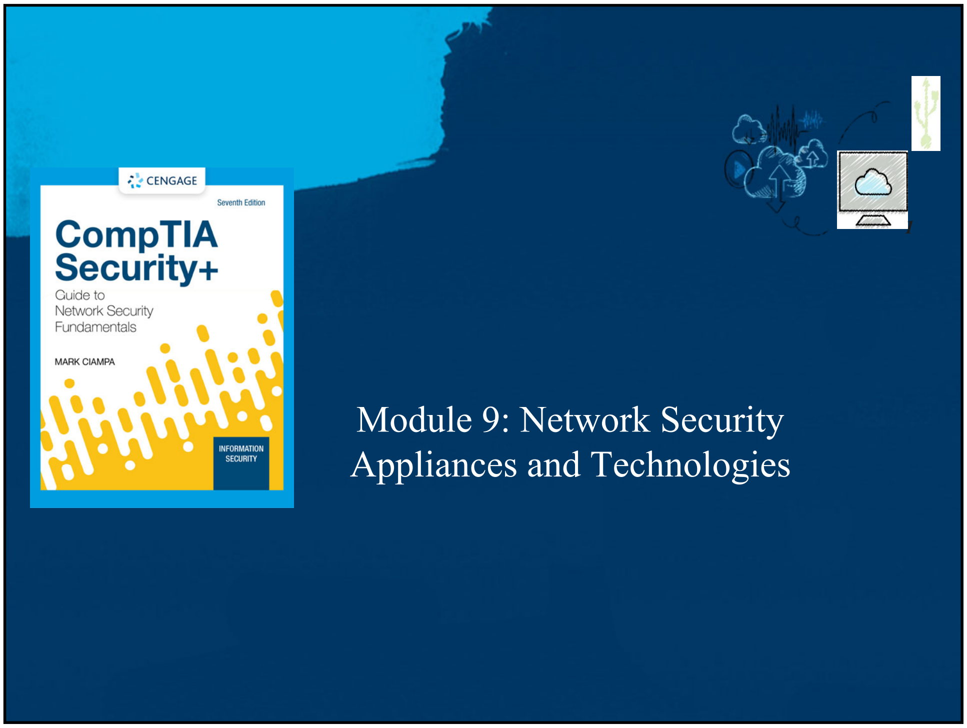
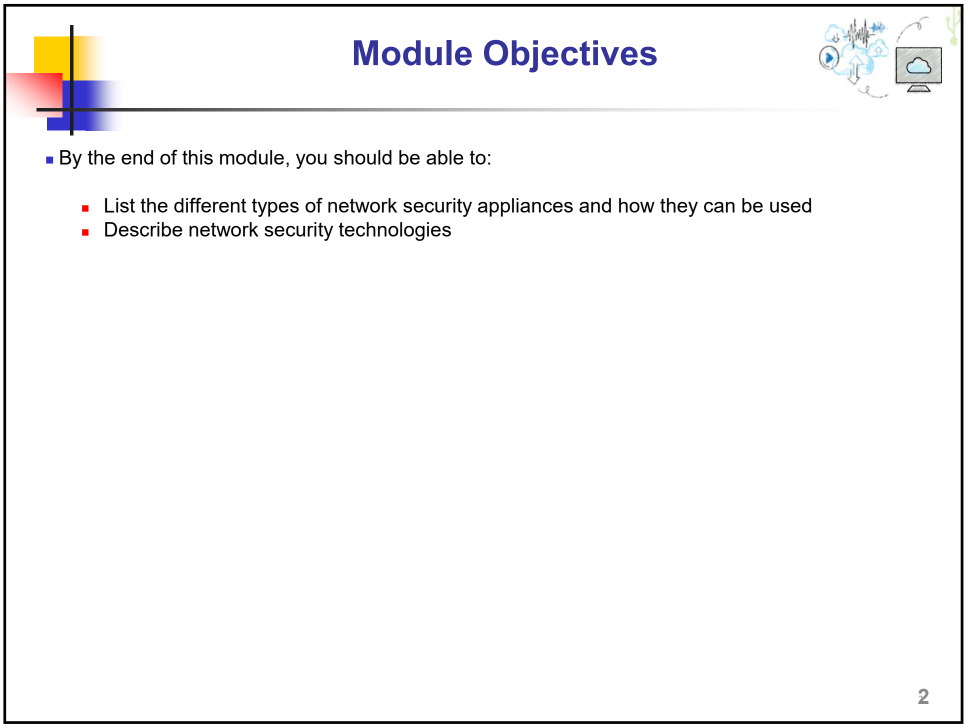


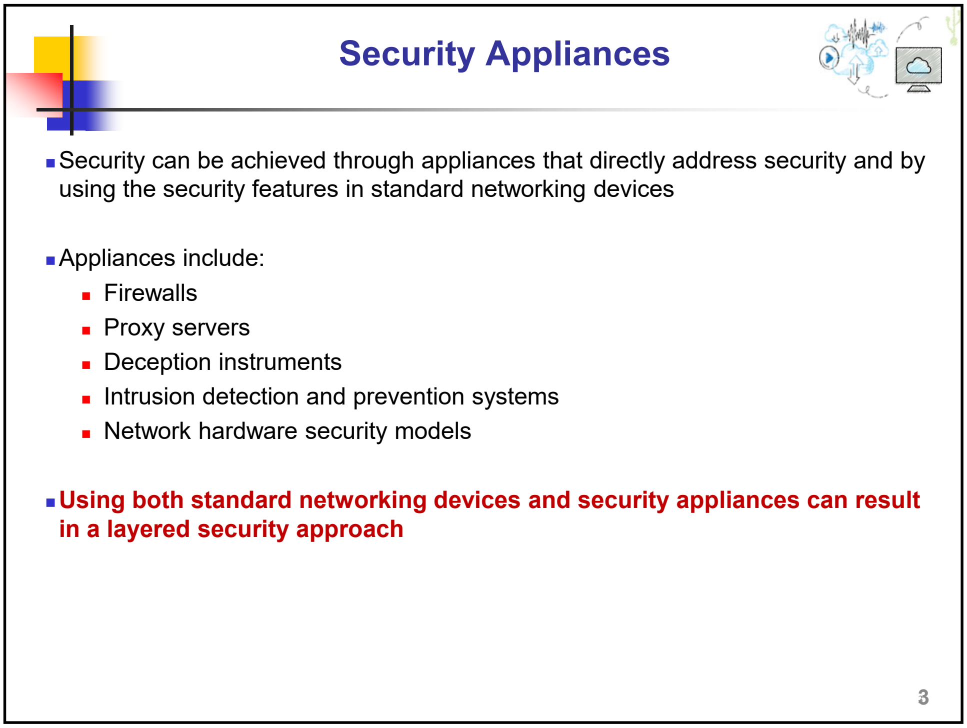
Module 9: Network Security Appliances and Technologies



Module Objectives

- By the end of this module, you should be able to:
  - List the different types of network security appliances and how they can be used
  - Describe network security technologies

