



Module 12: Network Security Infrastructure

CyberOps Associate v1.0



Module Objectives

Module Title: Network Security Infrastructure

Module Objective: Explain how devices and services are used to enhance network security.

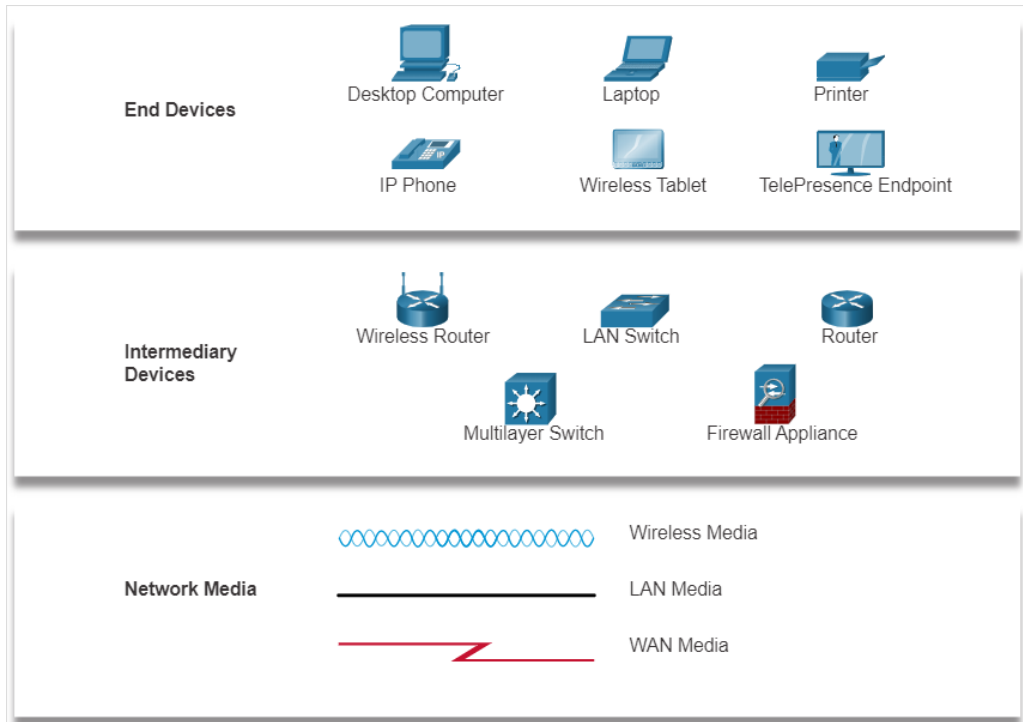
Topic Title	Topic Objective
Network Topologies	Explain how network designs influence the flow of traffic through the network.
Security Devices	Explain how specialized devices are used to enhance network security.
Security Services	Explain how network services enhance network security.

12.1 Network Topologies

Network Representations

- Network diagrams, often called topology diagrams, use symbols to represent different devices and connections within the network.
- The important terminologies to be known include:
 - **Network Interface Card (NIC)**
 - **Physical Port**
 - **Interface**

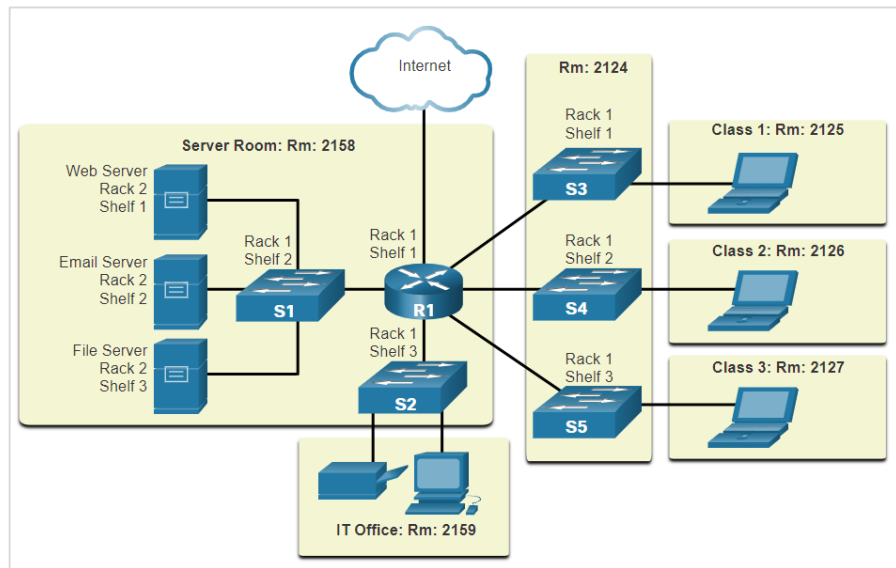
Note: The terms *port* and *interface* are often used interchangeably.



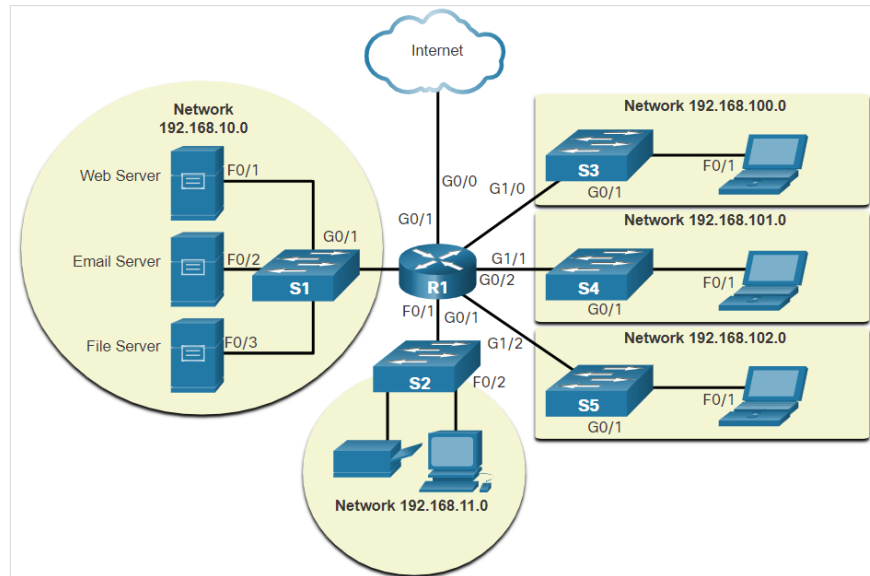
Network Security Infrastructure

Topology Diagrams

Physical topology diagrams illustrate the physical location of intermediary devices and cable installation.



Logical topology diagrams illustrate devices, ports, and the addressing scheme of the network.



Networks of Many Sizes

- Small Home Networks – connect a few computers to each other and the Internet.
- Small Office and Home Office (SOHO) – enables computer within a home, office or remote office to connect to a corporate network, or access centralized, shared resources.
- Medium to Large Networks – can have many locations with hundreds or thousands of interconnected computers.
- World Wide Networks – connects hundreds of millions of computers world-wide – such as the internet.



