The Notebook
of
CCNA

Huy Bui

PL
THE PUBLISHER

Contents

0.1 List of Codes

Chapter 1

Introduction

1.1 Securing network

1.1.1 Terminologies

An attack vector is a path or other means by which an attacker can gain access to a server, host, or network. Attack vectors can originate from outside (external threat) or inside (internal threat) the corporate network. Internal threats have the potential to cause greater damage than external threats because employees have direct access to infrastructure devices as well as the knowledge of the corporate network.

White hat hackers perform *ethical* network penetration test to discover network vulnerabilities. **Grey hat hackers** do unethical things, but not for personal gain or to cause damage (e.g. disclose vulnerability publicly). **Black hat hackers** violate computer and network security for personal gain and malicious purposes. The following list displays modern hacking terms and a brief description of each.

Security Artichoke is the analogy used to describe what a hacker must do to launch an attack in a Borderless network. They remove certain *artichoke leafs*, and each *leaf* of the network may reveal some sensitive data. And leaf after leaf, it all leads the hacker to more data.

Cryptography is the study and practice of hiding information. It ensures three components of information security: Confidentiality, Integrity, and Availability.

A **Security Policy** is a formal statement of the rules by which people that are given access to the technology and information assets of an organization, must abide.

1.1.2 Network topology

SOHO network: Attackers may want to use someone's Internet connection for free or illegal activity, or view financial transactions. Home networks and SOHOs are typically protected using a consumer *grade router*, such as a *Linksys home wireless router*.

WAN network: Main site and Regional site are protected by an ASA (stateful firewall and VPN). Branch site is secured using hardened ISR and VPN connection to the main site. The SOHO and Mobile users connect to the main site using Cisco Anyconnect VPN client.

Data center network: Data center networks are interconnected to corporate sites using VPN and ASA devices along with *integrated data center switches*, such as a high-speed Nexus switches. Data center physical security can be divided into two areas: Outside perimeter security and Inside perimeter security.

Cloud and virtual network: This kind of network uses virtual machines (VM) to provide services to their clients. VMs are also prone to specific targeted attacks as shown in the following list. The **Cisco Secure Data Center** is a solution to secure Cloud and virtual network. The core components of this solution provide: Secure Segmentation, Threat Defense, and Visibility.

- **Hyperjacking:** An attacker could hijack a VM hypervisor and use it as a starting point to attack other devices.
- **Instant on activation:** A VM that has not been used for a long period of time can introduce security vulnerabilities when activated.
- **Antivirus storm:** Multiple VMs attempt to download antivirus file at the same time

Borderless Network: To accommodate the BYOD trend, Cisco developed the Borderless Network. To support this network, Cisco devices support Mobile Device Management (MDM) features. MDM features secure, monitor, and manage mobile devices, including corporate-owned devices and employee-owned devices.

1.2 Network threats

1.2.1 Malware

A **virus** is malicious code that is attached to executable files which are often legitimate programs. A virus is triggered by an event. When activated, the virus can infect all the files it has not yet infected, but does not automatically propagate itself to other systems. Viruses are *spread* by USB memory drives, CDs, DVDs, network shares, and email. Email viruses are now the most common type of virus.

A **Trojan horse** is malware that carries out malicious operations under the guise of a desired function. A Trojan horse comes with malicious code hidden inside of it. This malicious code exploits the *privileges* of the user that *runs* it. Trojans are often found attached to online games.

Worms run by themselves, replicate and then spread very quickly (self-propagation) to slow down networks. They does not require user participation. After a host is infected, the worm is able to over the network. Most worm attacks consist of three components:

- **Enabling vulnerability:** A worm installs itself using an exploit mechanism, such as an email attachment, an executable file, or a Trojan horse.
- **Propagation mechanism:** After gaining access to a device, the worm replicates itself and locates new targets.
- **Payload:** Any malicious code that results in some action is a payload. Most often this is used to create a backdoor to the infected host or create a DoS attack.

Note! Worms never really stop on the Internet. After they are released, they continue to propagate until all possible sources of infection are properly patched.

Some other examples of modern malware:

- Ransomware – deny access to the infected computer system, then demand a paid ransom for the restriction to be removed.
- Spyware – gather information about a user and send the information to another entity
- Adware – display annoying pop-up advertising pertinent to websites visited
- Scareware – include scam software which uses social engineering to shock or induce anxiety by creating the perception of a threat
- Phishing – attempt to convince people to divulge sensitive information, e.g. receiving an email from their bank asking users to divulge their account and PIN numbers.
- Rootkits – installed on a compromised system, then hide its intrusion and maintain privileged access to the hacker.

1.2.2 Common network attacks

The method used in this course classifies attacks in three major categories: Reconnaissance, Access, and DoS Attacks.

Reconnaissance attacks gather information about a network and scan for access. Some examples of reconnaissance attacks: information query, ping sweep[1], port scan, Vulnerability Scanners, Exploitation tools.

Access attacks exploit network vulnerabilities to gain access or control to sensitive information. There are five common types of access attacks: Password attack, Trust exploitation, Port redirection, Man-in-the-middle, Buffer overflow, IP spoofing, MAC spoofing, DHCP Spoofing.

- Password attack – a dictionary is used for repeated login attempts
- Trust exploitation – uses granted privileges to access unauthorized material
- Port redirection – uses a compromised internal host to pass traffic through a firewall
- Man-in-the-middle – an unauthorized device positioned between two legitimate devices in order to redirect or capture traffic
- Buffer overflow – too much data sent to a buffer memory

Denial-of-Service (DoS) attacks prevent users from accessing a system. They are popular and simple to conduct. There are two major sources of DoS attacks:

- *Maliciously Formatted Packets* is forwarded to a host and the receiver is unable to handle an unexpected condition, which leads to slow or crashed system.
- *Overwhelming Quantity of Traffic* causes the system to crash or become extremely slow.

A Distributed DoS Attack (DDoS) is similar in intent to a DoS attack, except that a DDoS attack increases in magnitude because it originates from multiple, coordinated sources. As an example, a DDoS attack could proceed as follows:

1. A hacker builds a network of infected machines. A network of infected hosts is called a *botnet*. The compromised computers are called *zombie computers*, and they are controlled by *handler systems*.
2. The zombie computers continue to scan and infect more targets to create more zombies.
3. When ready, the hacker instructs the handler systems to make the botnet of zombies carry out the DDoS attack.

1.3 Mitigating Threats

1.3.1 Mitigating common network attacks

Malware: The primary means of mitigating virus and Trojan horse attacks is antivirus software. Antivirus software are host-based product that prevents hosts from getting infected and spreading malicious code. However, they do not prevent viruses from entering the network.

Worms: They are more network-based than viruses. The response to a worm attack can be broken down into four phases:

1. **Containment:** limit the spread of worm infection
2. **Inoculation:** run parallel to or subsequent to the Containment phase; all uninfected systems are patched with the appropriate vendor patch.
3. **Quarantine:** identify the infected machines
4. **Treatment:** disinfect the infected systems

[1] a network scanning technique that indicates the live hosts in a range of IP addresses

Reconnaissance: *Encryption* is an effective solution for sniffer attacks. Using *IPS* and *firewall* can limit the impact of *port scanning*. *Ping sweeps* can be stopped if *ICMP* echo and echo-reply are turned off on edge routers.

Access attacks: The network should be designed using the principle of minimum trust. This means that systems should not use one another unnecessarily. Other options are valid network security access protections (encrypted or hashed authentication protocols) but do not relate to the principle of minimum trust.

DoS attacks: One of the first signs of a DoS attack is a large number of user complaints about unavailable resources. To minimize the number of attacks, a network utilization software and anti-spoofing technologies (port security, DHCP snooping, IP source guard, ARP inspection, and ACL) should be running at all times.

1.3.2 Cisco SecureX architecture

The Cisco SecureX architecture is designed to provide effective security for any user, using any device, from any location, and at any time. This architecture includes the five major components: Scanning Engines, Delivery Mechanisms, Security Intelligence Operations (SIO), Policy Management Consoles, and Next-Generation Endpoints. The most important component of SecureX is SIO, which detects and blocks malicious traffic.

The SecureX is a huge and complex computing model. Therefore, a **context-aware scanning element** is used to scale SecureX. It is a device that examines packets as well as external information to understand the full context of the situation. To be accurate, this context-aware device defines security policies based on five parameters: person ID, application, device type, location, and access time.

Security Intelligence Operations (SIO) is a Cloud-based service that connects global threat information, reputation-based services, and sophisticated analysis, to SecureX network security devices.

1.3.3 Cisco Network Foundation Protection Framework

The Cisco Network Foundation Protection (NFP) framework provides comprehensive guidelines for protecting the network infrastructure. NFP logically divides routers and switches into three functional areas: Control plane, Management plane, and Data plane.

- **Control plane** is responsible for routing functions. Its security is implemented by Routing protocol authentication, CoPP, and AutoSecure. CoPP (Control Plane Policing) prevents unnecessary traffic from overwhelming the route processor. **AutoSecure** can lock down the management plane functions and the forwarding plane services and functions of a router.

- **Management plane** is responsible for network security and management. Its security is implemented by password policy, RBAC[2], authorization, access reporting.

- **Data plane** (Forwarding plane) is responsible for forwarding data. Its security can be implemented using *ACLs*, *antispoofing mechanisms*, and *Layer 2 security* features.

[2] Role-based access control restricts user access based on the role of the user. In Cisco IOS, the role-based CLI access feature implements RBAC for router management access.

Chapter 2

Securing the network infrastructure

2.1 Securing device access

2.1.1 Edge router

There are many approaches to secure the edge router:

- **Single router approach:** a single router connects internal LAN to the Internet. All security policies are configured on this device. This is commonly deployed in small networks such as branch and small office, SOHO sites. The required security features can be supported by ISRs.
- **Defense-in-depth approach:** there are three primary layers of defense: the edge router, the firewall, and an internal router that connects to the protected LAN (Figure 2.1). By default, the firewall denies the initiation of connections from the outside (untrusted) networks.
- **DMZ approach:** A variation of the defense-in-depth approach is the DMZ approach (Figure 2.2). The firewall is set up to permit the required connections, such as HTTP, from the outside networks to the public servers in the DMZ. The firewall serves as the primary protection for all devices in the DMZ.

Three areas of router security must be maintained:

- **Physical security:** Place the router and physical devices that connect to it in a secure locked and dedicated room
- **Operating system security:** Configure the router with the maximum amount of memory possible, Use the latest, stable version of the operating system, Keep a secure copy of router operating system images and router configuration files
- **Router Hardening:** Secure administrative control, Disable unnecessary ports, interfaces and services

Figure 2.1: Defense-in-depth approach

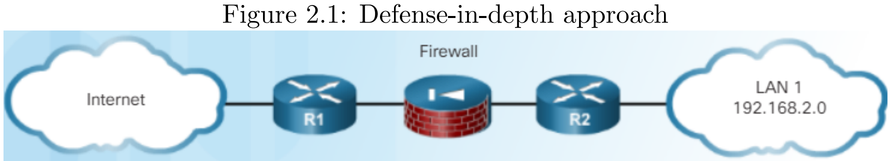
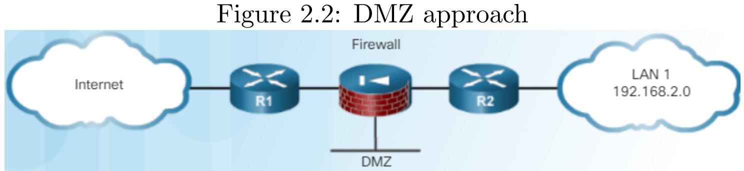


Figure 2.2: DMZ approach



2.1.2 Administrative access

Type of management access: When logging and managing information, the information flow between management hosts and the managed devices can take two paths: In-band (SSH, SNMP, etc.) and Out-of-band (console port). Out-of-band management is appropriate for large enterprise networks, because it remains unaffected by the downed link. In-band management is recommended in smaller networks as a means of achieving a more cost-effective security deployment.

