Module 6: Network Security Infrastructure

Cybersecurity Essentials 3.0

Module Objectives

Module Title: Network Security Infrastructure

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

Topic Title	Topic Objective
Security Devices	Explain how specialized devices are used to enhance network security.
Security Services	Explain how network services enhance network security.

6.1 Security Devices

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 Layer 7 firewall and inline intrusion prevention system (IPS).
- Cisco Talos provides global threat intelligence.

Firewalls

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

Common Firewall Properties:

- Firewalls are resistant to network attacks.
- Firewalls are the only transit point between internal corporate networks and external networks because all traffic flows through the firewall.
- Firewalls enforce the access control policy.

Firewall Benefits:

- They prevent the exposure of sensitive hosts, resources, and applications to untrusted users.
- They sanitize protocol flow, which prevents the exploitation of protocol flaws.
- They block malicious data from servers and clients.
- They reduce security management complexity by off-loading most of the network access control to a few firewalls in the network.

Firewalls (Cont.)

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

Firewall Limitations:

- A misconfigured firewall can have serious consequences for the network, such as becoming a single point of failure.
- The data from many applications cannot be passed over firewalls securely.
- Users might proactively search for ways around the firewall to receive blocked material, which exposes the network to potential attack.
- Network performance can slow down.
- Unauthorized traffic can be tunneled or hidden as legitimate traffic through the firewall.

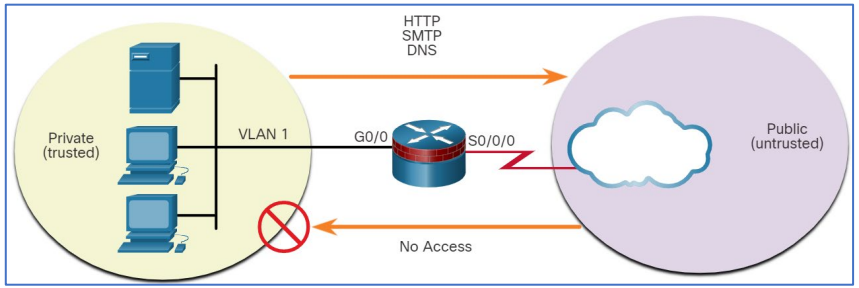
Common Security Architectures

Firewall design is primarily about device interfaces permitting or denying traffic based on the source, the destination, and the type of traffic. Three common firewall designs are:

Private and Public

The public network (or outside network) is untrusted, and the private network (or inside network) is trusted. Typically, a firewall with two interfaces is configured as follows:

- Traffic originating from the private network is permitted and inspected as it travels toward the public network. Inspected traffic returning from the public network and associated with traffic that originated from the private network is permitted.
- Traffic originating from the public network and traveling to the private network is generally blocked.



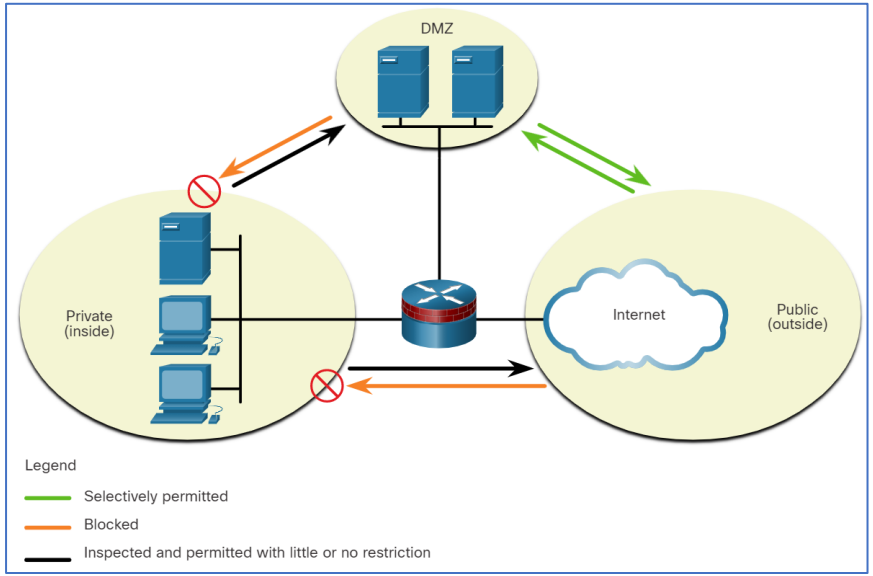
Common Security Architectures (Cont.)

Demilitarized Zone (DMZ)

A firewall design where there is typically one inside interface connected to the private network, one outside interface connected to the public network, and one DMZ interface.

