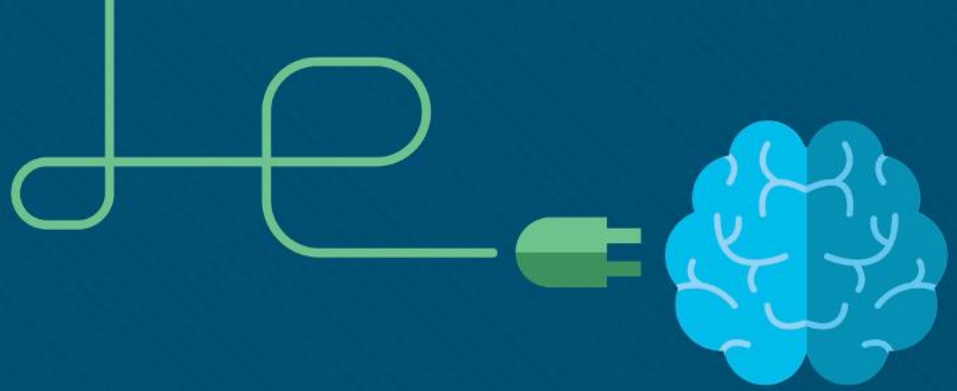


Topic 8: Firewalls and Access Control

Cybersecurity Essentials 3.0

Module 13: Access Control

Cybersecurity Essentials 3.0

Module Objectives

Module Title: Access Control

Module Objective: Configure local and server-based access control.

Topic Title	Topic Objective
Access Controls	Configure secure access on a host.
Access Control Concepts	Explain how access control protects network data.
Account Management	Explain the need for account management and access control strategies.
AAA Usage and Operation	Configure server-based authentication with TACACS+ and RADIUS.

13.1 Access Controls

Physical Access Controls

- **Physical access controls** are actual barriers deployed to prevent direct physical contact with systems.

- The goal is to prevent unauthorized users from gaining physical access to facilities, equipment, and other organizational assets.

- Some examples of physical access controls are:
  - Guards to monitor the facility
  - Fences to protect the perimeter
  - Motion detectors to detect moving objects
  - Laptop locks to safeguard portable equipment
  - Locked doors to prevent unauthorized access
  - Swipe cards to allow access to restricted areas
  - Guard dogs to protect the facility
  - Video cameras to monitor a facility by collecting and recording images
  - Mantrap-style entry systems to stagger the flow of people into the secured area and trap any unwanted visitors
  - Alarms to detect intrusion

Logical Access Controls

- **Logical access controls** are the hardware and software solutions used to manage access to resources and systems.

- These technology-based solutions include tools and protocols that computer systems use for identification, authentication, authorization, and accountability.

- Logical access control examples
  - Encryption is the process of taking plaintext and creating ciphertext.
  - Smart cards have an embedded microchip.
  - Passwords are protected strings of characters.
  - Biometrics are users' physical characteristics.
  - Access control lists (ACLs) define the type of traffic allowed on a network.
  - Protocols are sets of rules that govern the exchange of data between devices.
  - Firewalls prevent unwanted network traffic.
  - Routers connect at least two networks.
  - Intrusion detection systems monitor a network for suspicious activities.
  - Clipping levels are certain allowed thresholds for errors before triggering a red flag.

Administrative Access Controls

- **Administrative access controls** are the policies and procedures defined by organizations to implement and enforce all aspects of controlling unauthorized access.

- Administrative controls focus on personnel and business practices.

- Examples of administrative controls
  - Policies are statements of intent.
  - Procedures are the detailed steps required to perform an activity.
  - Hiring practices define the steps an organization takes to find qualified employees.
  - Background checks are a type of employee screening that includes information of past employment verification, credit history, and criminal history.
  - Data classification categorizes data based on its sensitivity.
  - Security training educates employees about the security policies at an organization.
  - Reviews evaluate an employee's job performance.

Administrative Access Controls in Detail

- The concept of administrative access controls involves three security services: authentication, authorization, and accounting (AAA).

- These services provide the primary framework to control access, preventing unauthorized access to a computer, network, database, or other data resource.

- **Authentication:**
  - It verifies the identity of each user, to prevent unauthorized access.
  - Users prove their identity with a username or ID.
  - In addition, users need to verify their identity by providing one of the following:
    - Something they know (such as a password)
    - Something they have (such as a token or card)
    - Something they are (such as a fingerprint)
    - In the case of two factor authentication, which is increasingly becoming the norm, the system requires a combination of two of the above rather than just one to verify someone's identity.

Administrative Access Controls in Detail (Cont.)

- **Authorization**:
  - It determines which resources users can access, along with the operations that users can perform.
  - Some systems accomplish this by using an access control list, or an ACL.
    - An ACL determines whether a user has certain access privileges once the user authenticates.
    - It can also control when a user has access to a specific resource.

- **Accounting:**
  - It keeps track of what users do — including what they access, the amount of time they access resources, and any changes they make.
  - Cybersecurity accounting services track each data transaction and provide auditing results.
  - System administrators can set up computer policies to enable system auditing.
  - Cybersecurity accounting tracks and monitors in real time.

- The concept of AAA is like using a credit card that identifies who can use it, how much that user can spend, and accounts for items or services the user purchased.

What Is Identification?

- It enforces the rules established by the authorization policy.
- Every time access to a resource is requested, the access controls determine whether to grant or deny access.
- A unique identifier ensures the proper association between allowed activities and subjects.
- A username is the most common method used to identify a user.
- A username can be an alphanumeric combination, a personal identification number (PIN), a smart card or biometric — such as a fingerprint, retina scan, or voice recognition.
- A unique identifier ensures that a system can identify each user individually, therefore allowing an authorized user to perform the appropriate actions on a particular resource.

Federated Identity Management

- It refers to multiple enterprises that let their users use the same identification credentials to gain access to the networks of all enterprises in the group.
- Unfortunately, this broadens the scope and increases the probability of a cascading effect should an attack occur.
- A federated identity links a subject's electronic identity across separate identity management systems, such as being able to access several websites using the same social login credentials.
- The goal of federated identity management is to share identity information automatically across castle boundaries.
- From the individual user's perspective, this means a single sign-on to the web.
- It is imperative that organizations scrutinize the identifying information shared with partners, even within the same corporate group, for example.
- The sharing of social security numbers, names, and addresses may allow identity thieves the opportunity to steal this information from a partner to perpetrate fraud.
- The most common way to protect federated identity is to tie login ability to an authorized device.

Authentication Methods

- Users prove their identity with a username or ID and need to verify their identity by providing one of the following.

What you know:

- Passwords, passphrases, or PINs are all examples of something that the user knows.
- The terms passphrase, passcode, passkey, and PIN are all generically referred to as password — a string of characters used to prove a user's identity.
- A password should be at least eight characters and contain a combination of upper and lowercase letters, numbers, and special characters.
- Users need to use different passwords for different systems because if a criminal cracks the user's password once, the criminal will have access to all the user's accounts.

Authentication Methods (Cont.)

What you have:

- Smart cards and security key fobs are examples of something that users possess that can be used for authentication purposes.
- A smart card is a small plastic card, about the size of a credit card, with a small chip embedded in it that is capable of processing, storing, and safeguarding data.
- A security key fob is a device that is small enough to attach to a keyring.
- In most cases, security key fobs are used for two factor authentication (2FA), which is much more secure than a username and password combination.

Authentication Methods (Cont.)

Who you are:

- Biometric security compares unique physical characteristics against stored profiles to authenticate users.

- There are two types of biometric identifiers:
  - **Physiological characteristics** — fingerprints, DNA, face, hands, retina, or ear features.
  - **Behavioral characteristics** — patterns of behavior such as gestures, voice, gait, or typing rhythm.

- Biometrics is becoming increasingly popular in public security systems, consumer electronics and point-of-sale applications.

- Implementing biometrics involves a reader or scanning device, software that converts the scanned information into digital form and a database that has biometric data stored for comparison.

Multi-Factor Authentication

- It uses at least two methods of verification — such as a password and something you have, for example, a security key fob.
- This can be taken a step further by adding something you are, such as a fingerprint scan.
- Multi-factor authentication can reduce the incidence of online identity theft because it means knowing a password will not give cybercriminals access to a user's account.
- Note that two-factor authentication (2FA) is a method of multi-factor authentication that entails two factors, but the two terms are often used interchangeably.

Authorization

Authorization controls what a user can and cannot do on the network after successful authentication.

- After a user proves their identity, the system checks to see what network resources the user can access and what they can do with the resources.

When to implement authorization

- Authorization uses a set of attributes that describes the user's access to the network, to answer the question, 'What read, copy, edit, create, and delete privileges does this user have?'

- The system compares these attributes to the information contained within the authentication database, determines a set of restrictions for that user, and delivers it to the local device where the user is connected.

- Authorization is automatic and does not require users to perform additional steps after authentication.

- System administrators have set the network up to implement authorization immediately after the user authenticates.

Authorization (Cont.)

Using authorization

- Defining authorization rules is the first step in controlling access.
- An authorization policy establishes these rules.
- A group membership policy defines authorization based on users' membership in a specific group.
- All employees of an organization may have a swipe card, for example, which provides access to the premises, but it might not allow access to a server room.
- An authority-level policy defines access permissions based on an employee's position within the organization.

Implementing Accountability

- **What is accountability?**
  - Accountability traces an action back to a person or process making this change to a system.
  - It then collects this information and reports the usage data.
  - The organization can use this data for such purposes as auditing or billing.
- **Implementing accountability**
  - Implementing accountability consists of technologies, policies, procedures, and education.
  - Log files provide detailed information based on the parameters chosen.
  - The organization's policies and procedures spell out what actions should be recorded and how the log files are generated, reviewed, and stored.

Implementing Accountability (Cont.)

- **Providing accountability**
  - Data retention, media disposal, and compliance requirements all provide accountability.
  - Many laws require the implementation of measures to secure different data types.
  - These laws guide an organization on the right way to handle, store, and dispose of data.
  - The education and awareness of an organization's policies, procedures, and related laws can also contribute to accountability.

13.2 Access Control Concepts

Zero Trust Security

- **Zero trust** is a comprehensive approach to securing all access across networks, applications, and environments.
- This approach helps secure access from users, end-user devices, APIs, IoT, microservices, containers, and more.
- A zero trust security framework helps to prevent unauthorized access, contain breaches, and reduce the risk of an attacker's lateral movement through a network.
- Traditionally, the network perimeter (edge) was the boundary between inside and outside, or trusted and untrusted.
- In a zero trust approach, any place at which an access control decision is required should be considered a perimeter.
- This means that although a user or other entity may have successfully passed access control previously, they are not trusted to access another area or resource until they are authenticated.

Zero Trust Security (Cont.)

The three pillars of zero trust are **workforce, workloads,** and **workplace:**

Zero Trust for the Workforce

- This pillar consists of people (e.g., employees, contractors, partners, and vendors) who access work applications by using their personal or corporate-managed devices.
- It ensures only the right users and secure devices can access applications, regardless of location.

Zero Trust for Workloads

- This pillar is concerned with applications that are running in the cloud, in data centers, and other virtualized environments that interact with one another.
- It focuses on secure access when an API, a microservice, or a container is accessing a database within an application.

Zero Trust for the Workplace

- This pillar focuses on secure access for all devices, including on the internet of things (IoT), that connect to enterprise networks, such as user endpoints, physical and virtual servers, printers, cameras, HVAC systems, kiosks, infusion pumps, industrial control systems, and more.

Access Control Models

- An organization must implement proper access controls to protect its network resources, information system resources, and information.
- A security analyst should understand the different basic access control models to have a better understanding of how attackers can break the access controls.
- One access control model is the principle of least privilege, which specifies a limited, as-needed approach to granting user and process access rights to specific information and tools.
- A common exploit is known as privilege escalation.
  - Vulnerabilities in servers or access control systems are exploited to grant an unauthorized user, or software process, higher levels of privilege than they should have.

Access Control Models (Cont.)

Access Control Models	Description
Discretionary access control (DAC)	This is the least restrictive model and allows users to control access to their data as owners of that data. DAC may use ACLs or other methods to specify which users or groups of users have access to the information.
Mandatory access control (MAC)	This applies the strictest access control and is typically used in military or mission critical applications. It assigns security level labels to information and enables users with access based on their security level clearance.
Role-based access control (RBAC)	Access decisions are based on an individual's roles and responsibilities within the organization. Different roles are assigned security privileges, and individuals are assigned to the RBAC profile for the role. Roles may include different positions, job classifications, or groups of job classifications. Also known as a type of non-discretionary access control.
Attribute-based access control (ABAC)	ABAC allows access based on attributes of the object (resource) to be accessed, the subject (user) accessing the resource, and environmental factors regarding how the object is to be accessed, such as time of day.
Rule-based access control (RBAC)	Network security staff specify sets of rules regarding or conditions that are associated with access to data or systems. These rules may specify permitted or denied IP addresses, or certain protocols and other conditions. Also known as Rule-Based RBAC.
Time-based access control (TAC)	TAC Allows access to network resources based on time and day.

Network Access Control (NAC) Systems

- They support access management by enforcing organizational policies regarding the people and devices that are attempting to access the network.

- NAC systems allow cybersecurity professionals to monitor the users and devices that are attached to the network, and manually control access as required.

- Network access control systems provide the following capabilities:
  - Rapidly enforcing access policies that have been created for different operational conditions.
  - Recognizing and profiling connected users and devices to prevent malicious software on non-compliant systems from causing damage.
  - Providing secure access to network guests, often through registration portals.
  - Evaluating device compliance with security policies by user type, device type, and operating system prior to permitting network access.
  - Mitigating security incidents by blocking, isolating, or repairing non-compliant devices.

Network Access Control (NAC) Systems (Cont.)

- Because BYOD and IoT networking greatly expand the network attack surface, NAC system automation features make focused control of network access by such devices practical.
- The NAC system is configured to enforce organizational policies.
- The relevant policies are enacted to permit or deny network access according to a wide range of factors that the NAC system detects on the devices that are attempting access.
- Without NAC systems it would be impossible for cybersecurity personnel to evaluate the thousands of devices that could attempt to access the network.
- NAC is an important component of a zero-trust security architecture that enforces security policy compliance with all devices and users that attempt to access the network.

13.3 Account Management

Account Types

- An organization should not share accounts for privileged users, administrators, or applications.
- The administrator account should only be used to administer a system.
- If a user accesses a malware-infected website or opens a malicious email while using the administrator account, this would put the organization at risk.
- Administrators must be aware of the default group and user accounts that might be installed by an operating system.
- Knowing about these accounts will help an administrator decide which should be permitted and which of these accounts should be disabled.
- Default accounts such as the guest or administrator accounts can be a security risk in older systems as attackers are familiar with the default settings used.
- To improve security, always replace any default accounts and make sure that all account types require a password.

Account Types (Cont.)

It's important to properly manage accounts to maintain security.

- On hiring a new employee, create an identity profile, register the employee's computer and mobile devices, and enable access to the organization's network. As the Identity Provider (IdP), the organization is responsible for authenticating their identity.
- Disable or deactivate any accounts that are no longer needed and retrieve any organizational data or applications from the user's devices.
- Grant a user no more access than is necessary to perform assigned tasks (least privilege).
- Review user access to identify any access control adjustments that need to be made.
- Use time of day restrictions to control when a user can log in.
- Use location restrictions to control where a device or user can log in from.
    - Geofencing is used to trigger an action when a user enters or exits a geographic boundary.
    - Geolocation identifies a device based on its geographic location.
    - Geotagging adds an identifier to something based on the location (like a photo taken on a smartphone tagged with the coordinates of where the photo was taken).

Privileged Accounts

- Cybercriminals target privileged accounts because these are the most powerful accounts in the organization with elevated, unrestricted access to systems.
- Administrators use these accounts to deploy and manage operating systems, applications, and network devices.
- Continuously securing and locking down privileged accounts is critical to the security of the organization. Regularly evaluate this process and adjust to improve protection.

Privileged Accounts (Cont.)

Organizations should adopt robust practices for securing privileged accounts.

- Identify and reduce the number of privileged accounts.
- Enforce the principle of least privilege. The principle means that users, systems, and processes only have access to resources (networks, systems, and files) that are necessary to perform their assigned function.
- Revoke access rights when employees leave or change jobs.
- Eliminate shared accounts with passwords that do not expire.
- Secure password storage.
- Eliminate shared credentials for multiple administrators.
- Automatically change privileged account passwords every 30 or 60 days.
- Record privileged sessions.
- Implement a process to change embedded passwords for scripts and service accounts.
- Log all user activity.
- Generate alerts for unusual behavior.
- Disable inactive privileged accounts.
- Use multi-factor authentication for all administrative access.
- Implement a gateway between the end user and sensitive assets to limit network exposure to malware.

File Access Control

- **Permissions** are rules configured to limit folder or file access for an individual or a group and can help secure data.
- Users should be limited to only the resources they need on a computer system or network.
- It may be easier to provide access to the entire drive, but it is more secure to limit access to only the folder they need.
- This is the principle of **least privilege** and closely connected to the concept of 'need to know' access.
- Limiting access to resources also prevents cybercriminals from accessing those resources if the user's computer becomes infected.

File Access Control (Cont.)

Permission levels available for files and folders

Full Control: Users can:

- See the contents of a file or folder.
- Change and delete existing files and folders.
- Create new files and folders.
- Run programs in a folder.

Modify: Users can change and delete existing files and folders but cannot create new ones.

Read and execute: Users can see the contents of existing files and folders and can run programs in a folder.

Write: Users can create new files and folders and make changes to existing files and folders.

Read: Users can see the contents of a folder and open files and folders.

File Access Control (Cont.)

- If an administrator denies an individual or group permissions to a network share, this will override any other permission settings.
  - The user cannot access that share, even if the user is the administrator or part of the administrator group.

- The local security policy must outline the resources and the type of access allowed for each user and group.

- After parent folder permissions have been set, folders and files created inside the parent folder inherit its permissions.

- The location of data and the action performed on it also determine the permission propagation:
  - Data moved to the same volume will keep the original permissions.
  - Data copied to the same volume will inherit new permissions.
  - Data moved to a different volume will inherit new permissions.
  - Data copied to a different volume will inherit new permission.