Strong password: To create a strong password, use a blank space in the password (only password-leading spaces are ignored) or create a phrase made of many words. This is called a *passphrase*. A passphrase is often easier to remember than a complex password and more difficult to guess.

Secret Password Algorithms: All passwords in Cisco IOS uses an MD5 hash by default. However, MD5 hashes are no longer considered secure. Therefore, it is now recommended that you configure all passwords using either type 8 `sha256` or type 9 `scrypt` passwords.

Listing 1: Secret password type 9

```
enable algorithm-type scrypt secret cisco12345
username Huy algorithm-type scrypt secret cisco12345
```

2.1.3 Virtual logins

The following Cisco IOS login enhancements commands increase the security of virtual login connections.

Listing 2: Login security commands

```
login block-for 15 attempts 5 within 60
login quite-mode access-class PERMIT-ADMIN
login delay 10
login on-access log
login on-failure log
```

The `login block-for` command can defend against DoS attacks by disabling logins for 60 seconds if more than 5 login failures occur in 15 seconds or less. Specifically, this command operates in two modes: **Normal** mode and **Quite** mode. When quiet mode is enabled, all login attempts, including valid administrative access, are not permitted. However, this behavior can be overridden using the `login quiet-mode` command with an ACL that identifies the permitted hosts.

The `login delay` command specifies a number of seconds the user must wait between unsuccessful login attempts. The `login on-success` and `login on-failure` commands generate syslog messages for successful and unsuccessful login attempts. The `security auth failure rate` command can be configured to generate a log message when the login failure rate is exceeded.

Use the `show login` command to verify the login block-for command settings and current mode. The `show login failures` command displays additional information regarding the failed attempts, such as the IP address from which the failed login attempts originated.

These login enhancements do *not* apply to console connections. When dealing with console connections, it is assumed that only authorized personnel have physical access to the devices.

Note! These login enhancements can only be enabled if the local database is used for authentication for local and remote access. If the lines are configured for password authentication only, then the enhanced login features are not enabled.

2.1.4 Configuring SSH

There are four requirements the router must meet before configuring SSH:

- Runs a Cisco IOS release that supports SSH
- Uses a unique hostname
- Contains the correct domain name of the network
- Configured for local authentication or AAA services

The five steps needed to configure a Cisco router to support SSH with local authentication:

1. Configure the IP domain name of the network
2. Create RSA key to encrypt the SSH traffic (Once RSA keys are generated, SSH is automatically enabled)
3. Ensure that there is a valid local database username entry.
4. Enable vty inbound SSH sessions using the line vty commands
5. Verify SSH and display the generated keys

Listing 3: Configuring SSH

```
ip domain-name cisco.com

crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024

ip ssh version 2
username Huy algorithm-type scrypt secret cisco12345

line vty 0 4
  login local
  transport input ssh

ip ssh time-out 90
ip ssh authentication-retries 2

sh crypto key mypubkey rsa
sh ssh
```

If there are existing key pairs, it is recommended that they are removed using the `crypto key zeroize rsa` command. To verify the status of the client connections, use the `sh ssh` command. The default SSH timeouts and authentication parameters can be altered using `ip ssh time-out` and `ip ssh authentication-retries` commands.

2.2 Administrative roles

Cisco IOS software has two methods of providing infrastructure access: privilege level and role-based CLI. Both methods help determine who should be allowed to connect to the device and what that person should be able to do with it. Role-based CLI access provides more granularity and control.

2.2.1 Privilege levels

There are 16 privilege levels (0 – 15) that can be applied to user accounts. Levels 0, 1, and 15 have predefined settings. This leaves levels 2 through 14 available for custom levels of access. Below is the detailed settings of level 1 and 15:

- **Level 1:** User EXEC mode – The lowest user privileges and allows only user-level commands available at the `router>` prompt.
- **Level 15:** Privileged EXEC mode – the user has full access to view and change the configuration, including viewing the running the configuration.

The first command shown below configures privilege level 5, so that any level-5 user has access to all the commands available for the level 1 to 4 and the `ping` command. Remember that not all commands are available for privilege level 5. For example, level-5 users cannot reload the router. To enable access to the reload command, use the command `privilege exec level 5 reload` . The second command assigns a privilege level to a specific EXEC mode password. The last assigns privilege level `5` to user `SUPPORT`.

Listing 4: Privilege level configuration

```
privilege exec level 5 ping
enable algorithm-type scrypt secret level 5 cisco5
username SUPPORT privilege 5 algorithm-type scrypt secret cisco5
```

The use of privilege levels has its limitations:

- No access control to specific interfaces, ports, logical interfaces, and slots on a router.
- Commands available at lower privilege levels are always executable at higher levels.
- Commands specifically set at a higher privilege level are not available for lower privileged users.
- Assigning a command with multiple keywords allows access to all commands that use those keywords. For example, allowing access to show ip route allows the user access to all show and show ip commands.

2.2.2 Role-based CLI

Role-based CLI enhances the security of the device by defining the set of CLI commands accessible by a specific user. Users only see the CLI commands applicable to the ports and CLI to which they have access. Therefore, the router appears to be less complex, and commands are easier to identify when using the help feature on the device. Role-based CLI provides three types of views that dictate which commands are available:

- **Root view:** Only a root view user can configure a new view and add or remove commands from the existing views.
- **CLI view:** A specific set of commands can be bundled into a CLI view. A view does not inherit commands from any other view. Additionally, the same commands can be used in multiple views.
- **Superview:** A superview consists of one or more CLI views. Users who are logged into a superview can access all the commands that are configured for any of the CLI views that are part of the superview. Deleting a superview does not delete the associated CLI views, and those views remain available to be assigned to another superview.

Note! Commands cannot be configured for a superview. An administrator must add commands to the CLI view and add that CLI view to the superview.

Listing 5: CLI View configuration

```
aaa new-model
parser view SUPPORT
  secret cisco
  commands exec include show
end

enable view SUPPORT
```

In the above example, the `commands exec include` command assigns all `show` commands to the EXEC mode of the view. To access existing views, enter the `enable view view-name` command in user mode and enter the password that was assigned to the custom view. Use the question mark (?) command to verify that the commands available in the view are correct.

Note! AAA must be enabled before configuring any views.

Listing 6: Superview configuration

```
parser view JR-ADMIN superview
  secret cisco2
  view SHOWVIEW
  view VERIFYVIEW
  view REBOOTVIEW
end
```

You must be in root view to configure a superview. To confirm that root view is being used, use either the `enable view` or `enable view root` command. In the above example, more than one CLI view are assigned to the current superview using `view` command. To access the superview, use the `enable view` command followed by the name of the superview, and provide the password. Use the question mark (?) command to verify that the commands available in the view are correct.

From the root view, use the `show parser view all` command to see a summary of all views. Notice how the asterisk identifies superviews.

2.3 IOS image and Configuration files

2.3.1 Backup and restore

The **Cisco IOS resilient configuration** feature maintains a secure working copy of the router IOS image file and a copy of the running configuration file. These secure files cannot be removed by the user and are referred to as the primary bootset.

To secure the IOS image and enable Cisco IOS image resilience, use the `secure boot-image` command. Once enabled, this feature can only be disabled through a console session. This command functions properly only when the system is configured to run an image from a flash drive with an ATA interface. Additionally, the running image must be loaded from secured storage. Images that are loaded from a remote location, such as a TFTP server, cannot be secured.

To take a snapshot of the router running configuration and securely archive it in persistent storage, use the `secure boot-config` global configuration mode command.Use the `show secure bootset` command to verify the existence of the archive.

Restore a primary bootset from a secure archive after the router has been tampered with:

1. Reload the router using the reload command. If necessary, issue the break sequence to enter ROMmon mode.
2. From ROMmon mode, enter the dir command to list the contents of the device that contains the secure bootset file.
3. Boot the router with the secure bootset image using the boot command followed by the flash memory location (e.g. flash0), a colon, and the filename found in Step 2.
4. Enter global configuration mode and restore the secure configuration to a filename of your choice.
5. Exit global configuration mode and issue the copy command to copy the rescued configuration file to the running configuration.

Listing 7: Restore a primary bootset

```
Router# reload

rommon 1 > dir flash0:
rommon 2 > boot flash0:c1900-universalk9-mz.SPA.154-3.M2.bin

Router> enable
Router# conf t
Router(config)# secure boot-config restore flash0:rescue-cfg
Router(config)# end
Router# copy flash0:rescue-cfg running-config
```

2.3.2 Secure Copy Protocol(SCP)

The Cisco IOS Resilient feature provides a secure and authenticated method for copying router configuration or router image files to a remote location, that is **Secure Copy Protocol (SCP) feature**. SCP relies on SSH and requires that AAA authentication. The following commands configure the router for server-side SCP with local AAA:

Listing 8: Configure SCP with local AAA

```
ip domain-name cisco.com
crypto key generate rsa general-keys modulus 1024
username Huy algorithm-type scrypt secret cisco12345

aaa new-model
aaa authentication login default local
aaa authorization exec default local

ip scp server enable
```

With the above configuration, R1 is now an SCP server and will use SSH connections to accept secure copy transfers from authenticated and authorized users. For example, you want to transfer a backup file from R2 to R1. On R2, use the `copy flash0:R2backup.cfg scp:` command.

2.3.3 Password recovery

An attacker could gain control of that device through the password recovery procedure. An administrator can mitigate this potential security breach by using the `no service password-recovery` global configuration mode command. This command disables all access to ROMmon mode.

To recover a device with password-recovery disabled, initiate the break sequence within **5** seconds after the image decompresses during the boot. You are prompted to confirm the break key action. After the action is confirmed, the startup configuration is completely erased, the router boots with the factory default configuration, and therefore, the password recovery procedure is enabled. If you do not confirm the break action, the router boots normally with the no service password-recovery command enabled.

2.4 Syslog

2.4.1 Introduction

The syslog protocol allows networking devices to send their system messages across the network to syslog servers. The syslog server serves as an event message collector. Syslog messages are sent using **UDP** port **514**.

Syslog operations include gathering information, selecting which type of information to capture, and redirecting the captured information to a storage location. The logging service stores messages in a logging buffer that is time-limited, and cannot retain the information when a router is rebooted. Syslog does not authenticate or encrypt messages.

Syslog messages sent to an internal buffer (RAM) are only viewable through the CLI of the device (console line, terminal line). Alternatively, syslog messages can be sent to an external syslog server. To view syslog messages, a syslog server must be installed on a workstation. One advantage of viewing syslog messages on a syslog server is the ability to perform granular searches through the data. Also, a network administrator can quickly delete unimportant syslog messages from the database.