2

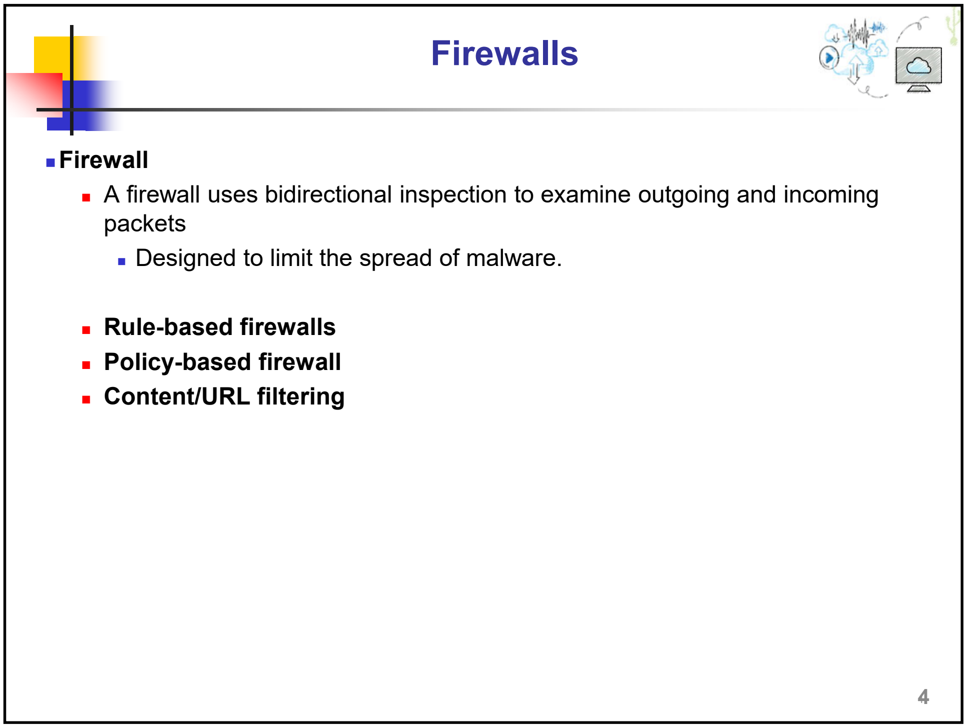


Security Appliances

- Security can be achieved through appliances that directly address security and by using the security features in standard networking devices

- Appliances include:
  - Firewalls
  - Proxy servers
  - Deception instruments
  - Intrusion detection and prevention systems
  - Network hardware security models

- **Using both standard networking devices and security appliances can result in a layered security approach**



Firewalls

- **Firewall**
  - A firewall uses bidirectional inspection to examine outgoing and incoming packets
    - Designed to limit the spread of malware.

  - **Rule-based firewalls**
  - **Policy-based firewall**
  - **Content/URL filtering**

- **Rule-based firewalls**
  - Actions are based on specific criteria or rules
    - *Source address*.
    - *Destination address*.
    - *Source port*.
    - *Destination port*.
    - *Protocol*.
    - *Direction*. (*Incoming*, *Outgoing*, or *Both*).
    - *Time*.
      - Rules can be set so they are active only during a scheduled time.
    - *Context*. : A rule can be created that is unique for specific circumstances (contexts).
      - For example, different rules may be in effect depending on whether a laptop is on-site or is remote (sometimes called **geographical consideration**).
    - *Action*. The action setting indicates what the firewall should do when the conditions of the rule are met

Firewalls

- **Policy-based firewall**
  - A more flexible type of firewall which allows more generic statements instead of specific rules
  - Allows more generic statements instead of specific rules.
    - For example, the policy statement
      - *Allow management traffic from trusted networks*
    - could translate into specific rules that allow traffic
      - from *192.2.0.0/24* to *TCP Port 22* and *192.2.100.0/24* to *TCP Port 3389*.

- **Content/URL filtering**
  - Monitor websites accessed through HTTP to create custom filtering profiles.
  - The filtering can be performed by assessing webpages by their content category and then creating whitelists and blacklists of specific URLs.

Firewalls

- **Firewall Categories**
  - *Stateful vs. stateless*
  - *Open source vs. proprietary*

- **Stateless packet filtering**
  - Filter firewall might allow a packet to pass through because it met all the necessary criteria (rules),

- **Stateful packet filtering**
  - Uses both the firewall rules and the state of the connection:
  - Keeps a record of the state of a connection between an internal endpoint and an external device.

Firewalls

- **Firewall Categories**
  - *Stateful vs. stateless*
  - *Open source vs. proprietary*

- **Open source**
  - Some firewalls are freely available.
  - Gaining wider acceptance as they incorporate more features and are built on a secure foundation.
  - For example, pfSense

- **Proprietary**
  - Owned by an entity that has an exclusive right to

Firewalls

- **Firewall Categories**
  - *Hardware vs. software*

- **Software firewall**
  - Runs as a program or service on a device, such as a computer or router.
  - A malware infection on the device on which it is running, such as a computer, could also compromise the software firewall.

- **Hardware firewalls**
  - Specialized separate devices that inspect traffic
  - Tend to have more features but are more expensive
  - Require more effort to configure and manage.
  - Footprint is smaller (to provide less of a target for attackers) or specialized.

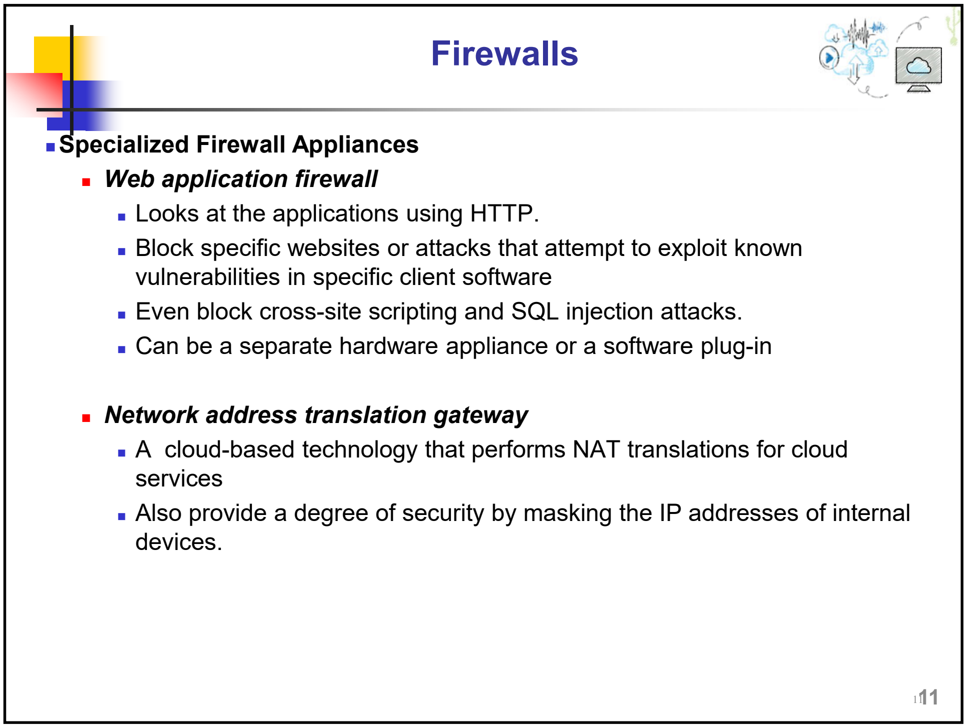
Firewalls

- **Firewall Categories**
  - *Host vs. appliance vs. virtual*

- **Host-based firewall**
  - A software firewall that runs on and protects a single endpoint device (a host). All modern OSs include a host-based firewall.
  - These firewalls tend to be application-centric: users can create an opening in the firewall for each specific application.
    - Only open when the application requires it and is then closed.
  - This approach is more secure than permanently opening a port in the firewall