Small Home



SOHO



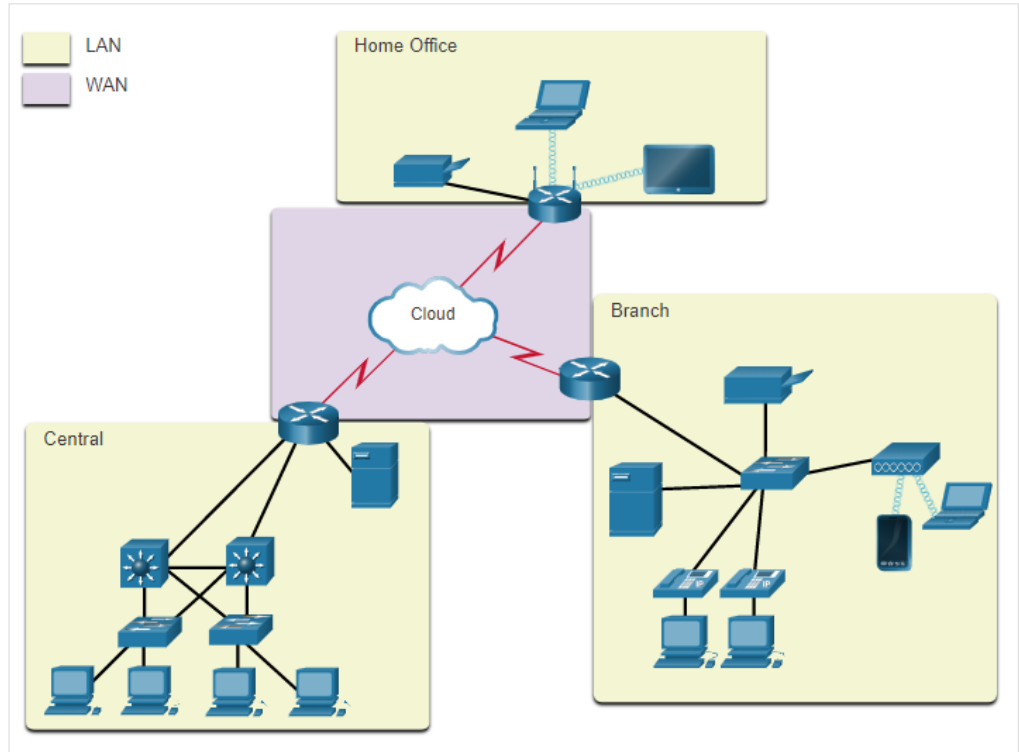
Medium/Large



World Wide

LANs and WANs

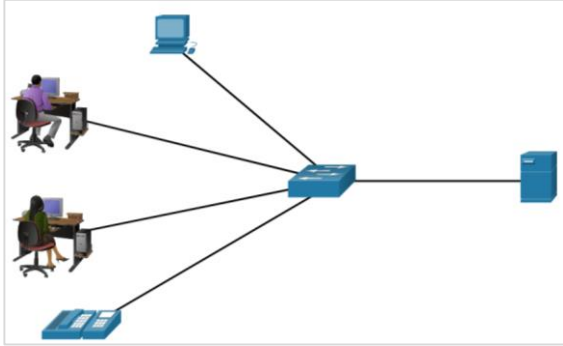
- Network infrastructures vary greatly in terms of:
 - Size of the area covered
 - Number of users connected
 - Number and types of services available
 - Area of responsibility
- The two most common types of network infrastructures are
 - Local Area Networks (LANs)
 - Wide Area Networks (WANs)



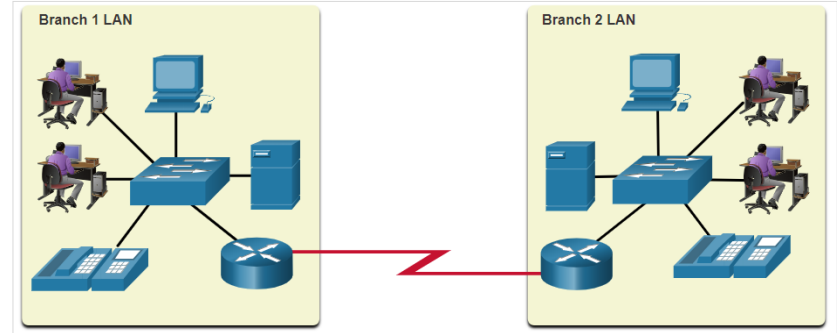
LANs connected to a WAN

LANs and WANs (Contd.)

A LAN is a network infrastructure that spans a small geographical area.



A WAN is a network infrastructure that spans a wide geographical area.



LAN

Interconnect end devices in a limited area.

Administered by a single organization or individual.

Provide high-speed bandwidth to internal end devices and intermediary devices.

WAN

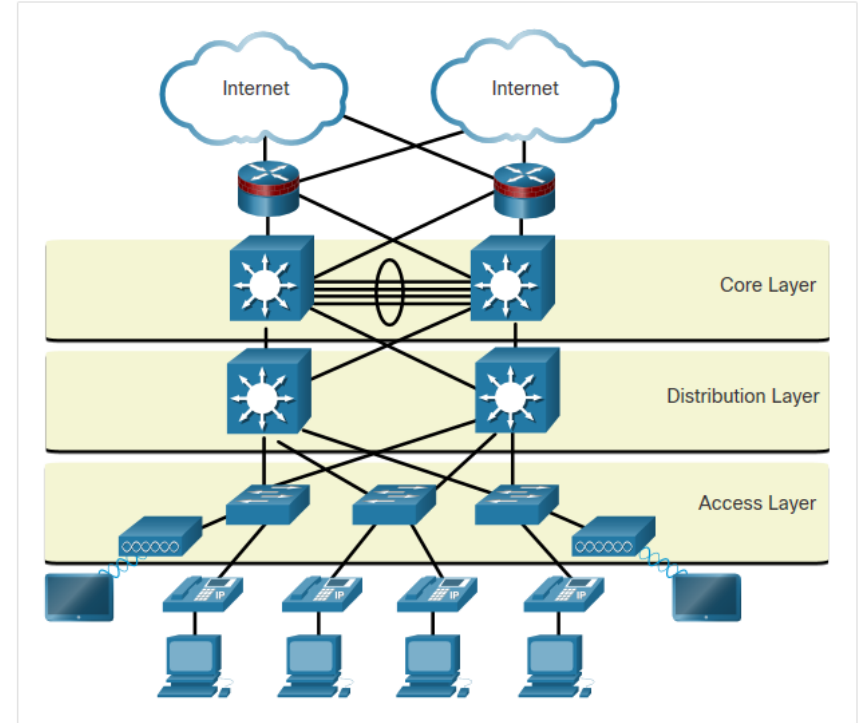
Interconnect LANs over wide geographical areas.

Typically administered by multiple service providers.

Typically provide slower speed links between LANs.

The Three-Layer Network Design Model

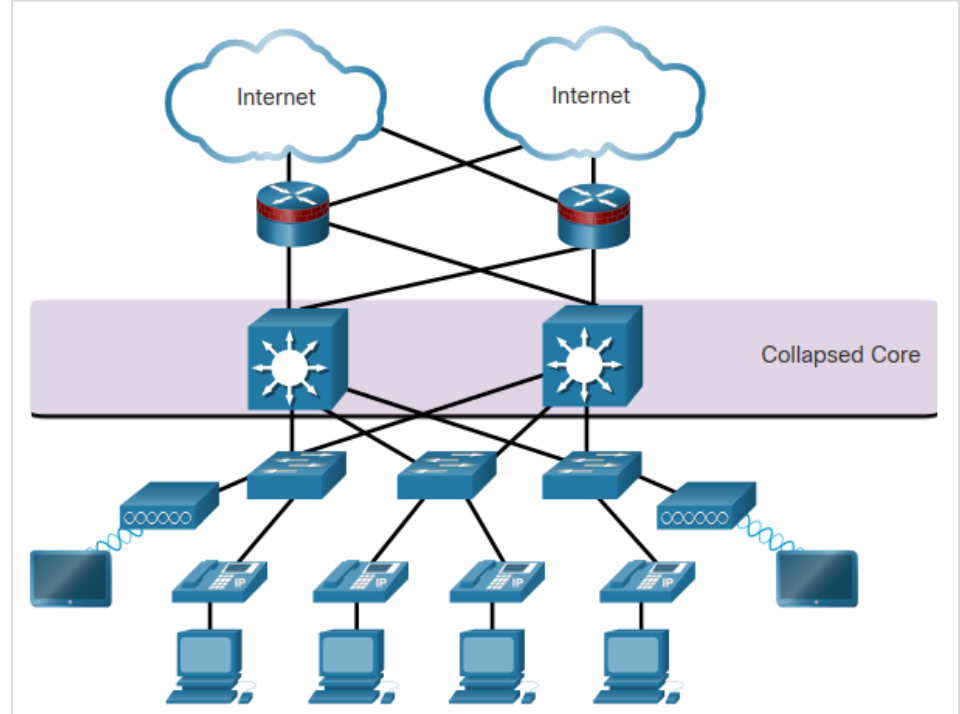
- The campus wired LAN uses a hierarchical design model to separate the network topology into modular groups or layers.
- The hierarchical LAN design includes three layers:
 - **Access** - Provides endpoints and users direct access to the network.
 - **Distribution** - Aggregates access layers and provides connectivity to services.
 - **Core** - Provides connectivity between distribution layers for large LAN environments.



Hierarchical Design Model

The Three-Layer Network Design Model (Contd.)

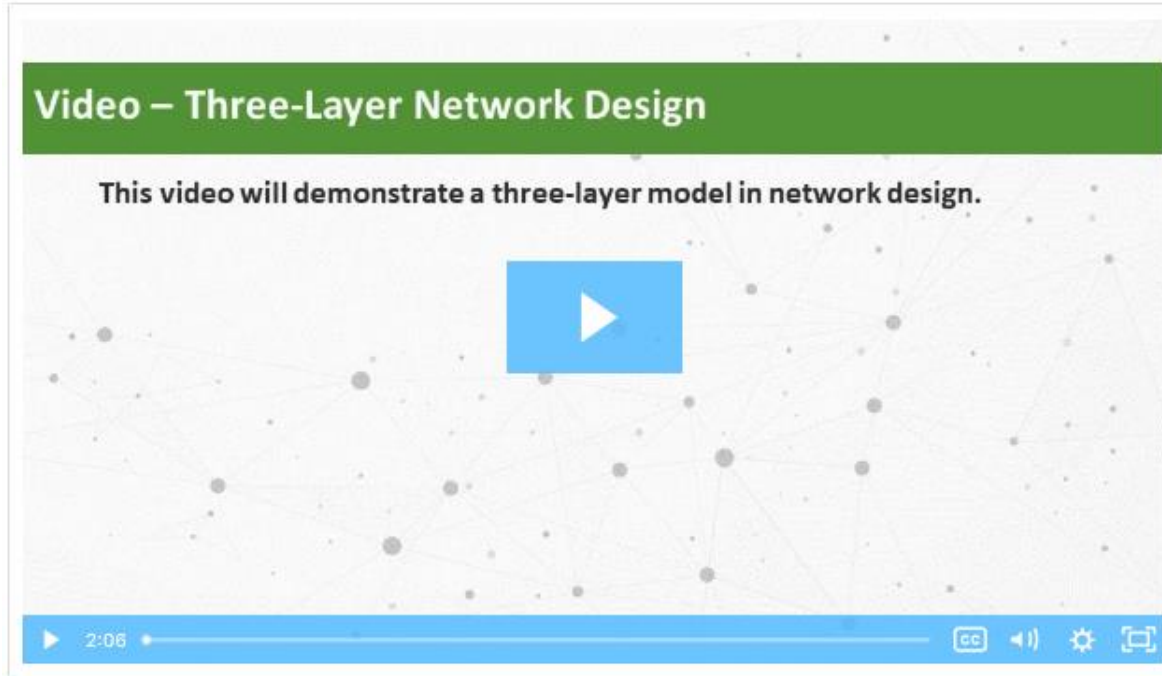
- Although the hierarchical model has three layers, some smaller enterprise networks may implement a two-tier hierarchical design.
- In this two-tier hierarchical design, the core and distribution layers are collapsed into one layer, thus reducing cost and complexity.



