5.1 Network segmentation and VLAN

Network segmentation

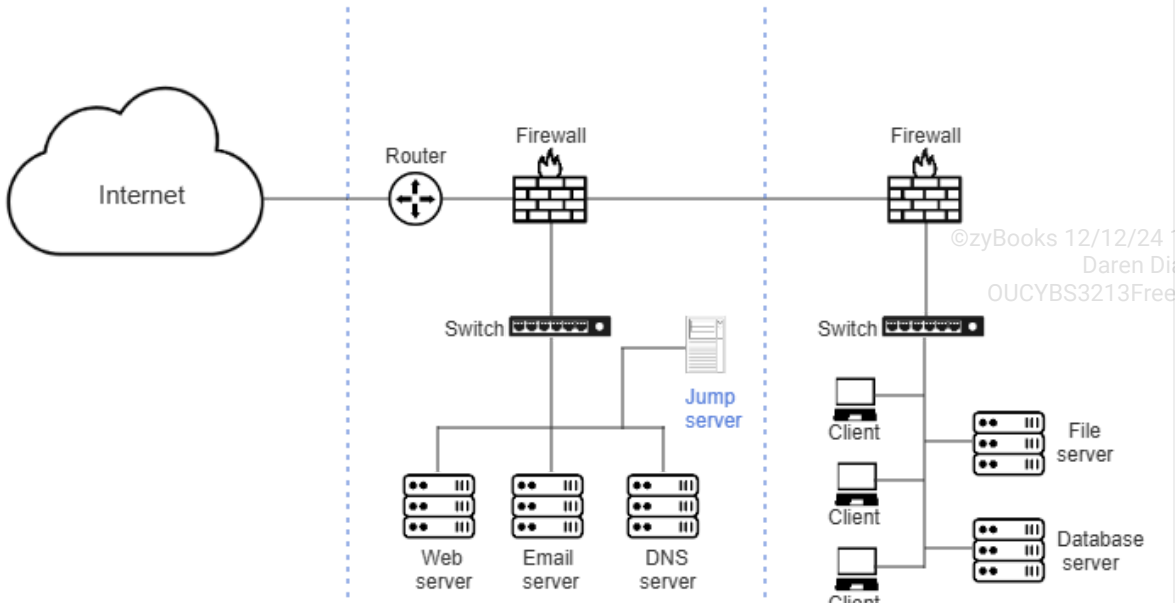
Network segmentation, also known as ***network zoning***, is the act of partitioning a network into segments. Network segmentation is used to create security zones. A ***security zone*** is a network segment that has specific security requirements. A Layer 3 device such as a firewall is used to separate security zones. Ex: A security zone can be defined for a company's internal network. The company's internal network can be separated from the Internet by a firewall.

The network resources in a security zone have the same trust level. Three commonly deployed security zones exist:

- A ***trusted zone***, also known as a ***private zone***, is a security zone that contains protected network resources that should only be accessible by an authorized user or system. A trusted zone has the highest trust level. A network resource in a trusted zone has a private IP address and is unreachable from outside the zone. Ex: A local area network (LAN) is a trusted zone.
- An ***untrusted zone***, also known as a ***public zone***, is a security zone that is outside an organization's control. An untrusted zone has the lowest trust level. Ex: The Internet is an untrusted zone.
- A ***demilitarized zone***, or ***DMZ***, or ***screened subnet***, is a security zone that lies between a trusted and an untrusted zone. A DMZ protects an organization's private network in a trusted zone from untrusted traffic. A DMZ has a higher trust level than an untrusted zone and lower trust level than a trusted zone. Ex: A web, email, or DNS server is commonly placed in a DMZ.

A jump server is used to manage network elements across different security zones. A ***jump server***, also known as a ***jump box*** or ***jump host***, is a minimally configured server in a security zone that is used for managing the hosts in the security zone. A jump server is a bridge between two different but controlled security zones. A jump server is commonly accessed from a host in a different security zone through SSH or remote desktop (RDP). Ex: An administrator in a trusted zone uses a jump server in a DMZ to manage the servers in the DMZ.

PARTICIPATION ACTIVITY 5.1.1: Security zones.



Animation content:

Static image: A diagram split into three vertical sections. The left section is labeled "Untrusted zone" and contains a cloud labeled "Internet". The middle section is labeled "DMZ". The DMZ shows a router connected to the Internet in the Untrusted zone. The router is also connected to a firewall within the DMZ. In the DMZ, the firewall is connected to a switch. The switch connects to three servers labeled "Web server", "Email server", and "DNS server". A Jump server is shown connected to the server connections. The right section is labeled the "Trusted zone". A firewall in the Trusted zone connects to the firewall in the DMZ. In the Trusted zone, the firewall connects to a switch. The switch connects to three client computers and two servers labeled "File server" and "Database server".

Animation captions:

1. The Internet is an untrusted zone or public zone.
2. A demilitarized zone (DMZ), or screened subnet, includes servers that should be accessible from an untrusted zone. A DMZ is protected from an untrusted zone by a firewall.
3. A trusted zone, or private zone, includes protected network resources that should only be accessible by an authorized user or system. A trusted zone is protected from the DMZ by a firewall.
4. A jump server in a DMZ is used to manage the servers in the DMZ.

PARTICIPATION ACTIVITY 5.1.2: Network segmentation.

How to use this tool

Untrusted zone **Demilitarized zone** **Trusted zone**

	A security zone that contains protected network resources that should only be accessible by an authorized user or system.
	A security zone that is outside an organization's control.
	A security zone that lies between a trusted and an untrusted zone.

Reset

PARTICIPATION ACTIVITY 5.1.3: Network segmentation.

1) Which network device is used to separate security zones?
   - Load balancer
   - Hub
   - Firewall

2) Which network device is used to manage servers in a security zone?
   - Switch
   - Jump box
   - Router

3) In which trust zone is an organization's web server located?
   - Trusted
   - Untrusted
   - DMZ

4) In which trust zone is an organization's protected network resources located?
   - Trusted
   - Untrusted
   - DMZ

5) Which trust zone has the highest trust level?
   - Trusted
   - Untrusted
   - DMZ

Virtual local area network (VLAN)

A network can be divided into physical or logical segments. Network devices such as routers and switches enable physical segmentation by partitioning the network into isolated segments using separate hardware systems, ensuring physical isolation between segments.

Logical segmentation is implemented through virtual local area networks (VLANs). A ***virtual local area network (VLAN)*** is a broadcast domain that is segmented at the data link layer. VLANs enable multiple logical networks to coexist on a single physical network infrastructure.

VLANs enable hosts to be assigned to specific network segments based on various criteria:

- ***Port-based VLAN***, also known as ***interface-based VLAN***, or ***static VLAN***, is a VLAN in which a host is connected to a specific switch port that is assigned to a VLAN.
- ***Protocol-based VLAN*** is a VLAN in which protocol types are used to assign a host to a VLAN.
- ***MAC-based VLAN*** is a VLAN in which a host's MAC address is used to assign the host to a VLAN.

A VLAN improves network performance and efficiency by restricting broadcast domains and reducing network latency.

PARTICIPATION ACTIVITY 5.1.4: VLAN.

1) Which network device is used to partition a network into physical segments?
   - Hub
   - Firewall
   - Router

2) Which VLAN type uses switch ports for assigning a host to a VLAN?
   - Port-based
   - Protocol-based
   - MAC-based

3) Which VLAN type may use IP header information to assign a host to a VLAN?
   - Port-based
   - Protocol-based
   - MAC-based

4) Which VLAN type uses a host's hardware characteristic for assigning the host to a VLAN?
   - Port-based
   - Protocol-based
   - MAC-based

5) At which network layer does a VLAN segment a broadcast domain?
   - Layer 1
   - Layer 2
   - Layer 3

©zyBooks 12/12/24 18:03 2172291
Daren Diaz
OUCYBS3213FreezeFall2024

Centralized vs. decentralized network architectures

In centralized network architectures, control and data processing are consolidated at a single point, enhancing management efficiency and simplifying policy enforcement.

However, centralization creates a single point of failure, making the network vulnerable to targeted attacks that could take down the entire network. In contrast, decentralized architectures distribute processing, data storage, and administrative tasks across multiple nodes, enhancing resilience and fault tolerance but complicating security management and data consistency.

5.2 Zero trust

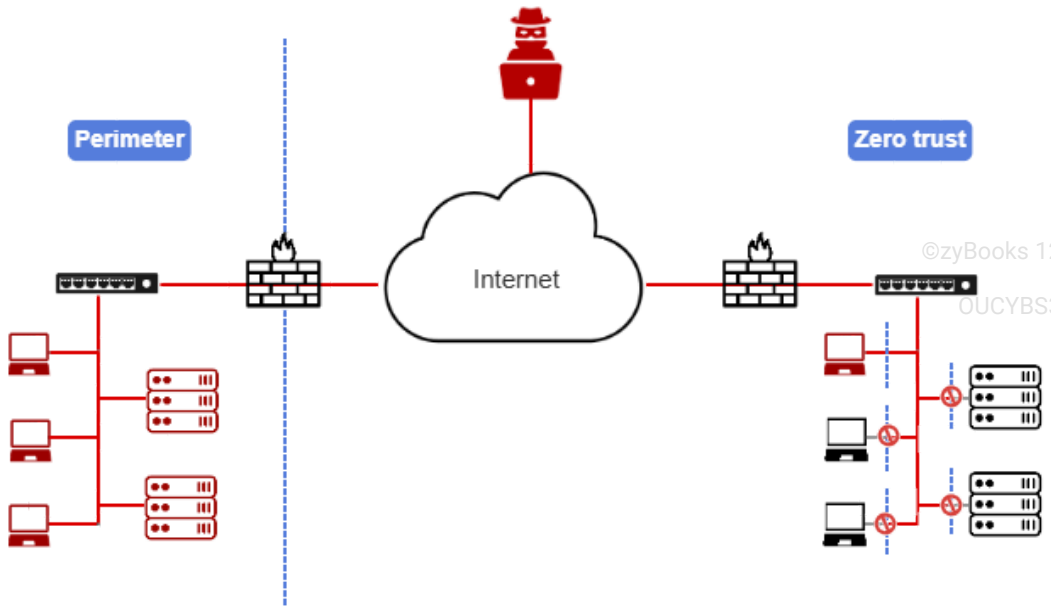
Zero trust framework

Traditional perimeter security operates by trusting internal network users and devices, while blocking external threats. Traditional perimeter security has become insufficient due to the rise of remote work and the increased reliance on cloud-based services. ***Zero trust*** is a security framework that enforces continuous authentication, authorization, and security configuration validation for all users and devices, regardless of proximity to the network perimeter. Zero trust aims to prevent unauthorized access to protected resources by assuming the existence of internal threats. Ex: Internal email server access requires authentication and authorization for all requests, regardless of whether the requesting device is inside or outside the company network perimeter.

A zero trust network follows the principles of the zero trust framework by assuming:

- The network is compromised
- External and internal threats exist on the network
- Device location is not sufficient for deciding trust
- Every device, user, and network flow is authenticated and authorized
- Policies must be dynamic and derived from several data sources

PARTICIPATION ACTIVITY 5.2.1: Perimeter vs. zero trust security.