2.4.2 Severity level and Facility

Cisco devices produce syslog messages as a result of network events. Every syslog message contains a **severity level** and a **facility**. The security level can be shown as a number. The smaller the number, the more critical syslog alarms (Table 2.1).

Table 2.1: Syslog Severity level

Severity level	**Name**	**Explanation**
0	Emergency	A "panic" condition, System unusable
1	Alert	Should be corrected immediately, e.g. loss of backup ISP connection
2	Critical	Critical condition
3	Error	Error condition, Non-urgent failures
4	Warning	NOT an error, but indication that an error will occur if action is not taken, e.g. file system 85% full
5	Notification	Normal but significant condition
6	Informational	Not affect functionality, harvested for reporting, measuring throughput,
7	Debugging	Debugging message

Level 0 – 4 are error messages. Level 5 notifies system messages such as interface up or down transitions and system restart messages. Level 6 generates messages , for example, when the device is booting. By default, Cisco routers and switches send log messages up to level 6 of severity (levels 0 through 6) to the console.

2.4.3 Message format

By default, the format of syslog messages on the Cisco IOS Software is as follows:

```
seq no: timestamp: %facility-severity-MNEMONIC: description
00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
```

The fields contained in the syslog message above are explained in Table 2.2.

Table 2.2: Syslog message format

Field	Example	Explanation
seq no	–	Will be shown only if the service `sequence-numbers` is configured
timestamp	00:00:46	Date and time of the message, which appears only if the service `timestamps` is configured
facility	LINK	The facility to which the message refers
severity	3	A number from 0 to 7 that indicates the severity of the message
MNEMONIC	UPDOWN	Briefly and Uniquely describe the message
description	Interface ...	Report the event in detail

2.4.4 Configuration

By default, log messages do not include a timestamp. The `show logging` command displays the default logging service settings.

Listing 9: Logging service

```
service timestamps log datetime msec
logging 192.168.1.3
logging trap 4
logging source-interface g0/0
```

Above is an example showing logging service configuration. The first command enable timestamp to log messages. R1 is configured to send log messages of levels 4 and lower to the syslog server at 192.168.1.3. The source interface is set as the g0/0 interface.

2.5 SNMP

2.5.1 Introduction

Simple Network Management Protocol (SNMP) was developed to allow administrators to manage nodes such as servers, workstations, routers, switches, and security appliances, on an IP network. The SNMP system consists of three elements:

- **SNMP manager**: a part of a network management system (NMS), run SNMP management software.
- **SNMP agents** (managed node): responsible for providing access to the MIB which resides on each SNMP client device.
- **MIB** (Management Information Base): store data about the device and operational statistics

Table 2.3: SNMP requests

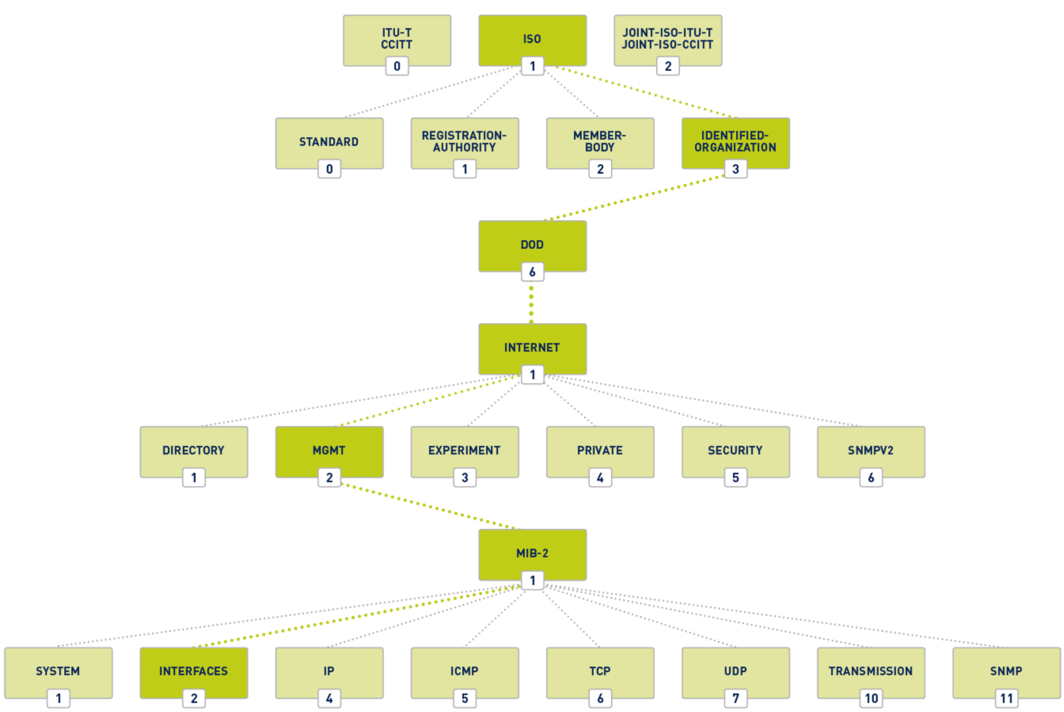
Operation	Description
`get-request`	Retrieves a value from a specific variable
`get-next-request`	Retrieves a value from a variable within a table
`get-bulk-request`	Retrieve large block of data such as multiple rows in a table
`get-response`	Replies to a `get-request`, `get-next-request`, and `set-request`
`set-request`	Stores a value in a specific variable

Polls vs Traps: An NMS periodically *polls* the SNMP agents, which provide information to monitor traffic loads and to verify device configurations. Disadvantages: A delay between the time that an event occurs and the time that it is noticed (via polling) by the NMS; A trade-off between polling frequency and bandwidth usage. SNMP *agent traps* are used to mitigate these disadvantages. SNMP agents send traps to inform the NMS immediately of certain events.

Community string: SNMPv1 and SNMPv2c use community strings as plaintext password to control access to the MIB. There are two types of community strings: Read-only (**ro**) and Read-write (**rw**).

Object ID: MIB saves data in variables and organizes them hierarchically. Formally, the MIB defines each variable as an Object ID (OID). OIDs uniquely identify managed objects in the MIB hierarchy (figure 2.3). For example, OIDs belonging to Cisco, are numbered as follows: .iso (1).org (3).dod (6).internet (1).private (4).enterprises (1).cisco (9). Therefore the OID is 1.3.6.1.4.1.9.

Figure 2.3: OID tree



SNMPv2 configuration

Listing 10: SNMPv2 configuration

```
snmp-server community batonaug ro SNMP_ACL

snmp-server enable traps
snmp-server host 192.168.1.3 version 2c batonaug

show snmp
```

The first command configures the community string, access level (read-only `ro` , read-write `rw`), and restrict SNMP access using ACL.The next two command enable traps and specify the recipient of the SNMP trap. By default, SNMP does not have any traps set. Without this command, SNMP managers must poll for all relevant information.

2.5.2 SNMPv3 configuration

SNMPv3 provides three security features: Message integrity and authentication, Encryption, Access control. The following commands show an example of basic SNMPv3 configuration:

Listing 11: SNMPv3 configuration

```
snmp-server view SNMP-RO iso included
snmp-server group ADMIN v3 priv read SNMP-RO access PERMIT-ADMIN
snmp-server user BOB ADMIN v3 auth sha cisco12345 priv aes 128 cisco54321
```

In the above example, the first command creates an SNMP view `SNMP-RO` and include the entire `iso` tree from the MIB. The next command creates an SNMP group `ADMIN` , the set to version 3 with authentication and encryption required. This command also gives read-only access to the view `SNMP-RO` to the group specified by the ACL called `PERMIT-ADMIN` .

2.6 NTP

2.6.1 System clock

The software clock on a router or switch starts when the system boots and is the primary source of time for the system. It is important to synchronize the time across all devices on the network because all aspects of managing, securing, troubleshooting, and planning networks require accurate time-stamping. Typically, the date and time settings on a router or switch can be set using one of two methods:

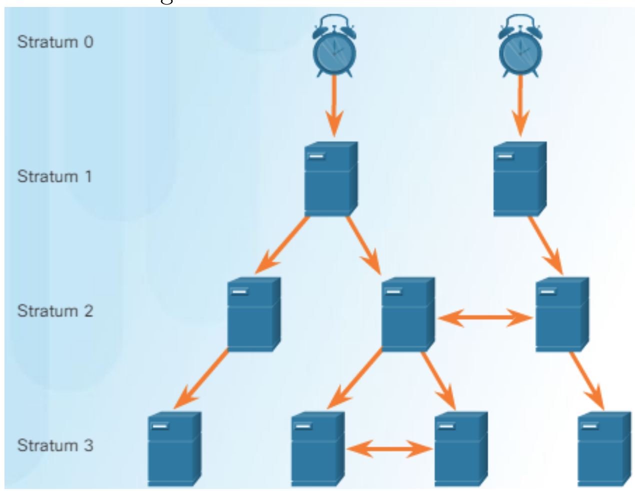
- Manually configure the date and time. For example, `clock set 20:36:00 aug 30 2016`
- Configure the NTP

2.6.2 Operation

NTP allows routers on the network to synchronize their time settings with an NTP server. It uses **UDP** port **123**.

NTP networks use a hierarchical system of time sources. Each level in this hierarchical system is called a **stratum**. The stratum level is defined as the number of hop counts from the authoritative time source (Figure 2.4). Smaller stratum numbers indicate that the server is closer to the authorized time source than larger stratum numbers. The max hop count is 15. Stratum 16, the lowest stratum level, indicates that a device is unsynchronized.

Figure 2.4: NTP Stratum levels



Stratum 0 is an NTP network that gets the time from authoritative time sources (represented by the clock in the figure 2.4). Stratum 1 are directly connected to the authoritative time sources. They act as the primary network time standard. The stratum 2 servers are connected to stratum 1 devices through network connections. Stratum 2 devices, such as NTP clients, synchronize their time using the NTP packets from stratum 1 servers. They can also act as servers for stratum 3 devices.

2.6.3 Configuration

The first command identifies NTP server. The second command periodically updates the hardware clock with the time learned from NTP. The following commands configure NTP authentication on R1 using key 1 and password NTPpa55. To verify the system clock, use `show clock` command. To see if the device is synchronized with the NTP server, use `sh ip ntp ass` and `sh ntp status`.

Listing 12: NTP authentication

```
ntp server 192.168.1.5
ntp update-calendar

ntp authenticate
ntp trusted-key 1
ntp authentication-key 1 md5 NTPpa55

sh ntp status
sh ip ntp ass
sh clock
```

2.7 Cisco AutoSecure

AutoSecure makes recommendations for fixing security vulnerabilities and then modifies the security configuration of the router. It can lock down the functions of data and management plane. During AutoSecure setup, the following steps occur:

1. The AutoSecure command is entered
2. The wizard gathers info about the outside interfaces
3. Disable unnecessary services

4. Prompt for a security banner
5. Prompt for passwords and login features
6. Secure interface
7. Secure data plane

Use the `auto secure` command to enable the Cisco AutoSecure feature setup. In interactive mode, the router prompts with options to enable and disable services and other security features. This is the *default* mode, but it can also be configured using the `auto secure full` command.