Collapsed Core

Video - Three-Layer Network Design

Play the video to view a demonstration of the three-layer network design model.

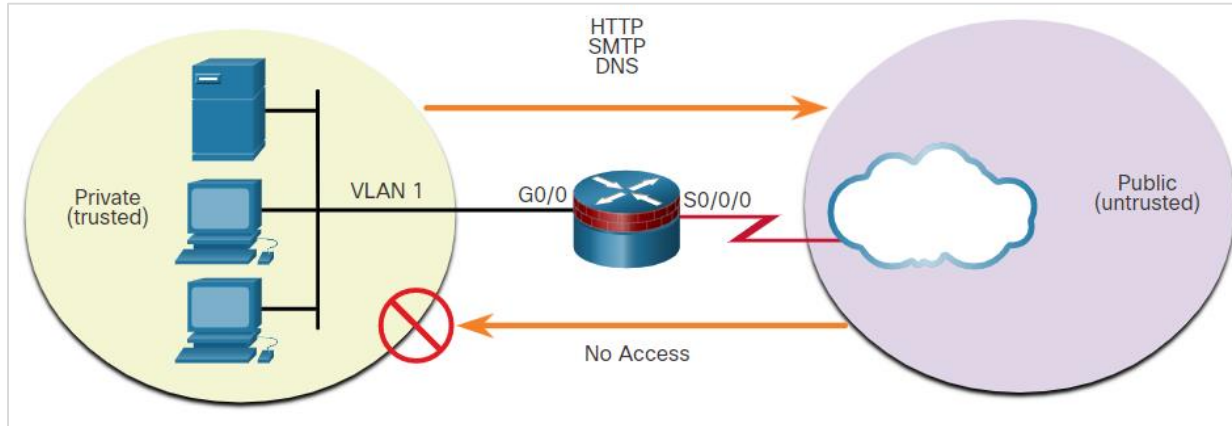


Common Security Architectures

Firewall design is primarily about device interfaces permitting or denying traffic based on the source, the destination, and the type of traffic.

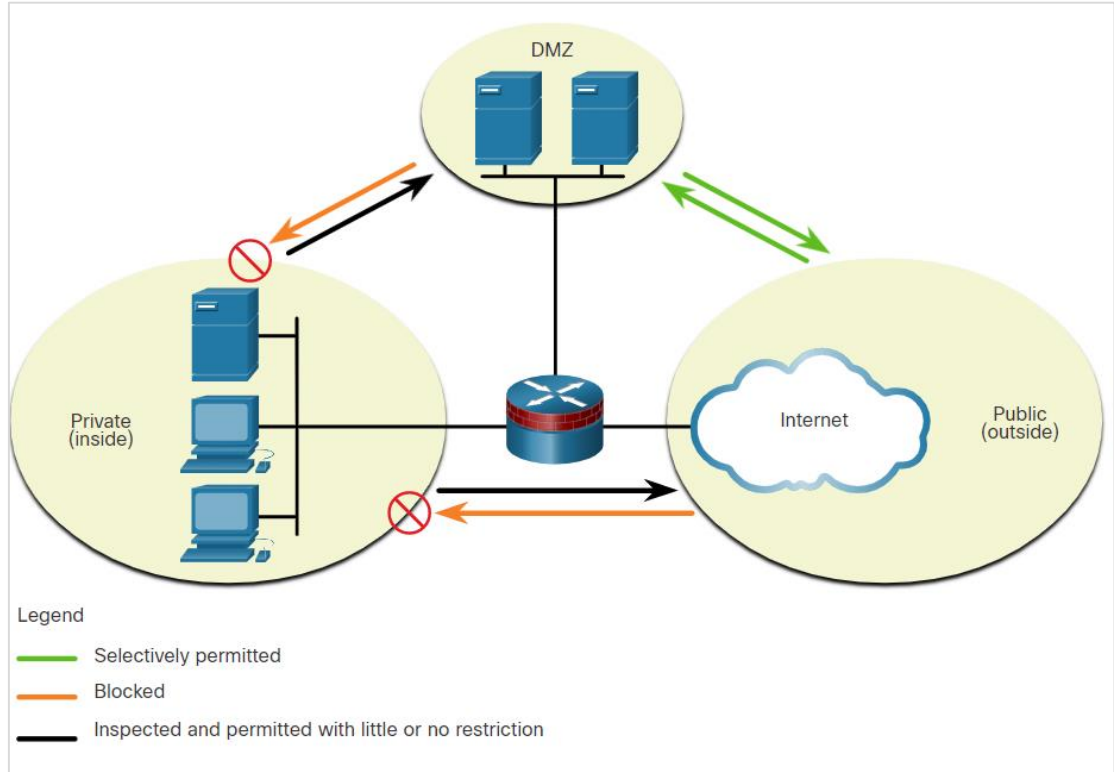
The three firewall designs are:

- **Public and Private**
 - The public network (or outside network) is untrusted, and the private network (or inside network) is trusted.



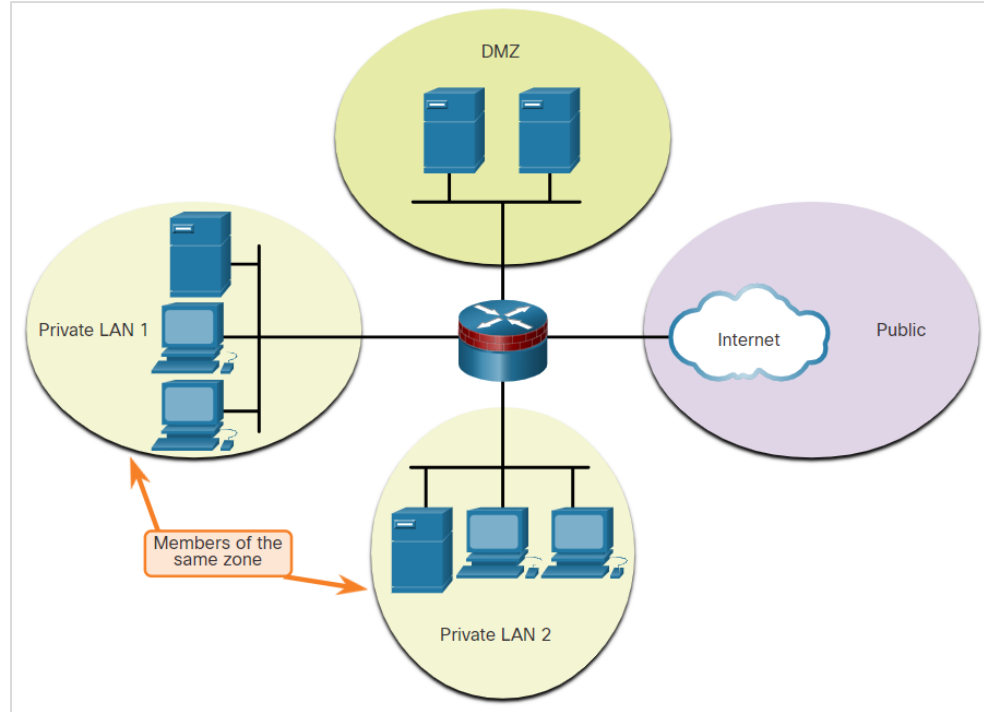
Common Security Architectures (Contd.)

- **Demilitarized Zone (DMZ)**
 - A firewall design where there is typically one:
 - Inside interface connected to the private network
 - Outside interface connected to the public network
 - DMZ interface



Common Security Architectures (Contd.)

- **Zone-based Policy Firewalls (ZPFs)**
 - ZPFs use the concept of zones to provide additional flexibility.
 - A zone is a group of one or more interfaces that have similar functions or features.
 - Zones help to specify where a Cisco IOS firewall rule or policy should be applied.