Account Policies in Windows

- In most networks that use Windows computers, an administrator configures Active Directory with domains on a Windows server.
- Windows computers that join the domain become domain members.
- The administrator configures a **domain security policy** that applies to all domain members.
- When a computer is not part of an Active Directory domain, the user configures policies through Windows Local Security Policy.
- In all versions of Windows except Home edition, enter ‘secpol.msc’ at the Run command to open the Local Security Policy tool.

Configuring Security Policies:

- **Password Policy**
  - An administrator can configure user account policies such as password policies and lockout policies.
  - Passwords must contain eight characters and three of the following four categories: uppercase letters, lowercase letters, numbers, and symbols.
  - Lastly, the user can reuse a password after 24 unique passwords.
  - Different password policies can be set, depending on organizational requirements and needs.

Account Policies in Windows (Cont.)

- **Account Lockout Policy**
  - An account lockout policy locks an account for a set duration when too many incorrect login attempts occur.
  - For example, a policy allows a user to enter the wrong username and/or password five times.
    - After five attempts, the account locks users out for 30 minutes.
    - After 30 minutes, the number of attempts resets to zero and the user can attempt to log in again.

- **Audit Policies**
  - More security settings are available by selecting the ‘local policies’ folder in Windows.
  - An audit policy creates a security log file used to track the following events:
    - Account logon events
    - Audit account management
    - Directory service access
    - Object access
    - Policy changes
    - Privilege use
    - Process tracking
    - System events

Authentication Management

- Authentication and authorization issues include unencrypted credentials, incorrect permissions, and access violations.

- Authentication management aims to ensure secure sign in while still providing ease of use:
  - A **Single Sign On (SSO)** solution allows the user to use one set of login credentials to authenticate across multiple applications. This way, the user only needs to remember one strong password.
  - **OAuth** is a standard that enables a user's account information to be used by third-party services such as Facebook or Google.
  - A **password vault** can protect and store the user's credentials with a single strong password required to access them.
  - Many organizations implement **Knowledge-Based Authentication (KBA)** to provide a password reset should a user forget their password. KBA is based on personal information known by the user or a series of questions.

Hash-Based Message Authentication Code (HMAC)

- HMAC uses an encryption key with a hash function to authenticate a web user.
  - Using HMAC, the user sends a private key identifier and an HMAC.
  - The server looks up the user's private key and creates an HMAC.
  - The user's HMAC must match the one calculated by the server.

- Many web services use basic authentication, which does not encrypt the username and password during transmission.

- VPNs using IPsec rely on HMAC functions to authenticate the origin of every packet and provide data integrity checking.

Hash-Based Message Authentication Code (HMAC) (Cont.)

- Cisco products use hashing for entity authentication, data integrity, and data authenticity purposes.
- Cisco IOS routers use hashing with secret keys in an HMAC-like manner to add authentication information to routing protocol updates.
- IPsec gateways and clients use hashing algorithms, such as MD5 and SHA-1 in HMAC mode, to provide packet integrity and authenticity.
- Cisco software images on Cisco.com have an MD5-based checksum available so that customers can check the integrity of downloaded images.

Authentication Protocols and Technologies

- An authentication protocol authenticates data between two entities to prevent unauthorized access.
- The word ‘entity’ can refer to any device or system within an organization.
- A protocol outlines the type of information that needs to be shared to authenticate and connect.

Authentication Protocols and Technologies

Extensible Authentication Protocol (EAP)	A password from the client is sent using a hash to the authentication server. The authentication server has a certificate (the client does not need a certificate).
Password Authentication Protocol (PAP)	A username and password are sent to a remote access server in plaintext. Most network operating system remote servers support PAP.
Challenge Handshake Authentication Protocol (CHAP)	It validates the identity of remote clients using a one-way hashing function created by the client. The service also calculates the expected hash value. The server (the authenticator) compares the two values. If the values match, transmission continues.
802.1X	An organization authenticates your identity and authorizes access to the network. Your identity is determined based on credentials or a certificate which is confirmed by a RADIUS server.
RADIUS	Use it to either accept or deny access when simple username/password authentication is needed. It only encrypts the user's password from client to the server.
TACACS+	It encrypts all data (username, password, accounting and authorized services) between the client and the server.
Kerberos	It uses strong encryption, requesting a client to prove its identity to a server, with the server in turn authenticating itself to the client.

Applications of Cryptographic Hash Functions

- Cryptographic hash functions help us to ensure data integrity and verify authentication.

- Cryptographic hash functions are used in the following situations:
  - To provide proof of authenticity when used with a symmetric secret authentication key such as IP security (IPsec) or routing protocol authentication.
  - To provide authentication by generating one-time and one-way responses to challenges in authentication protocols.
  - To provide message integrity check proof (such as those used in digitally signed contracts) and Public Key Infrastructure (PKI) certificates (like those accepted when accessing a secure website).

- When choosing a hashing algorithm, use SHA-256 or higher, as they are currently the most secure. Avoid SHA-1 and MD5 due to security flaws that have been discovered.

Access Control Strategies

Mandatory access control	It restricts the actions that a user can perform on an object (a file, a port or a device). An authorization rule enforces whether a user can access the object. Organizations use it where different levels of security classifications exist. Every object has a label, and every user has a clearance. Its system restricts a user based on the security classification of the object and the label attached to the user.
Discretionary access control	In systems that employ them, the owner of an object can decide which users can access that object and what specific access they may have. Permissions and access control lists can be used to implement it. The owner of a file can specify what permissions (read, write, or execute) other users may have. An ACL uses rules to determine what traffic can enter or exit a network.
Role-based access control	It depends on the role or job function of the user. It can work in combination with discretionary access controls or mandatory access controls by enforcing the policies of either one. It helps to implement security administration in large organizations with hundreds of users and thousands of possible permissions.
Rule-based access control	It uses ACLs to help determine whether to grant access. A series of rules is contained in the ACL and the decision to grant access depends on these rules. As with mandatory access control, users cannot change the access rules. Organizations can combine rule-based access control with other strategies for implementing access restrictions.

13.4 AAA usage and operation

AAA Operation

- A network must be designed to control who is allowed to connect to it and what they are allowed to do when they are connected.
- These design requirements are identified in the network security policy.
- The policy specifies how network administrators, corporate users, remote users, business partners, and clients access network resources.
- The network security policy can also mandate the implementation of an accounting system that tracks who logged in, when, and what they did while logged in.
- The **Authentication, Authorization, and Accounting (AAA)** protocol provides the necessary framework to enable scalable access security.
- The three independent security functions provided by the AAA architectural framework are authentication, authorization, and accounting.
- This concept is like the use of a credit card.
    - The credit card identifies who can use it, how much that user can spend, and keeps account of what items the user spent money on.

AAA Operation (Cont.)

The three independent security functions provided by the AAA architectural framework:

AAA Component	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. An example is “User ‘student’ can access host server XYZ using SSH only.”
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. An example is "User ‘student’ accessed host server XYZ using SSH for 15 minutes."

AAA Authentication

- AAA Authentication can be used to authenticate users for administrative access or remote network access.

- Cisco provides two common methods of implementing AAA services:
  - **Local AAA Authentication:** It is sometimes known as self-contained authentication because it authenticates users against locally stored usernames and passwords. Ideal for small networks.
  - **Server-Based AAA Authentication:** This method authenticates against a central AAA server that contains the usernames and passwords for all users. It is appropriate for medium-to-large networks.

- Centralized AAA is more scalable and manageable than local AAA authentication and it is the preferred AAA implementation.
  - Its system may independently maintain databases for authentication, authorization, and accounting.
  - It can leverage Active Directory or LDAP for user authentication and group membership, while maintaining its own authorization and accounting databases.

- Devices communicate with the centralized AAA server using either the RADIUS or TACACS+ protocols.

AAA Authentication (Cont.)

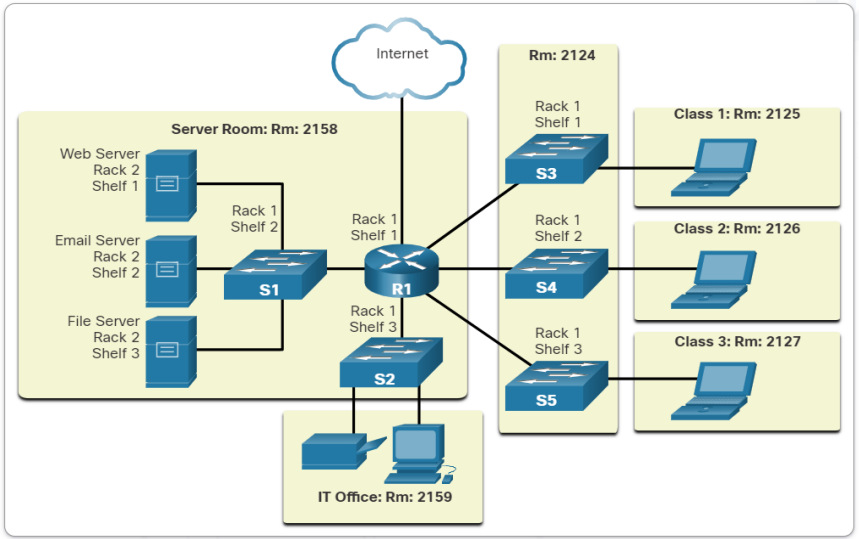
The table lists the differences between the two protocols.

	TACACS+	RADIUS
Functionality	It separates authentication, authorization, and accounting functions according to the AAA architecture, allowing modularity of the security server implementation.	It combines authentication and authorization but separates accounting, allowing less flexibility in implementation than TACACS+.
Standard	Mostly Cisco supported	Open/RFC standard
Transport	TCP port 49	UDP ports 1812/1813, or 1645/1646
Protocol CHAP	Bidirectional challenge and response as used in CHAP.	Unidirectional challenge and response from the RADIUS security server to the RADIUS client.
Confidentiality	Encrypts the entire body of the packet but leaves a standard TACACS+ header.	Encrypts only the password in the access-request packet from the client to the server. The remainder of the packet is unencrypted.
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

AAA Accounting Logs

- Centralized AAA also enables the use of the Accounting method.
- Accounting records from all devices are sent to centralized repositories, which simplifies auditing of user actions.
- AAA Accounting collects and reports usage data in AAA logs that are useful for security auditing.
- The collected data might include the start and stop connection times, executed commands, number of packets, and number of bytes.
- One widely deployed use of accounting is to combine it with AAA authentication.
- This helps with managing access to internetworking devices by network administrative staff.
- Accounting provides more security than just authentication.
- The AAA servers keep a detailed log of exactly what the authenticated user does on the device.
- The log contains numerous data fields, including the username, the date and time, and the actual command that was entered by the user.
- This information is useful when troubleshooting devices. It also provides evidence against individuals who perform malicious actions.

AAA Accounting Logs (Cont.)



1. When a user has been authenticated, the AAA accounting process generates a start message to begin the accounting process.

2. When the user finishes, a stop message is recorded and the accounting process ends.

AAA Accounting Logs (Cont.)

The table displays the various types of accounting information that can be collected:

Type of Accounting Information	Description
Network Accounting	It captures information for all PPP sessions, including packet and byte counts.
Connection Accounting	It captures information about all outbound connections made from the AAA client, such as by SSH
EXEC Accounting	It captures information about user EXEC terminal sessions (user shells) on the network access server, including username, date, start and stop times, and the access server IP address.
System Accounting	It captures information about all system-level events (for example, when the system reboots or when accounting is turned on or off).
Command Accounting	It captures information about the EXEC shell commands for a specified privilege level, as well as the date and time each command was executed, and the user who executed it.
Resource Accounting	The Cisco implementation of AAA accounting captures “start” and “stop” record support for connections that have passed user authentication. The additional feature of generating “stop” records for connections that fail to authenticate as part of user authentication is also supported.

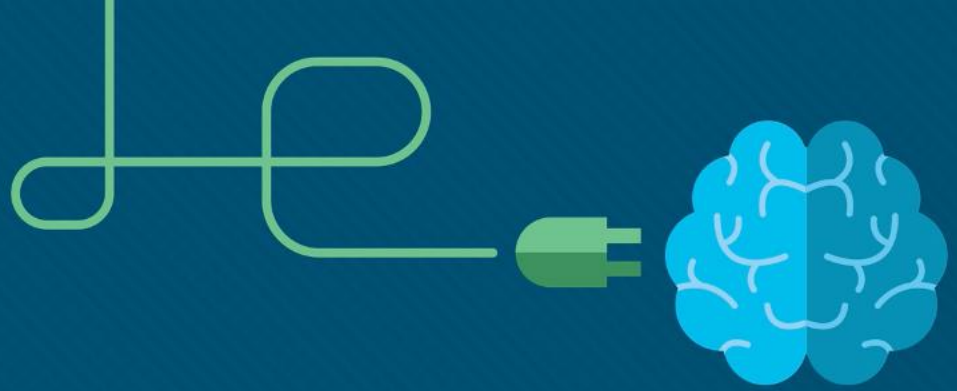
13.5 Access Control Summary

What Did I Learn in this Module?

- Physical access controls are actual barriers deployed to prevent direct physical contact with systems.
- Logical access controls are hardware and software solutions used to manage access resources and systems.
- Administrative access controls involves three security services: authentication, authorization, and accounting.
- Identification enforces the rules established by the authorization process.
- Authorization controls what a user can and cannot do on the network after successful authentication.
- Accountability traces an action back to a person or process making the change to the system.
- The CIA triad consists of confidentiality, integrity, and availability.
- Zero trust is a comprehensive approach to securing all access across networks, applications, and environments.
- Access control methods include DAC, MAC, RBAC, ABAC, RBAC, and TAC.
- Privilege escalation is a common exploit where vulnerabilities in servers or access control systems are exploited to grant access to an unauthorized user or software process.
- Account types can include administrator accounts, user accounts, service accounts, and guest accounts.
- Permission levels can be assigned to files and folders to include full control, modify, read and execute, write, and read.
- Robust practices for securing privileged accounts must be taken because they are often the target of cybercriminals.

What Did I Learn in this Module?

- Authentication management aims to ensure secure sign in while still providing ease of use.
- HMAC uses an encryption key with a hash function to authenticate a web user.
- An authentication protocol authenticates data between two entities to prevent unauthorized access.
- A network must be designed to control who is allowed to connect to it and what they are allowed to do when they are connected.
- AAA systems provide the necessary framework to enable scalable security.
- AAA authentication can be used to authenticate users for local access, or it can be used to authenticate users for remote network access.
- Cisco provides two common methods of implementing AAA services: Local AAA Authentication and Server-based AAA Authentication.
- Centralized AAA is more scalable and manageable than local AAA and is the preferred AAA implementation.
- A centralized AAA system can leverage Active Directory or LDAP for user authentication and group membership, while maintaining its own authorization and accounting databases.
- Devices communicate with the centralized AAA server using with the RADIUS or TACACS+ protocols.
- Centralized AAA also enables the use of the accounting method that reports usage data in AAA logs.
- Various types of accounting information that can be collected are network accounting, connection accounting, EXEC accounting, system accounting, command accounting, and resource accounting.



Module 14: Access Control Lists

Cybersecurity Essentials 3.0

Module Objectives

Module Title: Access Control Lists

Module Objective: Implement access control lists (ACLs) to filter traffic and mitigate network attacks.

Topic Title	Topic Objective
Introduction to Access Control Lists	Describe standard and extended IPv4 ACLs.
Wildcard Masks	Explain how ACLs use wildcard masks.
Configure ACLs	Explain how to configure ACLs.
Modify ACLs	Use sequence numbers to edit existing standard IPv4 ACLs.
Implement ACLs	Implement ACLs.
Mitigate Attacks with ACLs	Use ACLs to mitigate common network attacks.
IPv6 ACLs	Configure IPv6 ACLs using the CLI.

82

14.1 Introduction to Access Control Lists

83

What is an ACL?

- An ACL is a series of IOS commands that are used to filter packets based on information found in the packet header.
- By default, a router does not have any ACLs configured.
- However, when an ACL is applied to an interface, the router performs the additional task of evaluating all network packets as they pass through the interface to determine if the packet can be forwarded.
- An ACL uses a sequential list of permit or deny statements, known as access control entries (ACEs).
- When network traffic passes through an interface configured with an ACL, the router compares the information within the packet against each ACE, in sequential order, to determine if the packet matches one of the ACEs.

Note: ACEs are also commonly called ACL statements.

84

What is an ACL? (Cont.)

Several tasks performed by routers require the use of ACLs to identify traffic. The table lists some of these tasks with examples based on a corporate policy.

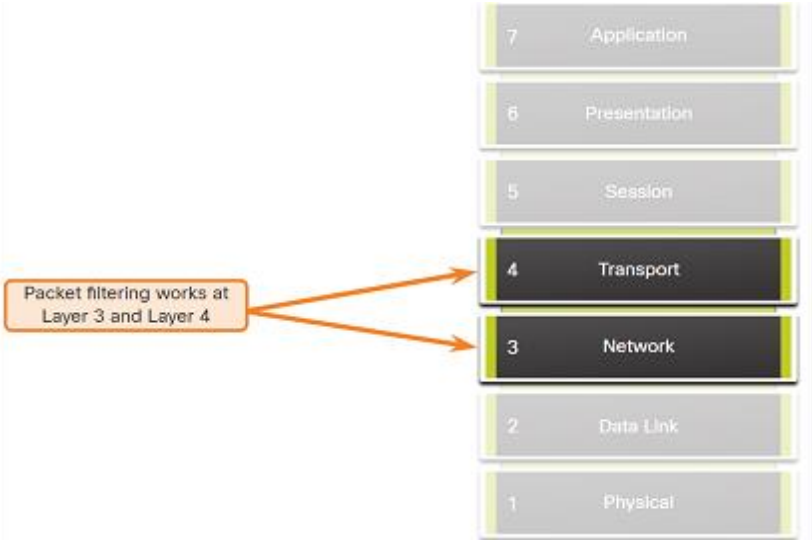
Task	Example
Limit network traffic to increase network performance	Video traffic is prohibited on the network to reduce the network load. A policy can be enforced using ACLs to block video traffic.
Provide traffic flow control	Routing protocol traffic should be limited to certain links only. A policy can be implemented using ACLs to restrict the delivery of routing updates to only those that come from a known source.
Provide a basic level of security for network access	Access to the Human Resources network should be restricted to authorized users only. A policy can be enforced using ACLs to limit access to specified networks.
Filter traffic based on traffic type	Email traffic should be permitted into a network, but Telnet access denied. A policy can be implemented using ACLs to filter traffic by type.
Screen hosts to permit or deny access to network services	Access to some file types should be limited to user groups. A policy can be implemented using ACLs to filter user access to services.
Provide priority to certain classes of network traffic	Voice traffic should be forwarded as fast as possible to avoid any interruption. A policy can be implemented using ACLs and QoS services to identify voice traffic and process it immediately.