The non-interactive mode is configured with the `auto secure no-interact` command. This will automatically execute the Cisco AutoSecure feature with the recommended Cisco default settings.

When the AutoSecure command is initiated, a CLI wizard steps the administrator through the configuration of the device. User input is required. AutoSecure should be used when a router is initially being configured. It is not recommended on production routers.

2.8 Control plane security

2.8.1 Routing protocol authentication

Routing Protocol Authentications mitigate against attacks like redirection of traffic to an insecure link, and redirection of traffic to discard it. OSPF supports routing protocol authentication using either MD5 or SHA.

OSPF MD5 authentication

Listing 13: OSPF MD5 interface authentication

```
interface s0/0/0
  ip ospf message-digest-key 1 md5 cisco12345
  ip ospf authentication message-digest
```

Listing 14: OSPF MD5 area authentication

```
router ospf 100
  area 50 authentication message-digest

interface s0/0/0
  ip ospf message-digest-key 1 md5 cisco12345
end
```

Note! The interface setting overrides the global setting. OSPF adjacency is lost until MD5 authentication is matched between two routers.

OSPF SHA authentication

MD5 is now considered vulnerable to attacks. Therefore, the administrator should use SHA authentication. OSPF SHA authentication includes two major steps:

1. Specify an authentication key chain
2. Assign the authentication key to the desired interfaces

Listing 15: OSPF SHA authentication

```
key chain HUY
  key 1
  key-string cisco12345
  cryptographic-algorithm hmac-sha-256

interface s0/0/0
  ip ospf authentication key-chain HUY
```

2.8.2 Control plane policing

Routers must be able to distinguish between data plane, control plane, and management plane packets to treat each packet appropriately:

- **Data plane packets:** always have a transit destination IP address and can be handled by normal destination IP address-based forwarding processes.
- **Control plane packets:** used for routing protocol (OSPF, EIGRP, BGP, etc.); sent to the router or network device
- **Management plane packets:** used for management and reporting protocol (SSH, SNMP, NTP, etc.)

The vast majority of packets handled by network devices are data plane packets. They are handled by CEF. This forwarding method uses the control plane to pre-populate the FIB table. Subsequent packets that flow between same source and destination are forwarded by the data plane based on the information contained in the FIB.

Chapter 3

AAA model

AAA network security services provide the primary framework to set up access control on a network device. AAA is a way to control who is permitted to access a network (authenticate), what they can do while they are there (authorize), and to audit what actions they performed while accessing the network (accounting).

3.1 Authentication

3.1.1 Local

Local AAA Authentication uses the local usernames and passwords stored on a router. A drawback of the this method is that user accounts must be configured locally on each device, which is an unscalable authentication solution. Therefore, local authentication should be configured for smaller networks with one or two routers. The local authentication can also serve as a backup method for if authentication servers are available. Configuring local AAA services to authenticate administrator access requires a few basic steps:

- Add usernames and passwords to the local router database for users that need administrative access to the router.
- Enable AAA globally on the router.
- Configure AAA parameters on the router.
- Confirm and troubleshoot the AAA configuration.

Listing 16: Local default authentication

```
username ADMIN algorithm-type scrypt secret Str0ng5rPa55w0rd
username JR-ADMIN algorithm-type scrypt secret Str0ng5rPa55w0rd
aaa new-model
aaa authentication login default local-case
```

The above commands allow the ADMIN and JR-ADMIN users to log into the router via the console or vty terminal lines. The `default` keyword means that the authentication method applies to all lines. Alternatively, a custom authentication method (or named method) can be configured using `list-name`. Unlike `default` method, a named method has to be assigned to a particular line (console, aux, or virtual line) using `login auth <list-name>` command.

Listing 17: Local named authentication

```
username ADMIN algorithm-type scrypt secret Str0ng5rPa55w0rd
username JR-ADMIN algorithm-type scrypt secret Str0ng5rPa55w0rd
aaa new-model
aaa authentication login SSH-LOGIN local-case
line vty 0 4
login auth SSH-LOGIN
```

The final portion of the `aaa authentication login` command identifies the type of methods that will be queried to authenticate the users, which is `local-case`. When a user attempts to log in, the first method listed is used. Cisco IOS software attempts the second authentication method only when there is no response or an error from the first method occurs. This process continues until no other authentication methods are available.

The `aaa local authentication attempts max-fail` command locks the user account if the authentication fails. The locked out user account remains locked until it is manually cleared by an administrator using the `clear aaa local user lockout` privileged EXEC mode command. This command is different from `login delay` command, which introduces a delay between failed login attempts without locking the account.

To display a list of all locked-out users, use the `sh aaa local user lockout` command. To display the history of activities (attributes), use the `sh aaa user` command. This command does not provide information for all users who are logged into a device, but only for those who have been authenticated or authorized using AAA, or whose sessions are being accounted for by the AAA module. The `sh aaa sessions` command can be used to show the unique ID of a session. The `debug aaa authentication` command is instrumental when troubleshooting AAA problems. The `debug tacacs events` command displays the opening and closing of a TCP connection to a TACACS+ server, the bytes that are read and written over the connection, and the TCP status of the connection.

3.1.2 Server-based

Table 3.1: TACACS+ and RADIUS protocols

TACACS+	**RADIUS**
Separates authentication and authorization	Combines RADIUS authentication and authorization as one process.
Encrypts all communication	Encrypts only the password using MD5
TCP port 49	UDP port 1645 or 1812 for authentication, UDP port 1646 or 1813 for accounting
Multiprotocol support	Supports remote-access technologies, VoIP, 802.1X, and Session Initiation Protocol (SIP)

Note! A next-generation AAA protocol alternative to RADIUS is the DIAMETER AAA protocol.

Integration of Windows AD and ACS: Many enterprise-level authentication servers are on the market today, but they lack the ability to combine both the TACACS+ and RADIUS protocols into a single solution. Fortunately, Cisco Secure ACS for Windows Server is a single solution that offers AAA for both TACACS+ and RADIUS. Cisco Secure ACS can be integrated to use the AD service. The configuration for Cisco IOS is the same as communicating with any RADIUS server. The only difference is that the Microsoft server's AD controller is used to perform the authentication and authorization services.

3.1.3 Configuration

There are three basic steps to configure server-based authentication:

1. Globally enable AAA
2. Specify the Cisco Secure ACS (TACACS+ or RADIUS server) and Configure the encryption key between the server and router.
3. Configure the AAA authentication method list to refer to the TACACS+ or RADIUS server. For redundancy, it is possible to configure more than one server.

The following commands show how to accomplish step 1 and 2:

Listing 18: Create a TACACS+ server

```
aaa new-models

#STEP 2: TACACS+ server
tacacs server Server-T
  address ipv4 192.168.1.101
  single-connection
  key TACACS-Pa55w0rd

#STEP 2: RADIUS server
radius server Server-R
  address ipv4 192.168.1.101 auth-port 1812 acct-port 1813
  single-connection
  key RADIUS-Pa55w0rd

aaa authentication login default group tacacs+ group radius local-base
```

The `address ipv4` command allows the option to modify IPv4 address of the server, authentication port, and accounting port. The `key` command is used to configure the shared secret key, which must be exactly the same way on both the router and the server.

The `single-connection` command (TACACS+ only) maintains a single TCP connection for the life of the session. Otherwise, by default, a TCP connection is opened and closed for each session. Because RADIUS uses UDP, there is no `single-connection` keyword.

When the AAA servers have been identified, the servers must be included in the method list of the `aaa authentication login` command. AAA servers are identified using the `group tacacs+` or `group radius` keywords. This command configures a method list for the default login to authenticate first using a TACACS+ server, second with a RADIUS server, and finally with a local username database. It is important to realize that R1 will only attempt to authenticate using RADIUS if the TACACS+ server is not reachable. Likewise, R1 would only attempt to authenticate using the local database if the TACACS+ and RADIUS servers are unavailable.

3.2 Authorization and Accounting (server-based only)

When AAA authorization is not enabled, all users are allowed full access. After authentication is started, the default changes to allow no access. This means that the administrator must create a user with full access rights before authorization is enabled.

To configure command authorization, use the `aaa authorization` command. The service type can specify the types of commands or services: `network` – For network services such as PPP, `exec` – For starting an exec (shell), `commands <level>` – For exec (shell) commands.

Listing 19: Authorization Configuration

```
aaa authorization {network | commands <level> | exec} {default | <list-name>}
  method1 ... method4

aaa authorization exec default group tacacs+
```

To configure AAA accounting, use the `aaa accounting` command.

Listing 20: Accounting Configuration

```
aaa accounting {network | connection | exec} {default | <list-name>}
         {statrt-stop | stop-only | none} [broadcast] method1 ... method4

aaa account exec default start-stop group tacacs+
```

The following three parameters are commonly used aaa accounting keywords:

- `network` - Runs accounting for all network-related service requests, including PPP.
- `exec` - Runs accounting for the EXEC shell session.
- `connection` - Runs accounting on all outbound connections such as SSH and Telnet.

Next, the record type, or trigger, is configured. The trigger specifies what actions cause accounting records to be updated. Possible triggers include:

- `start-stop` - Sends a ”start” accounting notice at the beginning of a process and a ”stop” accounting notice at the end of a process.
- `stop-only` - Sends a ”stop” accounting record for all cases including authentication failures.
- `none` - Disables accounting services on a line or interface.

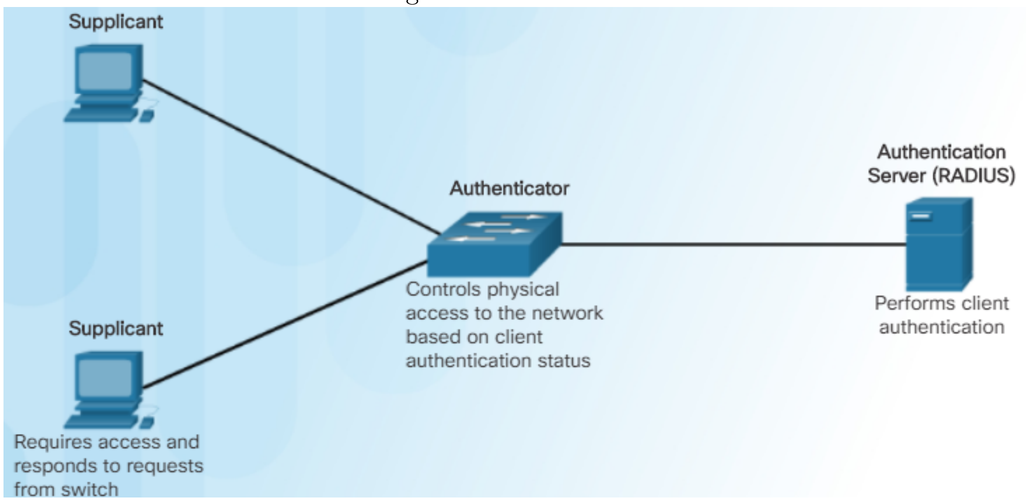
3.3 802.1X Port-Based Authentication

3.3.1 Operation

The IEEE 802.1X standard defines a port-based access control and authentication protocol that restricts unauthorized devices from connecting to a LAN through publicly accessible switch ports. Figure 3.1 shows that with 802.1X port-based authentication roles:

- **Supplicant (Client)** – The device that requests access to LAN. The workstation must be running 802.1X-compliant client software.
- **Authenticator (Switch)** – Controls physical access to the network based on the authentication status of the client. The switch acts as an intermediary (proxy) between the supplicants and the authentication server. It verifies information from the client and relays a response to the client. The switch uses a RADIUS software agent, which is responsible for encapsulating and de-encapsulating the EAP frames and interacting with the authentication server.
- **Authentication server** – Performs the actual authentication of the client. The authentication server validates the identity of the client and notifies the switch. Because the switch acts as the proxy, the authentication service is transparent to the client. The RADIUS security system with EAP extensions is the only supported authentication server.