Animation content:

Static image: Two networks connected to the internet. One network is labeled Perimeter and the other network is labeled Zero trust.
Step 1: Traditional perimeter security provides protection from external threats by creating a trusted zone within a guarded perimeter.
The perimeter network includes a firewall connected to the internet, a switch connected to the firewall, and three laptops and two servers connected to the switch. A dashed line runs through the firewall to separate the network from the internet.
Step 2: If an attacker gains access to one device in the trusted zone, the attacker can move laterally to access other devices within the trusted zone.
An attacker appears and a red line goes from the attacker to the internet. A red line then goes from the internet, through the firewall and switch, and to the first laptop. The laptop turns red. Red lines move from the red laptop to the other two laptops and the two servers. The other two laptops and the two servers turn red.
Step 3: Zero trust security provides protection from internal and external threats by requiring authentication and authorization for all network traffic, regardless of a device's location.
The zero trust network includes a firewall connected to the internet, a switch connected to the firewall, and three laptops and two servers connected to the switch. A dashed line is in front of each of the laptops and servers.
Step 4: Even if an attacker gains access to one device on the network, the attacker cannot move laterally because all network traffic requires authentication and authorization.
A red line goes from the internet, through the zero trust firewall and switch, and to the first laptop. The laptop turns red. Red lines move from the red laptop toward the other two laptops and the two servers, but are stopped at each dashed line before the laptops and servers. An access denied icon appears in front of the other two laptops and servers.

Animation captions:

1. Traditional perimeter security provides protection from external threats by creating a trusted zone within a guarded perimeter.
2. If an attacker gains access to one device in the trusted zone, the attacker can move laterally to access other devices within the trusted zone.
3. Zero trust security provides protection from internal and external threats by requiring authentication and authorization for all network traffic, regardless of a device's location.
4. Even if an attacker gains access to one device on the network, the attacker cannot move laterally because all network traffic requires authentication and authorization.

PARTICIPATION ACTIVITY 5.2.2: Zero trust principles.

1) In a zero trust network, trust is determined by _____.

   - ○ device IP address
   - ○ device location

- device, user, and application contexts

2) By eliminating the idea of a "trusted zone," zero trust prevents _____, an effective attack technique against perimeter security.
   - brute force
   - lateral movement
   - phishing

3) A zero trust network requires authentication and authorization for _____ network traffic.
   - all
   - incoming
   - outgoing

Zero trust network components

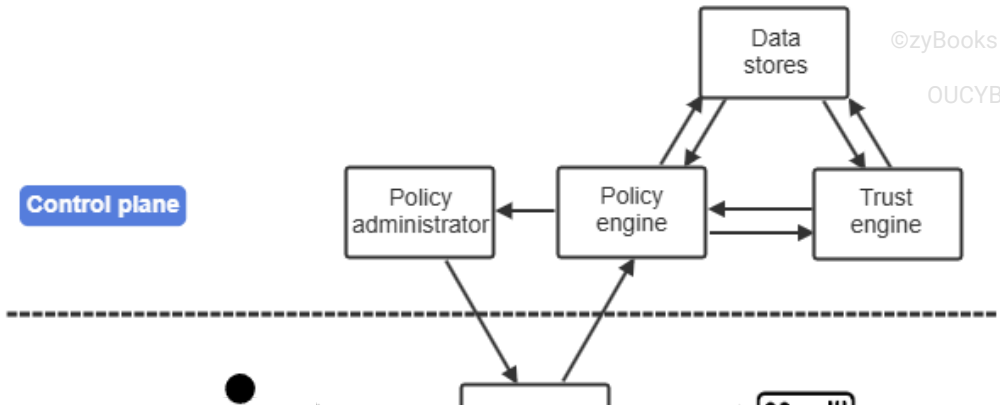
A zero trust network includes a control plane and a data plane. The ***control plane*** is responsible for managing authentication, authorization, and policy enforcement for network access. The control plane includes:

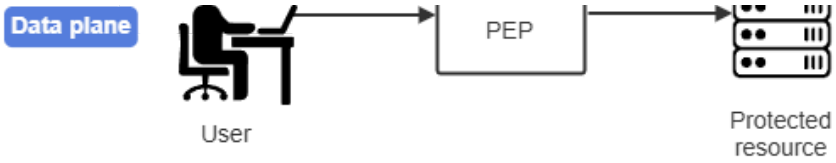
- Policy engine - The component that determines the application of policy for each request.
- Trust engine - The component that scores device and user trust.
- Data stores - The components that store authentication data for the requesting device and user.
- Policy administrator - The component that administers policy decisions, establishing or blocking connections to protected resources.

The ***data plane*** is responsible for enforcing security policies and controlling data access within the network. The data plane includes:

- Device and user - The components requesting access to protected resources.
- Policy enforcement point (PEP) - The component that enforces policy decisions.
- Protected resources - The component representing assets secured by policy enforcement.

PARTICIPATION ACTIVITY 5.2.3: Zero trust components.





Animation content:

Static image: A diagram showing the flow of data from a user to a server.
Step 1: A user requests access to a protected resource. The request is intercepted by a policy enforcement point (PEP).
An area labeled Data plane is separated by a dashed line from an area labeled Control plane. The data plane contains a user, a PEP, and a server. An arrow moves from the user's laptop to the PEP.
Step 2: The PEP sends the request to the policy engine. The policy engine communicates with the trust engine and data stores to determine whether access should be granted.
A policy engine appears in the control plane. An arrow moves from the PEP in the data plane to the policy engine in the control plane. A trust engine and data stores appear in the control plane. Arrows move from the policy engine to the trust engine and data stores. Arrows move between the trust engine and data stores. Arrows move from the trust engine and data stores back to the policy engine.
Step 3: The policy engine sends the decision to the policy administrator. The policy administrator establishes a secure connection to the protected resource if access is granted.
A policy administrator appears in the control plane. An arrow moves from the policy engine to the policy administrator. An arrow moves from the policy administrator to the PEP in the data plane. An arrow moves from the PEP to the server.

Animation captions:

1. A user requests access to a protected resource. The request is intercepted by a policy enforcement point (PEP).
2. The PEP sends the request to the policy engine. The policy engine communicates with the trust engine and data stores to determine whether access should be granted.
3. The policy engine sends the decision to the policy administrator. The policy administrator establishes a secure connection to the protected resource if access is granted.

PARTICIPATION ACTIVITY 5.2.4: Data flow in a zero trust network.

Order the path of data from a user request to a protected resource.

How to use this tool

Unused blocks	Zero trust data flow
Policy engine	Move blocks here
Data stores	
Protected resource	
Trust engine	
Policy engine	

PEP

User/device

Policy administrator

PEP

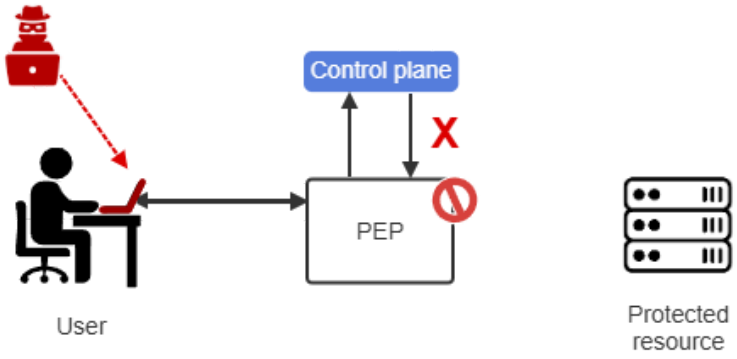
0 of 9 blocks correct

Zero trust authorization

In a zero trust network, fine-grained, dynamic policies control access based on resource and user/device trust scores. Applying policy against multiple data sources allows for granular authentication decisions, which improves the network's overall security and user experience. Ex: A login from an employee's new laptop prompts additional authentication for accessing a sensitive database, while allowing access to the employee's calendar.

All access is granted on a temporary basis, requiring users and devices to undergo regular reauthorization. Changes in a user's or device's trust score may result in connection blocking or necessitate additional authentication.

PARTICIPATION ACTIVITY 5.2.5: Determining trust.



Animation content:

Static image: A user attempting to access a server through a PEP.
Step 1: A user requests access to a protected resource. The request is sent to the control plane.
An arrow moves from the user's laptop to the PEP. An arrow moves from the PEP to the control plane.
Step 2: The control plane determines the user and device can be trusted, so access is granted. A secure connection is established between the user and the protected resource.
An arrow moves from the control plane to the PEP and a green check mark appears. An arrow moves from the PEP to the server.
Step 3: An attacker installs malware onto the device.
An attacker appears. A red arrow moves from the attacker to the user's laptop. The laptop turns red.
Step 4: When the control plane attempts to reauthorize, the device is no longer trusted due to the presence of malware. Access is denied and the connection is blocked.
An arrow moves from the PEP to the control plane. An arrow moves from the control plane to the PEP and a red X appears. An access denied icon appears, and the arrow between the PEP and the server disappears.

Animation captions:

1. A user requests access to a protected resource. The request is sent to the control plane.
2. The control plane determines the user and device can be trusted, so access is granted. A secure connection is established between the user and the protected resource.
3. An attacker installs malware onto the device.
4. When the control plane attempts to reauthorize, the device is no longer trusted due to the presence of malware. Access is denied and the connection is blocked.

PARTICIPATION ACTIVITY 5.2.6: Zero trust authorization.

1) A user's trust score would be reduced by _____.
   - accessing resources during working hours
   - logins on multiple devices on the same network
   - multiple failed login attempts

2) A zero trust network protects against unknown threats by _____.
   - calculating trust scores using multiple factors
   - incorporating threat intelligence into policy decisions
   - preventing malware-infected devices from accessing protected resources

3) The use of fine-grained policies based on multiple factors supports implementation of _____.
   - microsegmentation
   - multi-factor authentication (MFA)
   - the principle of least privilege

Air-gapped networks

*An **air-gapped** network physically isolates a network segment from the internet and all other unsecured networks, preventing unauthorized access through wired or wireless connections. Physical isolation is commonly used in high-security environments, such as military facilities and critical infrastructure systems, where sensitive data protection is*

vital. Security provided by air-gapping is highly effective at preventing data breaches, requiring physical presence and manual intervention for data transfer.

5.3 Firewalls: Types and security appliances

Firewall

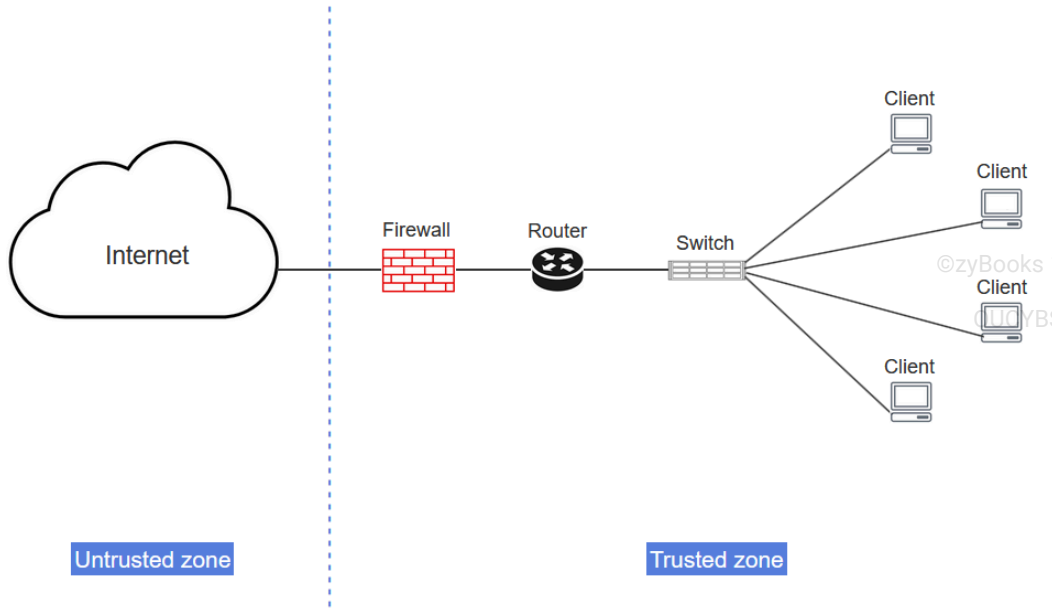
A ***firewall*** is a network device or a software program that controls inbound and outbound traffic based on a set of rules. A firewall rule can be general or specific. Ex: A general rule may allow inbound and outbound HTTP traffic on port 80 and a specific rule may block inbound traffic from IP address 192.168.74.12 on port 22. A firewall is used to separate two security zones. Ex: A firewall separates an organization's trusted internal network from an untrusted network, such as the Internet.