Typical firewall DMZ configuration:

- Traffic originating from the private network is permitted and inspected as it travels toward the public network. Inspected traffic returning from the public network and associated with traffic that originated from the private network is permitted.
- Traffic originating from the public network and traveling to the private network is generally blocked.

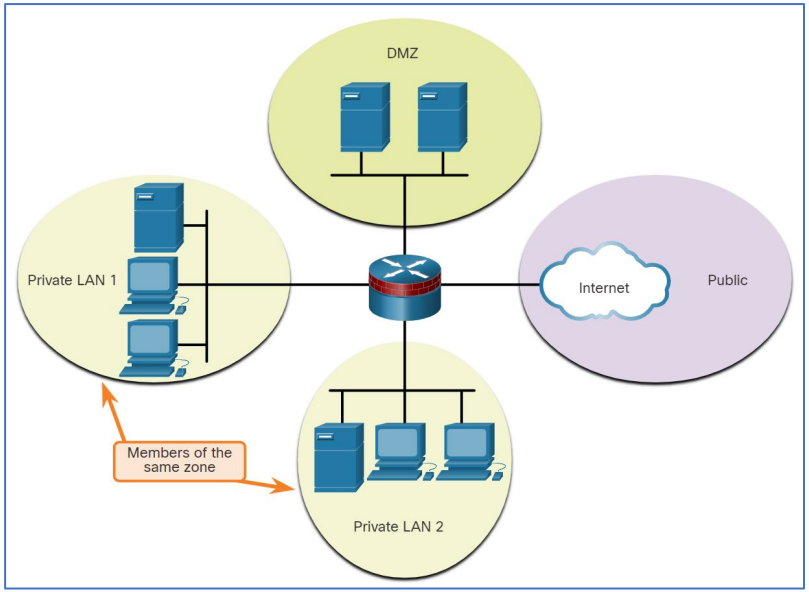


Common Security Architectures (Cont.)

Zone-Based Policy Firewalls (ZPFs)

ZPFs use zones to provide additional flexibility. A zone is a group of one or more interfaces that have similar functions or features. Zones are used to specify where a Cisco IOS firewall rule or policy should be applied.

- Security policies for LAN 1 and LAN 2 are similar and can be grouped into a zone for firewall.
- The traffic between interfaces in the same zone is not subject to any policy and passes freely.
- All zone-to-zone traffic is blocked and to permit traffic between zones, a policy allowing or inspecting traffic must be configured.
- The only exception to this default **deny any** policy is the router self-zone.



Firewall Type Descriptions

Four common types of firewalls are:

Firewall Type	Firewall Features
Packet Filtering (Stateless) Firewall	Packet filtering firewalls are usually part of a router firewall, which permits or denies traffic based on Layer 3 and Layer 4 information. They are stateless firewalls.
Stateful Firewall	Stateful firewalls provide stateful packet filtering by using connection information maintained in a state table. It analyzes traffic at OSI Layer 3 through 5.
Application Gateway Firewall	An application gateway firewall (proxy firewall) filters information at Layers 3, 4, 5, and 7 of the OSI model. Most of the firewall control and filtering is done in software.
Next Generation Firewalls	Next-generation firewalls (NGFW) go beyond stateful firewalls by providing integrated intrusion prevention, application awareness and control, upgrade paths to include future information feeds, and techniques to address evolving security threats.

Firewall Type Descriptions (Cont.)

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 the various firewall types.

Intrusion Prevention and Detection Devices

Common Characteristics of intrusion detection system (IDS) and intrusion prevention system (IPS):

- Both technologies are deployed as sensors in the form of several different devices:
  - A router configured with Cisco IOS IPS software
  - A device specifically designed to provide dedicated IDS or IPS services
  - A network module installed in an adaptive security appliance (ASA), switch, or router

- Both technologies use signatures to detect patterns of misuse in network traffic. A signature is a set of rules that an IDS or IPS uses to detect malicious activity.

- Both can detect atomic patterns (single-packet) or composite patterns (multi-packet).

Advantages and Disadvantages of IDS and IPS

Solution	Advantages	Disadvantages
IDS	• No Impact on network (latency, jitter) • No Network impact if there is a sensor failure • No network impact if there is sensor overload	• Response action cannot stop trigger packets • Correct tuning required for response actions • More vulnerable to network security evasion techniques
IPS	• Stops trigger packets • Can use stream normalization techniques	• Sensor issues might affect network traffic • Sensor overloading impacts the network • Some impact on network (latency, jitter)

Deployment Considerations:

- Both an IPS and an IDS can be deployed; they 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 available: host-based IPS (HIPS) and network-based IPS.

