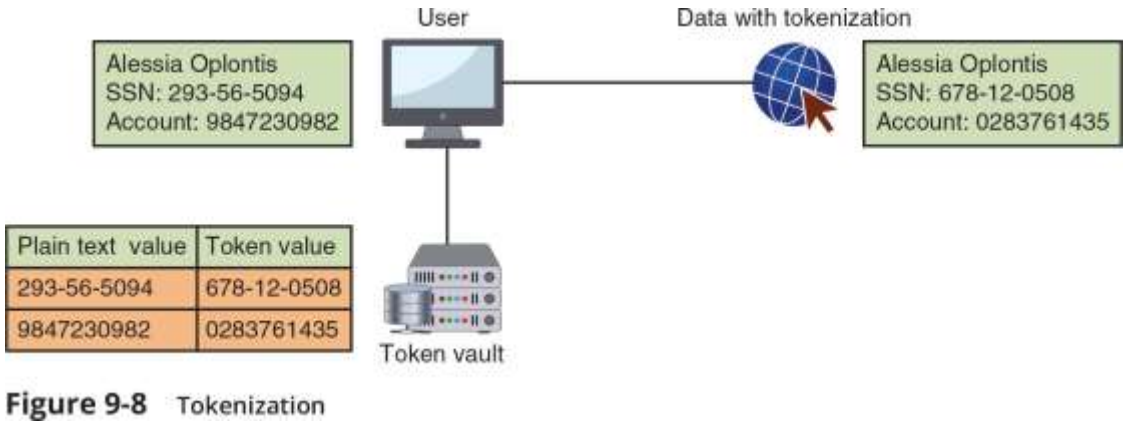

Figure 9-8 Tokenization

Figure 9-8 Tokenization

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)

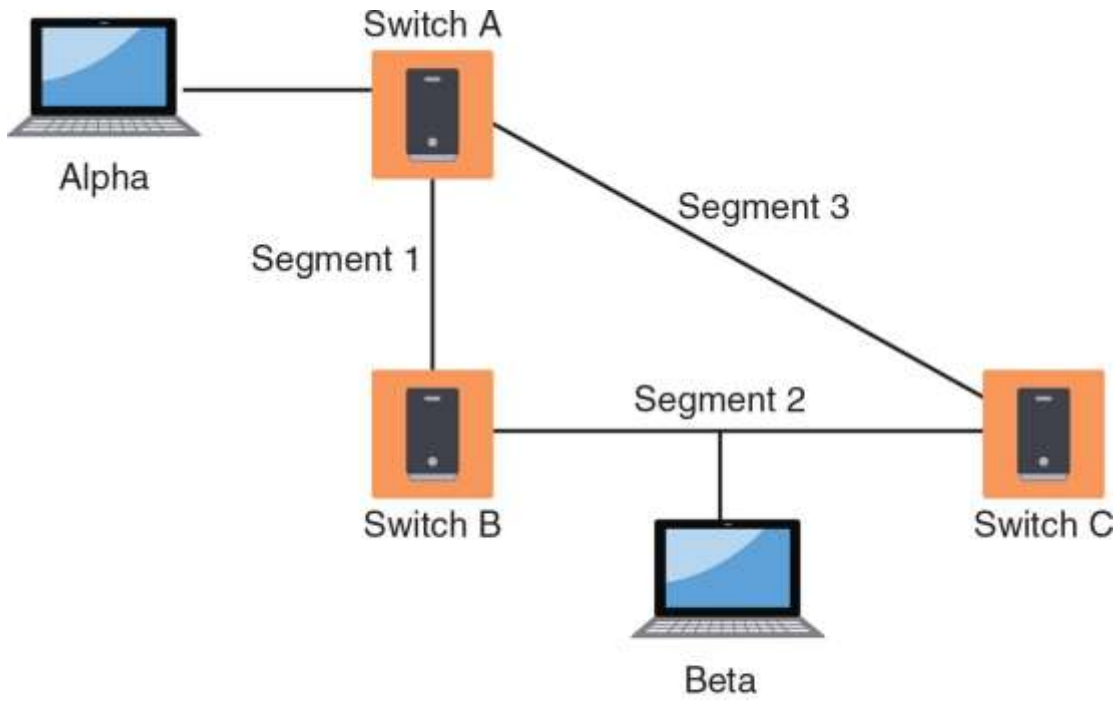

Figure 9-9 Broadcast storm

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)