Figure 3.1: 802.1X roles



When configured for 802.1X port-based authentication, the port starts in the *unauthorized state*. While in this state, the port disallows all ingress and egress traffic except for 802.1X protocol packets. When a client is successfully authenticated, the port transitions to the *authorized state*, allowing all traffic for the client to flow normally.

When a client logs out, or the supplicant does not support 802.1X, or the link state of the switch port changes from up to down, the switch port transitions to the unauthorized state. If a switch that is not running the 802.1X protocol, the client begins sending frames as if the port is in the authorized state.

3.3.2 Configuration

The following commands show a scenario where a PC is attached to F0/1 on the switch and the device is getting authenticated via 802.1X with a RADIUS server. Configuring 802.1X requires a few basic steps:

Listing 21: 802.1X configuration

```
aaa new-models

radius server Server-R
  address ipv4 192.168.1.101 auth-port 1812 acct-port 1813
  single-connection
  key RADIUS-Pa55w0rd
  exit

aaa authentication dot1x default group radius
dot1x system-auth-control

interface f0/1
  sw mode access
  authentication port-control auto
  dot1x pae authenticator
  exit
```

1. Enable AAA
2. Configure a RADIUS server
3. Create an 802.1X port-based authentication method list using the `aaa authentication dot1x` command.

4. Globally enable 802.1X port-based authentication using the `dot1x system-auth-control` command.
5. Enable port-based authentication on the interface using the `authentication port-control auto` command.
6. Enable 802.1X authentication on the interface using the `dot1x pae` command. The `authenticator` options sets the Port Access Entity (PAE) type so the interface acts only as an authenticator and will not respond to any messages meant for a supplicant.

The `authentication port-control` command has three options for port state:

- `auto` – Enable 802.1X authentication
- `force-authorized` – Disable 802.1X authentication. This option causes the port to remain authorized and transmit normal traffic. By default, a port is in the force-authorized state.
- `force-unauthorized` – This option causes the port to remain unauthorized and lock all authentication services.

Chapter 4

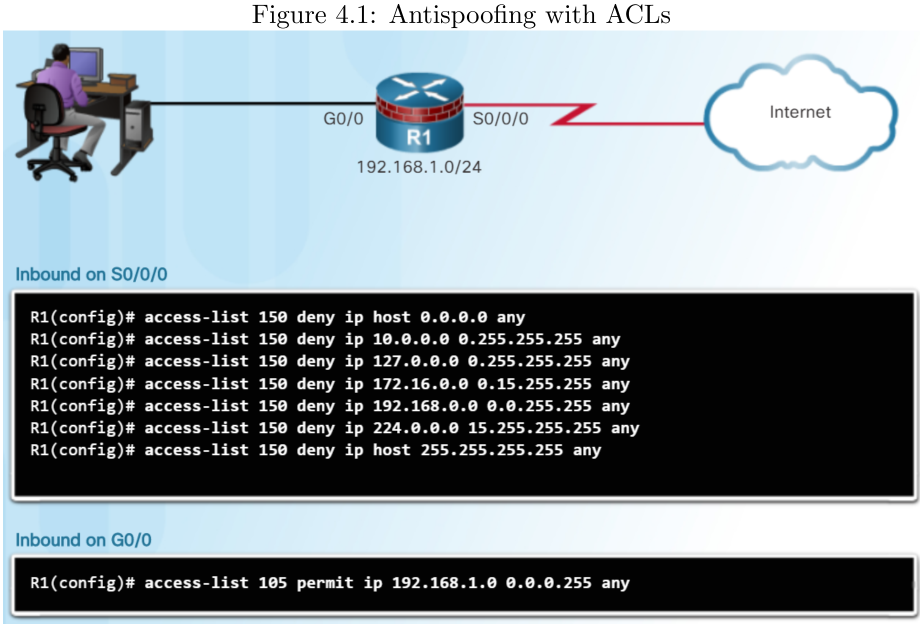
Firewall

4.1 ACL

ACLs can be used to mitigate IP address spoofing and denial of service (DoS) attacks (figure 4.1). Use ACL to block inbound packets from the following addresses:

- All zeros addresses
- Broadcast addresses
- Local host addresses (127.0.0.0/8)
- Reserved private addresses (prevent the spoofing of internal networks)
- IP multicast address range (224.0.0.0/4)

Figure 4.1: Antispoofing with ACLs



Hackers can use ICMP echo packets (pings) to discover network, generate DoS flood attacks, or alter host routing tables. Both ICMP echo and redirect messages should be blocked *inbound* by the router. Several ICMP messages are recommended for proper network operation and 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 are required for proper network operation and should be allowed to exit the network (outbound ACL):

- 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.

Traffic that originates within a router such as pings from a command prompt, remote access from a router to another device, or routing updates are not affected by outbound access lists. The traffic must flow through the router in order for the router to apply the ACEs.

If SNMP is necessary, exploitation of SNMP vulnerabilities can be mitigated by applying interface ACLs to filter SNMP packets from non-authorized systems. The most effective means of exploitation prevention is to disable the SNMP server on IOS devices for which it is not required.

Note! See also *CCNA notebook* for ACL configuration and IPv6 ACL.

4.2 Firewall

All firewalls share some common properties: resistant to attacks, the only transit point between networks because all traffic flows through the firewall, enforce the access control policy. There are two configuration models for Cisco IOS Firewall: Classic Firewall and Zone-based Policy Firewall (ZPF).

4.2.1 Packet filtering

Basic packet filtering firewalls can only filter based on Layer 3 and sometimes basic Layer 4 information.
Benefits: Simple implementation, Low impact on network performance, Initial degree of security at the network layer, Almost all the tasks of a high-end firewall at a much lower cost.

Limitations: Susceptible to IP spoofing, Not reliably filter fragmented packets, Complex ACLs (difficult to implement and maintain), *Stateless:* examine each packet individually rather than in the context of the state of a connection.

4.2.2 Statefull firewall

Stateful firewall monitors network traffic as it flows into and out of the organization and determines whether packets belong to an existing connection or are from an unauthorized source. Stateful filtering tracks each connection and confirms that they are valid. Stateful firewalls use a state table to keep track of the actual communication process.

Benefits: prevent spoofing and DoS attacks, provide more stringent control over security.

Limitations of stateful firewalls include the following:

- Stateful firewalls cannot prevent application layer attacks.
- Protocols such as UDP and ICMP are not stateful and do not generate information needed for a state table.
- An entire range of ports must sometimes be opened in order to support specific applications that open multiple ports.
- Stateful firewalls lack user authentication.

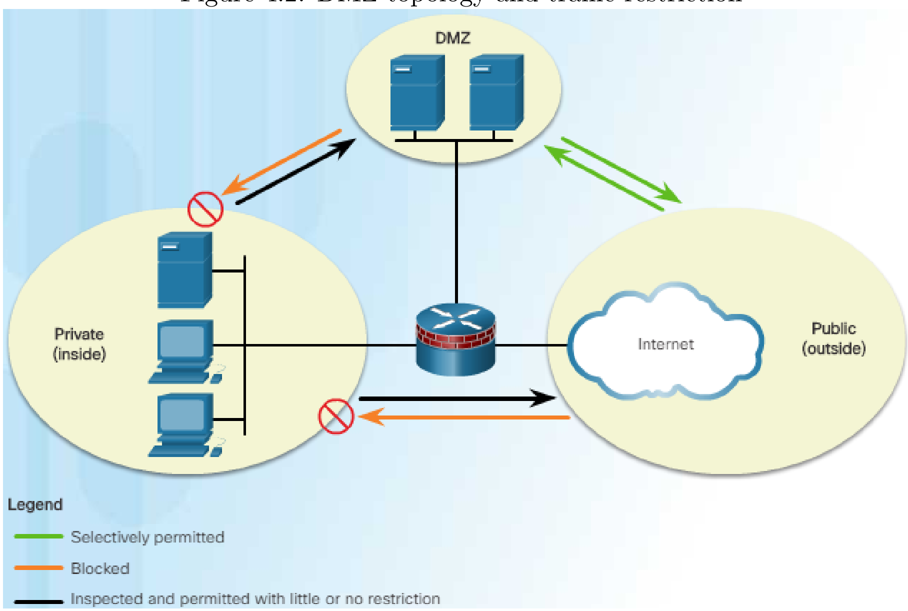
4.2.3 Next-Generation Firewall

Designed with advanced malware protection, the Cisco ASA with FirePOWER services is also called the **Cisco ASA Next-Generation Firewall** because it is an adaptive, threat-focused firewall. It is designed to provide defense across the entire attack continuum, which includes before, during, and after attacks.

4.2.4 DMZ

A demilitarized zone (DMZ) is 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, as shown in the figure 4.2.

Figure 4.2: DMZ topology and traffic restriction



- Private network → DMZ: Inspected
- DMZ → Private network: Blocked
- Public network ↔ DMZ: selectively permitted
- Private network → Public network: Inspected
- Public network → Private network: Blocked

4.2.5 Layered Defense

A layered defense uses different types of firewalls that are combined in layers. Security policies can be enforced between the layers and inside the layers. A traffic from the untrusted network has to go through the following layers and policies:

1. Edge router (packet filtering)
2. Bastion host (hardened computer located in the DMZ[1]) or Screened firewall
3. Interior screening router

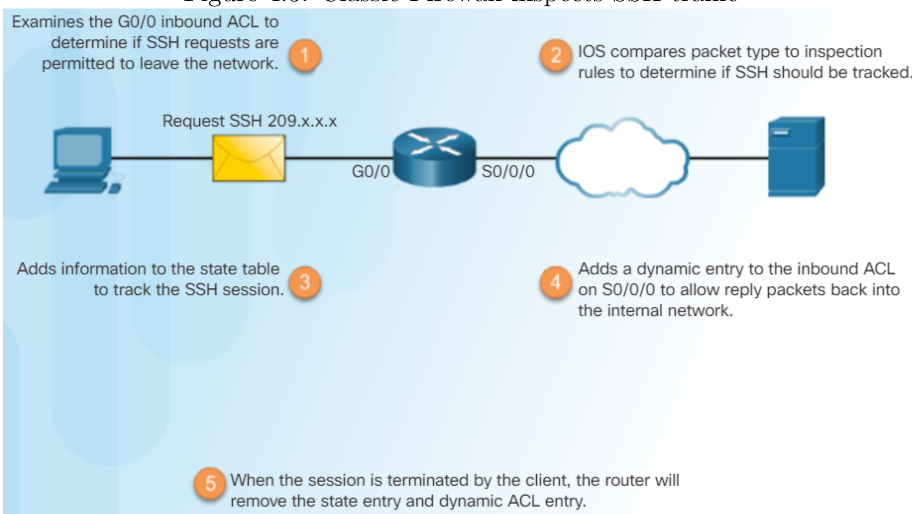
[1]This type of DMZ setup is called a *screened subnet configuration*.