Packet Tracer - Identify Packet Flow

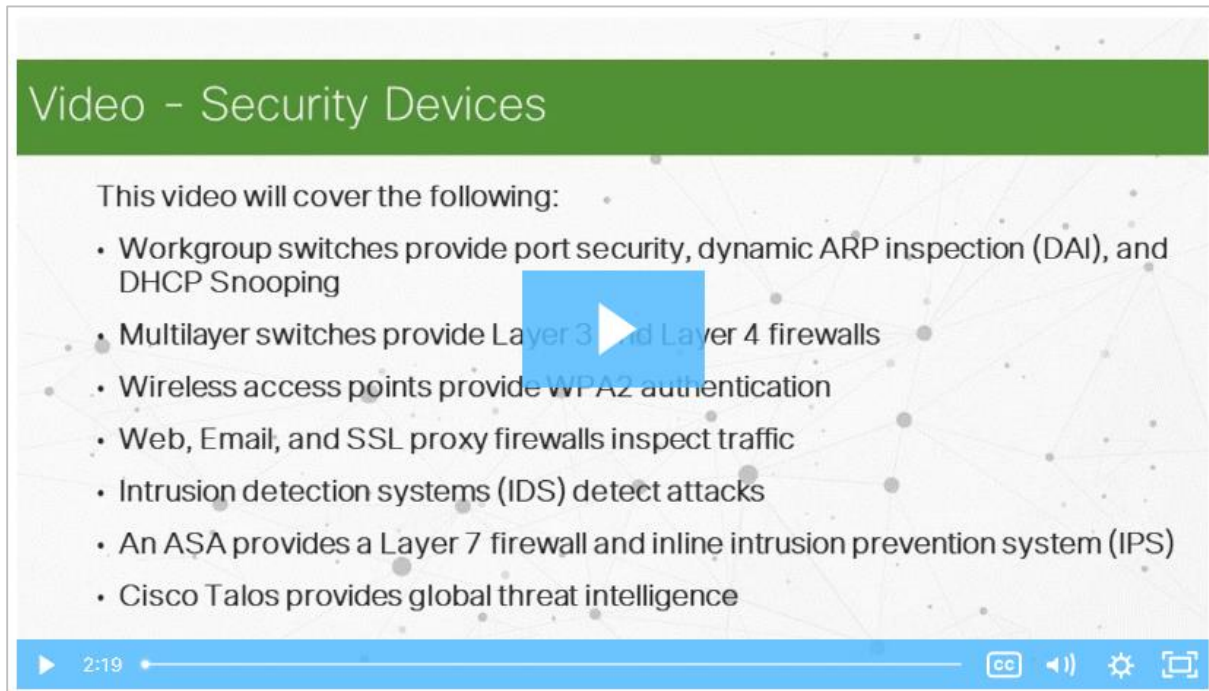
In this Packet Tracer activity, you will observe the following:

- Packet flow in a LAN and WAN topology.
- Change in the packet flow path when there is a change in the network topology.

12.2 Security Devices

Video - Security Devices

Play the video to learn more on security services.



The video player interface features a green header with the title 'Video - Security Devices'. Below the header, a list of topics is displayed. A large blue play button is centered over the list. The video progress bar at the bottom shows a duration of 2:19 and includes icons for closed captions, volume, settings, and full screen.

Video - Security Devices

This video will cover the following:

- Workgroup switches provide port security, dynamic ARP inspection (DAI), and DHCP Snooping
- Multilayer switches provide Layer 3 and Layer 4 firewalls
- Wireless access points provide WPA2 authentication
- Web, Email, and SSL proxy firewalls inspect traffic
- Intrusion detection systems (IDS) detect attacks
- An ASA provides a Layer 7 firewall and inline intrusion prevention system (IPS)
- Cisco Talos provides global threat intelligence

2:19

Security Devices

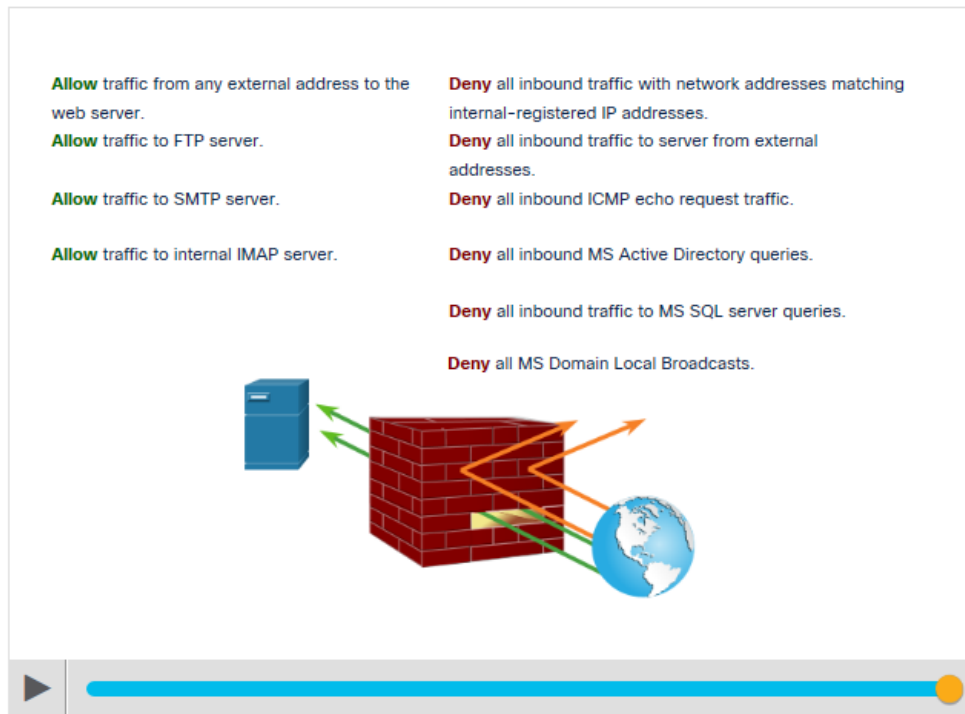
Firewalls

A firewall is a system, or group of systems, that enforces an access control policy between networks.

Common Firewall Properties:

- Resistant to network attacks
- The only transit point between internal corporate networks and external networks because all traffic flows through the firewall
- Enforce the access control policy

Play the animation in the figure to view a firewall in operation.



Firewalls (Contd.)

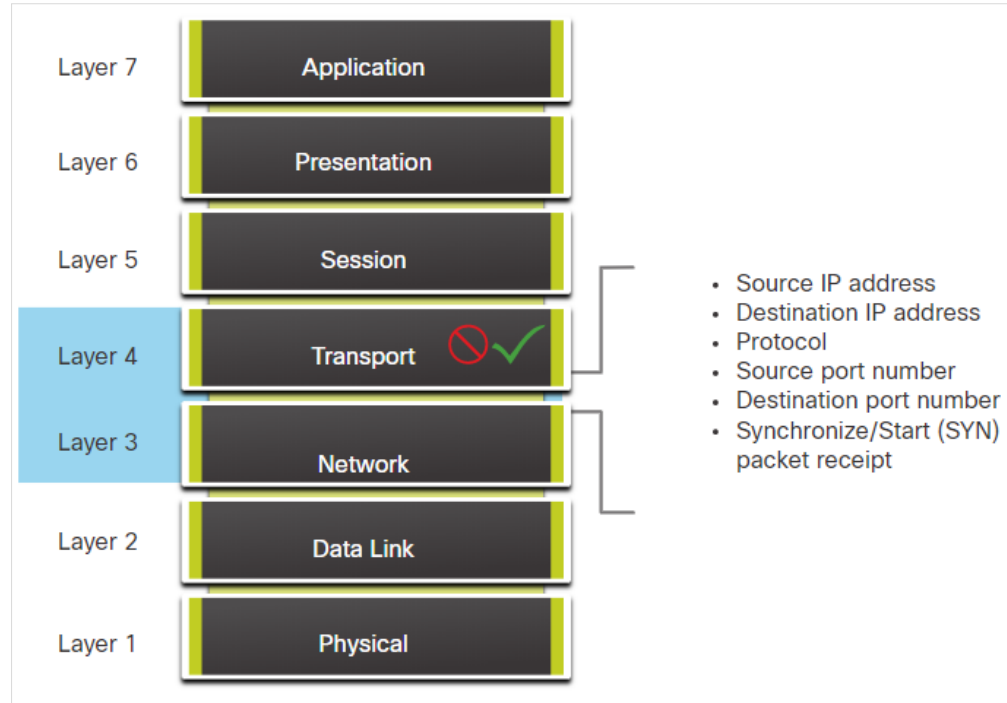
Following are the benefits and limitations of firewalls:

Firewall Benefits	Firewall Limitations
Prevent the exposure of sensitive hosts, resources, and applications to untrusted users.	A misconfigured firewall can have serious consequences for the network, such as becoming a single point of failure.
Sanitize protocol flow, which prevents the exploitation of protocol flaws.	The data from many applications cannot be passed over firewalls securely.
Block malicious data from servers and clients.	Users might proactively search for ways around the firewall to receive blocked material, which exposes the network to potential attack.
Reduce security management complexity.	Network performance can slow down.
	Unauthorized traffic can be tunnelled or hidden as legitimate traffic through the firewall.