Host-based IPS (HIPS)

- HIPS is Software installed on a host to monitor and analyze suspicious activity.
- HIPS can monitor abnormal activity and prevent the host from executing commands that do not match typical behavior.
- Network traffic can also be monitored to prevent the host from participating in a denial-of-service (DoS) attack or being part of an illicit FTP session.

HIPS Advantages	HIPS Disadvantages
• Provides protection specific to a host operating system • Provides operating system and application-level protection • Protects the host after the message is decrypted	• Operating system dependent • Must be installed on all hosts

Types of IPS (Cont.)

There are two primary kinds of IPS available: host-based IPS (HIPS) and network-based IPS.

Network-based IPS

- A network-based IPS can be implemented using a dedicated or non-dedicated IPS device.
- Network-based IPS implementations are a critical component of intrusion prevention.
- There are host-based IDS/IPS solutions, but these must be integrated with a network-based IPS implementation to ensure a robust security architecture.
- Sensors detect malicious and unauthorized activity in real-time and can act when required.

Specialized Security Appliances

There are a variety of specialized security appliances available. Three examples are:

Appliance	Explanation
Cisco Advanced Malware Protection (AMP)	• An enterprise-class advanced malware analysis and protection solution • Provides comprehensive malware protection for organizations before, during, and after an attack • Accesses the collective security intelligence of the Cisco Talos Security Intelligence and Research Group
Cisco Web Security Appliance (WSA)	• A secure web gateway that combines leading protections to help organizations address the growing challenges of securing and controlling web traffic • Protects the network by automatically blocking risky sites and testing unknown sites before allowing users to access them • Provides malware protection, application visibility and control, acceptable use policy controls, insightful reporting, and secure mobility
Cisco Email Security Appliance (ESA)	• Defends mission-critical email systems • Constantly updated by real-time feeds from the Cisco Talos • Features include spam blocking, advanced malware protection, and outbound message control

6.2 Security Services

Video - Security Services

This video will cover the follow:

- Intrusion Detection Systems (IDS)
- Switched Port Analyzer (SPAN)
- Syslog
- Authentication, Authorization, and Accounting (AAA)
- NetFlow
- SNMP

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. ACLs perform the following tasks:

- They limit network traffic to increase network performance.
- They provide traffic flow control.
- They provide a basic level of security for network access.
- They filter traffic based on traffic type
- They screen hosts to permit or deny access to network services.

In addition to either permitting or denying traffic, ACLs can be used for selecting types of traffic to be analyzed, forwarded, or processed in other ways.

ACLs: Important Features

Two types of Cisco IPv4 ACLs are standard and extended.

Standard ACLs can be used to permit or deny traffic only from source IPv4 addresses. The destination of the packet and the ports involved are not evaluated.

Extended ACLs filter 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

ACLs: Important Features (Cont.)

- Standard and extended ACLs can be created using either a number or a name to identify the ACL and its list of statements.

- By configuring ACL logging, an ACL message can be generated and logged when traffic meets the permit or deny criteria defined in the ACL.

- Cisco ACLs can also be configured to only allow TCP traffic that has an ACK or RST bit set, so that only traffic from an established TCP session is permitted. This can be used to deny any TCP traffic from outside the network that is trying to establish a new TCP session.

Packet Tracer - ACL Demonstration

In this Packet Tracer activity, you will complete the following objectives:

- Part 1: Verify Local Connectivity and Test Access Control List
- Part 2: Remove Access Control List and Repeat Test

SNMP

- Simple Network Management Protocol (SNMP) allows administrators to manage end devices such as servers, workstations, routers, switches, and security appliances, on an IP network.
- It enables network administrators to monitor and manage network performance, find and solve network problems, and plan for network growth.
- The SNMP system consists of two elements:
  - SNMP manager that runs SNMP management software
  - SNMP agents which are the nodes being monitored and managed
- The Management Information Base (MIB) is a database on the agents that stores data and operational statistics about the device.
- The SNMP manager is part of a network management system (NMS).
- The SNMP manager can collect information from an SNMP agent by using the “get” action and can change configurations on an agent by using the “set” action.
- In addition, SNMP agents can forward information directly to a network manager by using “traps”.

NetFlow

- 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, and IP accounting for billing purposes.
- NetFlow technology distinguishes packet flows using a combination of seven fields:
  - Source IP address
  - Destination IP address
  - Source port number
  - Destination port number
  - Layer 3 protocol type
  - Type of Service (ToS) marking
  - Input logical interface

Port Mirroring

- **Packet analyzer (packet sniffer or traffic sniffer) limitation** - because network switches can isolate traffic, traffic sniffers or other network monitors, such as IDS, cannot access all the traffic on a network segment.