Packet Filtering

- Packet filtering controls access to a network by analyzing the incoming and/or outgoing packets and forwarding them or discarding them based on given criteria.

- Packet filtering can occur at Layer 3 or Layer 4.

- Cisco routers support two types of ACLs:
  - **Standard ACLs** - ACLs only filter at Layer 3 using the source IPv4 address only.
  - **Extended ACLs** - ACLs filter at Layer 3 using the source and / or destination IPv4 address.
    - They can also filter at Layer 4 using TCP, UDP ports, and optional protocol type information for finer control.



Numbered and Named ACLs

- **Numbered ACLs**
  - ACLs number 1 to 99, or 1300 to 1999 are standard ACLs.
  - ACLs number 100 to 199, or 2000 to 2699 are extended ACLs, as shown in the output.

```
R1(config)# access-list ?
  <1-99>        IP standard access list
  <100-199>     IP extended access list
  <1100-1199>   Extended 48-bit MAC address access list
  <1300-1999>   IP standard access list (expanded range)
  <200-299>     Protocol type-code access list
  <2000-2699>   IP extended access list (expanded range)
  <700-799>     48-bit MAC address access list
  rate-limit    Simple rate-limit specific access list
  template      Enable IP template acls
R1(config)# access-list
```

Numbered and Named ACLs (Cont.)

- **Named ACLs**
  - It is the preferred method to use when configuring ACLs.
  - Specifically, standard and extended ACLs can be named to provide information about the purpose of the ACL.
  - The **ip access-list** global configuration command is used to create a named ACL

```
R1(config)# ip access-list extended FTP-FILTER
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq ftp
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq ftp-data
R1(config-ext-nacl)#
```

- The rules to follow for named ACLs:
  - Assign a name to identify the purpose of the ACL.
  - Names can contain alphanumeric characters.
  - Names cannot contain spaces or punctuation.
  - It is suggested that the name be written in CAPITAL LETTERS.
  - Entries can be added or deleted within the ACL.

ACL Operation

- ACLs define the set of rules that give added control for packets that enter inbound interfaces, packets that relay through the router, and packets that exit outbound interfaces of the router.
- ACLs can be configured to apply to inbound traffic and outbound traffic.

- Inbound ACL
  - It filters packets before they are routed to the outbound interface.
  - It is efficient because it saves the overhead of routing lookups if the packet is discarded.
  - If the packet is permitted by the ACL, it is then processed for routing.
  - Best used to filter packets when the network attached to an inbound interface is the only source of packets that need to be examined.

- Outbound ACL
  - It filters packets after being routed, regardless of the inbound interface.
  - Incoming packets are routed to the outbound interface and processed through the outbound ACL.
  - Best used when the same filter will be applied to packets coming from multiple inbound interfaces before exiting the same outbound interface.

89

ACL Operation (Cont.)

- When an ACL is applied to an interface, it follows a specific operating procedure.
- The operational steps used when traffic has entered a router interface with an inbound standard IPv4 ACL configured are:
  1. The router extracts the source IPv4 address from the packet header.
  2. The router starts at the top of the ACL and compares the source IPv4 address to each ACE in a sequential order.
  3. When a match is made, the router carries out the instruction, either permitting or denying the packet, and the remaining ACEs in the ACL, if any, are not analyzed.
  4. If the source IPv4 address does not match any ACEs in the ACL, the packet is discarded because there is an implicit deny ACE automatically applied to all ACLs.

- The last ACE statement of an ACL is always an implicit deny that blocks all traffic, and it is automatically implied at the end of an ACL even though it is hidden and not displayed in the configuration.

Note: An ACL must have at least one permit statement otherwise all traffic will be denied due to the implicit deny ACE statement.

14.2 Wildcard Masking

91

Wildcard Mask Overview

- An IPv4 ACE uses a 32-bit wildcard mask to determine which bits of the address to examine for a match.
- Wildcard masks are also used by the Open Shortest Path First (OSPF) routing protocol.
- A wildcard mask is like a subnet mask in that it uses the ANDing process to identify which bits in an IPv4 address to match.
- However, they differ in the way they match binary 1s and 0s.
- Unlike a subnet mask, in which binary 1 is equal to a match and binary 0 is not a match, in a wildcard mask, the reverse is true.
- Wildcard masks use the following rules to match binary 1s and 0s:
  - **Wildcard mask bit 0** - Match the corresponding bit value in the address
  - **Wildcard mask bit 1** - Ignore the corresponding bit value in the address

Wildcard Mask Overview (Cont.)

The table lists some examples of wildcard masks and what they would identify.

Wildcard Mask	Last Octet (in Binary)	Meaning (0 - match, 1 - ignore)
0.0.0.0	00000000	Match all octets.
0.0.0.63	00111111	Match the first three octets Match the two left most bits of the last octet Ignore the last 6 bits
0.0.0.15	00001111	Match the first three octets Match the four left most bits of the last octet Ignore the last 4 bits of the last octet
0.0.0.252	11111100	Match the first three octets Ignore the six left most bits of the last octet Match the last two bits
0.0.0.255	11111111	Match the first three octets Ignore the last octet

93

Wildcard Mask Types

- ACL 10 needs an ACE that only permits host 192.168.1.1.
- “0” equals a match and “1” equals ignore.
- To match a specific host IPv4 address, a wildcard mask 0.0.0.0 is required.
- The resulting ACE in ACL 10 would be **access-list 10 permit 192.168.1.1 0.0.0.0**.

	Decimal	Binary
IPv4 address	192.168.1.1	11000000.10101000.00000001.00000001
Wildcard Mask	0.0.0.0	00000000.00000000.00000000.00000000
Permitted IPv4 Address	192.168.1.1	11000000.10101000.0000001.0000001

- ACL 10 needs an ACE that permits all hosts in the 192.168.1.0/24 network.
- The wildcard mask 0.0.0.255 stipulates that the very first three octets must match exactly but not the fourth octet.
- The resulting ACE in ACL 10 would be **access-list 10 permit 192.168.1.0 0.0.0.255**.

	Decimal	Binary
IPv4 address	192.168.1.1	11000000.10101000.00000001.00000001
Wildcard Mask	0.0.0.255	00000000.00000000.00000000.11111111
Permitted Host IPv4 Addresses	192.168.1.1 to 192.168.1.254	11000000.10101000.00000001.00000001 11000000.10101000.00000001.11111111

Wildcard Mask Types (Cont.)

- ACL 10 needs an ACE that permits all hosts in the 192.168.16.0/24, 192.168.17.0/24, …, 192.168.31.0/24 networks.
- The wildcard mask 0.0.15.255 would correctly filter that range of addresses.
- The highlighted wildcard mask bits identify which bits of the IPv4 address must match.
- The resulting ACE in ACL 10 would be **access-list 10 permit 192.168.16.0 0.0.15.255.**

	Decimal	Binary
IPv4 address	192.168.16.0	11000000.10101000.00010000.0000000
Wildcard Mask	0.0.15.255	00000000.00000000.00001111.11111111
Permitted Host IPv4 Addresses	192.168.16.1 to 192.168.31.254	11000000.10101000.00010000.00000000 11000000.10101000.00011111.11111111

Wildcard Mask Calculation

- In this example, assume you wanted an ACE in ACL 10 to permit network access for the 14 users in the subnet 192.168.3.32/28.
- Subtract the subnet (i.e., 255.255.255.240) from 255.255.255.255, as shown in the table.
- This solution produces the wildcard mask 0.0.0.15.
- Therefore, the ACE would be **access-list 10 permit 192.168.3.32 0.0.0.15.**

Starting value	**255.255.255.255**
Subtract the subnet mask	- 255.255.255.240
Resulting wildcard mask	0.0.0.15

Wildcard Mask Calculation (Cont.)

- In this example you need an ACL number 10 to match networks in the range between 192.168.16.0/24 to 192.168.31.0/24.
- This network range could be summarized as 192.168.16.0/20 which is a subnet mask of 255.255.240.0.
- Therefore, subtract 255.255.240.0 subnet mask from 255.255.255.255, as shown in the table.
- This solution produces the wildcard mask 0.0.15.255.
- Therefore, the ACE would be **access-list 10 permit 192.168.16.0 0.0.15.255.**

Starting value	**255.255.255.255**
Substract the subnet maskk	- 255.255.240.0
Resulting wildcard mask	0.0.15.255

Wildcard Mask Keywords

- Cisco IOS provides two keywords to identify the most common uses of wildcard masking:
  - **host** - It substitutes the 0.0.0.0 mask. This mask states that all IPv4 address bits must match to filter just one host address.
  - **any** - It substitutes the 255.255.255.255 mask. This mask says to ignore the entire IPv4 address or to accept any addresses.

- In the example, the ACL 10 ACE permits only the 192.168.10.10 host and the ACL 11 ACE permits all hosts.

```
R1(config)# access-list 10 permit 192.168.10.10  0.0.0.0
R1(config)# access-list 11 permit  0.0.0.0 255.255.255.255
R1(config)#
```

- The keywords **host** and **any** could have been used to replace the highlighted output, accomplishing the same task as the previous commands.

```
R1(config)# access-list 10 permit  host  192.168.10.10
R1(config)# access-list 11 permit  any
R1(config)#
```

14.3 Configure ACLs

99

Create an ACL

- All ACLs must be planned, especially true for ACLs requiring multiple ACEs.

- When configuring a complex ACL, it is suggested to:
  - Use a text editor and write out the specifics of the policy to be implemented.
  - Add the IOS configuration commands to accomplish those tasks.
  - Include remarks to document the ACL.
  - Copy and paste the commands onto the device.
  - Always thoroughly test an ACL to ensure that it correctly applies the desired policy.

- These recommendations enable you to create the ACL thoughtfully without impacting the traffic on the network.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential 100

Numbered Standard IPv4 ACL Syntax

- To create a numbered standard ACL, use the following global configuration command:
  Router(config)# **access-list** *access-list-number* {**deny** | **permit** | **remark** *text*} *source* [*source-wildcard*] [**log**]
- Use the **no access-list** *access-list-number* global configuration command to remove it.
- The table provides a detailed explanation of the syntax for a standard ACL.

Parameter	Description
access-list-number	The decimal number of the ACL. Standard ACL number range is 1 to 99 or 1300 to 1999.
deny	This denies access if the condition is matched.
permit	This permits access if the condition is matched.
remark text (Optional)	This adds a text entry for documentation purposes. Remarks are extremely useful, especially in longer or more complex ACLs. Each remark is limited to 100 characters.
source	This identifies the source network or host address to filter. Use the **any** keyword to specify all networks. Use the **host** ip-address keyword or simply enter an ip-address to identify a specific IP address.
source-wildcard (Optional)	A 32-bit wildcard mask applied to the source. If omitted, a default 0.0.0.0 mask is assumed.
Log (Optional)	This keyword generates an informational message whenever the ACE is matched.

101

Named Standard IPv4 ACL Syntax

- To create a named standard ACL, use the following global configuration command:

  Router(config)# **ip access-list standard** *access-list-name*

- This command enters the named standard configuration mode where you configure the ACL ACEs.
- ACL names are alphanumeric, case sensitive, and must be unique.
- Capitalizing ACL names is not required but makes them stand out when viewing the running-config output.
- It also makes it less likely that you will accidentally create two different ACLs with the same name but with different uses of capitalization.

Note: Use the **no ip access-list standard** access-list-name global configuration command to remove a named standard IPv4 ACL.

Named Standard IPv4 ACL Syntax (Cont.)

- In the example, a named standard IPv4 ACL called NO-ACCESS is created.
- Notice that the prompt changes to named standard ACL configuration mode.
- ACE statements are entered in the named standard ACL sub configuration mode.
- Use the help facility to view all the named standard ACL ACE options.
- The three highlighted options are configured like the numbered standard ACL.
- Unlike the numbered ACL method, there is no need to repeat the initial **ip access-list** command for each ACE.

```
R1(config)# ip access-list standard NO-ACCESS
R1(config-std-nacl)# ?
Standard Access List configuration commands:
  <1-2147483647> Sequence Number
  default        Set a command to its defaults
  deny           Specify packets to reject
  exit           Exit from access-list configuration mode
  no             Negate a command or set its defaults
  permit         Specify packets to forward
  remark         Access list entry comment
R1(config-std-nacl)#
```

Numbered Extended IPv4 ACL Syntax

- The extended ACL is first configured, and then it is activated on an interface.
- To create a numbered extended ACL, use the following global configuration command:

Router(config)# **access-list** *access-list-number* {**deny** | **permit** | **remark** *text*} *protocol source source-wildcard* [*operator* {*port*}] *destination destination-wildcard* [*operator* {*port*}] [**established**] [**log**]

- Use the **no access-list** *access-list-number* global configuration command to remove an extended ACL.
- The command to apply an extended IPv4 ACL to an interface is the same for standard IPv4 ACLs.

Router(config-if)# **ip access-group** {*access-list-number* | *access-list-name*} {**in** | **out**}

- To remove an ACL from an interface, first enter the **no ip access-group** interface configuration command.
- To remove the ACL from the router, use the **no access-list** global configuration command.

104

Numbered Extended IPv4 ACL Syntax (Cont.)

Parameter	Description
access-list-number	The ACL decimal number Extended ACL number range is 100 to 199 and 2000 to 2699.
deny	This denies access if the condition is matched.
permit	This permits access if the condition is matched.
remark text (Opt.)	Adds a text entry for documentation purposes. Each remark is limited to 100 characters.
protocol	Name or number of an internet protocol.
source	The source network or host address to filter.
source-wildcard	(Optional) A 32-bit wildcard mask that is applied to the source.
destination	The destination network or host address to filter.
destination-wildcard	(Optional) This is a 32-bit wildcard mask that is applied to the destination.
operator	(Optional) This compares source or destination ports. Some operators: **lt**, **gt**, **eq**, **neq**.
port (Optional)	The decimal number or name of a TCP or UDP port.
established (Opt.)	For the TCP protocol only. This is a 1st generation firewall feature.
Log (Optional)	It generates and sends an informational message whenever the ACE is matched.

Protocols and Port Numbers

- Extended ACLs can filter on many different types of internet protocols and ports.

- **Protocol Options**
  - The four highlighted protocols are the most popular options.

Note: Use the **?** to get help when entering a complex ACE. If an internet protocol is not listed, then the IP protocol number could be specified.

```
R1(config)# access-list 100 permit ?
<0-255>           An IP protocol number
ahp               Authentication Header Protocol
dvmrp             dvmrp
eigrp             Cisco's EIGRP routing protocol
esp               Encapsulation Security Payload
gre               Cisco's GRE tunneling
icmp              Internet Control Message Protocol
igmp              Internet Gateway Message Protocol
ip                Any Internet Protocol
ipinip            IP in IP tunneling
nos               KA9Q NOS compatible IP over IP tunneling
object-group      Service object group
ospf              OSPF routing protocol
pcp               Payload Compression Protocol
pim               Protocol Independent Multicast
tcp               Transmission Control Protocol
udp               User Datagram Protocol
R1(config)# access-list 100 permit
```


106

Protocols and Port Numbers (Cont.)

- **Port Keyword Options**
  - Selecting a *protocol* influences *port* options. For instance, selecting the:
    tcp protocol would provide TCP related ports options
    udp protocol would provide UDP specific ports options
    icmp protocol would provide ICMP related ports (i.e., message) options
  - The highlighted ports are popular options.
  - Port names or number can be specified, but port names make it easier to understand the purpose of an ACE.

```
R1(config)# access-list 100 permit tcp any any eq ?
<0-65535>        Port number
bgp              Border Gateway Protocol (179)
chargen          Character generator (19)
cmd              Remote commands (rcmd, 514)
daytime          Daytime (13)
discard          Discard (9)
domain           Domain Name Service (53)
echo             Echo (7)
exec             Exec (rsh, 512)
finger           Finger (79)
ftp              File Transfer Protocol (21)
ftp-data         FTP data connections (20)
gopher           Gopher (70)
hostname         NIC hostname server (101)
ident            Ident Protocol (113)
irc              Internet Relay Chat (194)
klogin           Kerberos login (543)
kshell           Kerberos shell (544)
login            Login (rlogin, 513)
lpd              Printer service (515)
```

Protocols and Port Numbers Configuration Examples

- Extended ACLs can filter on different port number and port name options.
- This example configures an extended ACL 100 to filter HTTP traffic.
- The first ACE uses the **www** port name.
- The second ACE uses the port number **80**. Both ACEs achieve the same result.

```
R1(config)# access-list 100 permit tcp any any eq www
R1(config)# !or...
R1(config)# access-list 100 permit tcp any any eq 80
```

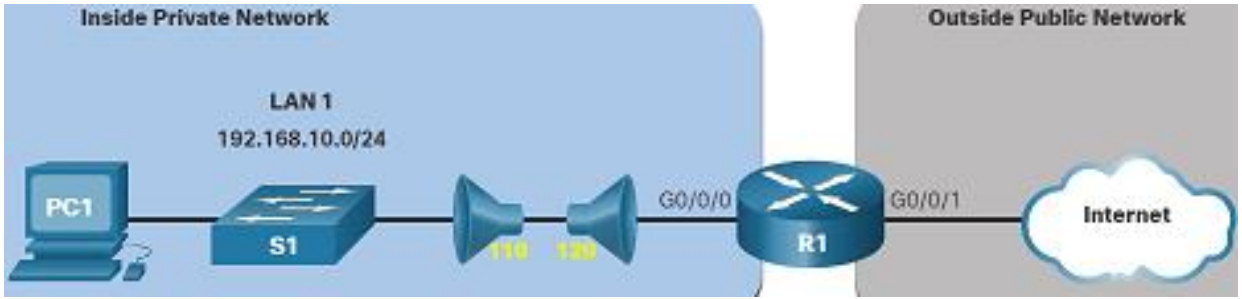
- Configuring the port number is required when there is not a specific protocol name listed such as SSH (port number 22) or an HTTPS (port number 443), as shown in the next example.

```
R1(config)# access-list 100 permit tcp any any eq 22
R1(config)# access-list 100 permit tcp any any eq 443
R1(config)#
```


108

TCP Established Extended ACL

- TCP can also perform basic stateful firewall services using the TCP **established** keyword, that enables inside traffic to exit the inside private network and permits the returning reply traffic to enter the inside private network.
- TCP traffic generated by an outside host and attempting to communicate with an inside host is denied.
- The **established** keyword can be used to permit only the return HTTP traffic from requested websites, while denying all other traffic.
- The topology shows ACL 110 (previously configured) that will filter traffic from the inside private network.
- ACL 120, using the **established** keyword, will filter traffic coming into the inside private network from the outside public network.