Firewall Type Descriptions

The different types of firewalls are:

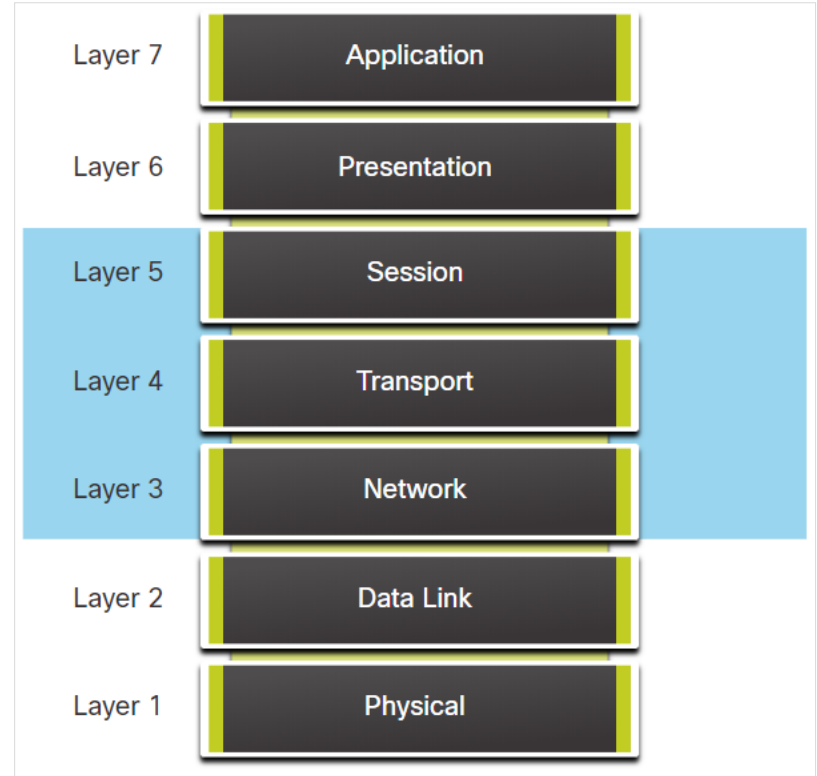
- **Packet Filtering (Stateless) Firewall**
 - Packet Filtering firewalls are part of a router firewall, which permits or denies traffic based on Layer 3 and Layer 4 information.
 - They are stateless firewalls that use a simple policy table look-up that filters traffic based on specific criteria.



Firewall Type Descriptions (Contd.)

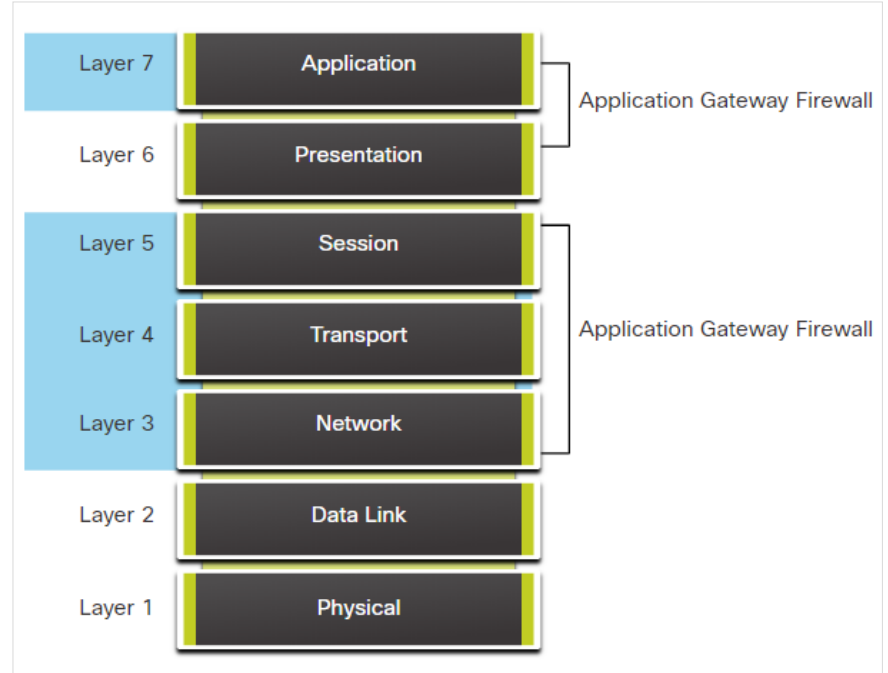
- **Stateful Firewalls**

- Stateful firewalls are the most versatile and the most common firewall technologies in use.
- These firewalls provide stateful packet filtering by using connection information maintained in a state table.



Firewall Type Descriptions (Contd.)

- **Application gateway firewall (proxy firewall)**
 - Application gateway firewall filters information at Layers 3, 4, 5, and 7 of the OSI reference model.
 - Most of the firewall control and filtering is done in the software.



Firewall Type Descriptions (Contd.)

- **Next-generation firewalls (NGFW)**
 - NGFW go beyond stateful firewalls by providing:
 - Integrated intrusion prevention
 - Application awareness and control to see and block risky apps
 - Upgrade paths to include future information feeds
 - Techniques to address evolving security threats



Firewall Type Descriptions (Contd.)

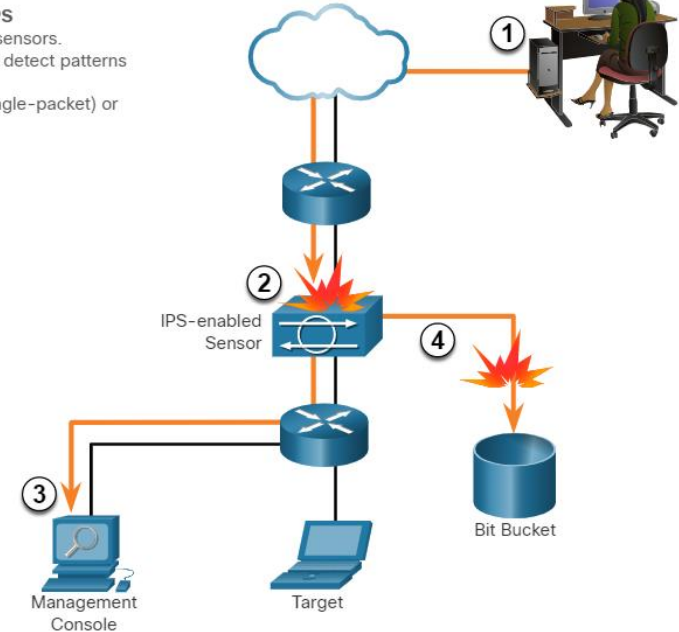
- Other methods of implementing firewalls include:
 - **Host-based (server and personal) firewall** - A PC or server with firewall software running on it.
 - **Transparent firewall** - Filters IP traffic between a pair of bridged interfaces.
 - **Hybrid firewall** - A combination of various firewall types.

Intrusion Prevention and Detection Devices

- A networking architecture paradigm shift is required to defend against fast-moving and evolving attacks. This must include cost effective and prevention systems such as:
 - Intrusion Detection Systems (IDS)
 - Intrusion Prevention Systems (IPS)
- The network architecture integrates these solutions into the entry and exit points of the network.
- The figure shows how an IPS device handles malicious traffic.

Common Characteristics of IDS and IPS

- Both technologies are deployed as sensors.
- Both technologies use signatures to detect patterns of misuse in network traffic.
- Both can detect atomic patterns (single-packet) or composite patterns (multi-packet).



1. Malicious traffic is sent to the target host that is inside the network.
2. The traffic is routed into the network and received by an IPS-enabled sensor where it is blocked.
3. The IPS-enabled sensor sends logging information regarding the traffic to the network security management console.
4. The IPS-enabled sensor kills the traffic. (It is sent to the "Bit Bucket.")

Advantages and Disadvantages of IDS and IPS

The table lists the advantages and disadvantages of IDS and IPS:

Solution	Advantages	Disadvantages
IDS	<ul style="list-style-type: none">• No Impact on network (latency, jitter)• No Network impact if there is a sensor failure• No network impact if there is sensor overload	<ul style="list-style-type: none">• Response action cannot stop trigger packets• Correct tuning required for response actions• More vulnerable to network security evasion techniques
IPS	<ul style="list-style-type: none">• Stops trigger packets• Can use stream normalization techniques	<ul style="list-style-type: none">• Sensor issues might affect network traffic• Sensor overloading impacts the network• Some impact on network (latency, jitter)

Deployment Consideration:

- IPS and IDS technologies can complement each other.
- Deciding which implementation to use is based on the security goals of the organization as stated in their network security policy.