A firewall can be implemented in hardware or software. A ***hardware firewall***, also known as an ***appliance firewall***, is a firewall that is implemented in a physical device. A hardware firewall has a dedicated processor, memory, and operating system. A hardware firewall has fast response times and the ability to handle high traffic loads. A ***software firewall*** is a firewall that is implemented in software and runs on a general purpose computer. A software firewall typically costs less and is slower than a hardware firewall.

Both hardware and software firewalls must handle unexpected situations, such as system crashes or software failures. Firewall failure modes:

- ***Fail-open*** configuration allows traffic to flow freely if the firewall fails, ensuring uninterrupted access to critical network services while potentially exposing the network to security threats during downtime.
- ***Fail-closed*** configuration blocks all traffic when the firewall fails, enhancing security by preventing unauthorized access during such periods, but risking disruption of legitimate network activity.

Example 5.3.1: A firewall separates two security zones.



An ***open-source firewall*** is a software firewall with freely available source code that can be modified and redistributed. Ex: pfSense is an open-source firewall. A ***proprietary firewall*** is a firewall that is built by an entity that has exclusive rights to the firewall. Ex: Cisco Adaptive Security Appliance (ASA) series are proprietary hardware firewalls.

PARTICIPATION ACTIVITY 5.3.1: Firewalls.

1) A firewall can block inbound network traffic based on a set of rules.
   - False
   - True

2) A software firewall cannot be used to separate two security zones.
   - False
   - True

3) An appliance firewall has a dedicated operating system.
   - False
   - True

4) A software firewall is typically faster than a hardware firewall.
   - False
   - True

5) An open-source firewall cannot be modified.
   - False
   - True

PARTICIPATION ACTIVITY 5.3.2: Firewalls.

How to use this tool

Hardware firewall **Proprietary firewall** **Open-source firewall** **Software firewall**

	A firewall that is implemented in a physical device.
	A firewall that runs on a general purpose computer.

	A software firewall with freely available source code that can be modified and redistributed.
	A firewall that is built by an entity that has exclusive rights to the firewall.

Reset

Firewall types

A ***stateless firewall***, also known as a ***packet filter***, is a firewall that allows or blocks a packet based on the information in the packet header. The information in a packet header includes source and destination IP addresses, port numbers, and protocol type. A stateless firewall inspects a packet independently from other packets and does not track traffic flows. A stateless firewall uses an access control list (ACL) to decide which type of traffic should be allowed or blocked. An ***access control list (ACL)*** is a list of rules used by a firewall to control inbound and outbound network traffic. Ex: A stateless firewall may block packets with destination IP address 182.168.68.18, or allow packets with source IP address 191.21.8.4.

A ***stateful firewall***, also known as a ***dynamic packet filter***, is a firewall that monitors and tracks active network connection sessions and blocks a packet that does not belong to an active session. A stateful firewall continuously analyzes the state or context of traffic on a network. A stateful firewall stores a connection session's information in a state table and uses the information to make packet filtering decisions. Ex: A stateful firewall creates a state table entry for a TCP stream and allows a packet that belongs to the TCP stream to pass through the firewall.

PARTICIPATION ACTIVITY 5.3.3: Firewall types.

Which firewall type is used in each of the following scenarios?

1) A firewall that blocks traffic from IP address 191.18.2.3.
   - ○ Stateless
   - ○ Stateful

2) A firewall that keeps track of a TCP session by using source and destination IP addresses, port numbers, and IP flags.
   - ○ Stateless
   - ○ Stateful

3) A firewall that only allows UDP traffic with source IP address 191.39.5.34 and destination IP address 191.38.31.79.
   - ○ Stateless
   - ○ Stateful

4) A firewall that allows a DNS response packet from an IP address by keeping

track of a DNS request packet's destination IP address.

- Stateless
- Stateful

5) A firewall that uses an access control list (ACL).

- Stateless
- Stateful

PARTICIPATION ACTIVITY 5.3.4: Firewall types.

How to use this tool

Stateful firewall **Stateless firewall** **Access control list (ACL)**

	A firewall that makes a packet filtering decision based on the information in a packet header.
	A firewall that monitors and tracks active network connection sessions and blocks a packet that does not belong to an active session. A.
	A list of allowed and blocked rules used by a firewall to control inbound and outbound network traffic.

Reset

Network security appliance

A network security appliance combines the functionality of several devices to improve network security and simplify the management of those devices. A ***unified threat management (UTM)*** is a security appliance that provides multiple security functions at a single point on a network. A UTM appliance provides a wide range of services, including network firewalling, intrusion detection and prevention, malware detection and removal, DDoS protection, and web, content, and e-mail filtering. A UTM simplifies security management by enabling an administrator to manage a wide range of security functions from a single console.

A ***next-generation firewall (NGFW)*** is a firewall that combines the functionality of a packet filtering firewall with other technologies to detect and block a network attack. An NGFW can enforce security policies at application, port and protocol levels. An NGFW may have the capability to inspect encrypted traffic, detect and block malware, and perform deep packet inspection (DPI). DPI enables a NGFW to inspect the data within a packet and identify and block a malicious packet. A NGFW may have the ability to act on real-time information provided by threat intelligence services to block new threats.

PARTICIPATION ACTIVITY 5.3.5: Network security appliances.

1) A UTM improves network security but does not simplify device management.
   - False
   - True

2) A NGFW can detect and remove malware from a network.
   - False
   - True

3) An NGFW cannot block a malicious packet.
   - False
   - True

Network access control (NAC)

Network access control (NAC) *is a security mechanism that manages access to a network by authenticating users and devices, enforcing access policies, and ensuring devices comply with security standards. NAC can be implemented as a standalone solution, or as a feature or add-on to a firewall. When integrated with a firewall, NAC can leverage the firewall's existing infrastructure and policies, making NAC an effective tool for enforcing network security.*

NAC is often used with the 802.1X port security standard to improve access control in LAN and WLAN environments. Ex: In a corporate network, a NAC system might restrict an employee's device from accessing sensitive company data until validating that the device has the latest security patches and antivirus software installed, ensuring that only compliant devices can connect to network resources.

CHALLENGE ACTIVITY 5.3.1: Firewalls.

581480.4344582.qx3zqy7

Start

Select the firewall type in each scenario.

A firewall that blocks all TCP packets.

Pick

A firewall that monitors the state of traffic on a network.

Pick

A firewall that does not track traffic flows.

Pick

A firewall that filters a packet based on the packet's source IP address.

Pick

1 2

Check Next

5.4 Firewalls: Host-based, virtual, and application

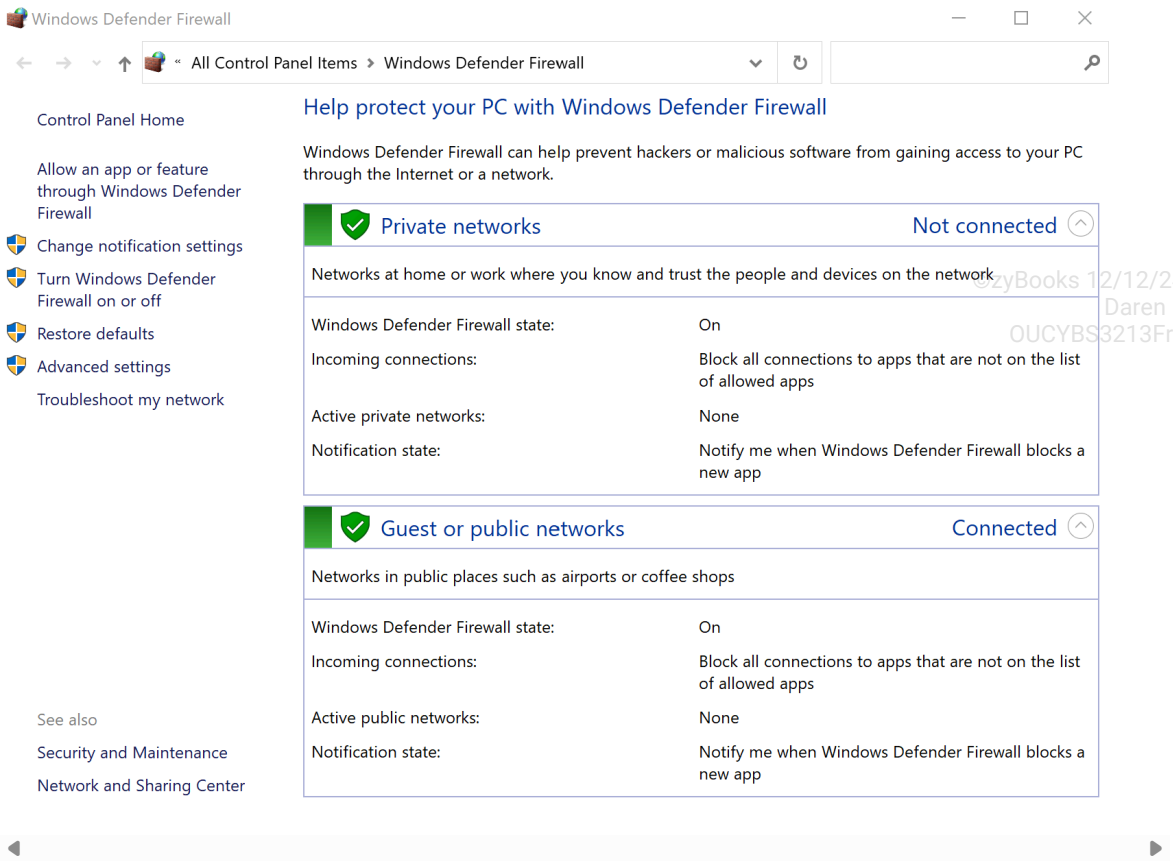
Virtual and host-based firewalls

A firewall can monitor and filter inbound and outbound network traffic on virtual machines. A ***virtual firewall*** is a software or hardware firewall that provides packet filtering within a virtualized environment. A virtual firewall can operate in two modes:

- ***Bridge mode*** is a virtual firewall mode in which a firewall runs on a virtual machine and monitors and controls inbound/outbound traffic on the virtual machine.
- ***Hypervisor mode*** is a virtual firewall mode in which a firewall resides in a host's hypervisor kernel and monitors and controls inbound/outbound traffic on the virtual machines running on the host.

A ***host-based firewall*** is a software firewall that runs on a host and controls the host's inbound and outbound network traffic. Most modern operating systems include a host-based firewall. Ex: Windows Defender Firewall in Windows 10 is a host-based firewall. A host-based firewall can have application-specific security rules. Ex: A host-based firewall may permit inbound traffic to an application on port 40 and block inbound traffic to another application on the same port.

Example 5.4.1: Windows Defender Firewall.



PARTICIPATION ACTIVITY 5.4.1: Virtual and host-based firewalls.