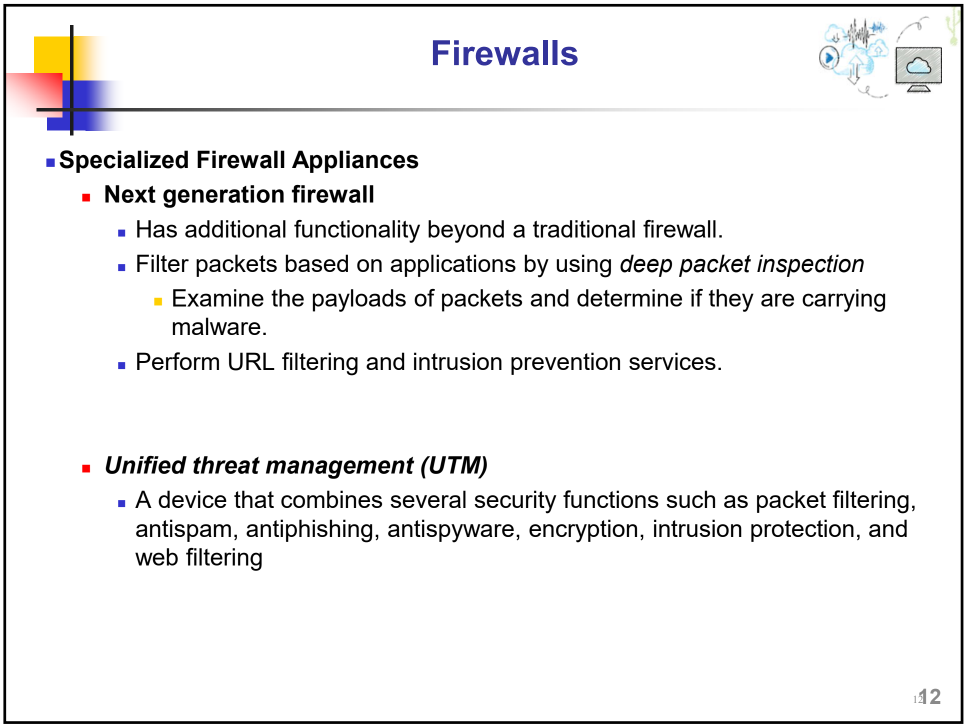
- **An appliance firewall**
  - A separate hardware device designed to protect an entire network

- **Virtual firewall**
  - Runs in the cloud.
  - Designed for settings, such as public cloud environments, in which deploying an appliance firewall would be difficult or even impossible.



Firewalls

- **Specialized Firewall Appliances**
  - ***Web application firewall***
    - Looks at the applications using HTTP.
    - Block specific websites or attacks that attempt to exploit known vulnerabilities in specific client software
    - Even block cross-site scripting and SQL injection attacks.
    - Can be a separate hardware appliance or a software plug-in
  - ***Network address translation gateway***
    - A cloud-based technology that performs NAT translations for cloud services
    - Also provide a degree of security by masking the IP addresses of internal devices.



Firewalls

- **Specialized Firewall Appliances**
  - **Next generation firewall**
    - Has additional functionality beyond a traditional firewall.
    - Filter packets based on applications by using *deep packet inspection*
      - Examine the payloads of packets and determine if they are carrying malware.
    - Perform URL filtering and intrusion prevention services.
  - ***Unified threat management (UTM)***
    - A device that combines several security functions such as packet filtering, antispam, antiphishing, antispyware, encryption, intrusion protection, and web filtering

Proxy Servers

- **Proxies**
  - Devices that act as substitutes on behalf of the primary device
  - 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
- **Forward proxy**
  - A computer or an application that intercepts user requests from the internal secure network and processes the requests on behalf of the user
- **Reverse proxy**
  - Routes requests coming from an external network to the correct internal server

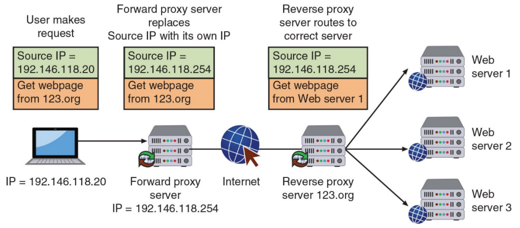
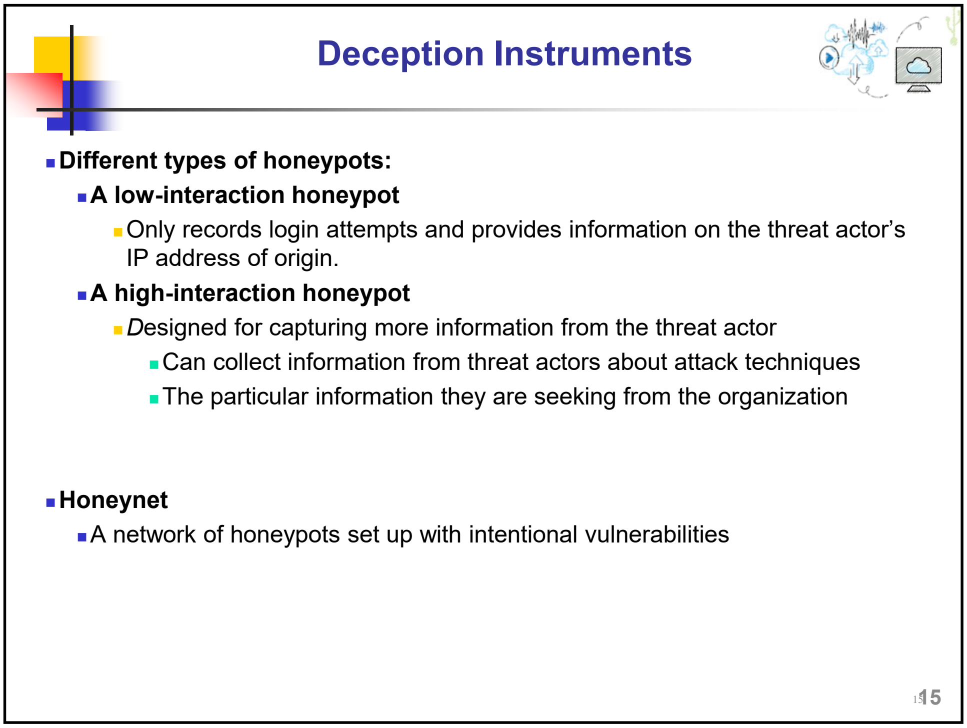

User makes request
Forward proxy server replaces Source IP with its own IP
Reverse proxy server routes to correct server
Source IP = 192.146.118.20
Get webpage from 123.org
Source IP = 192.146.118.254
Get webpage from 123.org
Source IP = 192.146.118.254
Get webpage from Web server 1
IP = 192.146.118.20
Forward proxy server
IP = 192.146.118.254
Internet
Reverse proxy server 123.org
Web server 1
Web server 2
Web server 3