4.2.6 Classic firewall

Classic Firewall (CBAC) is a *stateful* firewall that provides four main functions: Filtering, Inspection, Intrusion detection, and Generation of audits and alerts. It can only detects and protects against external attacks.

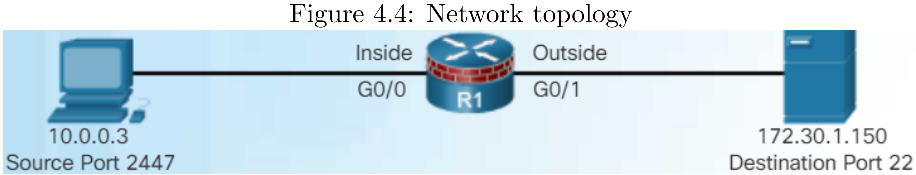
Classic Firewall creates *temporary* openings in the ACL to allow returning traffic. These entries are created as inspected traffic leaves the network and are removed when the connection terminates or the idle timeout period for the connection is reached. In addition to extended ACLs, Application layer protocol session information is used by a classic firewall to filter traffic. Figure 4.3 shows how Classic Firewall inspects SSH traffic.

Figure 4.3: Classic Firewall inspects SSH traffic



Take the topology in figure 4.4 as an example for configuration. Suppose that the administrator wants to allow SSH sessions between the 10.0.0.0 and 172.30.0.0 networks. However, only hosts from the 10.0.0.0 network are allowed to initiate SSH sessions. All other access is denied.

Figure 4.4: Network topology



Listing 22: Classic Firewall configuration

```
ip access-list extended INSIDE
  permit tcp 10.0.0.0 0.0.0.255 any eq 22
ip access-list extended OUTSIDE
  deny ip any any

ip inspect name FWRULE ssh

interface g0/0
  ip access-group INSIDE in
  ip inspect FWRULE in
interface g0/1
  ip access-group OUTSIDE in
```

There are four steps to configure this policy using a Classic Firewall:

1. **Define the internal and external interfaces**: G0/0 is the inside interface and G0/1 is the outside interface.
2. **Configure ACLs for each interface**: The INSIDE ACL allows only SSH traffic from the 10.0.0.0 network; the OUTSIDE ACL will deny inbound traffic from the 172.30.0.0 network.
3. **Define inspection rules**: The inspection rule FWRULE specifies that traffic will be inspected for SSH connections. This inspection rule has no effect until it is applied to an interface.
4. **Apply an inspection rule to an interface**: When the FWRULE is applied to inbound traffic on the G0/0 interface, the Classic Firewall configuration will dynamically add an entry to allow inbound SSH traffic from the 172.30.0.0 network. From now on, the FWRULE inspects SSH traffic between 10.0.0.0 and 172.30.0.0 network.
5. **Verification**: Use `show ip inspect sessions` command to verify inspect sessions.

4.2.7 Zone-based Policy Firewall (ZPF)

The Classic Firewall applies firewall policy to interfaces. Zone-Based Policy Firewall uses zones to apply firewall policy. ZPFs use the concept of zones to provide additional flexibility. A zone is a group of one or more interfaces that have similar functions or features. By default, the traffic between interfaces in the same zone is not subject to any policy and passes freely. However, all zone-to-zone traffic is blocked. In order to permit traffic between zones, a policy allowing or inspecting traffic must be configured.

There are several **benefits** of a ZPF:

- 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 can create traffic policies based on events and affect any given traffic with only one policy, instead of needing multiple ACLs and inspection actions.

There are three possible **actions** with Cisco IOS Zone-Based Policy Firewall:

- The **inspect** action configures Cisco IOS stateful packet inspection
- The **drop** action is similar to a deny ACE
- The **pass** action is similar to a permit ACE but does not track the state of connections or sessions.

ZPF Rules for **Transit Traffic** between two interfaces depends on the zone that those interfaces belongs to:

- Neither intefaces is a zone member: Pass
- Both interfaces are members of the same zone: Pass
- Interfaces belong to different zones: Action defined by policy
- Only one interface is a zone member: Drop

The **self zone** is a special zone which is the router itself and includes all the router interface IP addresses. By default, if the router (self zone) 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.
There are four steps to configure a ZPF zone (Take the topology in figure 4.5 as an example):

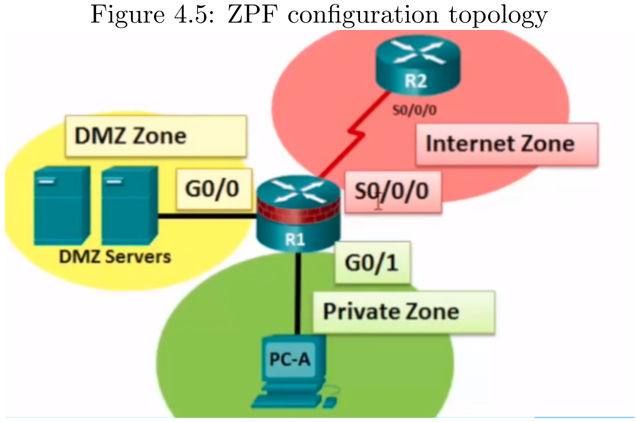
1. **Create the zones and Assign zones to appropriate interfaces:** Associating a zone to an interface will immediately apply the service-policy that has been associated with the zone. If no service-policy is yet configured for the zone, all transit traffic will be dropped. Use the `zone-member security` command to assign a zone to an interface. In the example, g0/1 is assigned the PRIVATE zone, and s0/0/0 is assigned the INTERNET zone, and g0/0 is assigned to DMZ zone.

2. **Identify traffic with class-map:** A class is a way of identifying a set of packets based on its contents using `match` conditions. Packets must meet one of the match criteria `match-any` or all of the match criteria `match-all` to be considered a member of the class. Table 4.1 shows the syntax for the `class-map` and its sub-commands.

3. **Define an action with policy-map:** Assign class-maps (PRIVATE-ACL-CLASS and PRIVATE-INTERNET-CLASS) to a policy-map and define what action (Inspect, Drop, or Pass) should be taken for traffic that is a member of a class.

4. **Identify a zone-pair and match it to a policy-map:** The example commands below create a zone pair PRIVATE-2-INTERNET between PRIVATE and INTERNET, and associate that zone pair to a policy-map PRIV-TO-PUB-POLICY.

Figure 4.5: ZPF configuration topology



Listing 23: ZPF configuration

```
#STEP 1
zone security PRIVATE
zone security INTERNET
zone security DMZ
int g0/1
  zone-member security PRIVATE
int s0/0/0
  zone-member security INTERNET
int g0/0
  zone-member security DMZ
exit

#STEP 2
class-map type inspect match-all PRIVATE-ACL-CLASS
  match access-group 100
class-map type inspect match-any PRIVATE-INTERNET-CLASS
  match protocol http
  match protocol https
  match protocol dns
exit

#STEP 3
policy-map type inspect PRIV-TO-PUB-POLICY
  class type inspect PRIVATE-ACL-CLASS
  inspect
  class type inspect PRIVATE-INTERNET-CLASS
  inspect
  class class-default
exit

#STEP 4
zone-pair security PRIVATE-2-INTERNET source PRIVATE destination INTERNET
  service-policy type inspect  PRIV-TO-PUB-POLICY
end
```

Table 4.1: The syntax of class-map command

`class-map type inspect [match-any | match-all] <class-name>`	
Parameter	**Description**
`match-any`	Packets must meet one of the criteria to be considered a member of the class.
`match-all`	Packets must meet all of the criteria to be considered a member of the class.
`match protocol <protocol-name>`	Configure criteria based on specified protocol.
`match access-group <acl-name>`	Configure criteria based on specified ACL.
`match class-map <class-name>`	Use another class-map as criteria.

- `inspect` – This action offers state-based traffic control. It tracks UDP or TCP connections and permit the return traffic.

- `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 to the end of every policy-map.
- `pass` – This action allows *one-direction* traffic between two zones, and does not track the state of connections. A corresponding policy must be applied to allow return traffic to pass in the opposite direction. This action is ideal for secure protocols, such as IPsec.

The fourth step is to identify a zone pair (

Listing 24: ZPF Verification

```
show run | begin class-map
show class-map type inspect
show zone security
show zone-pair security
show policy-map type inspect
show policy-map type inspect zone-pair sessions
```

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.

ZPF Configuration Considerations

- The router never filters the traffic between interfaces in the same zone.
- An interface cannot belong to multiple zones. 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.
- Communication between zones are, by default, dropped. Unless there exits a 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.

Chapter 5

Intrusion Prevention System (IPS)

5.1 Introduction

5.1.1 IDS and IPS

Firewalls can only do so much and cannot protect against malware and zero-day attacks. A zero-day attack is a computer attack that tries to exploit software vulnerabilities that are unknown or undisclosed by the software vendor.

Intrusion Detection Systems (IDSs) were implemented to passively monitor the traffic on a network. IDS-enabled device copies the traffic stream and analyzes the copied traffic rather than the actual forwarded packets. **Working offline**, it compares the captured traffic stream with known malicious signatures. Working offline means several things:

- IDS works passively
- IDS device is physically positioned in the network so that traffic must be mirrored in order to reach it
- Network traffic does not pass through the IDS unless it is mirrored

IDS advantage: No impact on the network (delay, jitter) even if there is a sensor failure or overload. **IDS disadvantage:** cannot stop trigger packets, cannot correct tuning required for response action.

Intrusion Prevention System (IPS) was upon IDS technology. However, an IPS device is implemented in **inline mode**. This means that all ingress and egress traffic must flow through it for processing. An IPS does not allow packets to enter the trusted side of the network without first being analyzed. It can detect and immediately address a network problem.

IPS advantage: stop trigger packets, utilize stream normalization[1]. **IPS disadvantage:** some impact on network (delay, jitter), IPS overloading or improper configuration negatively affect the network .

The biggest difference between IDS and IPS is that an IPS responds immediately and does not allow any malicious traffic to pass, whereas no action is taken on malicious packets by the IDS.

IDS and IPS technologies share several characteristics:

- Deployed as sensors
- Use signatures[2] to detect patterns in network traffic
- Can detect atomic signature patterns (single-packet) or composite signature patterns (multi-packet)

[1] a technique used to reconstruct the data stream when the attack occurs over multiple data segments.
[2] A signature is a set of rules that an IDS or IPS uses to detect malicious activity.

5.1.2 IPS technologies

There are two primary kinds of IPSs available: host-based and network-based.

Network-based IPS devices are implemented as inline mode to actively monitor the traffic on networks. They can take immediate actions when security criteria match. One limitation of them is that they cannot monitor/inspect encrypted packets.