1) In which mode does a virtual firewall run on a virtual machine and monitor inbound and outbound traffic on the virtual machine?
   - Bridge
   - Hypervisor

2) What type of network traffic does a host-based firewall control?
   - Inbound and outbound traffic on a network
   - Inbound and outbound traffic on a host

3) A host-based firewall can both allow and block traffic on the same port.
   - False
   - True

Applications and devices for traffic control

A ***network address translation (NAT) gateway*** is a device that enables multiple hosts with private IP addresses to connect to the Internet using a single public IP address. A NAT gateway acts as an intermediary between a group of hosts on an internal network and an external network. A NAT gateway is not a firewall but provides a security layer for an internal network by masking a private network's IP addresses. By default, a NAT gateway does not allow an external device to initiate an inbound connection. Ex: A NAT gateway can be used to enable virtual machines on a cloud VLAN to connect to the Internet.

A firewall can be used to protect an application. An ***application firewall*** is a firewall that controls an application's input and output. An application firewall can control communications at the application layer (OSI Layer 7). A ***web application firewall (WAF)*** is a specific form of application firewall that monitors and filters HTTP and HTTPS traffic between a web application and the Internet. A WAF protects a web application from application layer attacks, such as SQL injection attacks.

PARTICIPATION ACTIVITY 5.4.2: Applications and devices for traffic control.

How to use this tool

Host-based firewall | **Virtual firewall** | **Application firewall** | **NAT gateway** | **Web application firewall**

	A firewall that controls an application's input and output.
	A specific form of application firewall that monitors and filters HTTP and HTTPS traffic between a web application and the Internet.
	A device that enables multiple hosts with private IP addresses to connect to the Internet using a single public IP address..
	A software or hardware firewall that provides packet filtering within a virtualized environment.
	A software firewall that runs on a host and controls the host's inbound and outbound network traffic.

Reset

Web filtering

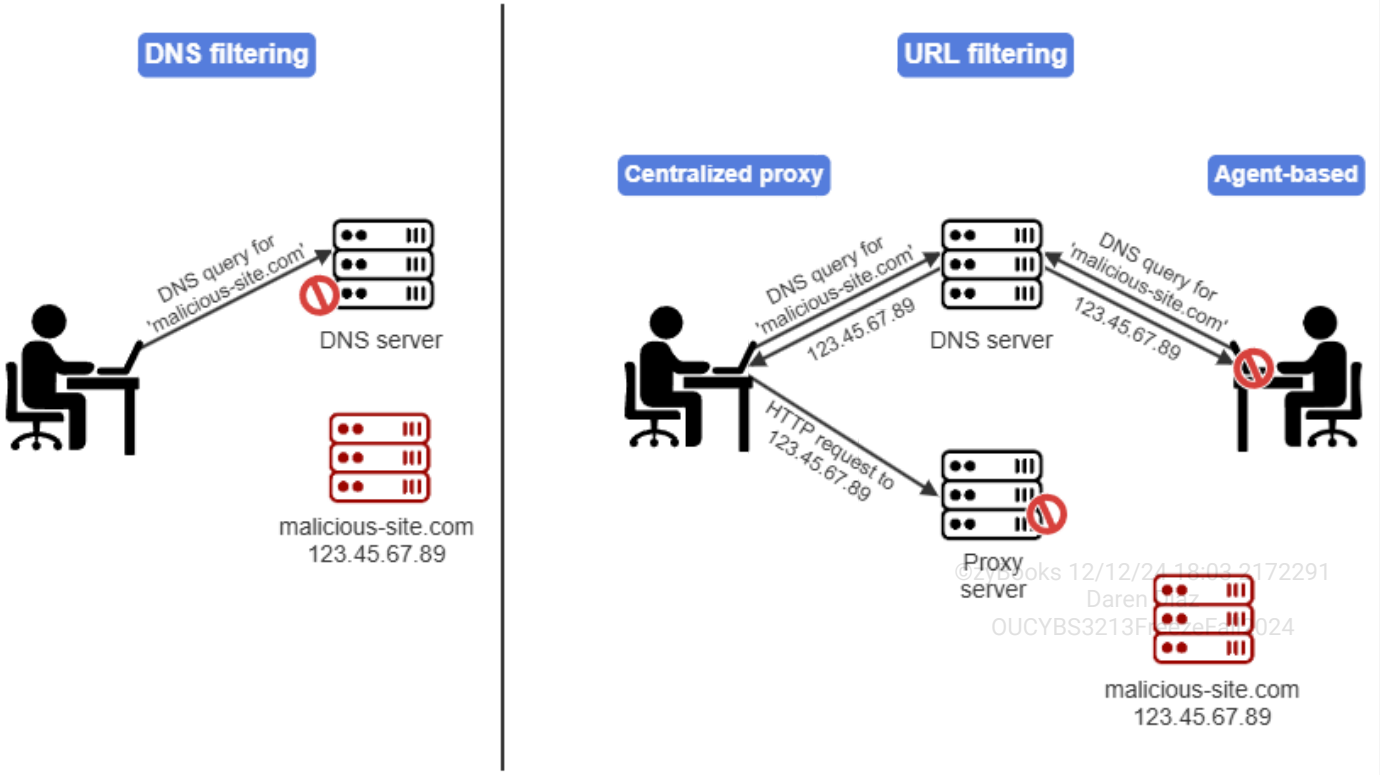
A firewall may have the capability to filter web resources. Web filtering is critical for protecting organizational resources from potential threats. Three web filtering methods exist:

- ***DNS filtering*** is a web filtering method that blocks access to specific webpages by preventing the resolution of DNS queries for blocked domains. Ex: An organization adds youtube.com to the DNS filter's blocklist. When an employee attempts to go to www.youtube.com, the DNS server refuses to resolve youtube.com to an IP address and redirects the employee to a page stating that the content is blocked.
- ***URL filtering*** is a web filtering method that blocks access to a specific webpage based on the webpage URL. Ex: An organization allows employees to view work-related YouTube videos but adds all other YouTube URLs to the URL filter's blocklist. When an employee attempts to connect to a YouTube URL for a work-related video, the page loads. However, when an employee attempts to connect to a YouTube URL for an unapproved video, access is denied.
- ***Content filtering*** is a web filtering method that controls access to web content based on the requested content and predefined criteria. Ex: When an employee visits a webpage with an embedded YouTube video, an organization's content filter blocks the video content, while allowing the rest of the webpage to load.

To simplify web filter management, block rules can be created to automatically block content without adding each URL or domain to the blocklist. Web pages are automatically analyzed and categorized so that a block rule can block all content in a given category. Ex: An organization's web filter is configured to block social networking sites, so www.facebook.com is automatically blocked without being explicitly added to the blocklist.

A web filter can also decide to allow or block a webpage based on the URL's reputation as trustworthy or risky. A website with a history of stealing personal information or spreading malware is marked as risky, whereas a well-known website without any history of suspicious activity is considered trustworthy. A URL scan can also detect the presence of malicious code and deem a webpage risky.

PARTICIPATION ACTIVITY 5.4.3: Web filtering.



Animation content:

Static figure: DNS filtering and URL filtering processes.
Step 1: DNS filtering is implemented on a DNS server. When a user attempts to access a trusted site, the DNS server resolves the domain to the domain's IP address so that the user's HTTP request is correctly routed.
A scenario labeled DNS filtering is shown with a user on a laptop, a DNS server, and a server labeled "trusted-site.com, 123.45.67.88." The user's laptop sends a DNS query for 'trusted-site.com' to the DNS server. The DNS server sends "123.45.67.88" to the user's laptop. The user's laptop sends an HTTP request to the trusted-site.com server.
Step 2: If the requested domain is on the DNS filter's blocklist, the DNS server refuses to resolve the DNS query.
The trusted-site.com server is replaced with a red server labeled "malicious-site.com, 123.45.67.89." The user's laptop sends a DNS query for 'malicous-site.com' to the DNS server. The DNS server refuses to respond.
Step 3: URL filtering can be implemented on a centralized proxy or agent-based software on the user's device. A centralized proxy approach sends all HTTP requests through a proxy server.
A scenario labeled URL filtering, Centralized proxy is shown with a user on a laptop, a DNS server, a proxy server, and a server labeled "trusted-site.com, 123.45.67.88." The user's laptop sends a DNS query for 'trusted-site.com' to the DNS server. The DNS server sends "123.45.67.88" to the user's laptop. The user's laptop sends a request to the proxy server to forward an HTTP request to 123.45.67.88. The proxy server sends an HTTP request to the trusted-site.com server.
Step 4: The URL filter is applied by the proxy server. Unauthorized requests are blocked.
The trusted-site.com server is replaced with a red server labeled "malicious-site.com, 123.45.67.89." The user's laptop sends a DNS query for 'malicous-site.com' to the DNS server. The DNS server sends "123.45.67.89" to the user's laptop. The user's laptop sends a request to the proxy server to forward an HTTP request to 123.45.67.89. The proxy server blocks the HTTP request.
Step 5: An agent-based URL filter blocks the HTTP request directly on the user's device.
A scenario labeled URL filtering, Agent-based is shown with a user on a laptop, a DNS server, and a red server labeled "malicious-site.com, 123.45.67.89." The user's laptop sends a DNS query for 'malicous-site.com' to the DNS server. The DNS server sends "123.45.67.89" to the user's laptop. The user's laptop blocks the HTTP request.

Animation captions:

1. DNS filtering is implemented on a DNS server. When a user attempts to access a trusted site, the DNS server resolves the domain to the domain's IP address so that the user's HTTP request is correctly routed.
2. If the requested domain is on the DNS filter's blocklist, the DNS server refuses to resolve the DNS query.
3. URL filtering can be implemented on a centralized proxy or agent-based software on the user's device. A centralized proxy approach sends all HTTP requests through a proxy server.
4. The URL filter is applied by the proxy server. Unauthorized requests are blocked.
5. An agent-based URL filter blocks the HTTP request directly on the user's device.

PARTICIPATION ACTIVITY 5.4.4: Web filtering.

Select the filtering method used to block the specified web resource.

1) Any webpage that contains the string "how to create malware"

- DNS filtering
- URL filtering
- Content filtering

2) Any webpage associated with the domain "malware-spreader.com"

- DNS filtering
- URL filtering
- Content filtering

3) Embedded ads

- DNS filtering
- URL filtering
- Content filtering

4) The sports section of a news website

- DNS filtering
- URL filtering
- Content filtering

5.5 Network intrusion detection and prevention systems (NIDS/NIPS)

Intrusion detection system (IDS)

An ***intrusion detection system (IDS)*** is a device or a software application that uses sensors to detect a malicious activity or a security policy violation in a system. Two types of IDS exist:

- A ***network intrusion detection system (NIDS)*** is an IDS that detects a threat to a network. A NIDS uses sensors, collectors, and aggregators to monitor and analyze network traffic and detect malicious network activity. Ex: Snort is a software NIDS.
- A ***host-based intrusion detection system (HIDS)*** is an IDS that detects a threat to a host. A HIDS monitors and analyzes a host's running processes, network traffic to and from a host, and a host's log files to detect a threat. Ex: A security information management (SIM) system running on a host is a HIDS.

A ***network intrusion prevention system (NIPS)*** is a NIDS that blocks a threat to a network. A NIPS can take autonomous actions to secure a network and is capable of performing corrective and protective functions. Ex: A NIPS can shut down a network service that is under attack or disconnect a suspicious network connection.

PARTICIPATION ACTIVITY 5.5.1: Intrusion detection systems.

Select the type of intrusion detection or prevention system that is deployed in each scenario.

1) A device that can block an attack on a LAN.
   - NIDS
   - HIDS
   - NIPS

2) A software application installed on a server that can detect an attack on a WAN.
   - NIDS
   - HIDS
   - NIPS

3) A software application installed on a host that can detect an attack on the host.
   - NIDS
   - HIDS
   - NIPS

PARTICIPATION ACTIVITY 5.5.2: Intrusion detection system (IDS).