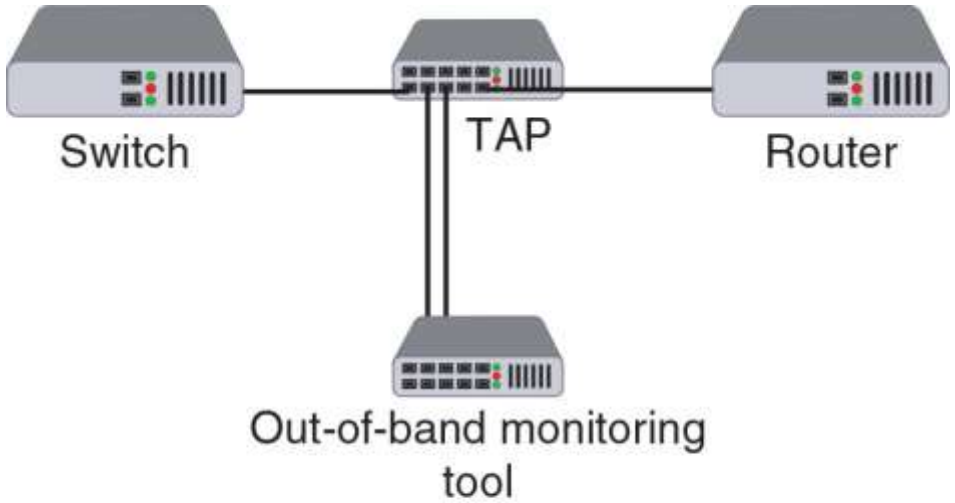

Figure 9-10 Port TAP

Figure 9-10 Port TAP

Technologies for Monitoring and Managing (5 of 6)

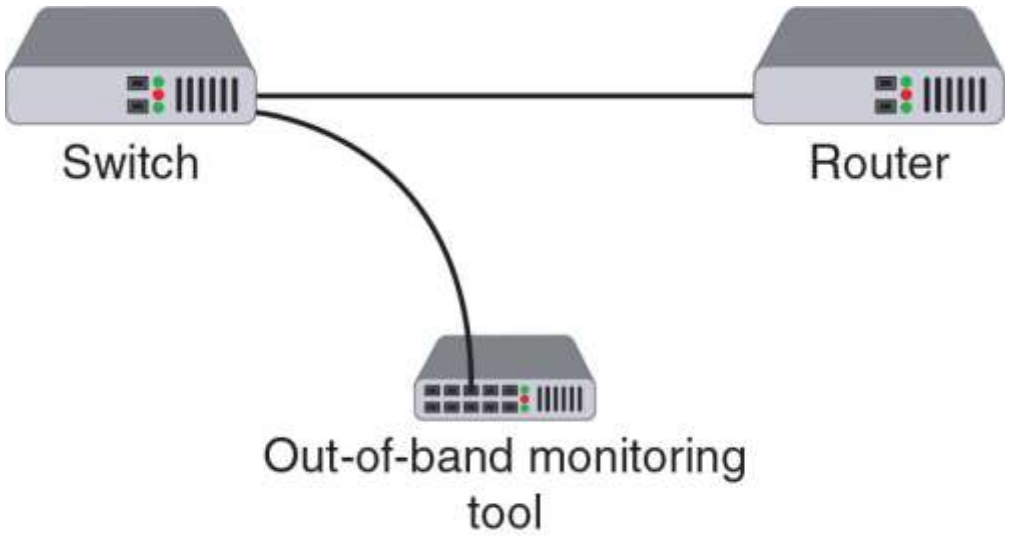

Figure 9-11 Port mirroring

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)