TCP Established Extended ACL (Cont.)

- ACL 120 is configured to only permit returning web traffic to the inside hosts, and then applied outbound the R1 G0/0/0 interface.
- The **show access-lists** command displays both ACLs.
- The match statistics shows that inside hosts have been accessing the secure web resources from the internet.

```
R1(config)# access-list 120 permit tcp any 192.168.10.0 0.0.0.255 established
R1(config)# interface g0/0/0
R1(config-if)# ip access-group 120 out
R1(config-if)# end
R1# show access-lists
Extended IP access list 110
    10 permit tcp 192.168.10.0 0.0.0.255 any eq www
    20 permit tcp 192.168.10.0 0.0.0.255 any eq 443 (657 matches)
Extended IP access list 120
    10 permit tcp any 192.168.10.0 0.0.0.255 established (1166 matches)
R1#
```

- The **established** parameter allows only responses to traffic that originates from the 192.168.10.0/24 network to return to that network.
- A match occurs if the returning TCP segment has the ACK or reset (RST) flag bits set.
- Without the **established** parameter in the ACL statement, all traffic would be permitted.

110

Named Extended IPv4 ACL Syntax

- To create a named extended ACL, use the following global configuration command:

  Router(config)# **ip access-list extended** *access-list-name*

- This command enters the named extended configuration mode.
- Recall that ACL names are alphanumeric, case sensitive, and must be unique.
- In the example, a named extended ACL called NO-FTP-ACCESS is created and the prompt changed to named extended ACL configuration mode.
- ACE statements are entered in the named extended ACL sub configuration mode.

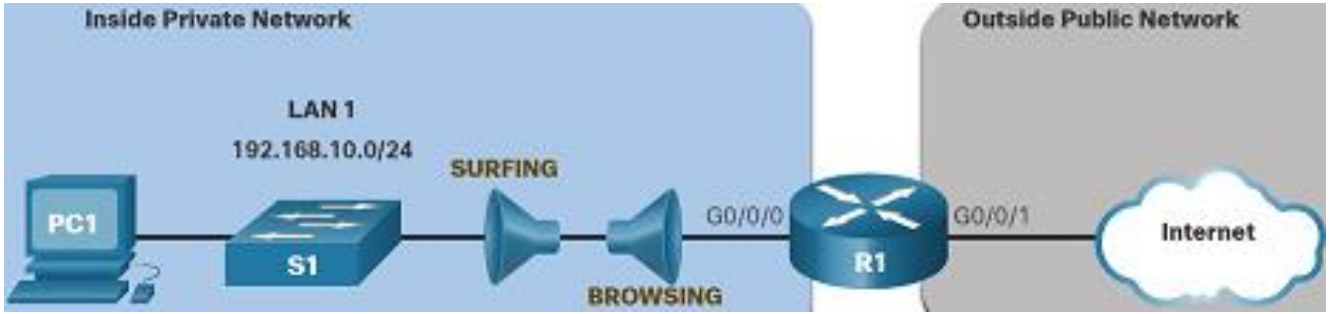
  R1(config)# **ip access-list extended NO-FTP-ACCESS**
  R1(config-ext-nacl)#

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential 111

Named Extended IPv4 ACL Example

- Named extended ACLs are created in essentially the same way that named standard ACLs are created.

- The topology demonstrates configuring and applying two named extended IPv4 ACLs to an interface:
  - **SURFING -** This will permit inside HTTP and HTTPS traffic to exit to the internet.
  - **BROWSING -** This will only permit returning web traffic to the inside hosts while all other traffic exiting the R1 G0/0/0 interface is implicitly denied.



Named Extended IPv4 ACL Example (Cont.)

- The SURFING ACL permits HTTP and HTTPS traffic from inside users to exit the G0/0/1 interface connected to the internet.
- Web traffic returning from the internet is permitted back into the inside private network by the BROWSING ACL.
- SURFING ACL is applied inbound and BROWSING ACL applied outbound on the R1 G0/0/0 interface.
- Inside hosts have been accessing the secure web resources from the internet.
- The **show access-lists** command is used to verify the ACL statistics.
- The permit secure HTTPS counters (i.e., eq 443) in the SURFING ACL and the return established counters in the BROWSING ACL have increased.

```
R1(config)# ip access-list extended SURFING
R1(config-ext-nacl)# Remark Permits inside HTTP and HTTPS traffic
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq 80
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1(config-ext-nacl)# exit
R1(config)#
R1(config)# ip access-list extended BROWSING
R1(config-ext-nacl)# Remark Only permit returning HTTP and HTTPS traffic
R1(config-ext-nacl)# permit tcp any 192.168.10.0 0.0.0.255 established
R1(config-ext-nacl)# exit
R1(config)# interface g0/0/0
R1(config-if)# ip access-group SURFING in
R1(config-if)# ip access-group BROWSING out
R1(config-if)# end
R1# show access-lists
Extended IP access list SURFING
    10 permit tcp 192.168.10.0 0.0.0.255 any eq www
    20 permit tcp 192.168.10.0 0.0.0.255 any eq 443 (124 matches)
Extended IP access list BROWSING
    10 permit tcp any 192.168.10.0 0.0.0.255 established (369 matches)
R1#
```

14.4 Named Standard IPv4 ACL Syntax

114

Two Methods to Modify an ACL

- After an ACL is configured, it may need to be modified.
- ACLs with multiple ACEs can be complex to configure. Sometimes the configured ACE does not yield the expected behaviors.
- For these reasons, ACLs may initially require a bit of trial and error to achieve the desired filtering result.
- This section will discuss two methods to use when modifying an ACL:
  - Use a Text Editor
  - Use Sequence Numbers

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential 115

Text Editor Method

- ACLs with multiple ACEs should be created in a text editor.
- This allows you to plan the required ACEs, create the ACL, and then paste it into the router interface.
- It also simplifies the tasks to edit and fix an ACL.
- For example, assume ACL 1 was entered incorrectly using **19** instead of **192** for the first octet, as shown in the running configuration.

```
R1# show run | section access-list
access-list 1 deny 19.168.10.10
access-list 1 permit 192.168.10.0 0.0.0.255
R1#
```


© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential 116

Text Editor Method (Cont.)

- The first ACE should have been to deny the host at 192.168.10.10., but it was incorrectly entered.

- To correct the error:
  - Copy the ACL from the running configuration and paste it into the text editor.
  - Make the necessary changes.
  - Remove the previously configured ACL on the router. Otherwise, pasting the edited ACL commands will only append (i.e., add) to the existing ACL ACEs on the router.
  - Copy and paste the edited ACL back to the router.

- Assume that ACL 1 has now been corrected. The incorrect ACL must be deleted, and the corrected ACL 1 statements must be pasted in global configuration mode, as shown in the output.

```
R1(config)# no access-list 1
R1(config)#
R1(config)# access-list 1 deny 19.168.10.10
R1(config)# access-list 1 permit 192.168.10.0 0.0.0.255
R1(config)#
```


117

Sequence Number Method

- An ACL ACE can also be deleted or added using the ACL sequence numbers. Sequence numbers are automatically assigned when an ACE is entered.

- These numbers are listed in the **show access-lists** command. The **show running-config** command does not display sequence numbers.

- In the previous example, the incorrect ACE for ACL 1 is using sequence number 10, as shown in the example.

```
R1# show access-lists
Standard IP access list 1
    10 deny 19.168.10.10
    20 permit 192.168.10.0, wildcard bits 0.0.0.255
R1#
```

Sequence Number Method (Cont.)

- Use the **ip access-list standard** command to edit an ACL. Statements cannot be overwritten using the same sequence number as an existing statement.
- Therefore, the current statement must be deleted first with the **no 10** command.
- Then the correct ACE can be added using sequence number 10 is configured.
- Verify the changes using the **show access-lists** command, as shown in the example.

```
R1# conf t
R1(config)# ip access-list standard 1
R1(config-std-nacl)# no 10
R1(config-std-nacl)# 10 deny host 192.168.10.10
R1(config-std-nacl)# end
R1# show access-lists
Standard IP access list 1
    10 deny 192.168.10.10
    20 permit 192.168.10.0, wildcard bits 0.0.0.255
R1#
```

14.5 Implement ACLs

120

ACL Configuration Guidelines

- An ACL is made up of one or more ACEs or statements.

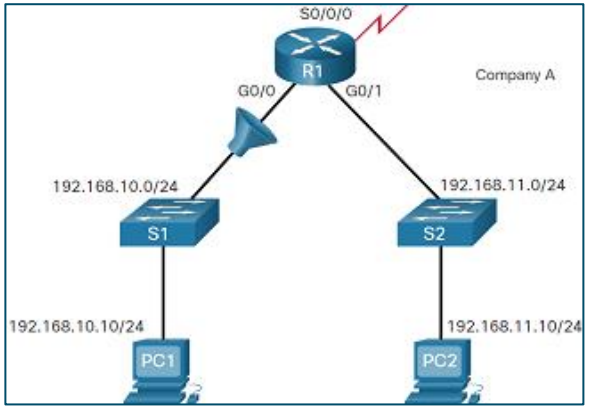
- When configuring and applying an ACL, be aware of the guidelines summarized in this list:
  - Create an ACL globally and then apply it.
  - Ensure the last statement is an implicit **deny any** or **deny ip any any**.
  - Statement order is important because ACLs are processed top-down.
  - As soon as a statement is matched the ACL is exited.
  - Always filter from the most specific to the most generic.
  - Only one ACL is allowed per interface, per protocol, per direction.
  - New statements for an existing ACL are added to the bottom of the ACL by default.
  - Router-generated packets are not filtered by outbound ACLs.
  - Place standard ACLs as close to the destination as possible.
  - Place extended ACLs as close to the source as possible.

Apply an ACL

- The command syntax to apply an ACL to an interface or to the vty lines.
  Router(config-if)# **ip access-group** {*acl-#* | *name*} {**in** | **out**}
  Router(config-line)# **ip access-class** {*acl-#* | *name*} {**in** | **out**}

- To remove an ACL from an interface, enter the **no ip access-group** interface configuration command.
- The ACL will still be configured on the router so use the **no access-list** global configuration command to remove it.

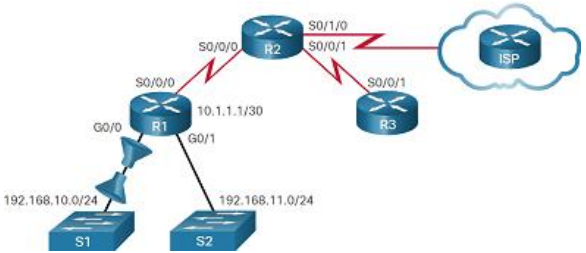
Named Standard ACL Example




```
R1(config)# ip access-list standard NO_ACCESS
R1(config-std-nacl)# deny host 192.168.11.10
R1(config-std-nacl)# permit any
R1(config-std-nacl)# exit
R1(config)# interface g0/0
R1(config-if)# ip access-group NO_ACCESS out
```

Apply an ACL (Cont.)

Named Extended ACL Example



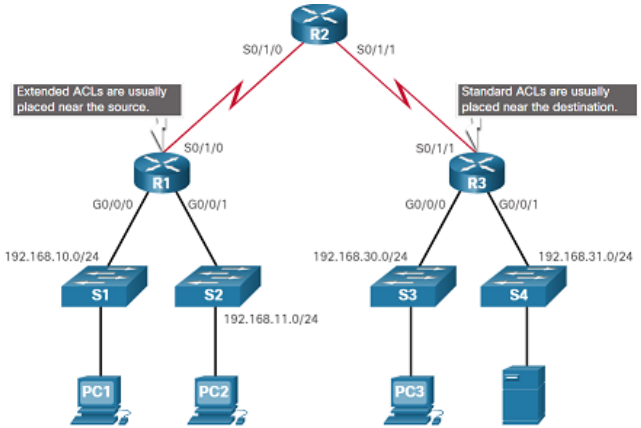

```
R1(config)# ip access-list extended SURFING
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq 80
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1(config-ext-nacl)# exit
R1(config)# ip access-list extended BROWSING
R1(config-ext-nacl)# permit tcp any 192.168.10.0 0.0.0.255 established
R1(config-ext-nacl)# exit
R1(config)# interface g0/0
R1(config-if)# ip access-group SURFING in
R1(config-if)# ip access-group BROWSING out
```

Named ACL on VTY Lines with Logging


```
R1(config)# ip access-list standard VTY_ACCESS
R1(config-std-nacl)# permit 192.168.10.10 log
R1(config-std-nacl)# deny any
R1(config-std-nacl)# exit
R1(config)# line vty 0 4
R1(config-line)# access-class VTY_ACCESS in
R1(config-line)# end
R1#
R1# !The administrator accesses the vty lines from 192.168.10.10
R1#
*Feb 26 18:58:30.579: %SEC-6-IPACCESSLOGNP: list VTY_ACCESS permitted 0
192.168.10.10 -> 0.0.0.0, 5 packets
R1# show access-lists
Standard IP access list VTY_ACCESS
   10 permit 192.168.10.10 log (6 matches)
   20 deny any
```

Where to Place ACLs

- Every ACL should be placed where it is the most efficient.
- Assume the objective is to prevent traffic that originates in the 192.168.10.0/24 network from reaching the 192.168.30.0/24 network.



- Extended ACLs should be located as close as possible to the source of the traffic to be filtered.
  - Undesirable traffic is denied close to the source network without crossing the network infrastructure.
- Standard ACLs should be located as close to the destination as possible.
  - If it was placed at the source of the traffic, the 'permit' or 'deny' will occur based on the given source address no matter where the traffic is destined.

124

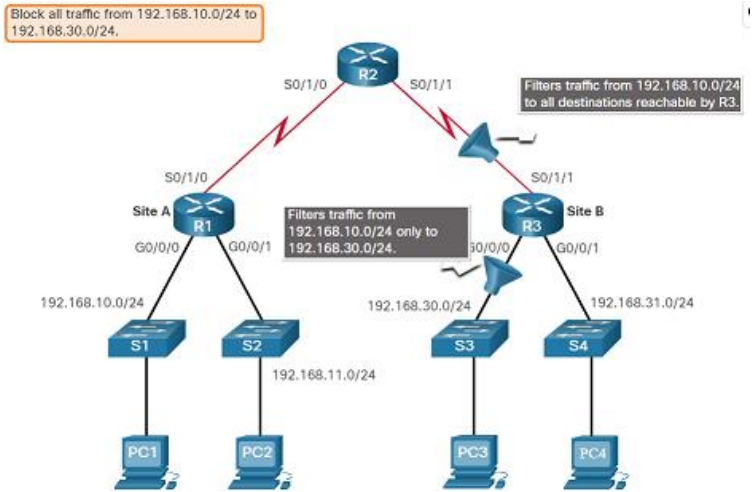
Where to Place ACLs (Cont.)

- Placement of the ACL and therefore, the type of ACL used, may also depend on a variety of factors as listed in the table.

Factors Influencing ACL Placement	Explanation
The extent of organizational control	Placement of the ACL can depend on whether or not the organization has control of both the source and destination networks.
Bandwidth of the networks involved	It may be desirable to filter unwanted traffic at the source to prevent transmission of bandwidth-consuming traffic.
Ease of configuration	It may be easier to implement an ACL at the destination, but traffic will use bandwidth unnecessarily. An extended ACL could be used on each router where the traffic originated. This would save bandwidth by filtering the traffic at the source, but it would require creating extended ACLs on multiple routers.

Standard ACL Placement Example

- Standard ACLs should be located as close to the destination as possible.
- In the figure, the administrator wants to prevent traffic originating in the 192.168.10.0/24 network from reaching the 192.168.30.0/24 network.



Two possible interfaces on R3 to apply the standard ACL:

- **R3 S0/1/1 interface (inbound)**
  - If applied this way to deny traffic from .10 network, it would also filter .10 traffic to the 192.168.31.0/24 (.31 in this example) network.
  - The standard ACL should not be applied to this interface.

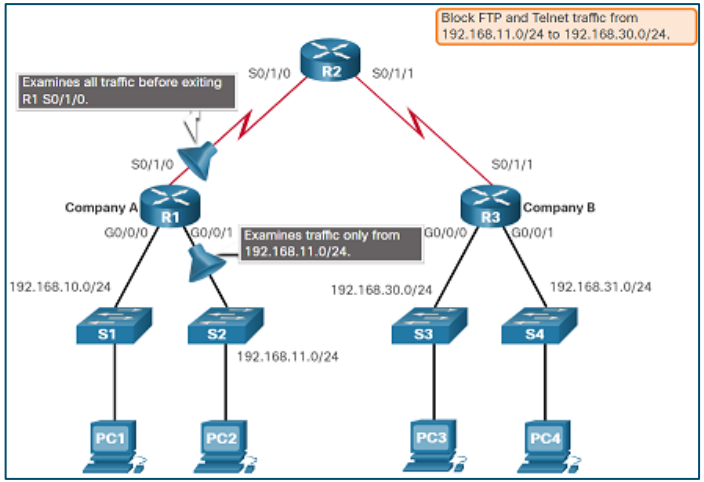
- **R3 G0/0/0 interface (outbound)**
  - If applied this way it will not affect other networks that are reachable by R3, so packets from .10 network will still be able to reach the .31 network.
  - This is the best interface to place the standard ACL.