How to use this tool

NIPS **NIDS** **HIDS**

	An IDS that detects a threat to a network.
	An IDS that detects a threat to a host.
	A NIDS that blocks a threat to a network.

Reset

NIDS/NIPS deployment modes

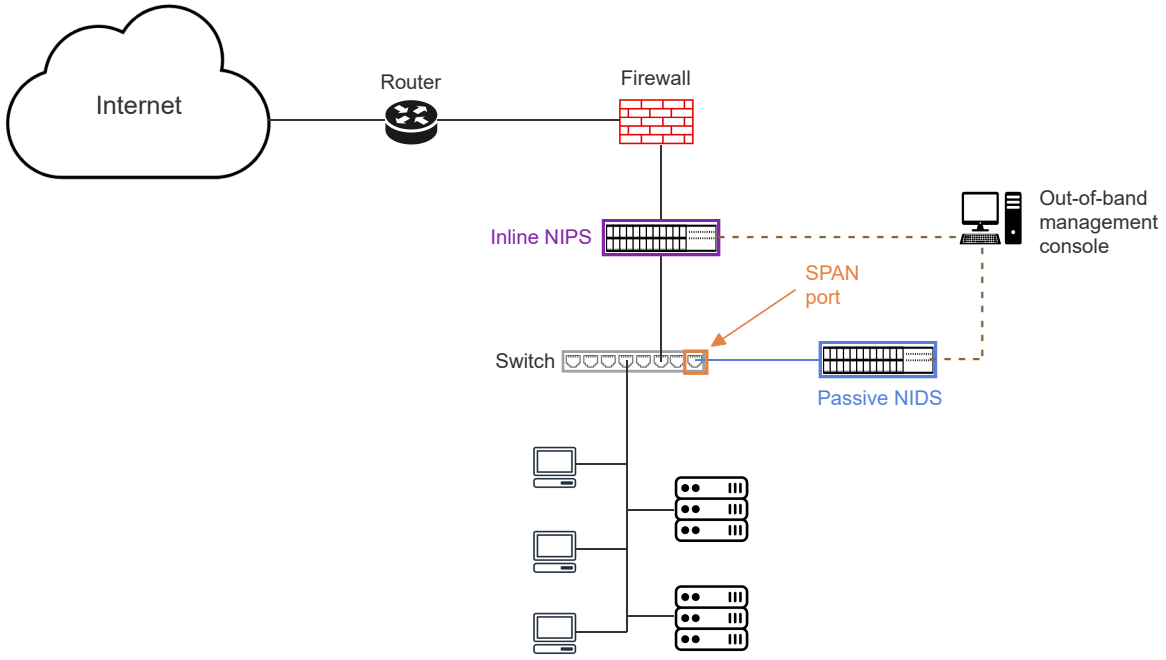
A NIDS/NIPS can be deployed in two modes:

- ***Inline mode***, or ***in-band mode***, is a NIDS/NIPS deployment mode in which network traffic is passed through a NIDS/NIPS. An inline NIDS/NIPS is deployed at a network edge. An inline NIPS can block a network attack.

- ***Passive mode***, or ***out-of-band mode***, is a NIDS/NIPS deployment mode in which a NIDS/NIPS receives a copy of network traffic. A passive NIDS/NIPS is connected to a data monitoring port, such as a switched port analyzer (SPAN) or a test access port (TAP). A passive NIPS cannot block a network attack.

To protect a NIDS/NIPS from a network attack, a NIDS/NIPS cannot be accessed from the protected network. A management console connects to a NIDS/NIPS through a dedicated link to the device's management interface.

PARTICIPATION ACTIVITY 5.5.3: NIDS and NIPS.



Animation content:

Static image: A cloud labeled "Internet" connects to a router. The router connects to a firewall. The firewall connects to an inline NIPS. The inline NIPS is connected to a computer labeled "Out-of-band management console" with a dashed line. The Out-of-band management console is connected to a passive NIDS with a dashed line. The passive NIDS is connected to a switch through a port labeled "SPAN port". The inline NIPS is also connected to the switch. The switch is connected to three computers and two servers.

Animation captions:

1. An inline or in-band NIPS is deployed at a network edge behind a firewall. An inline NIPS has access to real-time network traffic and can block a network attack.
2. A passive or out-of-band NIDS is connected to a switched port analyzer (SPAN) port. A passive NIDS receives a copy of network traffic and cannot block an attack.
3. A NIDS or NIPS is managed out-of-band through dedicated links for improved security.

PARTICIPATION ACTIVITY 5.5.4: NIDS/NIPS deployment modes.

1) An inline NIPS cannot block a network attack.
   - False
   - True

2) A passive NIDS can detect a network attack.
   - False
   - True

3) An inline NIDS can block a network attack.
   - False
   - True

4) A passive NIPS cannot block a network attack.
   - False
   - True

PARTICIPATION ACTIVITY 5.5.5: NIDS and NIPS deployment modes.

How to use this tool

Passive NIDS/NIPS **Inline NIDS/NIPS**

	A NIDS/NIPS deployment mode in which network traffic is passed through a NIDS/NIPS.
	A NIDS/NIPS deployment mode in which a NIDS/NIPS receives a copy of network traffic.

Reset

Intrusion detection methods

An intrusion detection system (IDS) can use different methods for detecting a network attack. Four IDS detection methods exist:

- ***Signature-based detection***, also known as ***knowledge-based detection***, is a detection method that detects an attack by using the attack's pattern. An attack's pattern is also known as the attack's fingerprint or signature. An attack signature may include network packet headers, data sequences of known malware, source or destination IP

addresses, malicious domains, and email subject lines. A signature-based IDS maintains a database of attack signatures and monitors network traffic to find a pattern that matches an attack signature. A signature-based IDS is unable to detect an unknown attack. Ex: A signature-based IDS can detect a Denial-of-Service (DoS) attack against a web server if the IDS knows the pattern of network activity during the DoS attack.

- ***Anomaly-based detection*** is a detection method that detects an attack by identifying a network state that is different from the network's normal state. An anomaly-based IDS builds a profile of normal network activity and flags any network activity that deviates from the profile. A profile may include user, host, and application behavior. Since an anomaly-based IDS flags legitimate but new network activity as malicious, an anomaly-based IDS may generate a large number of false positives. An anomaly-based IDS can detect an unknown attack. Ex: An anomaly-based IDS can detect a Denial-of-Service (DoS) attack against an application server because network activity during the attack is different from the normal network activity.

PARTICIPATION ACTIVITY 5.5.6: Intrusion detection systems.

1) A _____ IDS may generate a large number of false alarms.
   - ○ signature-based
   - ○ anomaly-based

2) A _____ IDS maintains a database of attack patterns.
   - ○ signature-based
   - ○ anomaly-based

- ***Behavior-based detection*** is a detection method that detects an attack by searching for a specific pattern that matches a threat behavior. A behavior-based IDS considers a process action that should not be performed by the process as abnormal behavior and a potential threat. Ex: A behavior-based IDS detects a process that scans multiple ports and flags the process as a threat because scanning multiple ports is a behavior associated with a malicious process.
- ***Heuristic-based detection*** is a detection method that detects an attack by adaptive techniques. A heuristic-based IDS uses an attack signature database similar to signature-based IDS but dynamically modifies those signatures based on learned behavior of real-time network traffic. A heuristic-based IDS can detect a previously unknown network attack.

PARTICIPATION ACTIVITY 5.5.7: Intrusion detection systems.

How to use this tool

Anomaly-based IDS **Signature-based IDS** **Heuristic-based IDS** **Behavior-based IDS**

	An IDS that detects an attack by using the attack's pattern.

	An IDS that detects an attack by identifying a network state that is different from the network's normal state.
	An IDS that detects an attack by searching for a specific pattern that matches a threat behavior.
	An IDS that detects an attack by adaptive techniques.

Reset

PARTICIPATION ACTIVITY 5.5.8: Intrusion detection systems.

1) Which detection method may flag a valid application program operation that may match a threat behavior?
   - Signature-based
   - Anomaly-based
   - Behavior-based
   - Heuristic-based

2) Which detection method modifies attack signatures?
   - Signature-based
   - Anomaly-based
   - Behavior-based
   - Heuristic-based

3) Which detection method cannot detect an attack that exploits a zero-day vulnerability?
   - Signature-based
   - Anomaly-based
   - Behavior-based
   - Heuristic-based

CHALLENGE ACTIVITY 5.5.1: Network intrusion detection and prevention systems.

581480.4344582.qx3zqy7

Start

Select the intrusion detection/prevention system in each scenario.

A device or software application that can shut down a network service that is under attack.

Pick

A device or software application that uses sensors and collectors to detect a network attack.

Pick

A software application that analyzes a host's log files to detect a threat against the host.

Pick

A device or software application that can disconnect a suspicious network connection.

Pick

1 2

Check Next

5.6 Virtual Private Networks (VPNs)

Virtual Private Network (VPN)

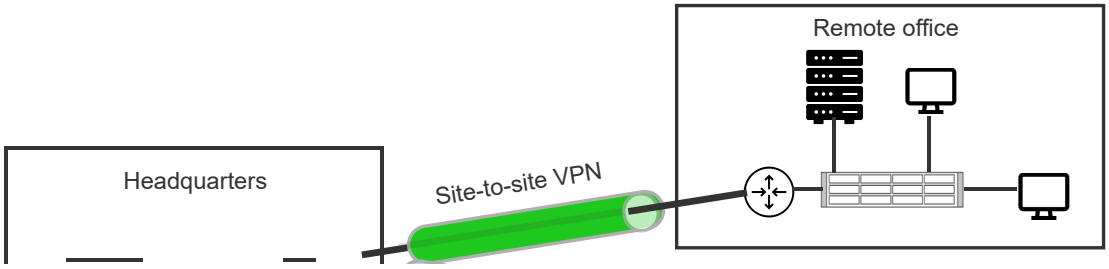
An organization needs to maintain control over the organization's private network for security and privacy. A VPN allows an organization to maintain a private network even though individual devices may be in different locations. An organization enjoys the benefits of a private network while data is exchanged over the internet.

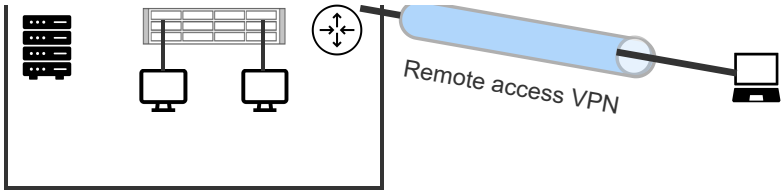
A ***virtual private network (VPN)*** is a service using encryption to connect devices over a public network. A VPN enables a private connection between two or more devices across a public network, such as the internet.

Two VPN types exist:

- A ***site-to-site VPN***, also known as a ***router-to-router VPN***, is a connection between two or more networks. A site-to-site VPN is used to connect different locations of the same organization. Ex: Connecting a bank branch office to the main office.
- A ***client-to-site VPN***, or ***remote access VPN***, is a connection between a client computer and a remote router. Software installed on a client computer makes VPN establishment possible. Ex: A company employee working from home connects to the company network using a client-to-site VPN.

PARTICIPATION ACTIVITY 5.6.1: Site-to-site and Remote-Access VPNs.





Animation content:

Static figure: A company with multiple network devices is connected through the internet to a company's remote office with multiple network devices. A work at home user is also displayed connected to the main office through the internet. The offices are connected using a site-to-site VPN. Network devices (routers) at each end maintain the VPN connection. The remote worker device is connected with a remote access VPN.

Animation captions:

1. A company has two offices located in different cities. Each office has a private network.
2. The offices are connected using a site-to-site VPN. Network devices (routers) at each end maintain the VPN connection.
3. The company also has remote workers. Remote worker devices are connected with a remote access VPN.