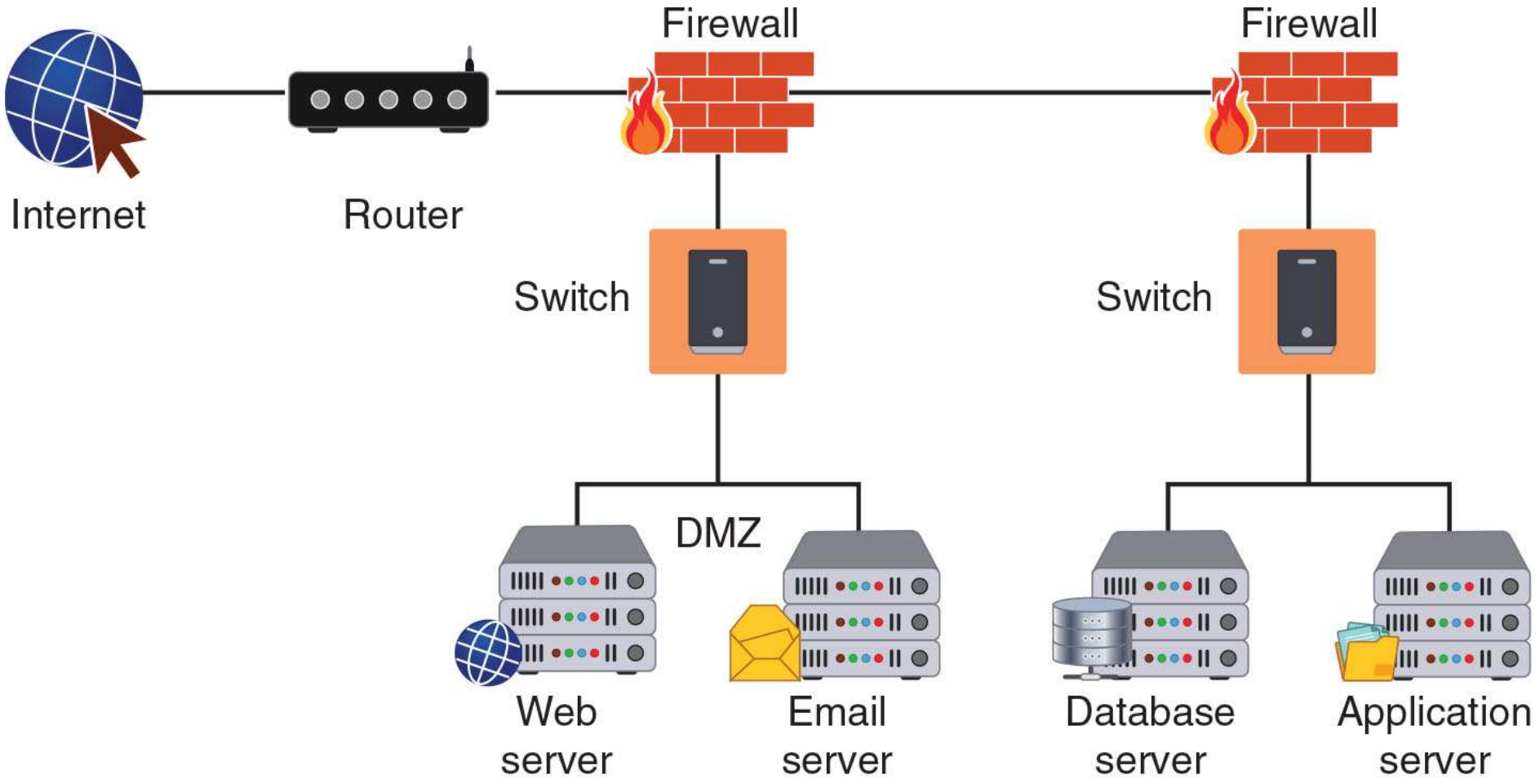

Figure 9-12 DMZ with two firewalls

Design Technologies (4 of 7)