126

Extended ACL Placement Example

- Extended ACLs should be located as close to the source as possible, but the organization can only place ACLs on devices that they control.

- In the figure, for example, Company A wants to deny Telnet and FTP traffic to Company B's 192.168.30.0/24 network from their 192.168.11.0/24 network while permitting all other traffic.



Two possible interfaces on R1 to apply the extended ACL:

- **R1 S0/1/0 interface (outbound) -** It will process all packets leaving R1 including packets from 192.168.10.0/24.

- **R1 G0/0/1 interface (inbound) -** Only packets from the 192.168.11.0/24 network are subject to ACL processing on R1.
  - Because the filter is to be limited to only those packets leaving the 192.168.11.0/24 network, applying the extended ACL to G0/0/1 is the best solution.

14.6 Mitigate Attacks with ACLs

132

Mitigate Spoofing Attacks

- ACLs can be used to mitigate many network threats, such as IP address spoofing and denial of service (DoS) attacks.
- Most DoS attacks use some type of spoofing.
- IP address spoofing overrides the normal packet creation process by inserting a custom IP header with a different source IP address.
- Attackers can hide their identity by spoofing the source IP address.
- There are many well-known classes of IP addresses that should never be seen as source IP addresses for traffic entering an organization's network.

133

Mitigate Spoofing Attacks (Cont.)

- The S0/0/0 interface is attached to the internet and should never accept inbound packets from all zeros addresses, broadcast addresses, 127.0.0.0/8, 169.254.0.0/16, reserved private addresses (RFC 1918), and 224.0.0.0/4
- The 192.168.1.0/24 network is attached to the R1 G0/0 interface, that should only allow inbound packets with a source address from that network.
- The ACL for G0/0 shown in the figure will only permit inbound packets from the 192.168.1.0/24 network. All others will be discarded.

Inbound on S0/0/0

```
R1(config)# access-list 150 deny ip host 0.0.0.0 any
R1(config)# access-list 150 deny ip 10.0.0.0 0.255.255.255 any
R1(config)# access-list 150 deny ip 127.0.0.0 0.255.255.255 any
R1(config)# access-list 150 deny ip 172.16.0.0 0.15.255.255 any
R1(config)# access-list 150 deny ip 192.168.0.0 0.0.255.255 any
R1(config)# access-list 150 deny ip 224.0.0.0 15.255.255.255 any
R1(config)# access-list 150 deny ip host 255.255.255.255 any
```

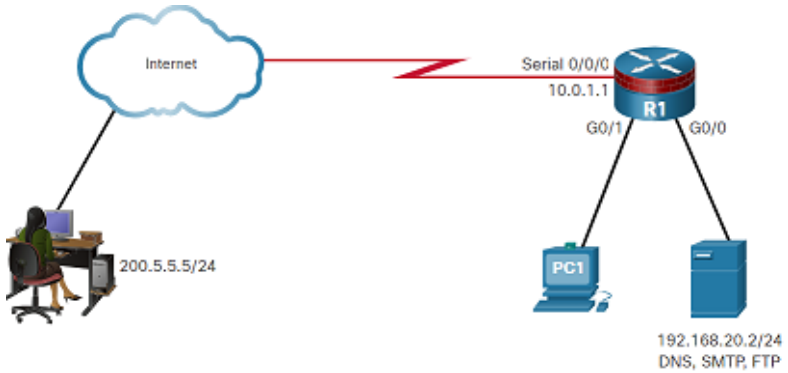
Inbound on G0/0:

```
R1(config)# access-list 105 permit ip 192.168.1.0 0.0.0.255 any
```


© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential 134

Permit Necessary Traffic through a Firewall

- An effective strategy for mitigating attacks: explicit permit only certain types of traffic through a firewall.
- DNS, SMTP, and FTP are services that often must be allowed through a firewall.
- Configure a firewall so that it permits administrators remote access through the firewall.
- SSH, syslog, and SNMP are examples of services that a router may need to include.
- While many of these services are useful, they should be controlled and monitored.
- Exploitation of these services leads to security vulnerabilities.
- An example topology with ACL configurations to permit specific services on the Serial 0/0/0 interface is shown.



Inbound on S0/0/0:

```
R1(config)# access-list 180 permit udp any host 192.168.20.2 eq domain
R1(config)# access-list 180 permit tcp any host 192.168.20.2 eq smtp
R1(config)# access-list 180 permit tcp any host 192.168.20.2 eq ftp
R1(config)# access-list 180 permit tcp host 200.5.5.5 host 10.0.1.1 eq 22
R1(config)# access-list 180 permit udp host 200.5.5.5 host 10.0.1.1 eq syslog
R1(config)# access-list 180 permit udp host 200.5.5.5 host 10.0.1.1 eq snmptrap
```

Mitigate ICMP Attacks

- Both ICMP echo and redirect messages should be blocked inbound by the router.

- Several ICMP messages should be allowed into the internal network:
  - **Echo reply -** Allows users to ping external hosts.
  - **Source quench -** Requests that the sender decrease the traffic rate of messages.
  - **Unreachable -** Generated for packets that are administratively denied by an ACL.

- Several ICMP messages should be allowed to exit the network:
  - **Echo -** Allows users to ping external hosts.
  - **Parameter problem -** Informs the host of packet header problems.
  - **Packet too big -** Enables packet maximum transmission unit (MTU) discovery.
  - **Source quench -** Throttles down traffic when necessary.

- As a rule, block all other ICMP message types outbound.

- ACLs are used to block IP address spoofing, selectively permit specific services through a firewall, and to allow only required ICMP messages.

136

Mitigate ICMP Attacks (Cont.)

- The figure shows a sample topology and possible ACL configurations to permit specific ICMP services on the G0/0 and S0/0/0 interfaces.

Inbound on S0/0/0:

```
R1(config)# access-list 112 permit icmp any any echo-reply
R1(config)# access-list 112 permit icmp any any source-quench
R1(config)# access-list 112 permit icmp any any unreachable
R1(config)# access-list 112 deny icmp any any
R1(config)# access-list 112 permit ip any any
```

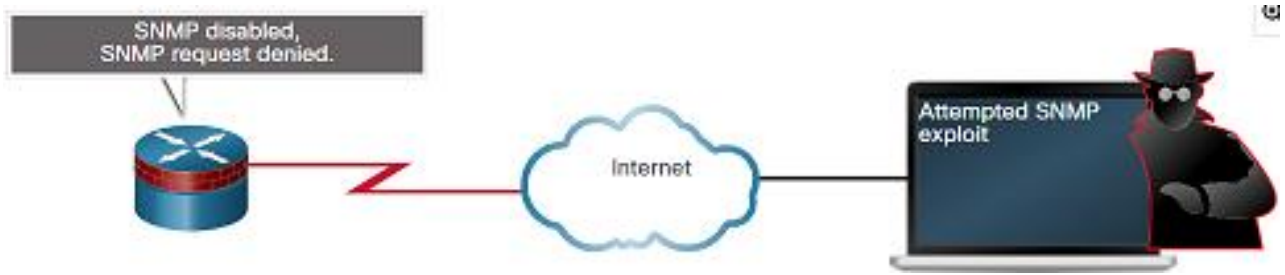
Inbound on S0/0/0:

```
R1(config)# access-list 114 permit icmp 192.168.1.0 0.0.0.255 any echo
R1(config)# access-list 114 permit icmp 192.168.1.0 0.0.0.255 any parameter-problem
R1(config)# access-list 114 permit icmp 192.168.1.0 0.0.0.255 any packet-too-big
R1(config)# access-list 114 permit icmp 192.168.1.0 0.0.0.255 any source-quench
R1(config)# access-list 114 deny icmp any any
R1(config)# permit ip any any
```


137

Mitigate SNMP Attacks

- Management protocols are useful for remote monitoring and management of networked devices, but they can still be exploited.
- If SNMP is necessary, exploitation of SNMP vulnerabilities can be mitigated by applying interface ACLs to filter SNMP packets from non-authorized systems.
- An exploit may still be possible if the SNMP packet is sourced from an address that has been spoofed and is permitted by the ACL.
- The most effective means of exploitation prevention is to disable the SNMP server on IOS devices for which it is not required.
  - Use Router(config)# **no snmp-server** to disable SNMP services on Cisco IOS devices.



138

14.7 IPv6 ACLs

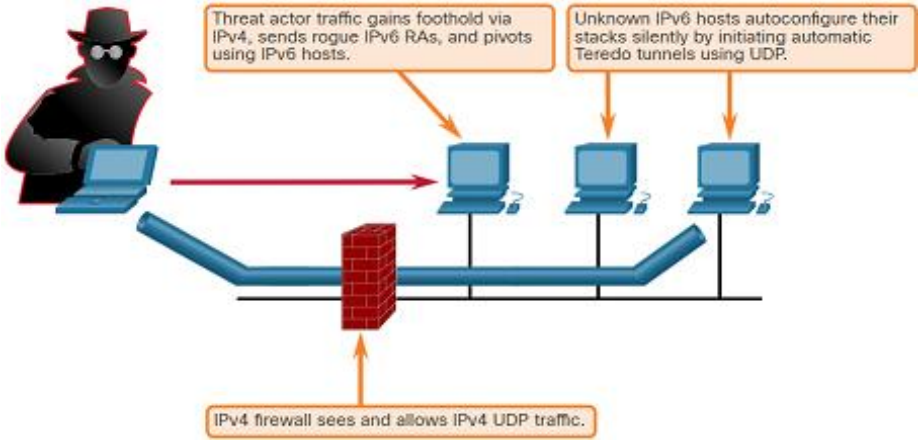
IPv6 ACL Overview

- IPv4 will coexist with IPv6 and then gradually be replaced by IPv6.
- An example of a security concern is threat actors leveraging IPv4 to exploit IPv6 in dual stack environments.
- In a dual stack environment devices operate with two IP protocol stacks.
- Threat actor can accomplish stealth attacks that result in trust exploitation by using dual-stacked hosts, rogue NDP messages, and tunneling techniques.
- Teredo tunneling, for example, is an IPv6 transition technology that provides automatic IPv6 address assignment when IPv4/IPv6 hosts are located behind IPv4 NAT devices.
- It accomplishes this by embedding the IPv6 packets inside IPv4 UDP packets.
- The threat actor gains a foothold in the IPv4 network.
- The compromised host sends rogue RAs, which triggers dual stacked hosts to obtain an IPv6 address.
- The threat actor can then use this foothold to move around, or pivot, inside the network.

141

IPv6 ACL Overview (Cont.)

- The threat actor can compromise additional hosts before sending traffic back out of the network, as shown in the figure.



- It is necessary to develop and implement a strategy to mitigate attacks against IPv6 infrastructures and protocols.
  - This mitigation strategy should include filtering at the edge using various techniques, such as IPv6 ACLs.

142

IPv6 ACL Syntax

- All IPv6 ACLs must be configured with a name and allows filtering based on source and destination addresses that are traveling inbound and outbound to a specific interface.
- They also support traffic filtering based on IPv6 option headers and optional, upper-layer protocol type information for finer granularity of control, like extended ACLs in IPv4.
- To configure an IPv6 ACL, use the **ipv6 access-list** command into IPv6 ACL configuration mode, and use the syntax shown in the figure to configure each ACE to specifically permit or deny traffic.
- The syntax shown is a simplified version of the IPv6 ACE syntax, but there are additional options.
- Apply an IPv6 ACL to an interface with the **ipv6 traffic-filter** command.

```
Router(config)# ipv6 access-list access-list-name
Router(config-ipv6-acl)# deny | permit protocol {source-ipv6-prefix / prefix-length |
any | host source-ipv6-address} [ operator [ port-number ]] { destination-ipv6-prefix
/ prefix-length | any | host destination-ipv6-address } [ operator [ port-number ]] [
dscp value ] [ fragments ] [ log ] [ log-input ] [ sequence value ] [ time-range name
]
```


© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential 143

IPv6 ACL Syntax (Cont.)

Parameter	Description
deny | permit	Specifies whether to deny or permit the packet.
protocol	Name or number of an Internet protocol, or an integer representing an IPv6 protocol number
source-ipv6-prefix / prefix-length destination-ipv6-addr / prefix-length	The source or destination IPv6 network or class of networks for which to set deny or permit conditions.
any	Enter any as an abbreviation for the IPv6 prefix ::/0. This matches all addresses.
host	The source or destination IPv6 host address for which to set deny or permit conditions
Operator (Optional)	An operand that compares the source or destination ports of the specified protocol.
port-number (Optional)	Decimal number or the name of a TCP or UDP port for filtering TCP or UDP, respectively.
Dscp (Optional)	Matches a differentiated services codepoint value against the traffic class value in the Traffic Class field of each IPv6 packet header. Acceptable range is from 0 to 63.
Fragments (Optional)	Matches non-initial fragmented packets where the fragment extension header contains a non-zero fragment offset.
Log (Optional)	Causes an informational logging message about the packet that matches the entry to be sent to the console.
log input (Optional)	Provides the same function as the log keyword, except that the logging message also includes the input interface.
sequence value	(Optional) Specifies the sequence number value for the access list statement.
time-range name	(Optional) Specifies the time range that applies to the permit statement.

Configure IPv6 ACLs

- An IPv6 ACL contains an implicit **deny ipv6 any any**.
- Each IPv6 ACL also contains implicit permit rules to enable IPv6 neighbor discovery.
- The IPv6 NDP requires the use of the IPv6 network layer to send NAs and NSs.
- If an administrator configures the **deny ipv6 any any** command without explicitly permitting neighbor discovery, then the NDP will be disabled.
- In the figure, R1 is permitting inbound traffic on G0/0 from the 2001:DB8:1:1::/64 network.
- NA and NS packets are explicitly permitted.
- Traffic sourced from any other IPv6 address is explicitly denied.
- If the administrator only configured the first permit statement, the ACL would have the same effect.


```
R1(config)# ipv6 access-list LAN_ONLY
R1(config-ipv6-acl)# permit 2001:db8:1:1::/64 any
R1(config-ipv6-acl)# permit icmp any any nd-na
R1(config-ipv6-acl)# permit icmp any any nd-ns
R1(config-ipv6-acl)# deny ipv6 any any
R1(config-ipv6-acl)# end
R1# show ipv6 access-list
IPv6 access list LAN_ONLY
    permit ipv6 2001:DB8:1:1::/64 any sequence 10
    permit icmp any any nd-na sequence 20
    permit icmp any any nd-ns sequence 30
    deny ipv6 any any sequence 40
R1#
```


Cisco Confidential 145

14.8 Access Control Lists Summary

147

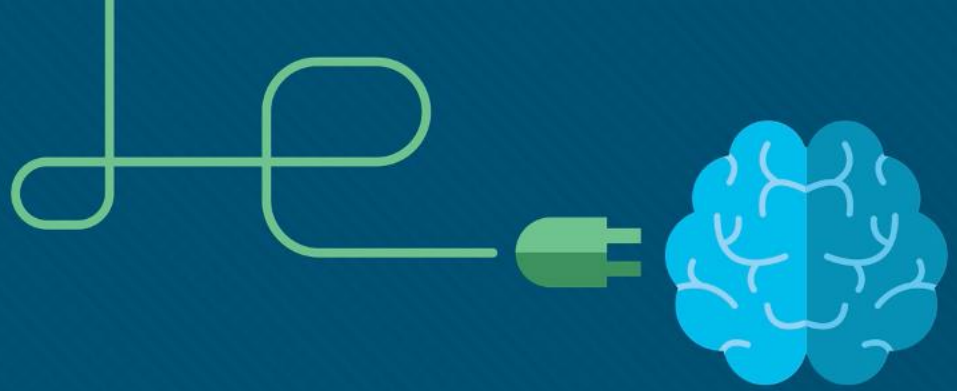
What Did I Learn in this Module?

- An ACL uses a sequential list of permit or deny statements, known as ACEs.
- Packet filtering can occur at Layer 3 or Layer 4, and Cisco routers support Standard and Extended ACLs.
- Standard ACLs number 1 to 99, or 1300 to 1999 while Extended ACLs number 100 to 199, or 2000 to 2699
- Named ACLs are the preferred method to use when configuring ACLs.
- ACLs define the set of rules that give added control for packets that enter inbound interfaces, packets that relay through the router, and packets that exit outbound interfaces of the router.
- An IPv4 ACE uses a 32-bit wildcard mask to determine which bits of the address to examine for a match.
- A wildcard mask is like a subnet mask in that it uses the ANDing process to identify which bits in an IPv4 address to match.
- Unlike a subnet mask, in which binary 1 is equal to a match and binary 0 is not a match, in a wildcard mask, the reverse is true.
- One shortcut method to calculate wildcard masks is to subtract the subnet mask from 255.255.255.255.
- Cisco IOS provides two keywords, **host** and **any**, to simplify the most common uses of wildcard masking.
- When configuring a complex ACL, it is suggested that you use a text editor, and copy and paste the commands onto the device.