Types of IPS

There are two primary kinds of IPS :

- Host-based IPS
- Network-based IPS
- **Host-based IPS (HIPS)**

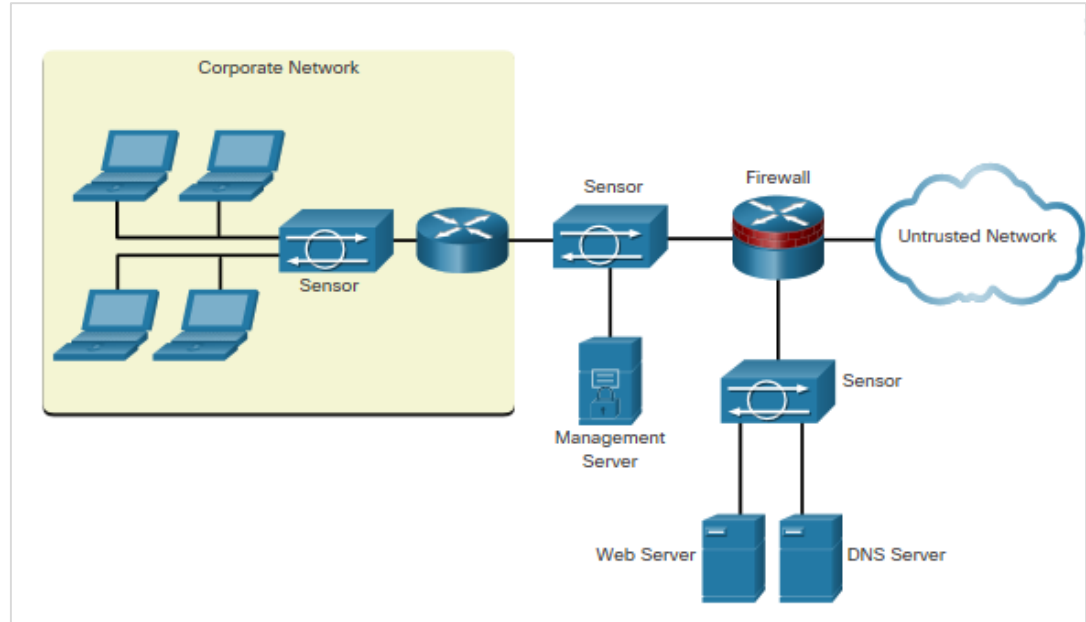
HIPS is a software installed on a host to monitor and analyze suspicious activity.

Advantages	Disadvantages
<ul style="list-style-type: none">• Provides protection specific to a host operating system• Provides operating system and application level protection• Protects the host after the message is decrypted	<ul style="list-style-type: none">• Operating system dependent• Must be installed on all hosts

Types of IPS (Contd.)

• Network-based IPS

- Network-based IPS are Implemented using a dedicated or non-dedicated IPS device.
- Host-based IDS/IPS solutions are integrated with a network-based IPS implementation to ensure a robust security architecture.
- Sensors detect malicious and unauthorized activity in real time and can take action when required.



Specialized Security Appliances

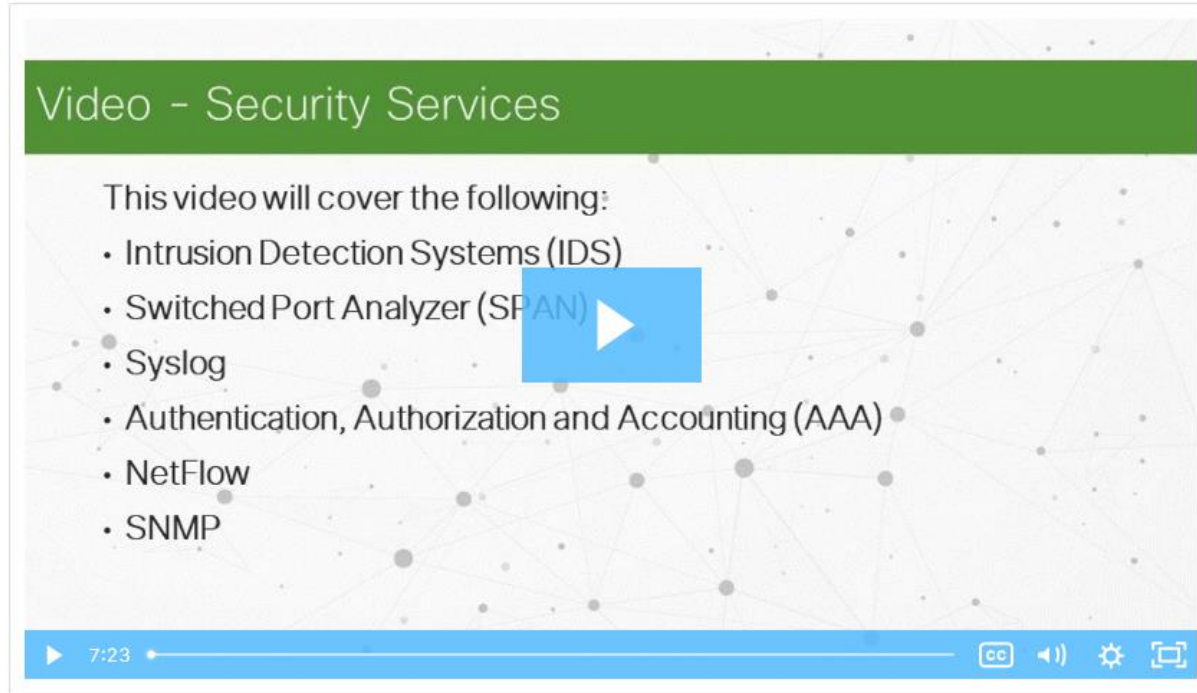
Few examples of specialized security appliances.

Cisco Advanced Malware Protection (AMP)	Cisco Web Security Appliance (WSA)	Cisco Email Security Appliance (ESA)
An enterprise-class advanced malware analysis and protection solution	A secure web gateway that combines leading protections to help organizations address the growing challenges of securing and controlling web traffic	ESA/Cisco Cloud Email Security helps to mitigate email-based threats and the ESA defends mission-critical email systems
It provides comprehensive malware protection for organizations before, during, and after an attack	Protects the network by automatically blocking risky sites and testing unknown sites before allowing users to access them	Constantly updated by real-time feeds from Cisco Talos, which detects and correlates threats using a worldwide database monitoring system
		Features: Global threat intelligence, Spam blocking, Advanced Malware Protection, Outbound Message Control

12.3 Security Services

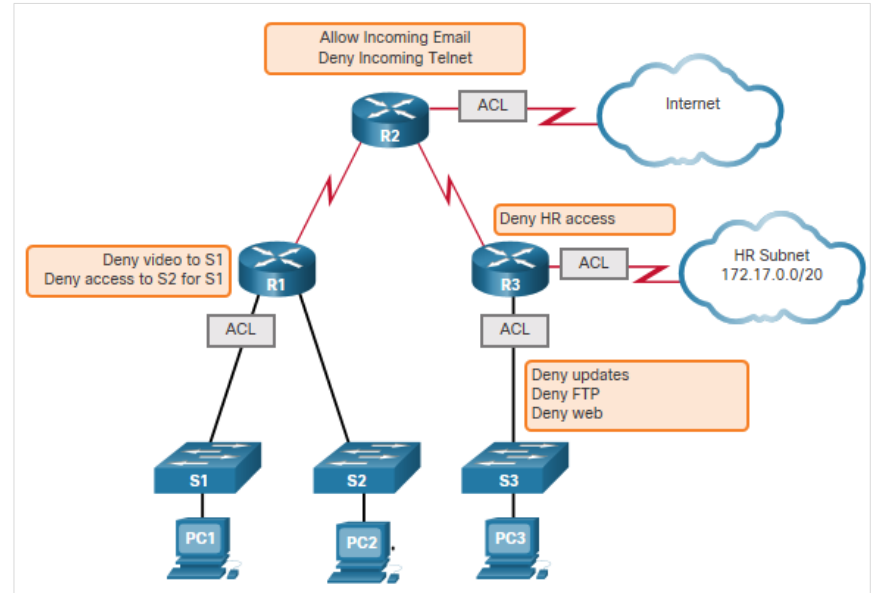
Video - Security Services

Watch the video to learn more on different security services.



Traffic Control with ACLs

- An Access Control List (ACL) is a series of commands that control whether a device forwards or drops packets based on information found in the packet header.
- When configured, ACLs perform the following tasks:
 - Limit network traffic to increase network performance.
 - Provide traffic flow control.
 - Provide basic level of security for network access.
 - Filter traffic based on traffic type.
 - Screen hosts to permit or deny access to network services.



Sample Topology with ACLs applied to routers R1, R2, and R3.

ACLs: Important Features

The two types of Cisco IPv4 ACLs are:

- **Standard ACL** - Used to permit or deny traffic only from source IPv4 addresses.
- **Extended ACL** - Filters IPv4 packets based on several attributes that include:
 - Protocol type
 - Source IPv4 address
 - Destination IPv4 address
 - Source TCP or UDP ports
 - Destination TCP or UDP ports
 - Optional protocol type information for finer control
- Standard and extended ACLs can be created using either a number or a name to identify the ACL and its list of statements.