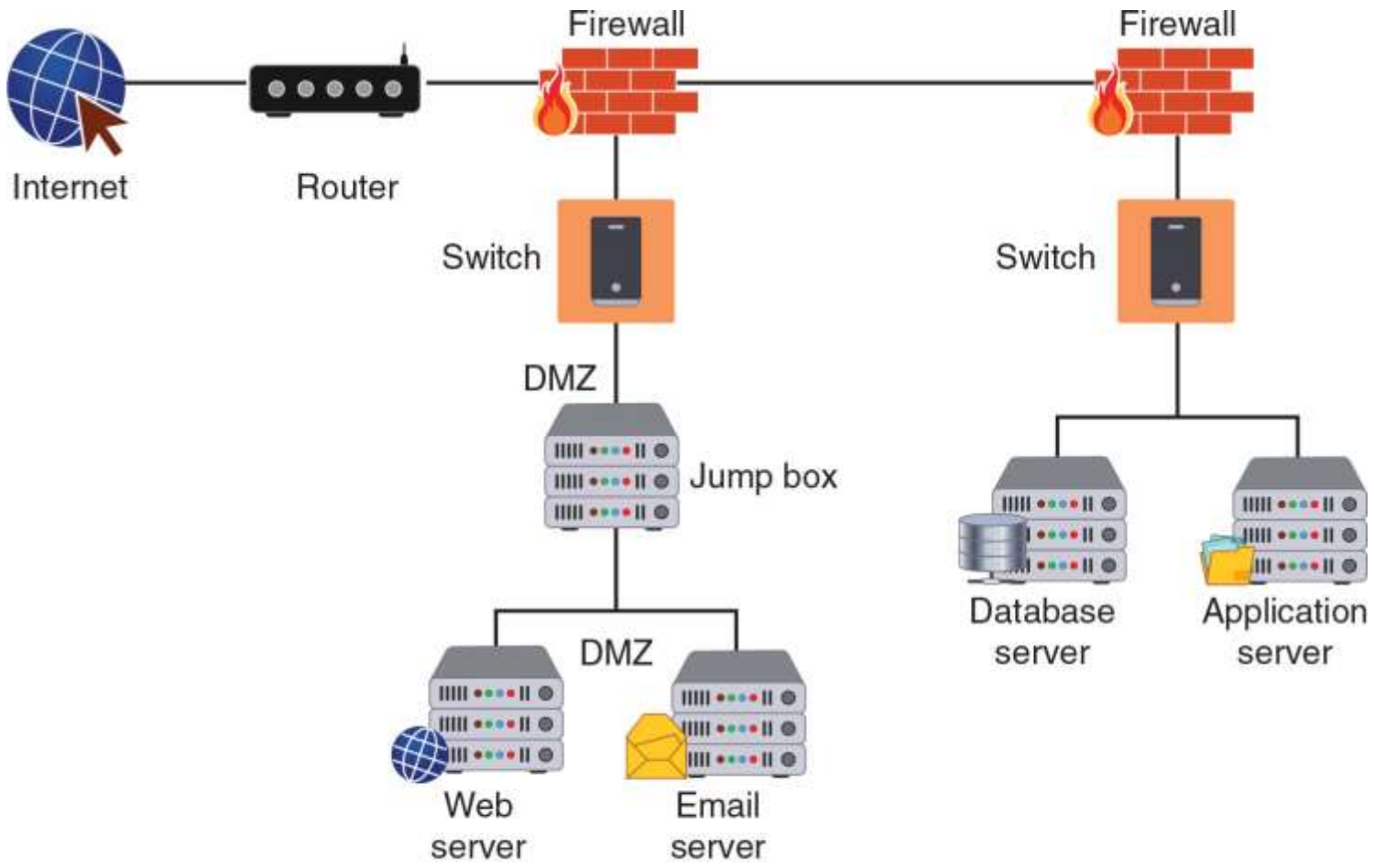

Figure 9-13 Jump box

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)