148

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

- ACL names are alphanumeric, case sensitive, and must be unique.
- The procedural steps for configuring extended ACLs are the same as for standard ACLs.
- Extended ACLs can filter on many different types of internet protocols and ports.
- TCP can also perform basic stateful firewall services using the TCP **established** keyword.
- ACLs with multiple ACEs should be created in a text editor to make editing the ACL simpler.
- An ACL ACE can also be deleted or added using the ACL sequence numbers.
- Sequence numbers are automatically assigned when an ACE is entered.
- Extended ACLs should be located as close as possible to the source of the traffic to be filtered.
- Standard ACLs should be located as close to the destination as possible.
- ACLs can be used to mitigate many network threats, such as IP address spoofing and DoS attacks.
- An effective strategy for mitigating attacks is to explicitly permit only certain types of traffic through a firewall.
- To mitigate attacks against IPv6 infrastructures and protocols, the strategy should include filtering using techniques such as IPv6 ACLs.
- The ACL functionality in IPv6 is like ACLs in IPv4, but there is no equivalent to IPv4 standard ACLs.
- In addition, all IPv6 ACLs must be configured with a name.
- IPv6 ACLs allow filtering based on source and destination addresses that are traveling inbound and outbound to a specific interface.
- They also support traffic filtering based on IPv6 option headers and optional, upper-layer protocol type information for finer granularity of control, like extended ACLs in IPv4.



Module 15: Firewall Technologies

Cybersecurity Essentials 3.0

Module Objectives

Module Title: Firewall Technologies

Module Objective: Explain how firewalls are implemented to provide network security.

Topic Title	Topic Objective
Secure Networks with Firewalls	Explain how firewalls are used to help secure networks.
Firewalls in Network Design	Explain design considerations for implementing firewall technologies

159

15.1 Secure Networks with Firewalls

160

Firewalls

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

Firewall features include:

Firewall Features	Description
Common Firewall Properties	• Firewalls are resistant to network attacks. • Firewalls are the only transit point between internal corporate networks and external networks. • 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 network access control to a few firewalls in the network.
Firewall Limitations	• A misconfigured firewall can have serious consequences for the network. • 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 attacks. • Network performance can slow down. • Unauthorized traffic can be tunneled or hidden as legitimate traffic through the firewall.

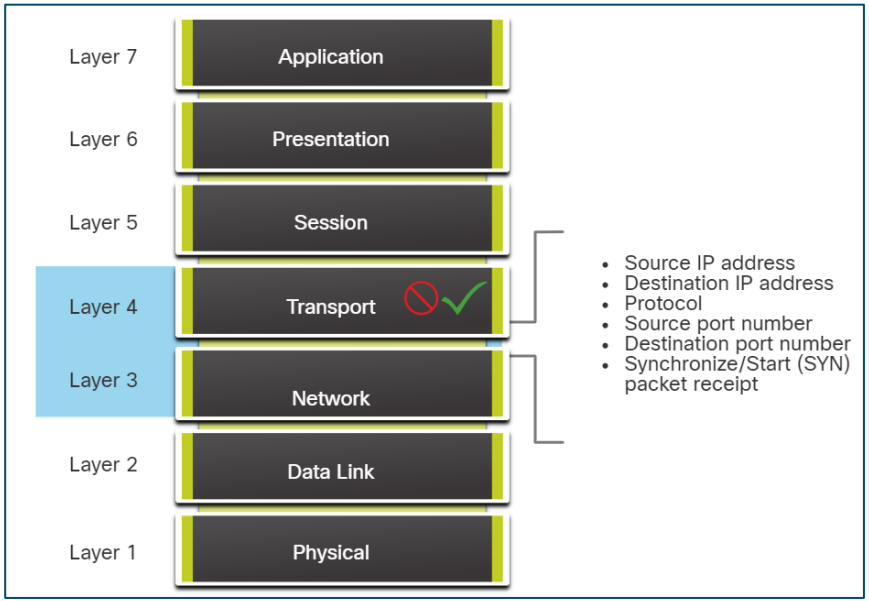
161

Types of Firewalls

Common firewall types include packet filtering, stateful, application gateway, and next generation firewalls.

Packet Filtering (Stateless) Firewall

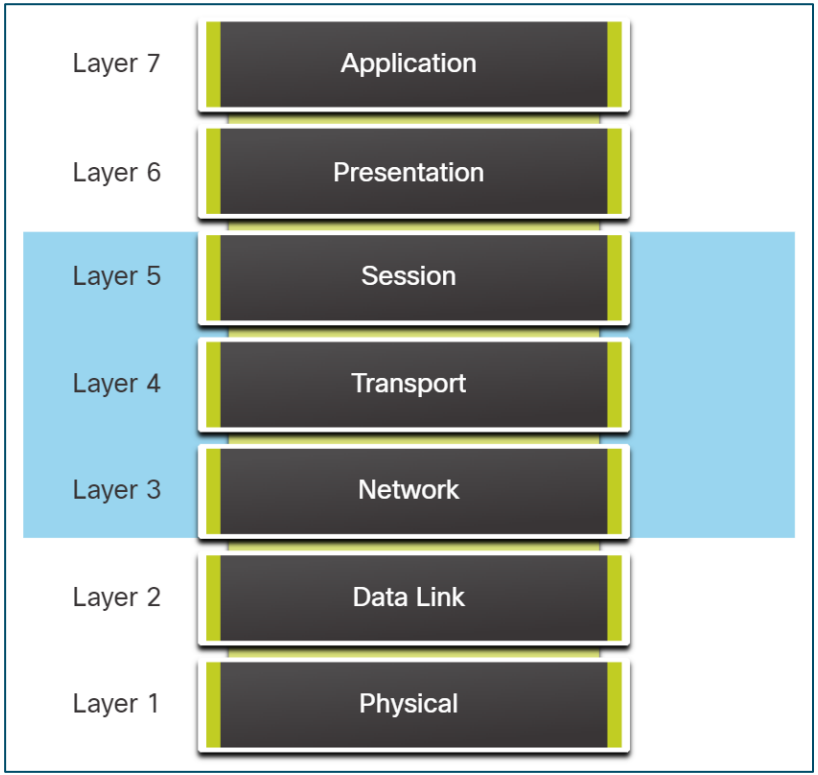
- Packet filtering firewalls are usually part of a router firewall, which permits or denies traffic based on Layer 3 and Layer 4 information.
- They are stateless firewalls that use a simple policy table look-up that filters traffic based on specific criteria.



Types of Firewalls (Cont.)

Stateful Firewall

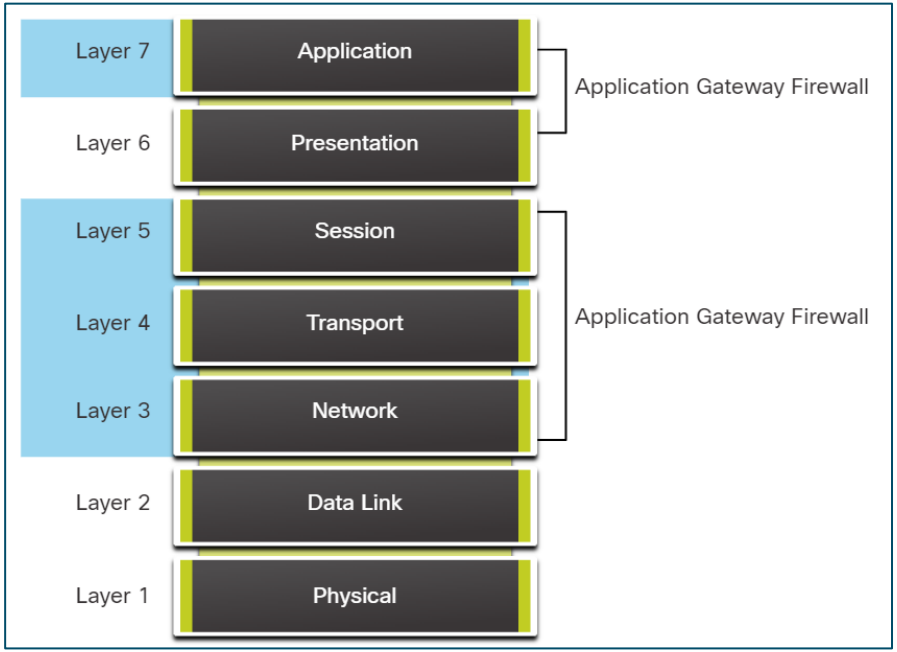
- Stateful firewalls are the most versatile and the most common firewall technologies in use.
- Stateful firewalls provide stateful packet filtering by using connection information maintained in a state table.
- Stateful filtering is a firewall architecture that is classified at the network layer.
- It also analyzes traffic at OSI Layer 4 and Layer 5.



Types of Firewalls (Cont.)

Application Gateway Firewall

- An application gateway firewall (proxy 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 software.
- When a client needs to access a remote server, it connects to a proxy server.
- The proxy server connects to the remote server on behalf of the client.
- Therefore, the server only sees a connection from the proxy server.



164

Types of Firewalls (Cont.)

Next Generation Firewall

Next-generation firewalls (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

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. For example, an application inspection firewall combines a stateful firewall with an application gateway firewall.

Packet Filtering Firewall Benefits and Limitations

Advantages and disadvantages of a packet filtering firewall include:

Packet Filtering Firewall	Description
Advantages of a packet filtering firewall	• Packet filters implement simple permit or deny rule sets. • Packet filters have a low impact on network performance. • Packet filters are easy to implement and are supported by most routers. • Packet filters provide an initial degree of security at the network layer. • Packet filters perform almost all the tasks of a high-end firewall at a much lower cost.
Disadvantages of a packet filtering firewall	• Packet filters are susceptible to IP spoofing. Threat actors can send arbitrary packets that meet ACL criteria and pass through the filter. • Packet filters do not reliably filter fragmented packets. Because fragmented IP packets carry the TCP header in the first fragment and packet filters filter on TCP header information, all fragments after the first fragment are passed unconditionally. Decisions to use packet filters assume that the filter of the first fragment accurately enforces the policy. • Packet filters use complex ACLs, which can be difficult to implement and maintain. • Packet filters cannot dynamically filter certain services. For example, sessions that use dynamic port negotiations are difficult to filter without opening access to a whole range of ports.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential 166

Stateful Firewall Benefits and Limitations

Some benefits and limitations to using a stateful firewall include:

Stateful Firewall	Description
Benefits	• Stateful firewalls are often used as a primary means of defense by filtering unwanted, unnecessary, or undesirable traffic. • Stateful firewalls strengthen packet filtering by providing more stringent control over security. • Stateful firewalls improve performance over packet filters or proxy servers. • Stateful firewalls defend against spoofing and DoS attacks by determining whether packets belong to an existing connection or are from an unauthorized source. • Stateful firewalls provide more log information than a packet filtering firewall.
Limitations	• Stateful firewalls cannot prevent application layer attacks because they do not examine the actual contents of the HTTP connection. • Not all protocols are stateful. For example, UDP and ICMP do not generate connection information for a state table, and, therefore, do not garner as much support for filtering. • It is difficult to track connections that use dynamic port negotiation. Some applications open multiple connections. This requires a whole new range of ports that must be opened to allow this second connection. • Stateful firewalls do not support user authentication.

167

15.2 Firewalls in Network Design

168

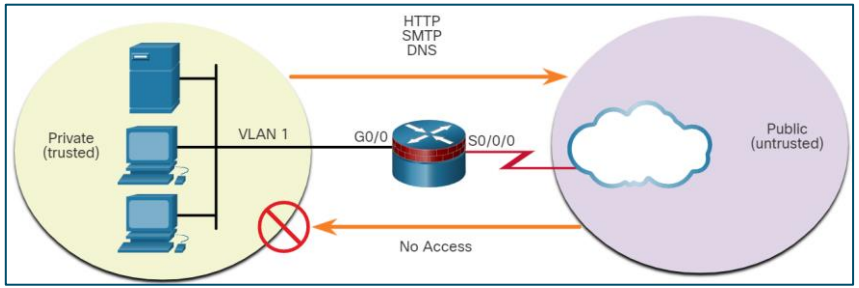
Common Security Architectures

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.

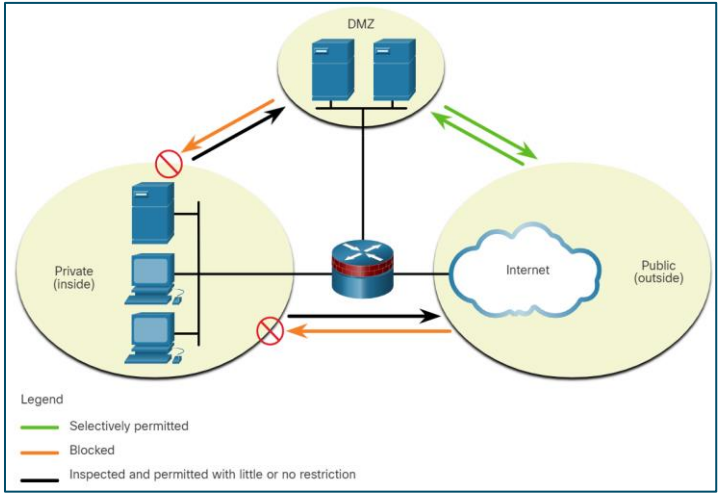


Common Security Architectures (Cont.)

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.

- Traffic originating from the private network is inspected as it travels toward the public or DMZ network. Inspected traffic returning from the DMZ or public network to the private network is permitted.
- Traffic originating from the DMZ network and traveling to the private network is usually blocked.
- Traffic originating from the DMZ network and traveling to the public network is selectively permitted based on service requirements.
- Traffic originating from the public network and traveling toward the DMZ is selectively permitted and inspected.



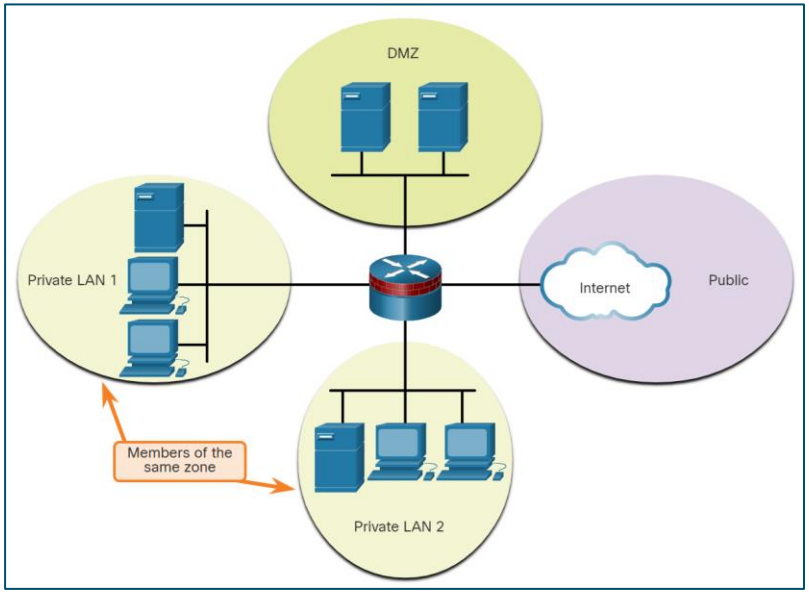
- Traffic originating from the public network and traveling to the private network is blocked.

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 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 the firewall.
- By default, the traffic between interfaces in the same zone is not subject to any policy and passes freely.
- All zone-to-zone traffic is blocked. Configure a policy allowing or inspecting traffic To permit traffic between zones.
- The only exception to this default **denying any** policy is the router's self-zone.



Layered Defense

A layered defense uses different types of firewalls combined in layers to add depth to an organization's security. For example:

- **Network core security** -Protects against malicious software and traffic anomalies, enforces network policies, and ensures survivability.
- **Perimeter security** -Secures boundaries between zones.
- **Communications security** -Provides information assurance.
- **Endpoint security** -Provides identity and device security policy compliance.

Policies can be enforced between layers and inside the layers. These policy enforcement points determine whether traffic is forwarded or discarded.

If the policy allows, the traffic goes to the screened firewall or bastion host system that applies more rules to the traffic and discards suspect packets.

172

Layered Defense (Cont.)

A layered defense approach is optional to ensure a secure internal network. A network administrator must consider many factors when building a complete in-depth defense:

- Firewalls typically do not stop intrusions from hosts within a network or zone.
- Firewalls do not protect against rogue access point installations.
- Firewalls do not replace backup and disaster recovery mechanisms resulting from attack or hardware failure.
- Firewalls are no substitute for informed administrators and users.

This partial list of best practices can serve as a starting point for a firewall security policy.

- Position firewalls at security boundaries.
- Deny all traffic by default and permit only services that are needed.
- Ensure controlled physical access to the firewall.
- Regularly monitor firewall logs.
- Practice change management for firewall configuration changes.
- Remember that firewalls primarily protect from technical attacks originating from the outside.

173

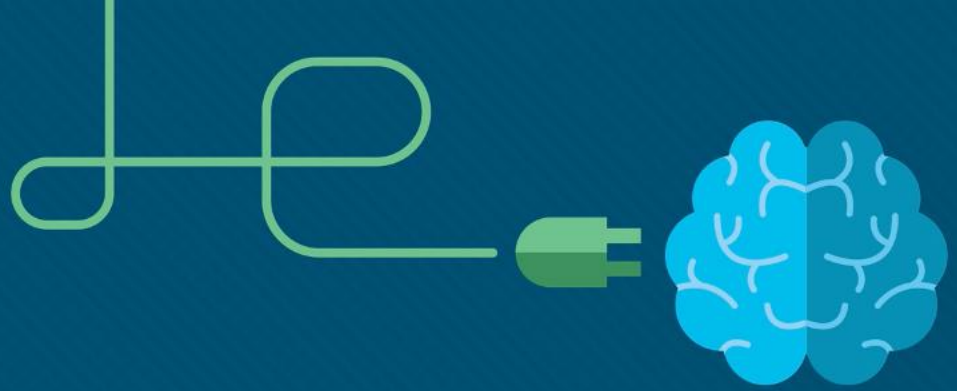
15.3 Firewall Technologies Summary

174

What Did I Learn in this Module?

- Packet filtering (stateless) firewalls provide Layer 3 and sometimes Layer 4 filtering.
- A stateful inspection firewall allows or blocks traffic based on state, port, and protocol.
- Application gateway firewalls (proxy firewall) filter information at Layers 3, 4, 5, and 7.
- Next-generation firewalls provide services beyond application gateways, such as integrated intrusion prevention, application awareness, control to see and block risky apps, access to future information feeds, and techniques to address evolving security threats.
- Common security architectures define the boundaries of traffic entering and leaving the network.
- Some designs are as simple as designating an outside network and an inside network determined by two firewall interfaces.
- Networks that require public can access to services will often include a DMZ that the public can access, while strictly blocking access to the inside network.
- ZPFs use the concept of zones to provide additional flexibility.
- A layered security approach uses firewalls and other security measures to provide security at different functional layers of the network.