Packet Tracer - ACL Demonstration

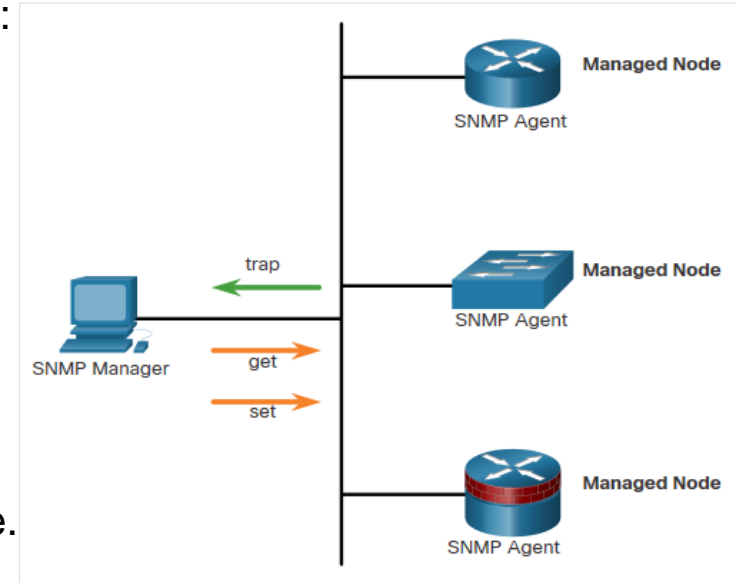
In this activity, you will observe the following:

- How an ACL can be used to prevent a ping from reaching hosts on remote networks.
- After removing the ACL from the configuration, the pings will be successful.

Security Services

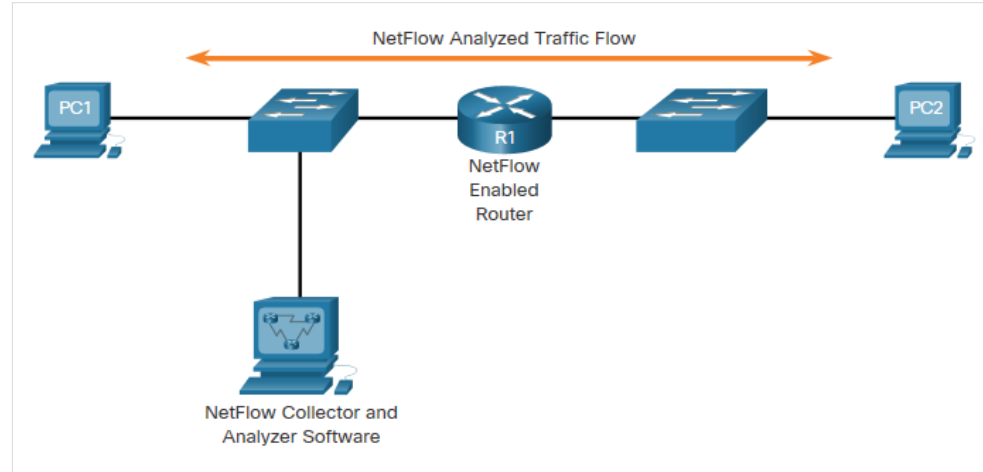
SNMP

- Simple Network Management Protocol (SNMP) is an application layer protocol that provides a message format for communication between managers and agents.
- It allows network administrators to perform the following:
 - Manage end devices such as servers, workstations, routers, switches, and security appliances, on an IP network.
 - Monitor and manage network performance.
 - Find and solve network problems.
 - Plan for network growth.
- The SNMP system consists of two elements:
 - **SNMP manager:** Runs SNMP management software.
 - **SNMP agents:** Nodes being monitored and managed.



NetFlow

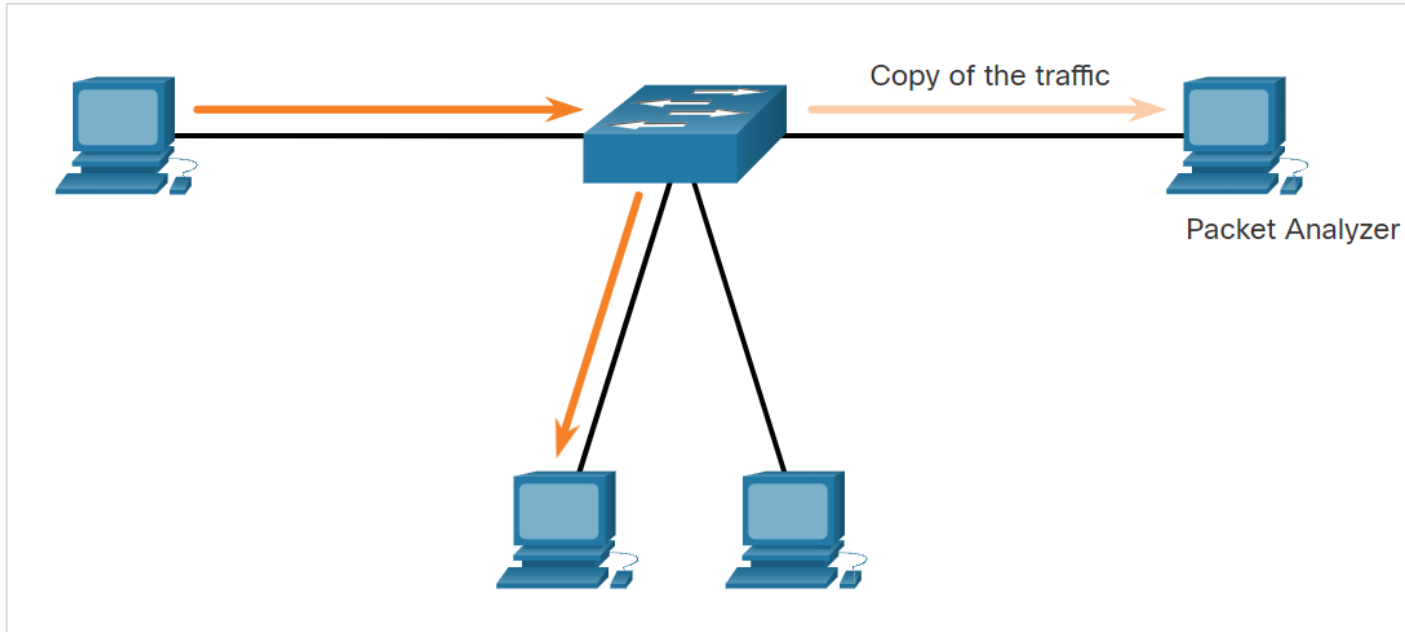
- NetFlow is a Cisco IOS technology that provides statistics on packets flowing through a Cisco router or multilayer switch.
- NetFlow provides data to enable:
 - network and security monitoring,
 - network planning
 - traffic analysis to include identification of network bottlenecks
 - IP accounting for billing purposes.
- NetFlow can monitor application connection, tracking byte and packet counts for that individual application flow.
- It then pushes the statistics over to an external server called a NetFlow collector.



PC 1 connects to PC 2 using HTTPS

Port Mirroring

Port mirroring is a feature that allows a switch to make duplicate copies of traffic passing through a switch, and then sending it out a port with a network monitor attached.