PARTICIPATION ACTIVITY 5.6.2: VPN types.

Which VPN type is best suited for the following scenarios?

1) IT support staff that work from home
   - ○ Remote access VPN
   - ○ Site-to-site VPN
   - ○ Both

2) A financial company with offices in multiple cities
   - ○ Remote access VPN
   - ○ Site-to-site VPN
   - ○ Both

3) A software development company with employees that work primarily from home but use office locations for meetings and demos
   - ○ Remote access VPN
   - ○ Site-to-site VPN
   - ○ Both

VPN Traffic Modes: Split tunnel vs full tunnel

A VPN is one type of tunneling protocol. VPNs ease of use is the main reason VPNs are used more often than other tunneling solutions.

Two tunneling mode types exist:

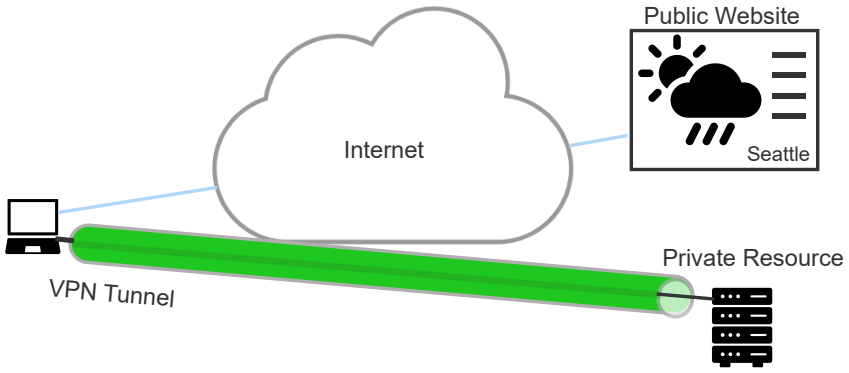
- A ***full tunnel*** routes and encrypts all network traffic through the VPN, regardless of where the VPN service is hosted. Full tunnel is generally recommended and more secure because all network traffic is encrypted.

  Full tunnel is the better option to handle confidential data, where split tunneling may be necessary if access to internet resources and office resources at the same time, but split tunneling is less secure.

- A ***split tunnel*** routes and encrypts all non-internet network traffic over the VPN. Traffic going to internet sites, such as Yahoo and Google, bypasses the VPN server in split tunnel mode.

  The process of split tunneling allows routing some of device or app traffic through an encrypted VPN tunnel while other devices or apps access the internet directly. Split tunneling can be used to protect confidential data, without losing access to local network devices.

PARTICIPATION ACTIVITY 5.6.3: VPN tunneling modes.



Animation content:

Static image: A computer and a server labeled "Private Resource" connected by a green tunnel labeled "VPN Tunnel". The computer is also separately connected to a browser labeled "Public Website" by a connection going through a cloud labeled "Internet".

Animation captions:

1. A VPN connects two devices that are physically separated through a private connection.
2. A split tunnel VPN separates traffic as private or public depending on the destination.
3. Traffic meant for a public website, such as a weather website, is sent unencrypted through the internet.
4. Traffic meant for a private connection, such an employer's data portal, is sent via the VPN.

PARTICIPATION ACTIVITY 5.6.4: Split tunnel and full tunnel VPNs.

1) Which VPN traffic modes deployment allows a client to have a private and public connection?

- Private tunnel
- Full tunnel
- Split tunnel

2) How is traffic separated in a split tunnel VPN?

- By app
- By website
- By both app and URL

3) Which VPN traffic modes routes and encrypts all traffic through a VPN?

- Private tunnel
- Full tunnel
- Split tunnel

VPN Protocols

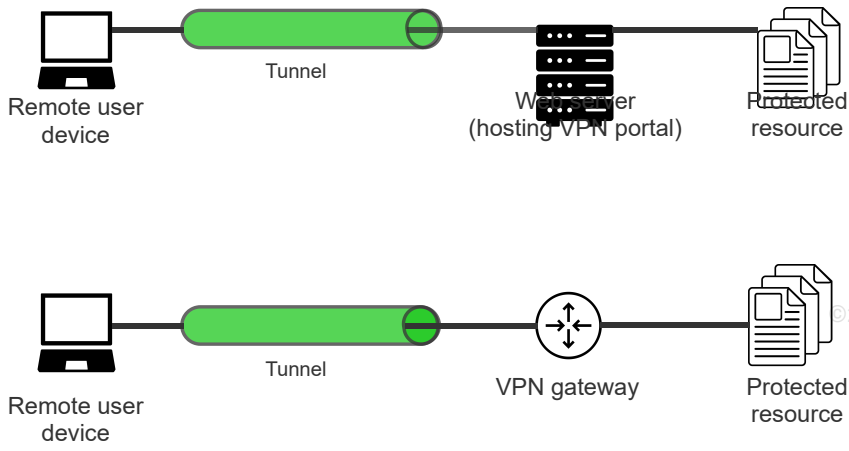
VPNs transmit data through encrypted tunnels to VPN servers. A VPN protocol determines how the tunnel is created. Each protocol provides a different solution to privacy requirements.

VPN protocols layer-by-layer view:

- Application/Transport Layer: SSL/TLS and HTML5
  Security on the web is provided through the use of ***HTTPS (Hypertext Transfer Protocol Secure)***. Communication on HTTPS is encrypted through the use of ***Transport Layer Security (TLS)***. In the past, communication was encrypted through the use of the ***Secure Sockets Layer***. Secure communication over HTTP is now referred to as ***SSL/TLS***.

  Unlike other VPN implementations, an SSL/TLS-based VPN does not require the installation of additional software at the remote-user end, which makes deployment easier.
- Network Layer: IPSec
  Internet Protocol Security (IPSec) is a protocol suite for securing data communications over an IP network. IPsec tunnel mode is used between two dedicated routers, with each router acting as one end of a virtual "tunnel" through a public network.
- Data Link Layer: L2TP
  Layer 2 Tunneling Protocol (L2TP) is a mechanism for setting up VPN tunnels at the data link layer. L2TP does not provide encryption by default and is typically used in conjunction with IPSec at the network layer. L2TP can be used in dissimilar layer 3 (L3) networks.

PARTICIPATION ACTIVITY 5.6.5: VPNs in the application/transport layer.



SSL/TLS VPNs using HTTPS: portal-based vs tunnel-based approaches.

Animation content:

Static figure: A remote computer connected through the internet to a company's web server that is hosting a VPN portal. In a portal-based approach, the remote user connects to a web portal using a browser.
Ex: user types in "vpn.school.edu" in the web browser. The web portal controls access to protected resources. HTML5 has built-in support for SSL/TLS VPN portals. In a tunnel-based approach the remote user connects to a VPN gateway, instead of a web server. A VPN tunnel is set up using SSL/TLS.
OpenVPN is an open source implementation that enables the creation of an SSL/TLS VPN tunnel.

Animation captions:

1. An SSL/TLS VPN can be setup using a portal-based approach, where the remote user connects to a web portal using a browser. Ex: "vpn.school.edu" is typed in a web browser.
2. The web portal controls access to protected resources. HTML5 has built-in support for SSL/TLS VPN portals.
3. An SSL/TLS VPN can be setup using a tunnel-based approach where the remote user connects to a VPN gateway.
4. A VPN tunnel is set up using SSL/TLS. OpenVPN is an open source implementation that enables the creation of an SSL/TLS VPN tunnel.

PARTICIPATION ACTIVITY 5.6.6: VPN protocols.

Which VPN type is best suited for each scenario?

1) Joe can connect to company documents by accessing the site "private.company.com" on a web browser.
   - ○ Tunnel-based SSL/TLS VPN
   - ○ Portal-based SSL/TLS VPN
   - ○ Site-to-site VPN

2) Jamie's company requires Jamie to first connect to a gateway which then allows Jamie to access company documents after entering credentials.

- Tunnel-based SSL/TLS VPN
- Portal-based SSL/TLS VPN
- Site-to-site VPN

3) Jennifer must download a software package before proceeding with accessing the company VPN.

- SSL/TLS
- IPSec
- L2TP

5.7 Port security

Port security

A port on a network device should be secured to prevent unauthorized access to a network. Network devices that have ports include switches, firewalls and routers. Port security is used for protecting data link layer traffic. Port security can be implemented by different methods, including:

- Port disablement
  A port can be disabled to prevent a device from connecting to the port. Ex: A switch port that is connected to an unused RJ-45 wall socket can be disabled to prevent a laptop from connecting to a network by plugging into the wall socket.
- MAC filtering
  A device's MAC address can be used to allow the device to connect to a port. Ex: A switch port can be configured to only allow a device with MAC address "DA-C4-97-C3-3E-B7" to connect to the port.
- IEEE 802.1X
  IEEE 802.1X is a protocol for port-based access control. IEEE 802.1X allows a device to connect to a network port only after the device authenticates to the network. Ex: A laptop that connects to a IEEE 802.1X-provisioned switch port is blocked from accessing a network if the laptop fails to authenticate to the network.

PARTICIPATION ACTIVITY 5.7.1: Port security.

1) Why should a port on a network device be secured?

- To prevent an authorized device from sending malicious traffic on a network.
- To prevent an authorized device from connecting to a network

- To prevent an unauthorized device from connecting to a network

2) Port security is used for protecting traffic on which OSI layer?
   - Layer 1 (physical layer)
   - Layer 2 (data link layer)
   - Layer 3 (network layer)

3) Why MAC filtering-based port security control does not provide full protection for a port?
   - Because a network device may not have a MAC address
   - Because a MAC address is not unique
   - Because a MAC address can be spoofed

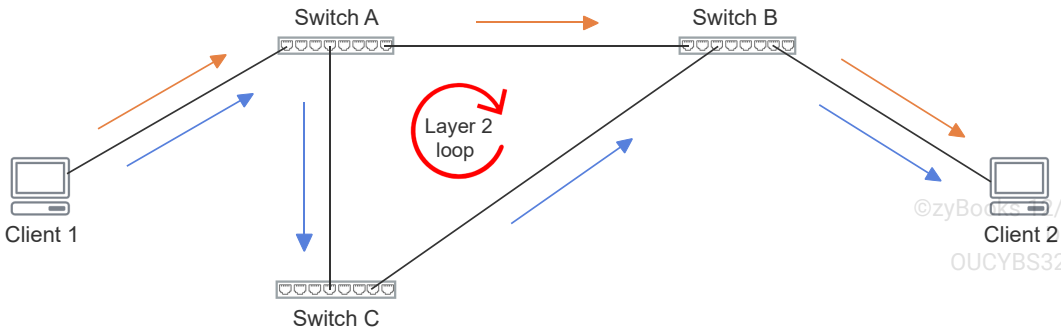
4) When does an IEEE 802.1X-provisioned switch port allow a device to connect to a network?
   - Before a device authenticates to a network
   - After a device authenticates to a network
   - IEEE 802.1X cannot be used on a switch port

Network loop prevention

A ***network loop***, also known as a ***Layer 2 loop*** or ***bridge loop***, is a network topology in which more than one path exists between two network endpoints. A network loop occurs at Layer 2 (data link layer). Ex: A network loop exists if more than one path exists between two hosts on a LAN.

Since a switch forwards broadcasts and multicasts to every switch port, a network loop causes a switch to repeatedly rebroadcast broadcast and multicast packets. A ***broadcast storm***, also known as a ***network storm***, is the occurrence of a large number of broadcast and multicast packets on a network within a short time period. A network loop degrades network performance by exhausting the network bandwidth. ***Broadcast storm prevention***, or ***storm control***, is the act of preventing or reducing packet rebroadcasts on a LAN. Broadcast storm prevention methods include the removal of network loops by disabling ports and limiting the rate of broadcast traffic.