175



Module 16: Zone-Based Policy Firewalls

Cybersecurity Essentials 3.0

Module Objectives

Module Title: Zone-Based Policy Firewalls

Module Objective: Implement Zone-Based Policy Firewall using the CLI.

Topic Title	Topic Objective
ZPF Overview	Explain how Zone-Based Policy Firewalls are used to help secure a network.
ZPF Operation	Explain the operation of a Zone-Based Policy Firewall.
Configure a ZPF	Configure a Zone-Based Policy Firewall with CLI.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential 186

16.1 ZPF Overview

187

Benefits of a ZPF

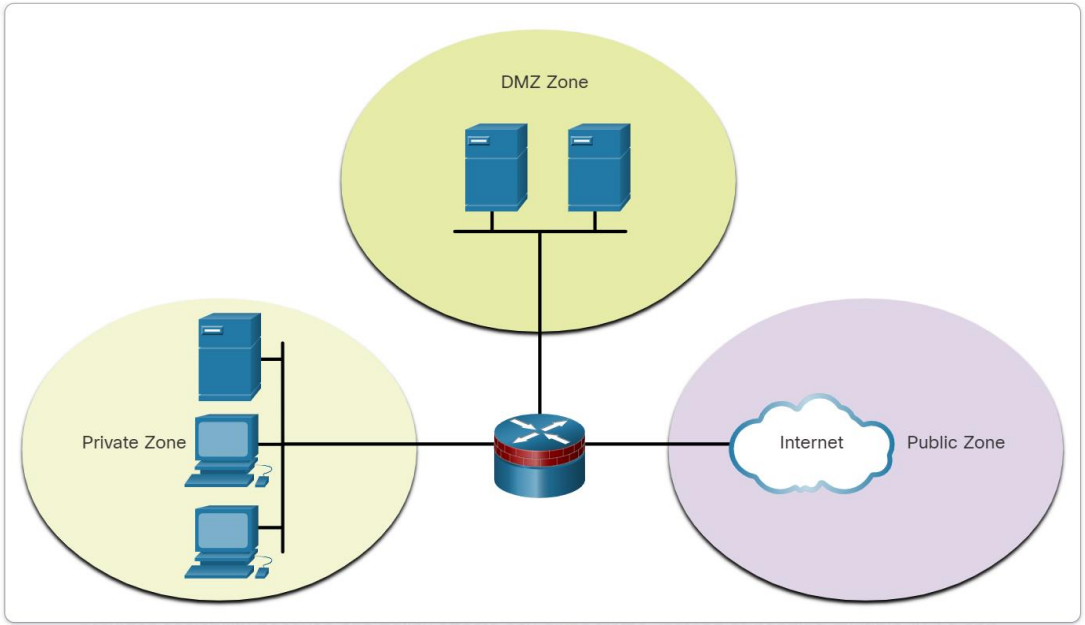
There are two configuration models for Cisco IOS Firewall:

- **Classic Firewall** - The traditional configuration model in which firewall policy is applied on interfaces.
- **Zone-based Policy Firewall (ZPF)** - The configuration model in which interfaces are assigned to security zones, and firewall policy is applied to traffic moving between the zones.

The primary motivations for network security professionals to migrate to the ZPF model are structure and ease of use. The structured approach is useful for documentation and communication.

The ease of use makes network security implementations more accessible to a larger community of security professionals.

Benefits of a ZPF (Cont.)



- If an additional interface is added to the private zone, the hosts connected to the new interface in the private zone can pass traffic to all hosts on the existing interface in the same zone.
- A simple three-zone network is shown in the figure.

Benefits of a ZPF (Cont.)

There are several benefits of a ZPF:

- It is not dependent on ACLs.
- The router security posture is to block unless explicitly allowed.
- Policies are easy to read and troubleshoot with the Cisco Common Classification Policy Language (C3PL).
- C3PL is a structured method to create traffic policies based on events, conditions, and actions. This provides scalability because one policy affects any given traffic, instead of needing multiple ACLs and inspection actions for different types of traffic.
- Virtual and physical interfaces can be grouped into zones.
- Policies are applied to unidirectional traffic between zones.

When deciding whether to implement IOS Classic Firewall or a ZPF, it is important to note that both configuration models can be enabled concurrently on a router.

ZPF Design

Designing ZPFs involves several steps:

Step 1: Determine the Zone:

- The administrator focuses on the separation of the network into zones.
- Zones establish the security borders of a network.
- A zone defines a boundary where traffic is subjected to policy restrictions as it crosses to another region of the network.

Step 2: Establish policies between zones:

- For each pair of 'source-destination' zones, define the sessions that clients in the source zones can request from servers in destination zones.
- These sessions are most often TCP and UDP sessions, but may also be ICMP sessions, such as ICMP echo.
- For traffic that is not based on the concept of sessions, the administrator must define unidirectional traffic flows from source to destination and vice versa.

191

ZPF Design (Cont.)

Step 3: Design the physical infrastructure:

- After the zones have been identified, and the traffic requirements between them documented, the administrator must design the physical infrastructure.
- The administrator must consider security and availability requirements when designing the physical infrastructure.
- This includes dictating the number of devices between most-secure and least-secure zones and determining redundant devices.

Step 4: Identify subsets within zones and merge traffic requirements:

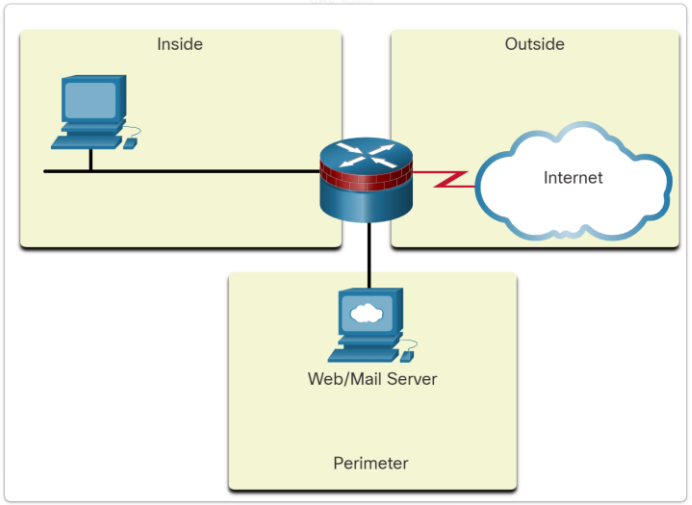
- For each firewall device in the design, the administrator must identify zone subsets that are connected to its interfaces and merge the traffic requirements for those zones.
- For example, multiple zones might be indirectly attached to a single interface of a firewall. This would result in a device-specific interzone policy.
- Although an important consideration, implementing zone subsets is beyond the scope of this curriculum.

192

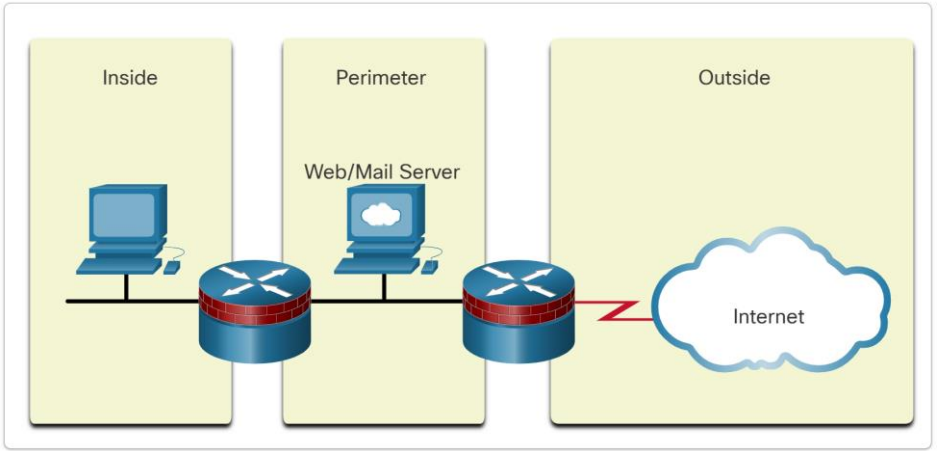
ZPF Design (Cont.)

Examples of ZPF Designs

Firewall-with-public-servers-1



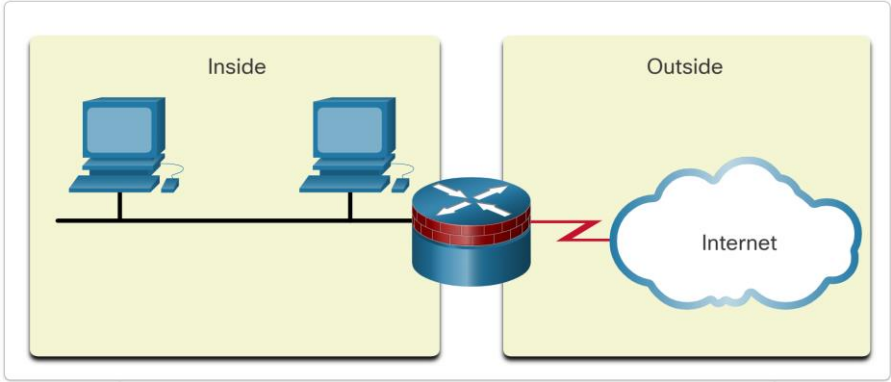
Firewall-with-public-servers-2



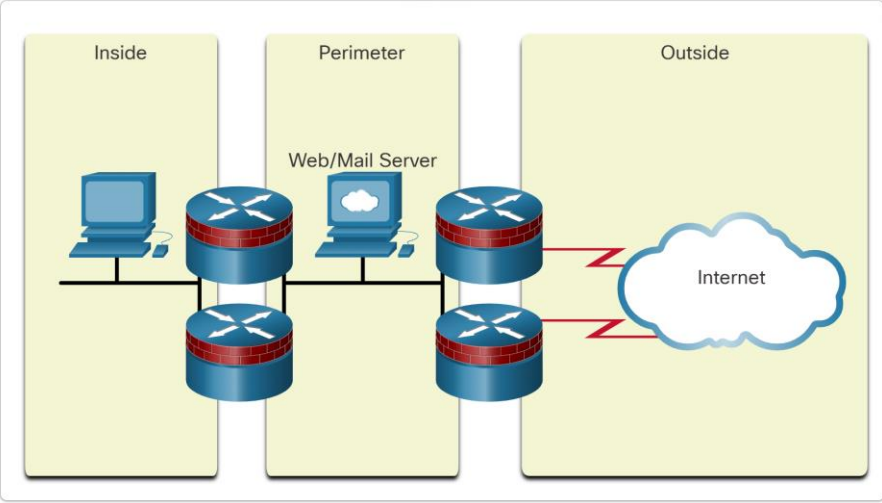
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential 193

ZPF Design (Cont.)

LAN-to-Internet



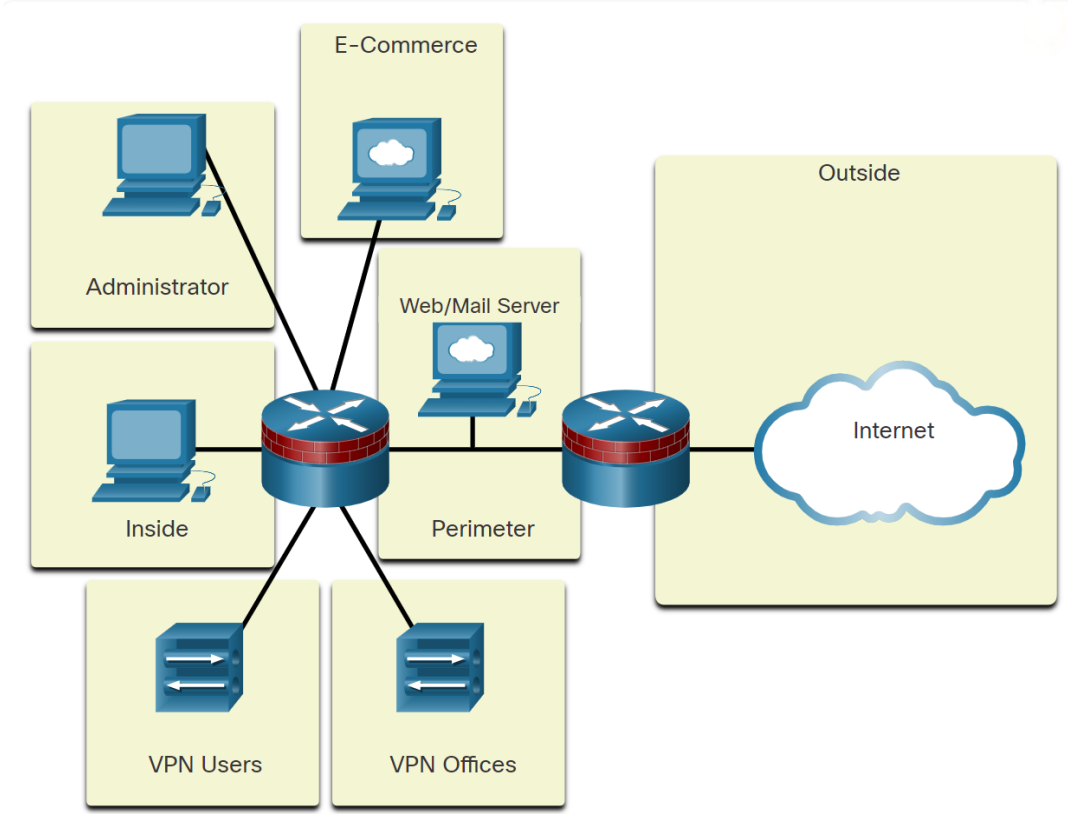
Redundant Firewall



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential 194

ZPF Design (Cont.)

Complex Firewall



16.2 ZPF Operation

196

ZPF Actions

Policies identify actions that the ZPF will perform on network traffic.

Three possible actions can be configured to process traffic by protocol, source, destination zones (zone pairs), and other criteria.

- **inspect** - This performs Cisco IOS stateful packet inspection.
- **drop** - This is analogous to a **deny** statement in an ACL. A log option is available to **log** the rejected packets.
- **pass** - This is analogous to a **permit** statement in an ACL. The pass action does not track the state of connections or sessions within the traffic.

197

Rules for Transit Traffic

The rules depend on whether or not the ingress and egress interfaces are members of the same zone:

- If neither interface is a zone member, then the resulting action is to pass the traffic.
- If both interfaces are members of the same zone, then the resulting action is to pass the traffic.
- If one interface is a zone member, but the other is not, then the resulting action is to drop the traffic regardless of whether a zone-pair exists.
- If both interfaces belong to the same zone-pair and a policy exists, then the resulting action is inspect, allow, or drop as defined by the policy.

198

Rules for Transit Traffic (Cont.)

The table summarizes the rules for transit traffic.

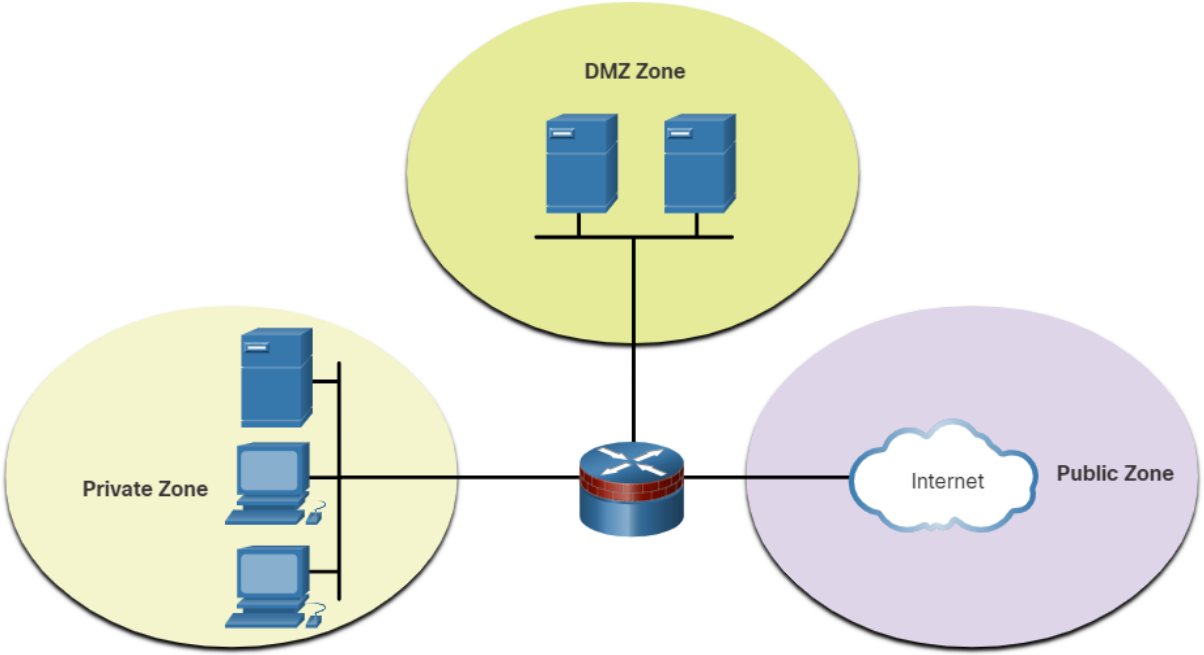
Source Interface Member of Zone?	Destination Interface Member of Zone?	Zone-Pair Exists?	Policy Exists?	Result
NO	NO	N/A	N/A	PASS
YES	NO	N/A	N/A	DROP
NO	YES	N/A	N/A	DROP
YES (private)	YES (private)	N/A	N/A	PASS
YES (private)	YES (public)	NO	N/A	DROP
YES (private)	YES (public)	YES	NO	PASS
YES (private)	YES (public)	YES	YES	INSPECT

199

Rules for Transit Traffic (Cont.)