Figure 9-5 Forward and reverse proxy servers

Deception Instruments

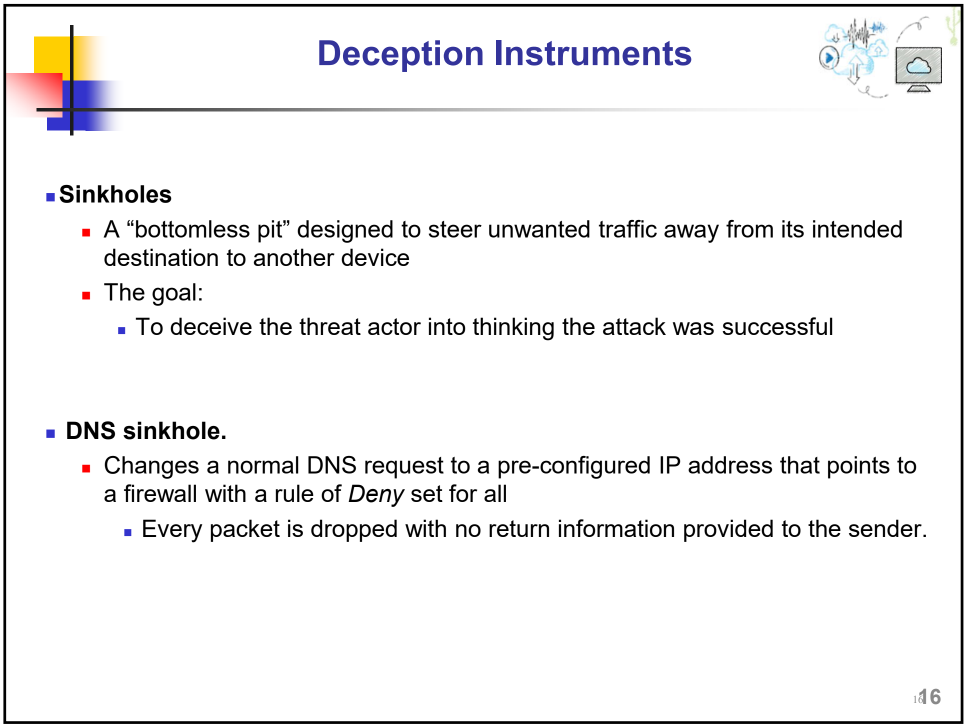
- **Deception**
  - Used as a security defense
  - By directing threat actors away from a valuable asset to something that has little or no value
- **Network deception**
  - Involve creating and using honeypots and sinkholes
- **Honeypots**
  - A computer located in an area with limited security that serves as "bait" to threat actors
- **Two goals of using a honeypot:**
  - **Deflect**
    - Redirect threat actors' attention away from legitimate servers
    - Encouraging them to spend their time and energy on the decoy server,
    - Distract their attention from the data on the actual server.
  - **Discover.**
    - Trick threat actors into revealing their attack techniques.
    - Security experts can then determine if actual production systems could thwart such an attack.



Deception Instruments

- **Different types of honeypots:**
  - **A low-interaction honeypot**
    - Only records login attempts and provides information on the threat actor’s IP address of origin.
  - **A high-interaction honeypot**
    - *D*esigned for capturing more information from the threat actor
      - Can collect information from threat actors about attack techniques
      - The particular information they are seeking from the organization
- **Honeynet**
  - A network of honeypots set up with intentional vulnerabilities

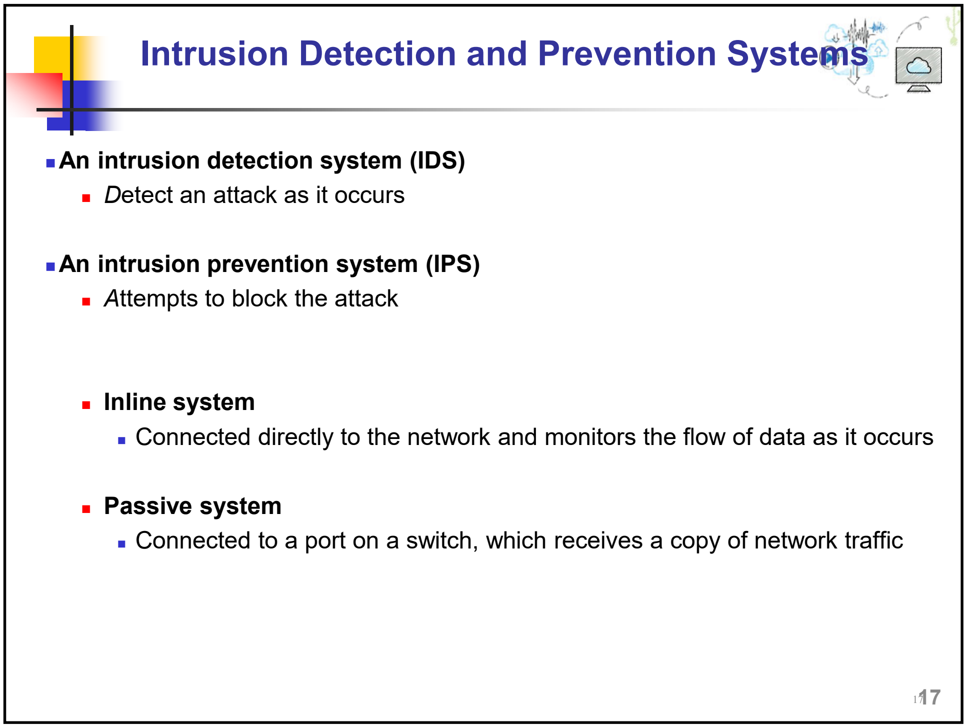
15



Deception Instruments

- **Sinkholes**
  - A “bottomless pit” designed to steer unwanted traffic away from its intended destination to another device
  - The goal:
    - To deceive the threat actor into thinking the attack was successful
- **DNS sinkhole.**
  - Changes a normal DNS request to a pre-configured IP address that points to a firewall with a rule of *Deny* set for all
    - Every packet is dropped with no return information provided to the sender.

16



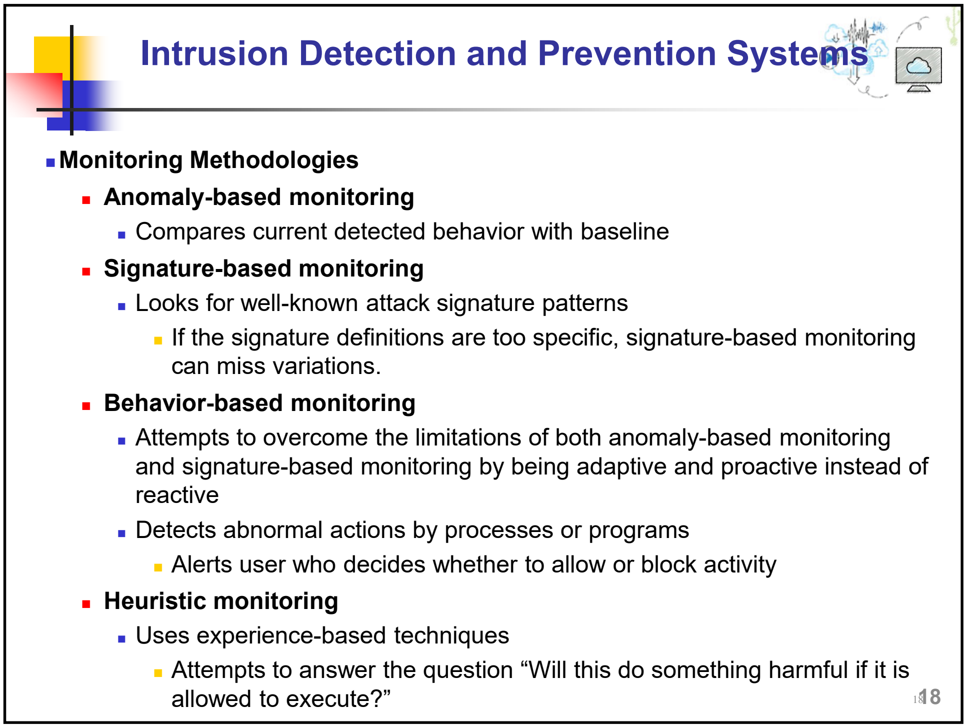
Intrusion Detection and Prevention Systems