Host-based IPS (HIPS) is software installed on a single host to monitor and analyze suspicious activity. Two disadvantages of deploying HIPS are (1) that it cannot create a complete view of the network and (2) every host operating system within the organization must be supported. However, an advantage of using HIPS is that it can monitor and protect the operating system as well as critical system processes on each network host.

5.2 IPS Signatures

5.2.1 Characteristics

Signatures have three distinctive attributes: Type, Trigger (alarm), Action. Signature types are generally categorized as atomic or composite.

An **atomic signature** consists of a *single* packet, activity, or event that is examined to determine if it matches a configured signature. Because these signatures can be matched on a single event, they do not require an intrusion system to maintain state[3] information. Detecting atomic signatures consumes minimal resources. For example, a LAND attack has an atomic signature because it sends a spoofed TCP SYN packet, therefore, one packet is enough to identify this type of attack.

A **composite signature** is a *stateful* signature which identifies a sequence of operations distributed across multiple hosts over an arbitrary period of time. Because this type of attack involves multiple packets, an IPS sensor must maintain the state information. However, an IPS sensor cannot maintain the state information indefinitely. The length of time that the signatures must maintain state is known as the **event horizon**.

The two main alert generation mechanisms for IDS/IPS devices are atomic and summary alerts. **Atomic alerts** are generated every time a signature triggers. With a **summary alert**, a single atomic alert is generated for the first detection of an attack. Then the duplicate alarms are counted, but not sent, for a specific time period. When the specified time period is reached, an alert is sent that indicates the number of alarms that occurred during the time interval.

All signatures are contained in a signature file and uploaded to an IPS on a regular basis.

Cisco IOS software relies on **signature micro-engines (SMEs)** to categorize common signatures in groups. Cisco IOS software can then scan for multiple signatures based on group characteristics, instead of one at a time. When IDS or IPS is enabled, an SME is loaded or built on the router. When an SME is built, the router might need to compile the regular expression[4] found in a signature.

IPS process: Atomic and composite packets are scanned by the SMEs to recognize the protocols contained in the packets. Then, each SME extracts values from the packet and passes portions of the packet to the regular expression engine. The regular expression engine can search for multiple patterns at the same time.

5.2.2 Alarms

The heart of any IPS signature is the signature alarm (signature trigger). There are four types of signature triggers:

- **Pattern-based detection** (signature-based detection) is the simplest triggering mechanism. It compares the network traffic to a database of known attacks, and triggers an alarm or prevents communication if a match

[3] State refers to situations in which multiple packets of information are required, but the packets of information are not necessarily received at the same time.

[4] A regular expression is a systematic way to specify a search for a pattern in a series of bytes.

is found. The mechanism is only suitable for the suspect packets that are associated with *services* or *ports*. However, it cannot deal with unknown protocols and attacks.

- **Anomaly-based detection** (profile-based detection) defines a profile of what is considered normal for the network. This normal profile can be learned by monitoring activity on the network, or be based on a defined specification, such as an RFC. After defining normal activity, the signature triggers an action if excessive activity occurs beyond a specified threshold that is not included in the normal profile. **Advantage:** new and previously unpublished attacks can be detected. **Disadvantage:** Attack activity may be defined as normal traffic; Difficult to correlate alert back to a specific attack.

- **Policy-based detection** (behavior-based detection) is similar to pattern-based detection. However, instead of trying to define specific patterns, the administrator defines behaviors that are suspicious based on *historical* analysis. The use of behaviors enables a single signature to cover an entire class of activities without having to specify each individual situation.

- **Honey pot-based detection** uses a dummy server to attract attacks. By staging different types of vulnerabilities in the honey pot server, administrators can analyze incoming types of attacks and malicious traffic patterns. Antivirus and other security vendors tend to use them for research.

- **Protocol decodes:** This mechanism breaks down a packet into the fields of a protocol, and then search for specific patterns in a specific protocol field. Advantage: enable a more granular inspection of traffic and reduces the number of false positives.

Table 5.1: Alarm types

Alarm type	**Traffic**	**Alarm**	**Outcome**
False Positive	normal	•	tune alarm
False Negative	attack		tune alarm
True Positive	attack	•	ideal setting
True Negative	normal		ideal setting

5.2.3 Actions

Alerts: there are two types of alert, which are atomic and summary alerts. **Atomic alerts** are generated every time a signature triggers. A **summary alert** is a single alert that indicates multiple occurrences of the same signature from the same source address or port.

Logging: this activity may start on packets that contain attacker's address (logging attacker packets), or attacker-victim address pair (logging pair packet), or victim's address (logging victim packet).

Deny: IPS terminates the current and future packets from a particular attacker address for a period of time. If attacker A is currently denied, but issues another attack, then the timer for attacker A is reset and this attacker remain denied until the timer expires. IPS also denies TCP connection.

Blocking is the action that updates ACL on *one* of the infrastructure devices. After a configured period of time, the IPS device removes the ACL. This action allows a single IPS device can stop traffic at multiple locations throughout the network, regardless of the location of the IPS device.

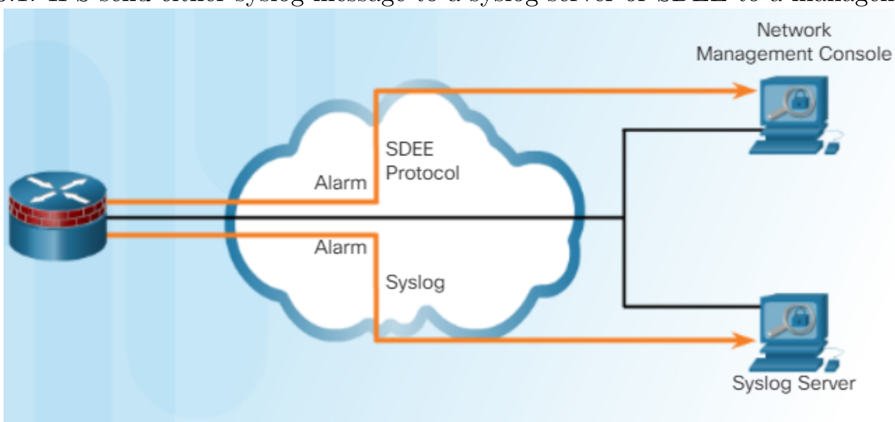
5.2.4 Logging and management task

SDEE: When an attack signature is detected, the Cisco IOS IPS feature can send either a syslog message or an alarm in SDEE (Secure Device Event Exchange) format, as shown in the figure 5.1. SDEE uses HTTP and XML to provide a standardized approach. Administrators must also enable HTTP or HTTPS on the router when enabling

SDEE. The use of HTTPS ensures that data is secured as it traverses the network.

When sending IPS notification with SDEE format, the buffer on the router stores up to 200 events by default. If a smaller buffer is requested, all stored events are lost. If a larger buffer is requested, all stored events are saved. The default buffer can be altered with the `ip sdee events <number>` command. All stored events are lost when Cisco SDEE notification is disabled. A new buffer is allocated when the notifications are re-enabled.

Figure 5.1: IPS send either syslog message to a syslog server or SDEE to a management app

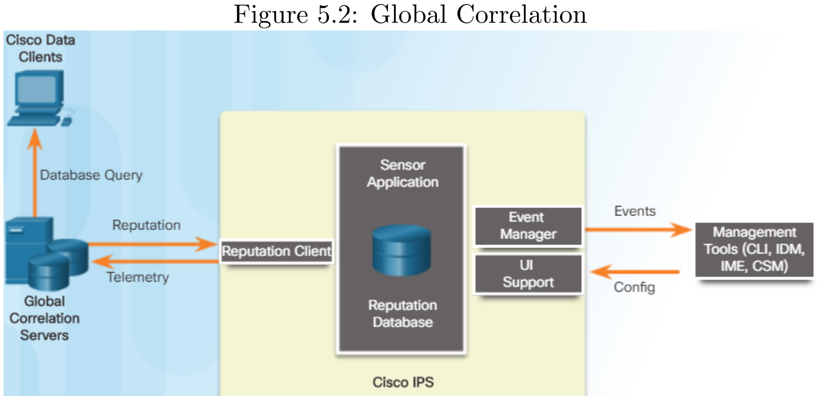


There are three GUI-based IPS device managers available: Cisco Configuration Professional, Cisco IPS Manager Express (IME), and Cisco Security Manager.

5.2.5 Global correlation

When participating in Global correlation, IPS receives regular threat updates from a database called the Cisco SensorBase Network. This database provides information to the IPS sensor about IP addresses with a *reputation*, as shown in the figure 5.2. The sensor uses this information to determine which actions to perform when harmful traffic is received from a host with a known reputation. Since the global correlation database changes rapidly, the sensor must periodically download global correlation updates from the global correlation servers. It is possible to view reputation scores in events and see the reputation score of attackers.

Figure 5.2: Global Correlation



The SensorBase Network is part of **Security Intelligence Operation (SIO)**, a back-end security ecosystem. SIO detects, researches and analyzes threats, and provides real-time security updates. SIO consists of three elements:

- *Threat intelligence* from the Cisco SensorBase Network
- *Threat Operations Center*, which is the combination of automated and human processing and analysis

- *Automated and best practices content* that is pushed to network elements in the form of dynamic updates

5.3 Implementation

5.3.1 Configuration

Step 1. Download the IOS IPS files

Prior to configuring IPS, it is necessary to download the IOS IPS signature package files, and a public crypto key from cisco.com. Only registered customers can download the package files and key.

- `IOS-Sxxx-CLI.pkg` – The latest signature package.
- `realm-cisco.pub.key.txt` – The public crypto key used by IOS IPS.

Step 2. Create an IOS IPS configuration directory in Flash

This step creates a directory in flash to store the signature files and configurations using `mkdir <dir-name>` privileged EXEC command. Other useful commands include `rename <current-name> <new-name>` which allows the name of the directory to be changed.

Step 3. Configure an IOS IPS Crypto Key

The third step configures the crypto key used by IOS IPS. This key is located in the `realm-cisco.pub.key.txt` file that was obtained in Step 1. The crypto key verifies the digital signature for the master signature file `sigdef-default.xml`. The content of the file is signed by a Cisco private key to guarantee its authenticity and integrity.

Open the text file to configure the IOS IPS crypto key. Next, copy the contents of the file, and paste the contents to the router at the global configuration prompt. The text file issues the various commands to generate the RSA key.

If the key is configured incorrectly, an error message is generated as follow

```
%IPS-3-INVALID_DIGITAL_SIGNATURE: Invalid Digital Signature found (key not found)
```

In such case, the key must be removed and then reconfigured. Use the `no crypto key pubkey-chain rsa` and the `no named-key realm-cisco.pub signature` commands. Then repeat the procedure in Step 3 to reconfigure the key. Finally, enter the `show run` command to confirm that the crypto key is configured.

Step 4. Enable IOS IPS

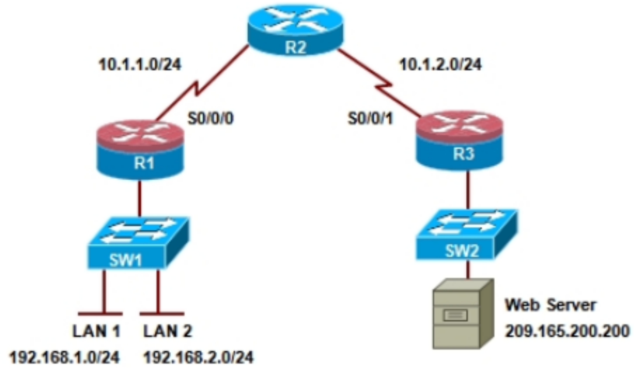
The fourth step is to configure IOS IPS, which is a process that consists of four sub-steps.