- **Port mirroring** is a feature that allows a switch to make duplicate copies of traffic passing through a switch, and then send it out a port with a network monitor attached. The original traffic is forwarded in the usual manner.

Syslog Servers

- When certain events occur on a network, networking devices have trusted mechanisms to notify the administrator with detailed system messages.
- Network administrators have a variety of options for storing, interpreting, and displaying these messages, and for being alerted to those messages.
- Syslog protocol is the most common method of accessing system messages.

- The syslog logging service 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

- Network Time Protocol (NTP) is important to synchronize the time across all devices on the network. When the time is not synchronized between devices, it will be impossible to determine the order of the events that have occurred in different parts of the network.

- As a network grows, it becomes difficult to ensure that all infrastructure devices are operating with synchronized time.

- A solution to keep time setting synchronized is configuring the Network Time Protocol (NTP).

- NTP protocol allows routers on the network to synchronize their time settings with an NTP server.

- A group of NTP clients that obtain time and date information from a single source have more consistent time settings.

NTP (Cont.)

NTP networks use a hierarchical system of time sources. Each level in this hierarchical 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. These authoritative time sources, also referred to as stratum 0 devices, are high-precision timekeeping devices assumed to be accurate and with little or no delay associated with them.
- **Stratum 1** -The stratum 1 devices are directly connected to the authoritative time sources. They act as the primary network time standard.
- **Stratum 2 and lower strata** - The stratum 2 servers are connected to stratum 1 devices through network connections. Stratum 2 devices, such as NTP clients, synchronize their time using the NTP packets from stratum 1 servers. They could also act as servers for stratum 3 devices.

AAA Servers

Three independent security functions provided by the AAA architectural framework are authentication, authorization, and accounting.

AAA Provides	Description
Authentication	• 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	• After the user is authenticated, authorization services determine which resources the user can access and which operations the user is allowed to perform.
Accounting	• 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.

AAA Servers (Cont.)

Terminal Access Controller Access-Control System Plus (TACACS+) and Remote Authentication Dial-In User Service (RADIUS) are both authentication protocols used to communicate with AAA servers.

	TACACS+	RADIUS
Functionality	Separates AAA according to the AAA architecture, allowing modularity of the security server implementation	Combines authentication and authorization but separates accounting, allowing less flexibility in implementation than TACACS+
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 a per-user or per-group basis	Has no option to authorize router commands on a per-user or per-group basis
Accounting	Limited	Extensive

VPN

- A virtual private network (VPN) is a private network that is created over a public network, usually the internet. VPN uses virtual connections that are routed through the internet from the organization to the remote site.
- A VPN connects two endpoints, such as a remote office to a central office, over a public network, to form a logical connection. The logical connections can be made at either Layer 2 or Layer 3.
- A VPN is private in that the traffic is encrypted to keep the data confidential while it is transported across the public network.
- Common examples of Layer 3 VPNs are GRE, Multiprotocol Label Switching (MPLS), and IPsec.
- Layer 3 VPNs can be point-to-point site connections, such as GRE and IPsec, or they can establish any-to-any connectivity to many sites using MPLS.
- VPNs are commonly deployed in a site-to-site topology to securely connect central sites with remote locations. They are also deployed in a remote-access topology to provide secure remote access to external users travelling or working from home.

6.3 Network Security Infrastructure Summary

What Did I Learn in this Module?

Security Devices

- There are several different types of firewalls include packet filtering (stateless), stateful inspection firewall, application gateway (proxy), and next-generation firewalls.
- Firewall design is primarily about device interfaces permitting or denying traffic based on the source, the destination, and the type of traffic.
- Intrusion prevention systems (IPS) and intrusion detection systems (IDS) are used to detect potential security risks and alert/stop unsafe traffic.
- IDS/IPS can be implemented as host-based or network based.
- Specialized security appliances include Cisco Advanced Malware Protection (AMP), Cisco Web Security Appliance (WSA), and Cisco Email Security Appliance (WSA).
- These security appliances utilize the services of the Cisco Talos Security Intelligence and Research Group.
- Talos detects and correlates threats in real-time using the largest threat-detection network in the world.

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

Security Services

- ACLs are a series of statements that control whether a device forwards or drops packets based on information found in the packet header.
- NTP synchronizes the system time across all devices on the network to ensure accurate and consistent timestamping of system messages.
- Syslog servers compile and provide access to the system messages generated by networking devices.
- 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.
- AAA is a framework for configuring user authentication, authorization, and accounting services. AAA typically uses a TACACS+ or RADIUS server for this purpose.
- VPNs are private networks that are created between two endpoints across a public network.