- **An intrusion detection system (IDS)**
  - *D*etect an attack as it occurs

- **An intrusion prevention system (IPS)**
  - *A*ttempts to block the attack

  - **Inline system**
    - Connected directly to the network and monitors the flow of data as it occurs

  - **Passive system**
    - Connected to a port on a switch, which receives a copy of network traffic



Intrusion Detection and Prevention Systems

- **Monitoring Methodologies**
  - **Anomaly-based monitoring**
    - Compares current detected behavior with baseline
  - **Signature-based monitoring**
    - Looks for well-known attack signature patterns
      - If the signature definitions are too specific, signature-based monitoring can miss variations.
  - **Behavior-based monitoring**
    - Attempts to overcome the limitations of both anomaly-based monitoring and signature-based monitoring by being adaptive and proactive instead of reactive
    - 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

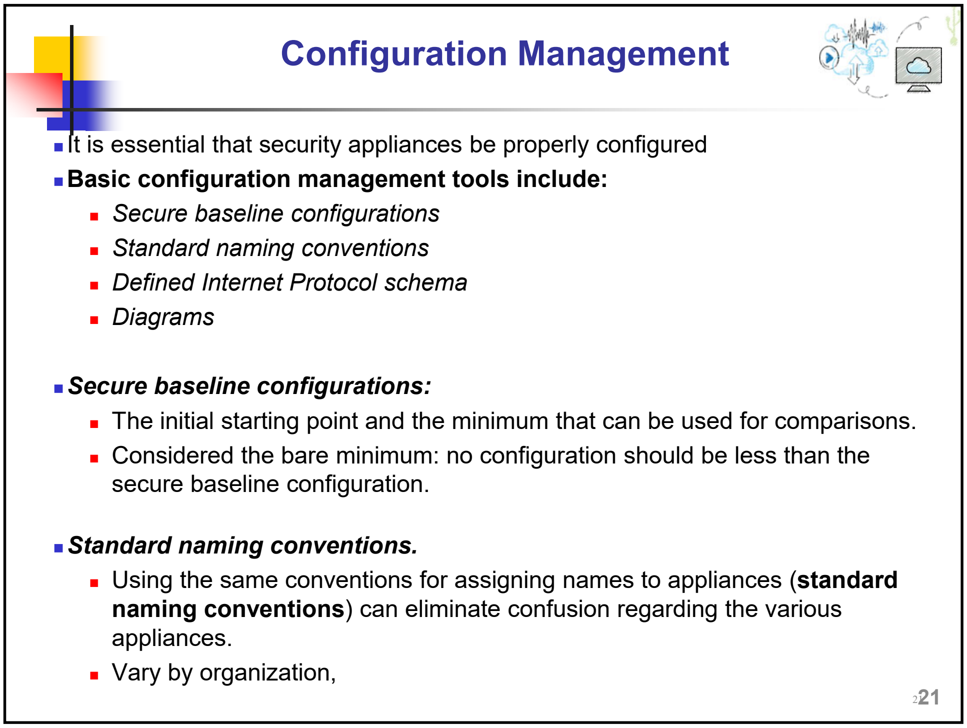
- **Network intrusion detection system (NIDS)**
  - Watches for attacks on the network
  - NIDS sensors installed on firewalls and routers gather information and report back to central device
- **Network intrusion prevention system (NIPS)**
  - Monitors to detect malicious activities and also attempts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

19

Network Hardware Security Modules

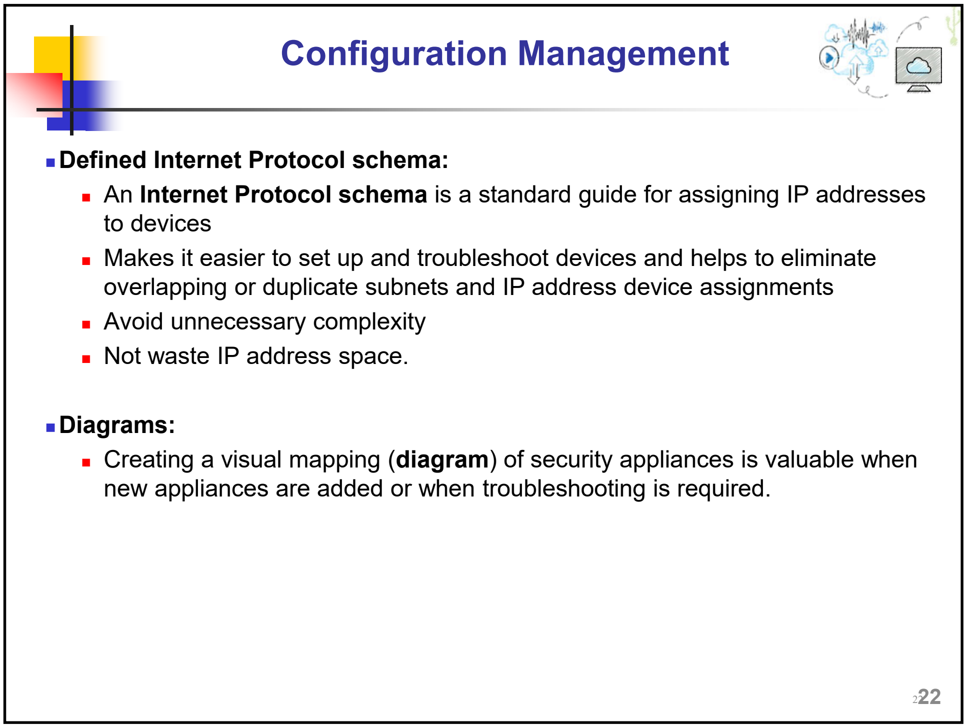
- **A hardware security module (HSM)**
  - *A* removable external cryptographic device
    - For endpoints, an HSM is typically a USB device, an expansion card, or a device that connects directly to a computer through a port
- **Network hardware security module**
  - A special trusted network computer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

20



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*
- ***Secure baseline configurations:***
  - The initial starting point and the minimum that can be used for comparisons.
  - Considered the bare minimum: no configuration should be less than the secure baseline configuration.
- ***Standard naming conventions.***
  - Using the same conventions for assigning names to appliances (**standard naming conventions**) can eliminate confusion regarding the various appliances.
  - Vary by organization,



Configuration Management

- **Defined Internet Protocol schema:**
  - An **Internet Protocol schema** is a standard guide for assigning IP addresses to devices
  - Makes it easier to set up and troubleshoot devices and helps to eliminate overlapping or duplicate subnets and IP address device assignments
  - Avoid unnecessary complexity
  - Not waste IP address space.
- **Diagrams:**
  - Creating a visual mapping (**diagram**) of security appliances is valuable when new appliances are added or when troubleshooting is required.