PARTICIPATION ACTIVITY 5.7.2: Network loop.



Animation content:

Static image: A computer icon labeled "Client 1" connects to a switch labeled "Switch A". Switch A connects to two switches labeled "Switch B" and "Switch C". Switch C also connects to Switch B. Switch B connects to a computer labeled "Client 2". Orange arrows show a path from Client 1 to Switch A to Switch B to Client 2. Blue arrows show a path from Client 1 to Switch A to Switch C to Switch B to Client 2. A circular arrow between switches A, B, and C is labeled "Layer 2 loop".
Step 1: A network path exists between "Client 1" and "Client 2" through switch A and switch B.
A computer icon labeled "Client 1" connects to a switch labeled "Switch A". Switch A connects to two switches labeled "Switch B" and "Switch C". Switch C also connects to Switch B. Switch B connects to a computer labeled "Client 2". Orange arrows appear showing a path from Client 1 to Switch A to Switch B to Client 2.
Step 2: A second network path exists between "Client 1" and "Client 2" through switches A, B, and C.
The network has a Layer 2 loop because more than one path exists between two network endpoints.
The orange arrows disappear. Blue arrows appear showing a path from Client 1 to Switch A to Switch C to Switch B to Client 2. The orange arrows reappear. A circular arrow between switches A, B, and C labeled "Layer 2 loop" appears.
Step 3: The network loop can be removed by disabling the ports on switch B and switch C that are connected to each other.
The connection between Switch C and Switch B disappears. The blue arrows disappear. The circular arrow labeled "Layer 2 loop" disappears. The orange arrows now show the only path from Client 1 to Client 2.

Animation captions:

1. A network path exists between "Client 1" and "Client 2" through switch A and switch B.
2. A second network path exists between "Client 1" and "Client 2" through switches A, B, and C. The network has a Layer 2 loop because more than one path exists between two network endpoints.
3. The network loop can be removed by disabling the ports on switch B and switch C that are connected to each other.

A ***bridge protocol data unit (BPDU)*** is a packet exchanged between switches on a local area network (LAN) to detect the network's loops. A BPDU packet is used by the spanning tree protocol (STP) to construct a loop-free logical topology for

a LAN. A BPDU packet should only be sent by a switch. An end-device such as a laptop or desktop computer that is connected to a switch port should be prevented from sending a BPDU packet. An attacker can use a switch port to inject a malicious BPDU packet into a LAN to modify the network's logical topology and manipulate Layer 2 traffic. A ***bridge protocol data unit (BPDU) guard*** is a control mechanism for preventing a BPDU packet from entering a switch port. BPDU guard protects a Layer 2 STP topology from a BPDU-based attack.

PARTICIPATION ACTIVITY 5.7.3: Network loop prevention.

How to use this tool

Network loop **Broadcast storm prevention** **Network storm**

Bridge protocol data unit (BPDU)

	A network topology in which more than one path exists between two network endpoints.
	The occurrence of a large number of broadcast and multicast packets on a network within a short time period.
	The act of preventing or reducing packet rebroadcasts on a LAN.
	A packet exchanged between switches on a local area network (LAN) to detect the network's loops.

Reset

PARTICIPATION ACTIVITY 5.7.4: Network loop prevention.

1) A network loop exists if two ports on the same switch are connected to each other.
   - False
   - True

2) A switch does not forward broadcasts and multicasts to every switch port.
   - False
   - True

3) Disabling ports cannot prevent a broadcast storm.

- False
- True

4) A BPDU is exchanged between end-devices on a LAN.
   - False
   - True

5) A BPDU is used by STP to construct a loop-free logical topology for a LAN.
   - False
   - True

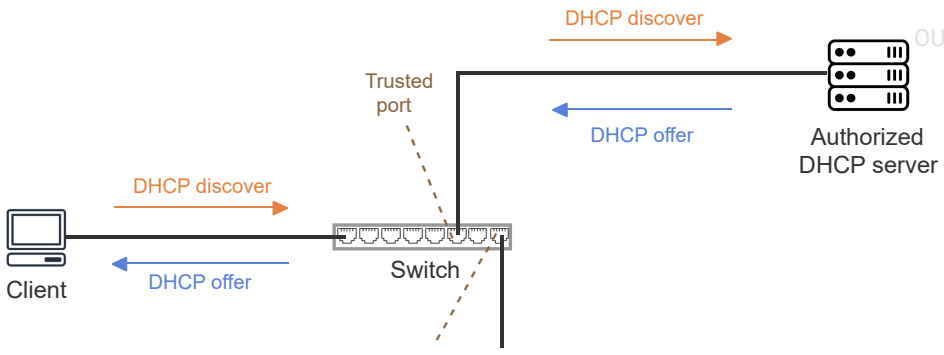
6) A BPDU guard prevents a switch from sending a BPDU packet to another switch on a LAN.
   - False
   - True

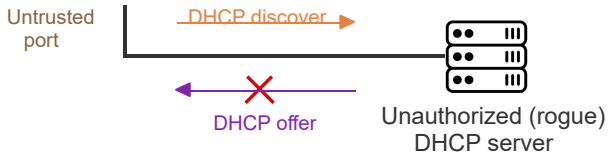
DHCP snooping

Dynamic host configuration protocol (DHCP) is a network management protocol used for automating the assignment of IP addresses and network configuration parameters to devices on an IP network. DHCP simplifies IP address management. Ex: A DHCP server provides an IP address, subnet mask, and the IP addresses of default gateway and DNS server to an DHCP client.

Dynamic host configuration protocol (DHCP) snooping is a Layer 2 control for preventing an unauthorized or rogue DHCP server from offering network configuration parameters to a DHCP client. DHCP snooping is enabled on the switch that connects a client to a DHCP server. DHCP snooping classifies a switch's interfaces into trusted and untrusted ports. A trusted port only receives traffic from within a network. Traffic from a DHCP server is allowed to be received on a trusted port. An untrusted port only receives traffic from client devices. Traffic from a DHCP server is not allowed to be received on an untrusted port.

PARTICIPATION ACTIVITY 5.7.5: DHCP snooping.





Animation content:

Static image: A computer labeled "Client" connected to a switch. The switch connects to a server labeled "Authorized DHCP server" through a port labeled "Trusted port". The switch connects to a server labeled "Unauthorized (rogue) DHCP server" through a port labeled "Untrusted port". An orange arrow labeled "DHCP discover" points from the Client to the switch. Another orange arrow labeled "DHCP discover" points from the switch to the Authorized DHCP server. A blue arrow labeled "DHCP offer" points from the Authorized DHCP server to the switch. Another blue arrow labeled "DHCP offer" points from the switch to the Client. An orange arrow labeled "DHCP discover" also points from the switch to the Unauthorized (rogue) DHCP server. A purple arrow labeled "DHCP offer" points from the Unauthorized (rogue) DHCP server to the switch with a red "X" on the arrow.
Step 1: A client broadcasts a "DHCP discover" message on a network. A switch forwards the message on all the switch's ports.
A computer labeled "Client" connected to a switch. The switch connects to a server labeled "Authorized DHCP server" through a port labeled "Trusted port". The switch connects to a server labeled "Unauthorized (rogue) DHCP server" through a port labeled "Untrusted port". An orange arrow labeled "DHCP discover" appears pointing from the Client to the switch. Two more orange arrows labeled "DHCP discover" appear pointing from the switch to the Authorized DHCP server and the Unauthorized (rogue) DHCP server.
Step 2: Both authorized and unauthorized DHCP servers respond to the client's "DHCP discover" message with a "DHCP offer" message.
A blue arrow labeled "DHCP offer" appears pointing from the Authorized DHCP server to the switch. A purple arrow labeled "DHCP offer" appears pointing from the Unauthorized (rogue) DHCP server to the switch.
Step 3: DHCP snooping blocks a "DHCP offer" message received on an untrusted port, and forwards a "DHCP offer" message received on a trusted port to a DHCP client.
A red "X" appears on the purple arrow. A blue arrow labeled "DHCP offer" appears pointing from the switch to the Client.

Animation captions:

1. A client broadcasts a "DHCP discover" message on a network. A switch forwards the message on all the switch's ports.
2. Both authorized and unauthorized DHCP servers respond to the client's "DHCP discover" message with a "DHCP offer" message.
3. DHCP snooping blocks a "DHCP offer" message received on an untrusted port, and forwards a "DHCP offer" message received on a trusted port to a DHCP client.

DHCP snooping prevents two types of attacks:

- ***DHCP spoofing attack*** is an attack in which an attacker configures a rogue DHCP server to send a forged DHCP response to a DHCP request. A DHCP spoofing attack is used to replace the IP addresses of default gateway and DNS server in a DHCP client, and thereby divert the DHCP client's traffic to a malicious server. A DHCP spoofing attack is a type of Man-In-The-Middle (MITM) attack.
- ***DHCP starvation attack*** is an attack that aims to deplete a DHCP server's IP address pool. A DHCP starvation attack floods a DHCP server with DHCP request messages that have spoofed source MAC addresses. A DHCP starvation attack depletes a DHCP server's IP address pool and prevents a DHCP client from obtaining network configuration parameters and connecting to a network. A DHCP starvation attack is a type of Denial-of-Service (DoS) attack.

PARTICIPATION ACTIVITY 5.7.6: DHCP snooping.

How to use this tool

DHCP snooping **DHCP starvation attack** **DHCP spoofing attack** **DHCP**

	A network management protocol used for automating the assignment of IP addresses and network configuration parameters to devices on an IP network.
	A Layer 2 control for preventing an unauthorized or rogue DHCP server from offering network configuration parameters to a DHCP client.
	An attack in which an attacker configures a rogue DHCP server to send a forged DHCP response to a DHCP request by a DHCP client.
	An attack that aims to deplete a DHCP server's IP address pool.

Reset

PARTICIPATION ACTIVITY 5.7.7: DHCP snooping.

1) Which network parameter is not offered to a DHCP client by a DHCP server?
   - ○ IP address of DNS server
   - ○ IP address of DHCP server
   - ○ IP address of default gateway

2) DHCP snooping is used for protecting traffic on which OSI layer?

- Layer 1 (physical layer)
- Layer 2 (data link layer)
- Layer 3 (network layer)

3) What type of attack is a DHCP spoofing attack?

- MITB
- MITM
- DoS

4) What type of attack is a DHCP starvation attack?

- MITB
- MITM
- DoS

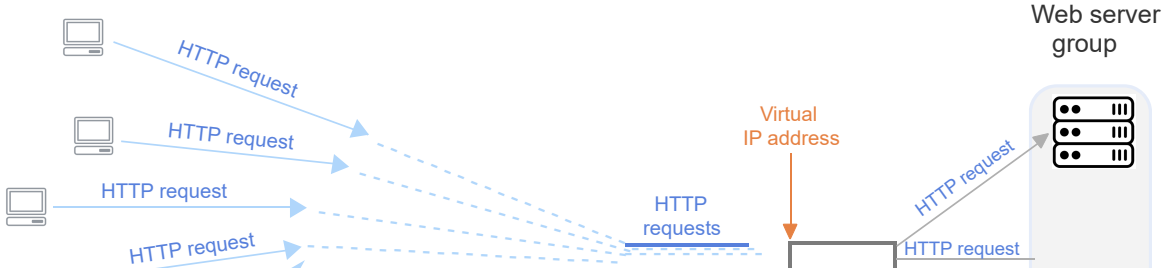
5.8 Load balancing

Load balancing

Load balancing is the act of distributing network or application traffic across multiple servers in a server group. A ***load balancer*** is a hardware device or a software program that performs load balancing. A load balancer commonly operates in the transport layer (Layer 4) or application layer (Layer 7). A load balancer can be used to increase capacity and improve reliability, availability and performance. Ex: A web server load balancer is an application layer load balancer that distributes web traffic across multiple web servers.