Traffic transiting through router interfaces is subject to several rules governing interface behavior. For the transit traffic example, refer to the topology shown in the figure.

Basic Security Zone Topology



Rules for Traffic to the Self Zone

- The self-zone is the router itself and includes all the IP addresses assigned to the router interfaces.
  - This is traffic that originates at the router or is addressed to a router interface.
  - Specifically, the traffic is either for device management, for example SSH, or traffic forwarding control, such as routing protocol traffic.
  - The rules for a ZPF are different for the self-zone.

- The rules depend on whether the router is the source or the destination of the traffic, as shown in the table on the next slide.
  - If the router is the source or the destination, then all traffic is permitted.
  - The only exception is if the source and destination are a zone-pair with a specific service-policy.
  - In that case, the policy is applied to all traffic.

Rules for Traffic to the Self Zone (Cont.)

Source Interface Member of Zone?	Destination Interface Member of Zone?	Zone-Pair Exists?	Policy Exists?	Result
YES (self zone)	YES	NO	N/A	PASS
YES (self zone)	YES	YES	NO	PASS
YES (self zone)	YES	YES	YES	INSPECT
YES	YES (self zone)	NO	N/A	PASS
YES	YES (self zone)	YES	NO	PASS
YES	YES (self zone)	YES	YES	INSPECT

16.3 Configure a ZPF

203

Configure a ZPF

Step 1: Create the zones.

Step 2: Identify traffic with a class-map.

Step 3: Define an action with a policy-map.

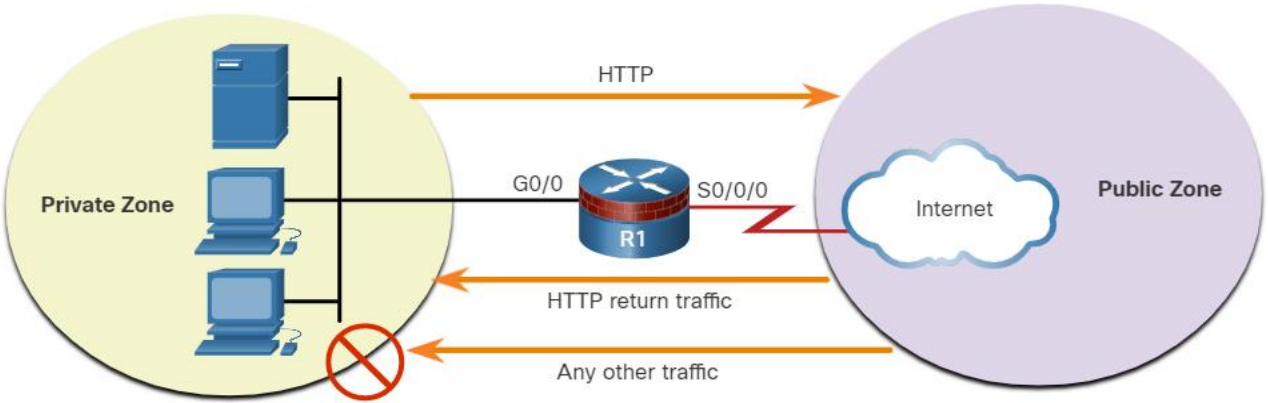
Step 4: Identify a zone pair and match it to a policy-map.

Step 5: Assign zones to the appropriate interfaces.

204

Configure a ZPF (Cont.)

The topology shown in the figure will be used throughout the remainder of this topic to demonstrate ZPF configuration. The sequence of steps is not required. However, some configurations must be completed in order. For instance, you must configure a class-map before you assign a class-map to a policy-map. Similarly, you cannot assign a policy-map to a zone-pair until you have configured the policy. If you try to configure a section that relies on another portion of the configuration that you have not yet configured, the router responds with an error message.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential 205

Step 1. Create the Zones

The first step is to create the zones. However, before creating the zones answer a few questions:

- What interfaces should be included in the zones?
- What will be the name for each zone?
- What traffic is necessary between the zones and in which direction?

In the example topology, we have two interfaces, two zones, and traffic flowing in one direction. Traffic sourced from the public zone will not be allowed. Create the private and public zones for the firewall with the zone security command, as shown here.

```
Router(config)# zone security zone-name
```

```
R1(config)# zone security PRIVATE
R1(config-sec-zone)# exit
R1(config)# zone security PUBLIC
R1(config-sec-zone)# exit
R1(config)#
```

Step 2. Identify Traffic

The second step is to use a class-map to identify the traffic to which a policy will be applied.

- A class is a way of identifying a set of packets based on its contents using “match” conditions. Typically, you define a class so that you can apply an action to the identified traffic that reflects a policy. A class is defined with class-maps.

- The example below shows the syntax for the **class-map** command. There are several types of class-maps. For a ZPF configuration, use the **inspect** keyword to define a class-map. Determine how packets are evaluated when multiple match criteria exist. Packets must meet one of the match criteria **(match-any)** or all the match criteria **(match-all)** to be considered a member of the class.

```
Router(config)# class-map type inspect [match-any |
match-all] class-map-name
```

Step 2. Identify Traffic (Cont.)

Parameter	Description
match-any	Packets must meet one of the match criteria to be considered a member of the class.
match-all	Packets must meet all of the match criteria to be considered a member of the class.
class-map-name	Name of the class-map that will be used to configure the policy for the class in the policy-map.

208

Step 2. Identify Traffic (Cont.)

The example below shows the syntax for the match statements in **class-map** sub-configuration mode. Match traffic to an ACL, a specific protocol, or even another class-map.

```
Router(config-cmap)# match access-group {acl-# | acl-name
}
Router(config-cmap)# match protocol protocol-name
Router(config-cmap)# match class-map class-map-name
```

Parameter	Description
match access-group	Configures the match criteria for a class-map based on the specified ACL number or name.
match protocol	Configures the match criteria for a class-map based on the specified protocol.
match class-map	Uses another class-map to identify traffic.

Step 2. Identify Traffic (Cont.)

In the topology, HTTP traffic is allowed to cross R1 from the PRIVATE to the PUBLIC zone.

- When allowing HTTP traffic, it is recommended to specifically include HTTPS and DNS protocols, as shown in the example below.
- Traffic can match any of the statements to become a member of the HTTP-TRAFFIC class.

```
R1(config)# class-map type inspect match-any HTTP-TRAFFIC
R1(config-cmap)# match protocol http
R1(config-cmap)# match protocol https
R1(config-cmap)# match protocol dns
```

Step 3. Define an Action

The third step is to use a policy-map to define what action should be taken for traffic that is a member of a class.

The example below shows the command syntax to configure a policy-map. An action is a specific functionality. It is typically associated with a traffic class. For example, **inspect**, **drop**, and **pass** are actions.

```
R1(config)# policy-map type inspect policy-map-name
R1(config-pmap)# class type inspect class-map-name
R1(config-pmap-c)# {inspect | drop | pass}
```

Parameter	Description
inspect	An action that offers state−based traffic control. The router maintains session information for TCP and UDP and permits return traffic.
drop	Discards unwanted traffic
pass	A stateless action that allows the router to forward traffic from one zone to another

Step 3. Define an Action (Cont.)

The example below shows an example of a policy-map configuration.

- The class HTTP-TRAFFIC that was configured in the previous step is associated with a new policy-map named PRIV-TO-PUB-POLICY.
- The third **inspect** command configures R1 to maintain state information for all traffic that is a member of the class HTTP-TRAFFIC.

```
R1(config)# policy-map type inspect PRIV-TO-PUB-POLICY
R1(config-pmap)# class type inspect HTTP-TRAFFIC
R1(config-pmap-c)# inspect
```

Step 3. Define an Action (Cont.)

- **inspect** - This action offers state-based traffic control. For example, if traffic traveling from the PRIVATE zone to the PUBLIC zone is inspected, the router maintains connection or session information for TCP and UDP traffic. The router would then permit return traffic sent from PUBLIC zone hosts in reply to PRIVATE zone connection requests.

- **drop** - This is the default action for all traffic. Similar to the implicit deny any at the end of every ACL, there is an explicit drop applied by the IOS to the end of every policy−map. It is listed as class class-default in the last section of any policy-map configuration. Other class−maps within a policy−map can also be configured to drop unwanted traffic. Unlike ACLs, traffic is silently dropped, and no ICMP unreachable messages are sent to the source of the traffic.

- **pass** - This action allows the router to forward traffic from one zone to another. The pass action does not track the state of connections. Pass only allows the traffic in one direction. A corresponding policy must be applied to allow return traffic to pass in the opposite direction. The pass action is ideal for secure protocols with predictable behavior, such as IPsec. However, most application traffic is better handled in the ZPF with the inspect action.

213

Step 4. Identify a Zone-Pair and Match to a Policy

The fourth step is to identify a zone pair and associate that zone pair to a policy-map.

The example below shows the command syntax. Create a zone-pair with the **zone-pair security** command. Then use the **service-policy type inspect** command to attach a policy-map and its associated action to the zone-pair.

```
Router(config)# zone-pair security zone-pair-name source
{source-zone-name | self} destination {destination-zone-
name | self}
Router(config-sec-zone-pair)# service-policy type inspect
policy-map-name
```

Parameter	Description
source source-zone-name	Specifies the name of the zone from which traffic is originating.
destination destination-zone-name	Specifies the name of the zone to which traffic is destined.
self	Specifies the system-defined zone. Indicates whether traffic will be going to or from the router itself.

Step 4. Identify a Zone-Pair and Match to a Policy (Cont.)

- The example below shows an example of a zone-pair configuration. A zone-pair named PRIV-PUB is created with PRIVATE assigned as the source zone and PUBLIC assigned as the destination zone. Then the policy-map created in the previous step is associated to the zone-pair.

- After the firewall policy has been configured, the administrator applies it to traffic between a pair of zones using the zone-pair security command. To apply a policy, it is assigned to a zone pair. The zone pair needs to specify the source zone, the destination zone, and the policy for handling the traffic between the source and destination zones.

```
R1(config)# zone-pair security PRIV-PUB source PRIVATE
destination PUBLIC
R1(config-sec-zone-pair)# service-policy type inspect
PRIV-TO-PUB-POLICY
```


215

Step 5. Assign Zones to Interfaces

The fifth step is to assign zones to the appropriate interfaces.

- Associating a zone to an interface will immediately apply the service-policy that has been associated with the zone.
- If no service-policy is yet configured for the zone, all transit traffic will be dropped.
- Use the zone-member security command to assign a zone to an interface, as shown in the example below.

```
Router(config-if)# zone-member security zone-name
```


© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential 216

Step 5. Assign Zones to Interfaces (Cont.)

- In the following example, GigabitEthernet 0/0 is assigned the PRIVATE zone, and Serial 0/0/0 is assigned the PUBLIC zone.

```
R1(config)# interface GigabitEthernet 0/0
R1(config-if)# zone-member security PRIVATE
R1(config-if)# interface Serial 0/0/0
R1(config-if)# zone-member security PUBLIC
```

- The service-policy is now active. HTTP, HTTPS, and DNS traffic sourced from the PRIVATE zone and destined for the PUBLIC zone will be inspected. Traffic sourced from the PUBLIC zone and destined for the PRIVATE zone will only be allowed if it is part of sessions originally initiated by PRIVATE zone hosts.

Verify a ZPF Configuration

```
R1# show run | begin class-map
!
<some output omitted>
!
class-map type inspect match-any HTTP-TRAFFIC
 match protocol http
 match protocol https
 match protocol dns
!
policy-map type inspect PRIV-TO-PUB-POLICY
 class type inspect HTTP-TRAFFIC
  inspect
 class class-default
  drop
!
zone security PRIVATE
zone security PUBLIC
zone-pair security PRIV-PUB source PRIVATE destination PUBLIC
 service-policy type inspect PRIV-TO-PUB-POLICY
!
interface GigabitEthernet0/0
 zone-member security PRIVATE
!
interface Serial0/0/0
 zone-member security PUBLIC
!
```

- Verify a ZPF configuration by viewing the running configuration. Notice that the class-map is listed first. Then the policy-map makes use of the class-map. Also, notice the highlighted **class class-default** that will drop all other traffic that is not a member of the HTTP-TRAFFIC class.
- The zone configurations follow the policy-map configurations with zone naming, zone pairing, and associating a service-policy to the zone pair. Finally, the interfaces are assigned zones.

Verify a ZPF Configuration (Cont.)

```
R1# show policy-map type inspect zone-pair sessions

policy exists on zp PRIV-PUB
  Zone-pair: PRIV-PUB

  Service-policy inspect : PRIV-TO-PUB-POLICY

   Class-map: HTTP-TRAFFIC (match-any)
      Match: protocol http
        12 packets, 384 bytes
        30 second rate 0 bps
      Match: protocol https
        5 packets, 160 bytes
        30 second rate 0 bps
      Match: protocol dns
        0 packets, 0 bytes
        30 second rate 0 bps

Inspect

  Number of Established Sessions = 1
  Established Sessions
   Session 2204E220 (192.168.1.3:1049)=>(10.1.1.2:443) https:tcp
  SIS_OPEN/TCP_CLOSEWAIT
          Created 00:00:14, Last heard 00:00:11
          Bytes sent (initiator:responder) [821:1431]

   Class-map: class-default (match-any)
     Match: any
     Drop
       4 packets, 160 bytes
R1#
```

- The example below shows verification information after a test of the ZPF configuration.
- A PRIVATE zone host 192.168.1.3 established an HTTPS session with a web server at 10.1.1.2.
- Notice further down in the command output that four packets matched the class class-default.
- This verification information was generated by having host 192.168.1.3 ping the web server at 10.1.1.2.

219

Verify a ZPF Configuration (Cont.)

```
R1# show class-map type inspect
Class Map type inspect match-any HTTP-TRAFFIC (id 1)
   Match protocol http
   Match protocol https
   Match protocol dns

R1# show zone security
zone self
Description: System Defined Zone

zone PRIVATE
 Member Interfaces:
 GigabitEthernet0/0

zone PUBLIC
 Member Interfaces:
 Serial0/0/0

R1# show zone-pair security
Zone-pair name PRIV-PUB
    Source-Zone PRIVATE Destination-Zone PUBLIC
    service-policy PRIV-TO-PUB-POLICY

R1# show policy-map type inspect
Policy Map type inspect PRIV-TO-PUB-POLICY
    Class HTTP-TRAFFIC
      Inspect
    Class class-default
      Drop
```

- The example shows four other ZPF verification commands that allow a view of specific portions of the ZPF configuration.

ZPF Configuration Considerations

When configuring a ZPF with the CLI, there are several factors to consider:

- The router never filters the traffic between interfaces in the same zone.
- An interface cannot belong to multiple zones. To create a union of security zones, specify a new zone and appropriate policy map and zone pairs.
- ZPF can coexist with Classic Firewall although they cannot be used on the same interface. Remove the **ip inspect** interface configuration command before applying the **zone-member security** command.
- Traffic can never flow between an interface assigned to a zone and an interface without a zone assignment. Applying the **zone-member** configuration command always results in a temporary interruption of service until the other zone-member is configured.
- The default inter-zone policy is to drop all traffic unless otherwise specifically allowed by the service-policy configured for the zone-pair.
- The **zone-member** command does not protect the router itself (traffic to and from the router is not affected) unless the zone- pairs are configured using the predefined self zone.

221

16.4 Zone-Based Firewalls Summary

224

What Did I Learn in this Module?

ZPF Overview:

- The IOS ZPF provides a flexible and powerful replacement for the older Classic IOS Firewall.
- It provides a new configuration mode in which interfaces are assigned to security zones and firewall policies are applied to traffic moving between the zones.
- The ZPF provides a structured and simplified method of designing and implementing network security on routers that are performing a firewall function.

225

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

ZPF Operation:

- ZPFs use user-defined policies to act on specific traffic that is travelling from a source zone to a destination zone. Three actions can be specified:
  - **inspect** - The ZPF performs stateful packet inspection.
  - **drop** - The traffic is not permitted to travel to the destination. The rejected packets can be logged.
  - **pass** - The traffic is permitted to travel to the destination zone. This does not track the state of connections or sessions.
- Default rules are applied to transit traffic based on the configuration of the ingress and egress interfaces and the existence of policies.

A special zone exists that is known as the self zone. The self zone is the router itself. In the self zone, the router interfaces serve as either the source or destination of the traffic. Self zone traffic is either for management of the device, or for traffic forwarding control. Like the rules for transit traffic, rules exist for how traffic in the self zone will be handled.

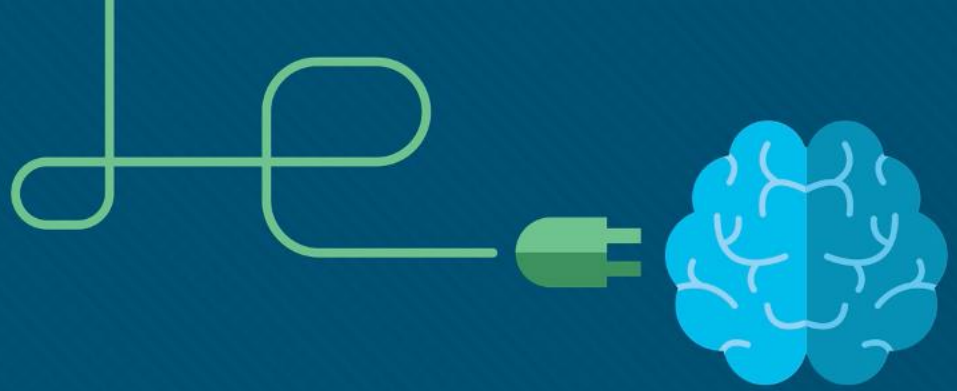
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential 226

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

Configure a ZPF:

- There are five steps in the process of configuring a ZPF.
  - First the zones are created.
  - Next, one or more class maps are created to specify the traffic which should be associated with a policy.
  - Then, policies are created that associate the class-map traffic with the pass, drop, or inspect actions.
  - It is then necessary to create zone pairs that will be associated with policy maps.
  - Finally, interfaces are associated with zones.
  - At this point, the ZPF policy is active.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential 227



Thank You

Cybersecurity Essentials 3.0