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

- **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:**
  - **Filesystem ACLs**
    - *F*ilter 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**
  - Used on external routers to restrict vulnerable protocols and limit traffic from entering the network

- **Internal router ACLs**
  - Configured with explicit allow and deny statements for specific addresses and protocol services

Access Technologies

- **Virtual Private Network (VPN)**
  - 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)

Access Technologies

- **Network Access Control (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
  - 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**)

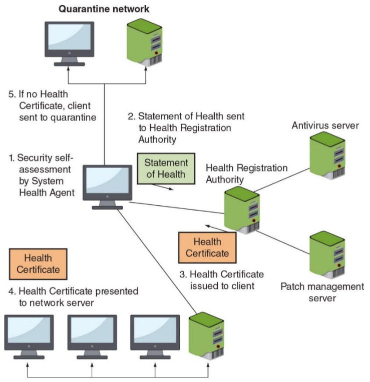
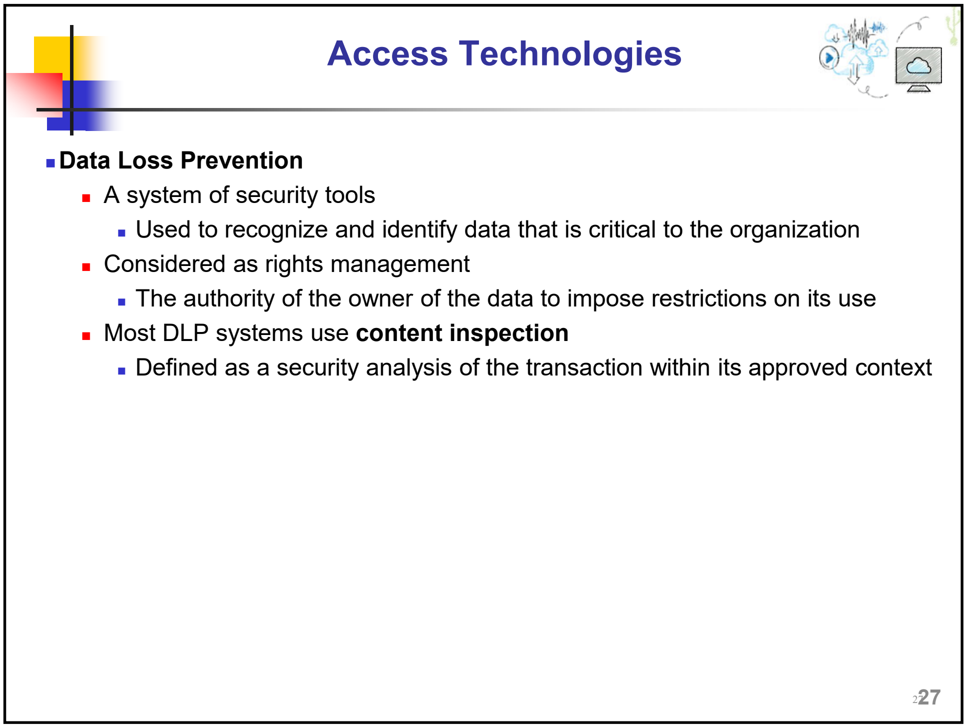
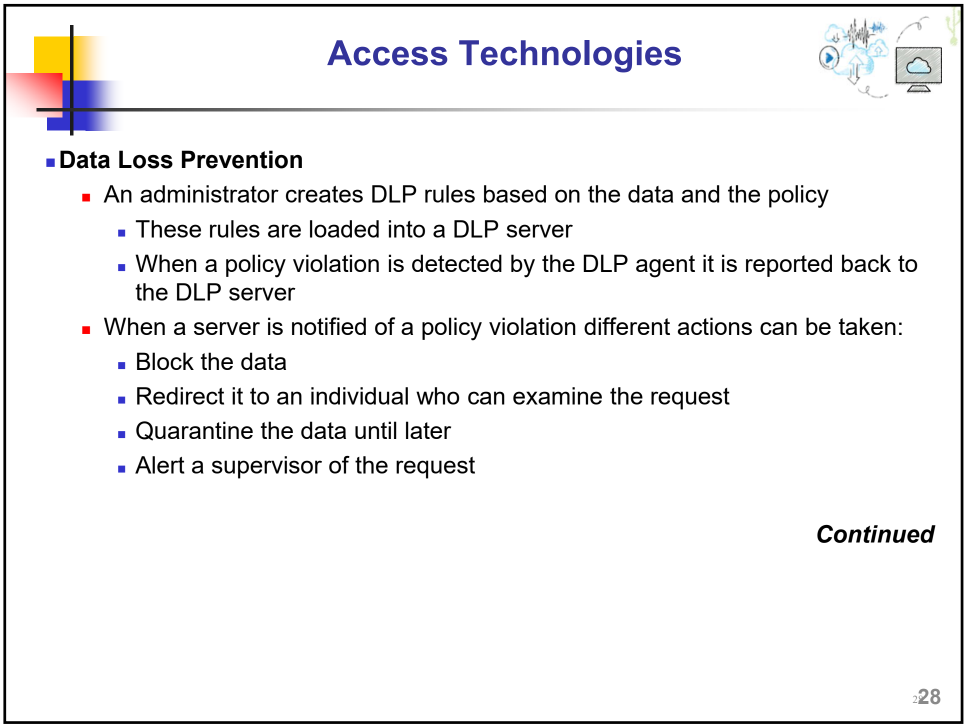

Quarantine network
5. If no Health Certificate, client sent to quarantine
2. Statement of Health sent to Health Registration Authority
Antivirus server
1. Security self-assessment by System Health Agent
Statement of Health
Health Registration Authority
Health Certificate
Health Certificate
3. Health Certificate issued to client
Patch management server
4. Health Certificate presented to network server

Figure 9-7 Network access control (NAC) process



Access Technologies

- **Data Loss Prevention**
  - A system of security tools
    - Used to recognize and identify data that is critical to the organization
  - Considered as rights management
    - The authority of the owner of the data to impose restrictions on its use
  - Most DLP systems use **content inspection**
    - Defined as a security analysis of the transaction within its approved context



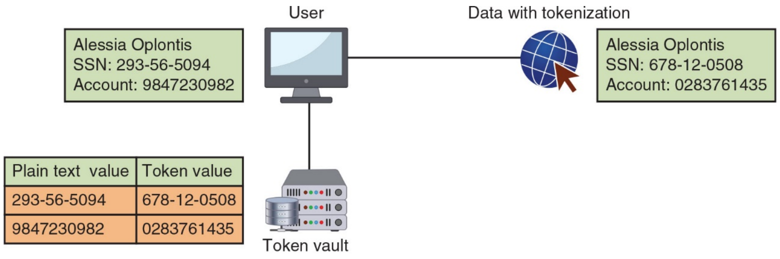
Access Technologies

- **Data Loss Prevention**
  - 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
  - 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