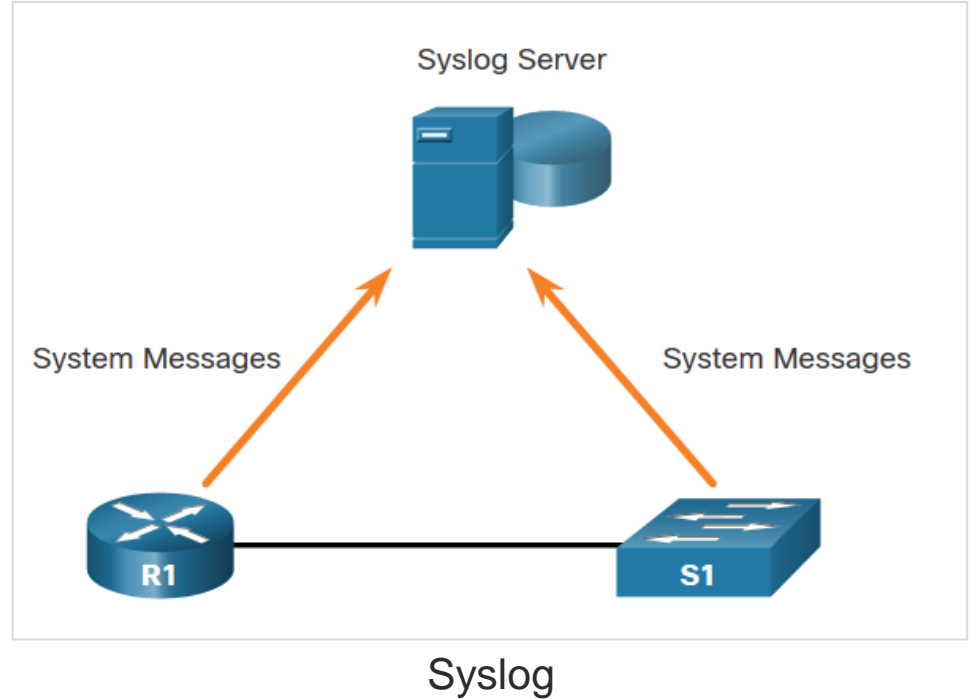


Traffic Sniffing Using a Switch

Security Services

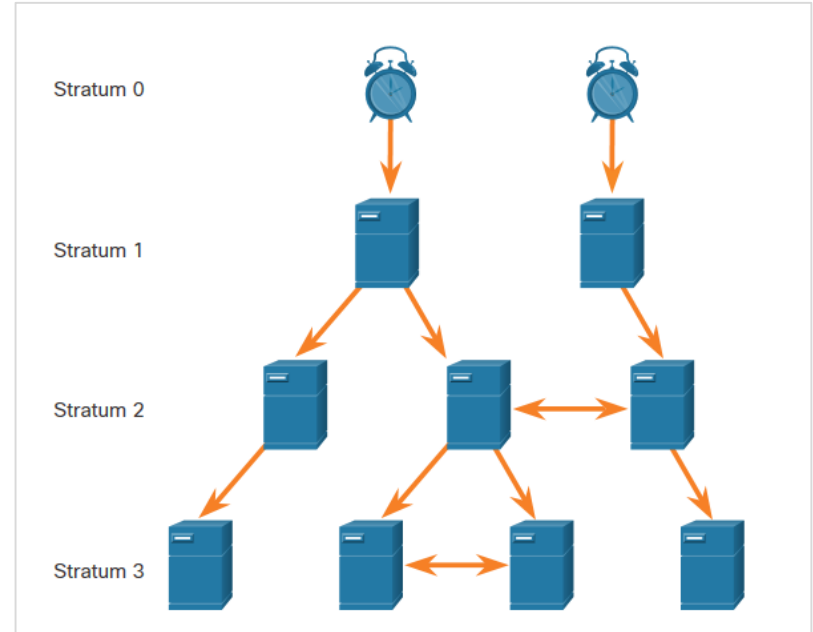
Syslog Servers

- The most common method of accessing system messages is to use a protocol called syslog.
- The Syslog protocol allows networking devices to send their system messages across the network to syslog servers.
- It provides three primary functions:
 - The ability to gather logging information for monitoring and troubleshooting
 - The ability to select the type of logging information that is captured
 - The ability to specify the destination of captured syslog messages



NTP

- It is important to synchronize the time across all devices on the network. The date and time settings on a network device can be set using one of two methods:
 - Manual configuration of the date and time
 - Configuring the Network Time Protocol (NTP)
- NTP networks use a hierarchical system of time sources, where each level in this system is called a stratum. NTP servers are arranged in three levels known as strata:
 - **Stratum 0:** An NTP network gets the time from authoritative time sources.
 - **Stratum 1:** Devices are directly connected to the authoritative time sources.
 - **Stratum 2 and lower strata:** Stratum 2 devices, such as NTP clients, synchronize their time using the NTP packets from stratum 1 servers.



NTP Stratum Levels

Security Services

AAA Servers

The below table lists the three independent security functions provided by the AAA architectural framework.

Functions	Description
Authentication	<ul style="list-style-type: none">• Users and administrators must prove that they are who they say they are.• Authentication can be established using username and password combinations, challenge and response questions, token cards, and other methods.• AAA authentication provides a centralized way to control access to the network.
Authorization	<ul style="list-style-type: none">• After the user is authenticated, authorization services determine which resources the user can access and which operations the user is allowed to perform.• An example is "User 'student' can access host serverXYZ using SSH only."
Accounting	<ul style="list-style-type: none">• Accounting records what the user does, including what is accessed, the amount of time the resource is accessed, and any changes that were made.• Accounting keeps track of how network resources are used.• An example is "User 'student' accessed host serverXYZ using SSH for 15 minutes."

AAA Servers (Contd.)

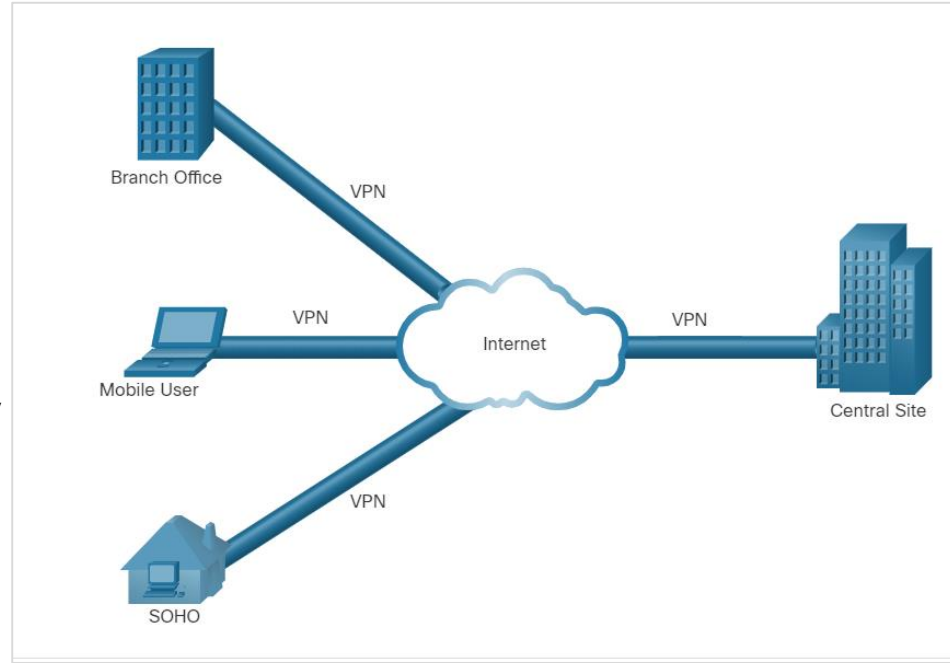
The below table lists the difference between Terminal Access Controller Access-Control System Plus (TACACS+) and Remote Authentication Dial-In User Service (RADIUS) protocols.

	TACACS+	RADIUS
Functionality	Separates AAA according to the AAA architecture,	Combines authentication and authorization but separates accounting,
Standard	Mostly Cisco supported	Open/RFC standard
Transport	TCP	UDP
Protocol CHAP	Bidirectional challenge and response as used in Challenge Handshake Authentication Protocol (CHAP)	Unidirectional challenge and response from the RADIUS security server to the RADIUS client
Confidentiality	Entire packet encrypted	Password encrypted
Customization	Provides authorization of router commands on per-user or per-group basis	No option to authorize router commands on a per-user or per-group basis
Accounting	Limited	Extensive

Security Services

VPN

- A VPN is a private network that is created over a public network (usually the internet).
- A VPN uses virtual connections routed through the Internet from the organization to the remote site.
- A VPN is a communications environment in which access is strictly controlled to permit peer connections within a defined community of interest.
- Confidentiality is achieved by encrypting the traffic within the VPN.
- In short, VPN connects two endpoints over a public network, to form a logical connection which can be made at Layer 2 or Layer 3.



Virtual Private Network

12.4 Network Security Infrastructure Summary

What Did I Learn in this Module?

- Networks are typically represented as physical and logical topologies.
- A physical topology represents physical connections and how end devices are connected whereas a logical topology refers to the standards and protocols that devices use to communicate.
- The two most common types of network infrastructures are LANs and WANs.
- The campus wired LAN design consists of hierarchical layers (access, distribution, core) with each layer assigned specific functions.
- Common security architectures define the boundaries of traffic entering and leaving the network.
- The different types of firewalls are Packet filtering firewalls, stateful inspection firewall, Application gateway firewalls, Next-generation firewalls.

What Did I Learn in this Module? (Contd.)

- Intrusion prevention systems (IPS) and intrusion detection systems (IDS) are used to detect potential security risks and alert/stop unsafe traffic.
- Specialized security appliances are available including Cisco Advanced Malware Protection (AMP), Cisco Web Security Appliance (WSA), and Cisco Email Security Appliance (WSA).
- ACLs are a series of statements that control whether a device forwards or drops packets based on information found in the packet header.
- SNMP enables network administrators to monitor and manage network performance, find and solve network problems, and plan for network growth.
- NetFlow provides statistics on packets that are flowing through a Cisco router or multilayer switch.
- Port mirroring is a feature that allows a switch to make duplicate copies of traffic that is passing through the switch, and then send it out a port that has a network monitor attached.

What Did I Learn in this Module? (Contd.)

- Syslog servers compile and provide access to the system messages generated by networking devices.
- NTP synchronizes the system time across all devices on the network to ensure accurate and consistent timestamping of system messages.
- AAA is a framework for configuring user authentication, authorization, and accounting services. It typically uses a TACACS+ or RADIUS server for this purpose.
- VPNs are private networks that are created between two endpoints across a public network.