A load balancer provides an interface to the servers in a server group through a virtual IP address and a port number. The virtual IP address is only used for routing traffic to server group servers. Different port numbers correspond to different services provided by the server group servers. Ex: A load balancer may use virtual IP address and port number 10.23.4.1:80 for HTTP traffic, and virtual IP address and port number 10.23.4.1:443 for HTTPS traffic.

PARTICIPATION ACTIVITY 5.8.1: Load balancer.



Animation content:

Static image: Five computer icons with blue arrows labeled "HTTP request" pointing to a cloud labeled "Internet". The arrows continue as dotted lines within the cloud and converge on the right side of the cloud into an arrow labeled "HTTP requests" that points to an icon labeled "Load balancer". An orange arrow labeled "Virtual IP address" points to the left side of the Load balancer. The Load balancer has three arrows labeled "HTTP request" pointing to three different servers. The servers are in a box labeled "Web server group".

Animation captions:

1. Clients send HTTP requests to the virtual IP address of a web server load balancer.
2. A load balancer distributes the HTTP requests to the web servers in a web server group.

Load balancing can support session persistence. ***Session persistence***, also known as ***sticky session***, is the process in which a load balancer directs a client request to the same server in a server group for the duration of a session. Session persistence optimizes network resource usage and improves user experience by reducing network latency.

PARTICIPATION ACTIVITY 5.8.2: Load balancing.

How to use this tool

Session persistence **Load balancer**

	A hardware device or a software program that distributes network or application traffic across multiple servers in a server group.
	The process in which a load balancer directs a client request to the same server in a server group for the duration of a session.

Reset

PARTICIPATION ACTIVITY 5.8.3: Load balancing.

1) A load balancer can only be a hardware device.

- False
- True

2) A load balancer operates in the data link layer.

- False
- True

3) Session persistence ensures that a client request is never directed to the same server in a server group.

- False
- True

4) A virtual IP address is sufficient to specify a load balancer service.

- False
- True

Load balancer modes of operation

A load balancer can operate in two modes:

- ***Active/active*** is a load balancer mode in which two load balancers share the workload and distribute traffic across multiple servers.
- ***Active/passive*** is a load balancer mode in which a primary load balancer distributes traffic across multiple servers and a standby load balancer that is activated when the primary load balancer fails.

The active/active mode offers more computing capacity and provides redundancy with higher cost. Active/passive mode allows for uninterrupted service and can handle planned and unplanned service outages. Active/passive mode is commonly used in a disaster recovery environment.

PARTICIPATION ACTIVITY 5.8.4: Load balancer modes of operation.

1) In which load balancer mode of operation two load balancers work together to distribute traffic across multiple servers?

- Active/active
- Active/passive

2) Which load balancer mode of operation is commonly used in a disaster recovery environment?

- Active/active
- Active/passive

3) In which load balancer mode of operation a load balancer is on standby?

- Active/active
- Active/passive

4) In which load balancer mode of operation only one load balancer is active at any given time?

- Active/active
- Active/passive

PARTICIPATION ACTIVITY 5.8.5: Load balancer modes of operation.

How to use this tool

Active/passive **Active/active**

	A load balancer mode in which two load balancers share the workload and distribute traffic across multiple servers.
	A load balancer mode in which a primary load balancer distributes traffic across multiple servers and a standby load balancer that is activated when the primary load balancer fails.

Reset

Load balancer scheduling algorithms

A load balancer uses a scheduling algorithm to distribute data traffic. Four commonly used scheduling algorithms exist:

- ***Least connection load balancing*** is a scheduling algorithm in which data traffic is distributed to a server with the fewest number of active connections.
- ***Least response time load balancing*** is a scheduling algorithm in which data traffic is distributed to a server with the fewest number of active connections and the lowest average response time.
- ***Round robin load balancing*** is a scheduling algorithm in which data traffic is distributed across a group of servers sequentially.
- ***IP hash load balancing*** is a scheduling algorithm in which data traffic is routed to a specific server based on a client's IP address.

The current level of load balancer requests determines the most optimal scheduling algorithm. The round robin scheduling algorithm is commonly used for low traffic loads and the least response time scheduling algorithm for high

traffic loads.

PARTICIPATION ACTIVITY 5.8.6: Load balancing scheduling algorithms.

How to use this tool

Least response time **IP hash** **Least connection** **Round robin**

	A load balancing scheduling algorithm in which data traffic is distributed to a server with the fewest number of active connections.
	A load balancing scheduling algorithm in which data traffic is distributed to a server with the fewest number of active connections and the lowest average response time.
	A load balancing scheduling algorithm in which data traffic is distributed across a group of servers sequentially.
	A load balancing scheduling algorithm in which data traffic is routed to a specific server based on a client's IP address.

Reset

PARTICIPATION ACTIVITY 5.8.7: Load balancing scheduling algorithms.

Select the load balancer scheduling algorithm used in each scenario.

1) A load balancer only considers a server's number of active connections.
   - ○ Least connection
   - ○ Least response time
   - ○ Round robin
   - ○ IP hash

2) A load balancer considers a server's lowest average response time.
   - ○ Least connection
   - ○ Least response time
   - ○ Round robin

- IP hash

3) A load balancer only considers a client's IP address.
   - Least connection
   - Least response time
   - Round robin
   - IP hash

4) A load balancer considers a server's lowest average response time and number of active connections.
   - Least connection
   - Least response time
   - Round robin
   - IP hash

5) A load balancer distributes data traffic sequentially across all server group servers.
   - Least connection
   - Least response time
   - Round robin
   - IP hash

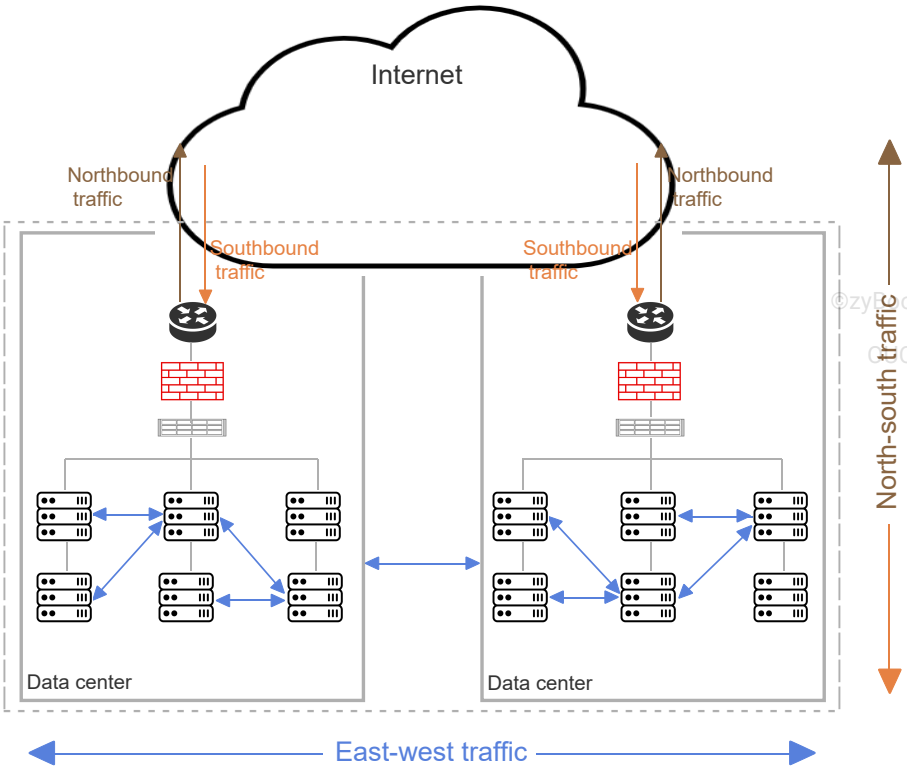
5.9 Data center traffic, intranet, and extranet

Data center traffic

Data center traffic can be classified into two transit segments:

- ***East-west traffic*** is the traffic between a data center's network components. East-west traffic is between network components in the same security zone. Ex: East-west traffic occurs when a LAN client communicates with a server in a data center.
- ***North-south traffic*** is the traffic that enters or leaves a data center. North-south traffic is between network devices in different security zones. ***Southbound traffic*** is the traffic that enters a data center. ***Northbound traffic*** is the traffic that leaves a data center. North-south traffic includes commands and data queries sent to a data center and data sent to be stored in a data center. Ex: North-south traffic occurs when a web client requests access to a web application.

PARTICIPATION ACTIVITY 5.9.1: Data center traffic.



Animation content:

Static image: A cloud labeled "Internet". Two boxes below the Internet cloud are both labeled "Data center". Each box has a router at the top connected to a firewall. The firewall is connected to a switch, and the switch is connected to six servers. Blue two-way arrows are between some of the servers to show traffic between servers within a single data center. A single blue two-way arrow is between the Data center boxes. A two-way arrow labeled "East-west traffic" spans the width of the Data center boxes. Brown arrows labeled "Northbound traffic" go from each router up to the Internet cloud. Orange arrows labeled "Southbound traffic" go from the Internet cloud to each router. A two-way arrow labeled "North-south traffic" spans the height of the Data center boxes.

Animation captions:

1. East-west traffic is the lateral data flow between servers in a data center, or between servers in different data centers hosting an internal network.
2. Northbound traffic is the traffic that leaves a data center. Southbound traffic is the traffic that enters a data center.
3. North-south traffic is the data flow that enters or leaves a data center.

PARTICIPATION ACTIVITY | 5.9.2: Data center traffic.

How to use this tool

Southbound traffic | **East-west traffic** | **North-south traffic** | **Northbound traffic**

	Traffic between a data center's network components.
	Traffic that leaves a data center.
	Data traffic that enters a data center
	Traffic that enters or leaves a data center.

Reset

PARTICIPATION ACTIVITY 5.9.3: Intranet and extranet.

What type of traffic occurs in the following scenarios?

1) Routing table information is exchanged between two routers in a data center.
   - East-west traffic
   - North-south traffic

2) An application running on a data center server retrieves data from a database in the same data center.
   - East-west traffic
   - North-south traffic

3) A user sends an HTML form to a web server in a data center.
   - East-west traffic
   - North-south traffic

Intranet and extranet

Intranet and extranet are security zones with specific security requirements. An ***intranet*** is a private network that can only be accessed by an organization's authorized internal users. An intranet is designed for internal communications among an organization's employees. An intranet cannot be accessed from the public and screened subnet zones. Ex: A website on a company's intranet may be used to deliver information on the company's retirement plan to the company's employees.

An ***extranet*** is a controlled private network that allows access to a subset of an organization's intranet to the organization's external partners, vendors, suppliers, and customers. An extranet extends an organization's private network onto the Internet. Ex: A website on a company's extranet may be used to inform the company's suppliers about the company's purchasing needs.

PARTICIPATION ACTIVITY 5.9.4: Intranet and extranet.

What type of network should be used in each scenario ?

1) A customer portal website

- Intranet
- Extranet

2) An employee directory website

- Intranet
- Extranet

3) An employee timesheet management website

- Intranet
- Extranet

4) A website for a retailer's supply chain partners

- Intranet
- Extranet

5.10 LAB: Firewalls (Walkthrough)

IT-Labs are not printable at this time.

5.11 LAB: Virtual private network (VPN) (Walkthrough)

IT-Labs are not printable at this time.

5.12 LAB: Securing the network (Scenario)

IT-Labs are not printable at this time.