Continued

Access Technologies

- **Data Loss Prevention (contd.)**
  - 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*
      - If the actual data element is needed, it can be retrieved as needed



Plain text value	Token value
293-56-5094	678-12-0508
9847230982	0283761435

Figure 9-8 Tokenization

Technologies for Monitoring and Managing

- **Port Security**
  - Threat actors who access a network device through an unprotected port can reconfigure the device to their advantage

- **Route security**
  - The trust of packets sent through a router
    - False route information can be injected or altered by weak port security

Technologies for Monitoring and Managing

- **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

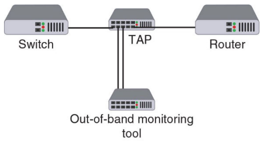


Figure 9-10 Port TAP

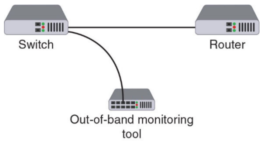


Figure 9-11 Port mirroring

- **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

- **File Integrity Monitors**
  - Examine files to see if they have changed
  - Used for detecting malware as well as maintaining compliance with industry-specific regulations

- **Quality of Service (QoS)**
  - 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

- **Zero trust**
  - A strategic initiative about networks that is designed to prevent successful attacks
  - Recognizes that trust is a vulnerability.
  - Attempts to eliminate the concept of trust from an organization’s network architecture
  - Requires that networks be segmented

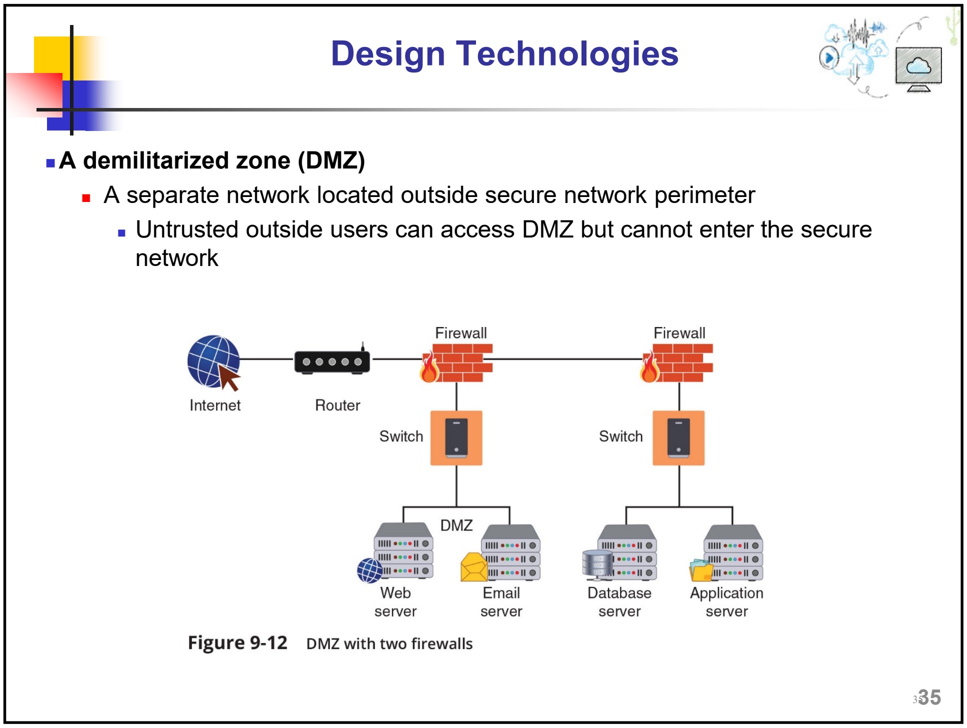
Zero trust is not designed to make a system trusted but, instead, to eliminate trust. The motto of zero trust is “Never trust; always verify.”

33

Design Technologies

- **Network Segmentation**
  - Examples of network segmentation include
    - Virtual LANs
    - Demilitarized zone
- **Virtual LAN (VLAN)**
  - A network segmented by separating devices into logical groups
  - VLANs can be isolated so that sensitive data is transported only to members of the VLAN

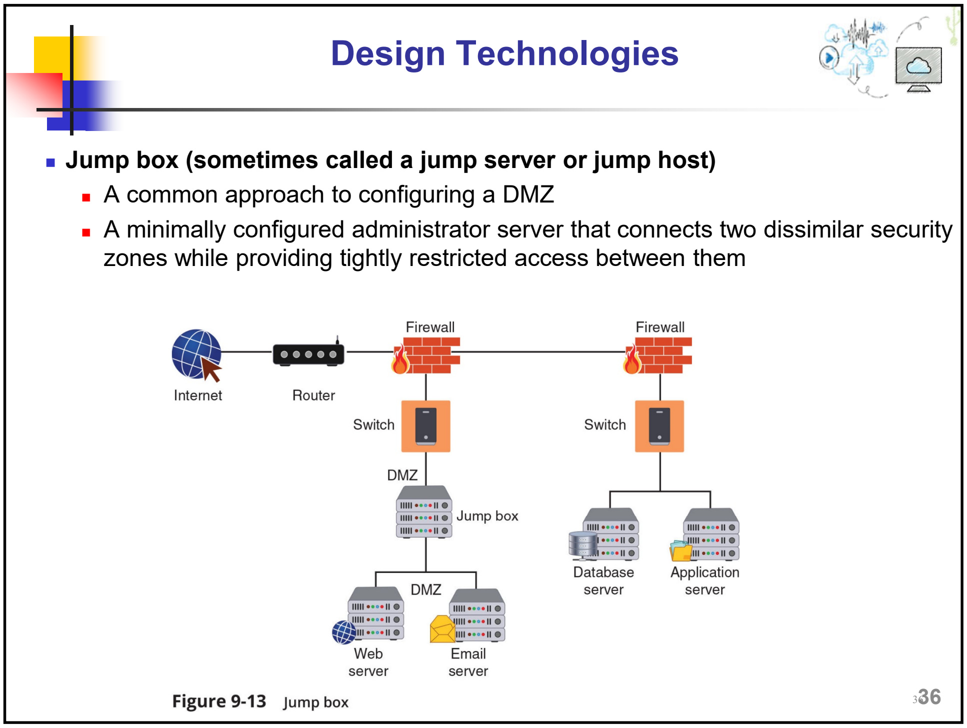
34



Design Technologies

- **A demilitarized zone (DMZ)**
  - A separate network located outside secure network perimeter
    - Untrusted outside users can access DMZ but cannot enter the secure network

Figure 9-12 DMZ with two firewalls



Design Technologies

- **Jump box (sometimes called a jump server or jump host)**
  - A common approach to configuring a DMZ
  - A minimally configured administrator server that connects two dissimilar security zones while providing tightly restricted access between them

Figure 9-13 Jump box

Design Technologies

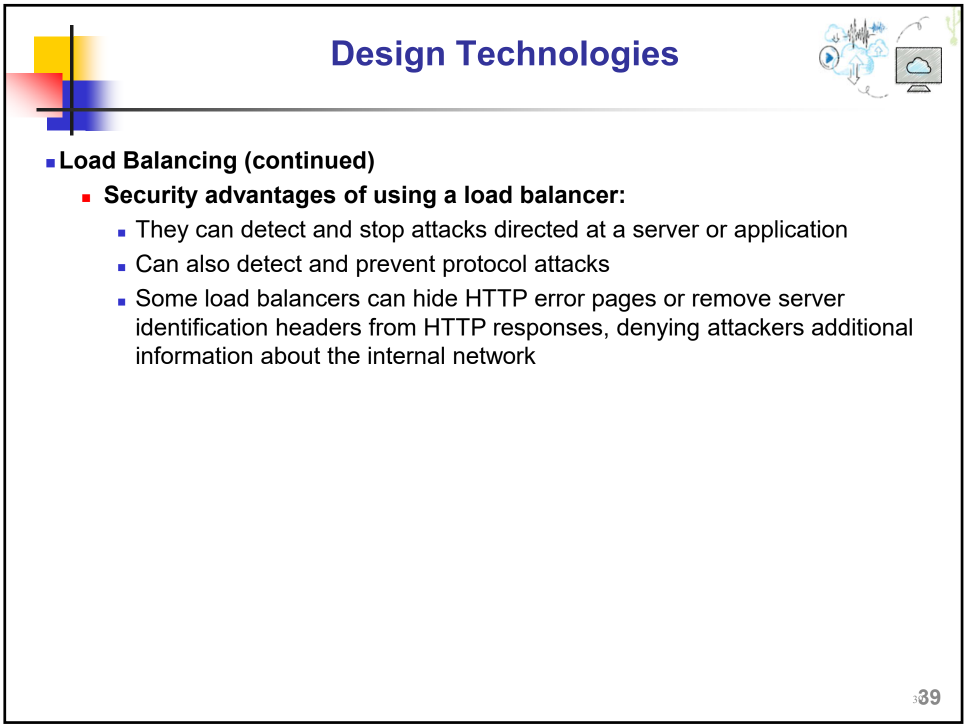
- **Load Balancing**
  - A technology to evenly distribute work across a network and can allocate requests among multiple devices
  - Achieved through software or hardware device (*load balancer*)
  - To the user, this distribution is transparent and appears as if a single server is providing the resources

- **Advantages of load-balancing technology:**
  - Reduces probability of overloading a single server
  - Optimizes bandwidth of network computers

Design Technologies

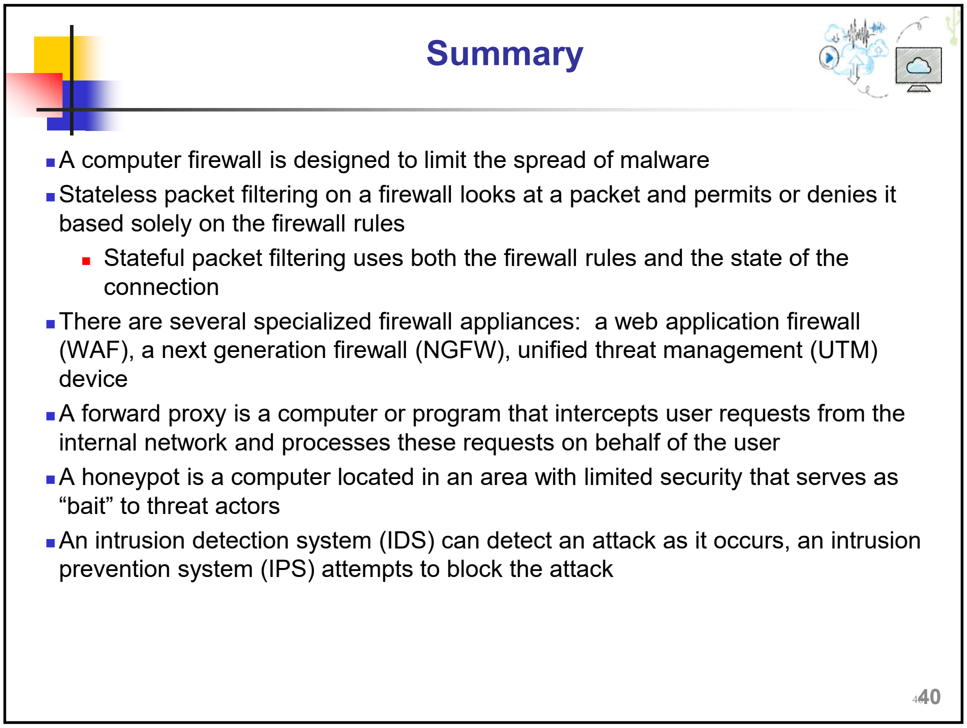
- **Load Balancing (continued)**
  - When multiple load balancers are used together, they can be placed in different configurations that include:
    - In an **active-passive configuration**,
      - the primary load balancer distributes the network traffic to the most suitable server, while the secondary load balancer operates in a “listening mode”
      - 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
    - Help improve the user experience and optimize network resource usage



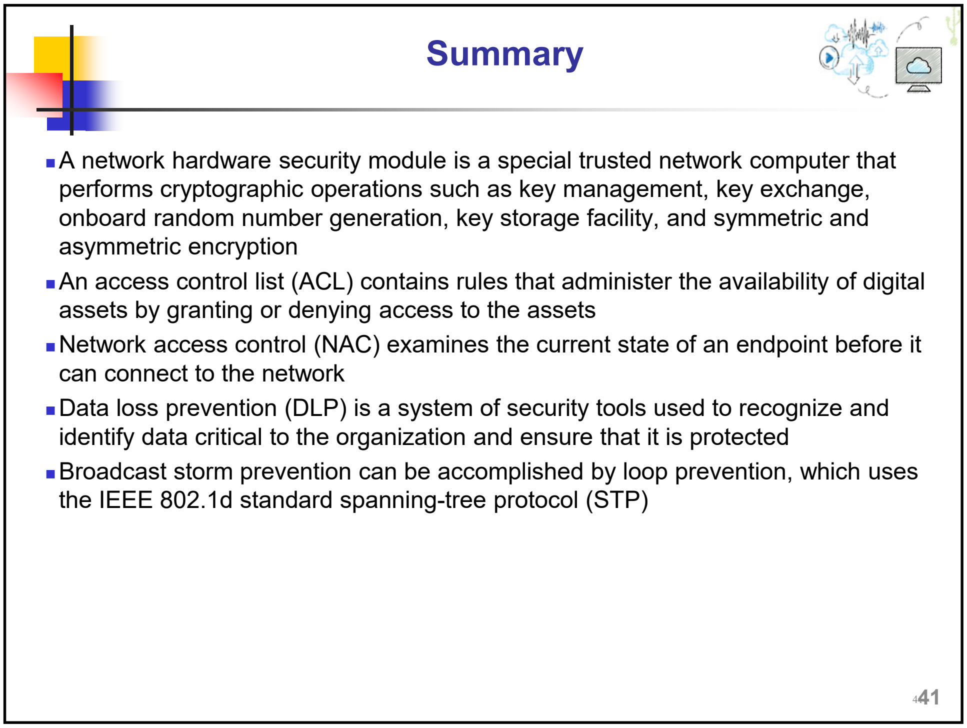
Design Technologies

- **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



Summary

- 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

- 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)