1. **Identify the IPS rule name and specify the location:** Create a rule name associated with an optional extended or standard ACL. All traffic that is permitted by the ACL is subject to inspection by the IPS. Next, configure the IPS signature storage location as directory `flash:IPS` (created in step 2).
2. **Enable SDEE and logging event notification:** To use SDEE, the HTTP or HTTPS server must first be enabled with the `ip http server` or `ip https server` command. Enable SDEE event notification by using the `ip ips notify sdee` command. The buffer size can be altered with the `ip sdee events` command. The `clear ip ips sdee` command clears SDEE events or subscriptions.
3. **Enable syslog:** Logging notification is enabled by default. If the logging console is enabled, IPS log messages are displayed on the console. Use the `ip ips notify log` command to enable logging.
4. **Configure the signature category:** All signatures are grouped into categories. The three most common categories are `all`, `basic`, and `advanced`. The signatures that IPS uses to scan traffic can be retired or unretired. **Retiring** a signature means that IPS does not compile that signature into memory for scanning. **Un-retiring** a signature instructs IPS to compile the signature into memory and use it to scan traffic. When IOS IPS is first configured, all signatures in the all category should be retired. Then, selected signatures should be unretired in a less memory-intensive category.

5. **Apply the IPS rule to interfaces**

Below is an example of IPS configuration:

Figure 5.3: Topology for IPS example




```
R1(config)# ip ips name myips
R1(config)# ip ips name myips list 101
R1(config)# access-list 101 permit tcp 192.168.0.0 0.0.255.255 any eq http established
R1(config)# interface serial0/0/0
R1(config-if)# ip address 10.1.1.1 255.255.255.0
R1(config-if)# ip ips myips in
R1(config-if)# no shut
```

In figure 5.3, the IPS inspection is configured on the S0/0/0 interface with inbound direction, but the ACL source address range is 192.168.0.0/16 and the traffic type is http established, there will be no traffic to match these criteria (note, there is no web server on LAN 1 or LAN 2). Hence no traffic inspection will take place.

Note! Do not unretire the `all` category. The `all` signature category contains all signatures in a signature release. The IPS cannot compile and use all the signatures at one time because it will run out of memory.

Note! The order in which the signature categories are configured on the router is also important. IOS IPS processes the category commands in the order listed in the configuration. Some signatures belong to multiple categories. If multiple categories are configured and a signature belongs to more than one of them, IOS IPS uses the signature's properties in the last configured category, for example, retired, unretired, or actions.

Step 5. Loading IOS IPS Signature Package to the Router

The last step is for the administrator to upload the signature package to the router. The most common methods are FTP or TFTP.

Listing 25: Enable IPS

```
ip ips name IOSIPS list ALLOW-HTTP
ip ips config location flash:IPS

ip http server
ip https server

ip ips notify sdee
ip sdee events 500

ip ips notify log
logging 192.168.10.100
logging on

ip ips signature-category
  category all
  retired true
exit
  category ios_ips basic
  retired false
end

conf t

interface g0/0
  ip ips IOSIPS in
interface g0/1
  ip ips IOSIPS in
  ip ips IOSIPS out
end

copy tftp://192.168.1.3/IOS-S416-CLI.pkg idconf
# copy ftp://ftp_user:password@Server_IP_addr/signature_packg  idconf

show ip ips signature count

clear ip ips sdee {events | subscription}
```

5.3.2 Modification

Listing 26: Retire a specific signature

```
ip ips signature-definition
  signature 6130 10
  status
    retired true
end
```

Listing 27: Change actions of a signature

```
ip ips signature-definition
  signature 6130 10
  engine
    event-action produce alert
    event-action deny-packet-inline
    event-action reset-tcp-connection
end
```

Table 5.2: Parameters of event-action command

`deny-attacker-inline`	Terminates the current and future packets from a particular attacker address for a period of time
`deny-connection-inline`	Terminates packets come on this TCP flow.
`deny-packet-inline`	Terminates the packet.
`produce-alert`	Writes event to Event Store as an alert.
`reset-tcp-connection`	Send TCP reset signal and terminate the TCP flow. Only works on TCP signatures that analyze a single connection. Not work for sweeps or floors.

Listing 28: Change actions of a signature category

```
ip ips signature-definition
  category ios_ips basic
    event-action produce alert
    event-action deny-packet-inline
    event-action reset-tcp-connection
end
```

The IOS command `ip ips signature-definition` is used to configure a specific signature, including retire/un-retire and event action. To configure a signature category, the command `ip ips signature-category` is used.

Use the `clear ip ips config` command to disable IPS, remove all IPS configuration entries, and release dynamic resources. The `clear ip ips stat` command resets statistics on packets analyzed, and alarms sent.

Listing 29: IPS verification

```
show running-config
show ip ips
show ip ips all
show ip ips configuration
show ip ips signatures
show ip ips statistics
```

Chapter 6

Securing LAN

6.1 Port security

CAM table overflow attacks (also called MAC address overflow attacks) take place by bombarding the switch with fake source MAC addresses until the switch MAC address table is full. If enough entries are entered into the CAM table, the table fills up to the point that no new entries can be accepted. When this occurs, the switch treats the frame as an unknown unicast and begins to flood all incoming traffic to all ports. As a result, the attacker can capture all of the frames sent from one host to another.

The simplest and most effective method to prevent CAM table overflow attacks is to enable **port security**. When a port configured with port security receives a frame, the source MAC address of the frame is compared to the list of secure source addresses that were manually configured or autoconfigured (learned) on the port.

To enable port security, use the `sw port-security` interface configuration command on an access port. Notice that, the port must be configured as an access port before port security can be enabled. This is because port security can only be configured on access ports and, by default, Layer 2 switch ports are set to dynamic auto (trunking on). Therefore, the port must be initially configured with the `sw mode access` interface configuration command.

To set the maximum number of MAC addresses allowed on a port use the `sw port-security max <value>`.

A security **violation** is created when a station with a MAC address that is not in the address table attempts to access the interface when the table is full. Another example of a situation that creates a security violation is when an address is being used on two secure interfaces in the same VLAN. If a MAC address of a device attached to the port differs from the list of secure addresses, then a port violation occurs, and the port enters the error-disabled state.

To set the port security violation mode, use the `sw port-security violation protect | restrict | shutdown | shutdown vl` interface configuration command. To re-enable an error-disable port, manually re-enable the disabled port by entering the `shutdown` and `no shutdown` interface configuration commands. Alternatively, the switch could be configured to automatically re-enable an error-disabled port using the `errdisable recovery cause psecure-violation` global configuration mode command.

Port security aging remove secure MAC addresses on a secure port without manually deleting the existing secure MAC addresses. Use the `sw port-security aging` command to enable or disable static aging for the secure port, or to set the aging time or type. Two types of aging are supported per port:

- Absolute – The secure addresses on the port are deleted after the specified aging time.
- Inactivity – The secure addresses on the port are deleted only if they are inactive for the specified aging time.

The **MAC address notification** feature sends SNMP traps to the network management station (NMS) whenever a new MAC address is added to, or an old address is deleted from the forwarding tables. MAC address notifications are generated only for dynamic and secure MAC addresses. Use the `mac address-table notification` global configuration command to enable the MAC address notification feature on a switch.

6.2 DTP, trunking and access mode

A **VLAN hopping attack** enables traffic from one VLAN to be seen by another VLAN without the aid of a router. A VLAN hopping attack can be launched in one of two ways:

- Spoofing DTP messages from the attacking host to cause the switch to enter trunking mode. From here, the attacker can send traffic tagged with the target VLAN, and the switch then delivers the packets to the destination.
- Introducing a rogue switch and enabling trunking. The attacker can then access all the VLANs on the victim switch from the rogue switch.

Double-tagging takes advantage of 802.1Q de-encapsulation, in which the attacker adds a hidden 802.1Q tag inside the frame. This tag allows the frame to go to another VLAN. For example, an attacker on VLAN 10 tags a frame for VLAN 10 and inserts an additional tag for VLAN 20. An important characteristic of the double-encapsulated VLAN hopping attack is that it works even if trunk ports are disabled, as a host typically sends a frame on a segment that is not a trunk link. The best way to prevent basic VLAN hopping attacks:

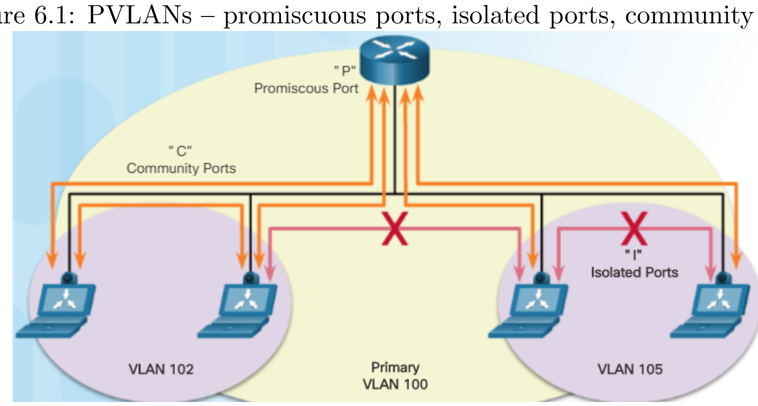
- Manually enable trunking and access ports
- Disable DTP
- Be sure that native VLAN is only used for trunk lines.

6.3 Priavte VLAN

Private VLANs (PVLAN) provide Layer 2 isolation between hosts within the same VLAN. There are three types of PVLAN ports (figure 6.1):

- A **promiscuous** port can talk to everyone. This is often the port connected to the router.
- An **isolated** port can only talk to promiscuous ports. If you want to isolate hosts within the same VLAN, configure them as isolated port.
- **Community** ports can talk to ports in the same community and promiscuous ports.

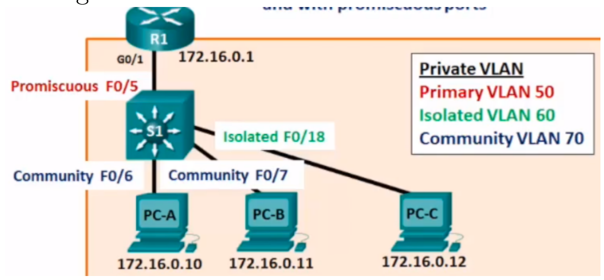
Figure 6.1: PVLANs – promiscuous ports, isolated ports, community ports



Full PVLAN support is available on 3560 Multiplayer switches or higher. The 2960 Switches only support a part of PVLAN (PVLAN Edge).

In creating full PVLAN, you need to create three special VLANs: primary VLAN (goes with the promiscuous ports), isolated VLAN, and community VLAN (can be different communities based on the VLAN number). Look at the figure 6.2 for sample configuration. In order for PVLAN to work, you need to set VTP mode to transparent.

Figure 6.2: Configuration of Private VLANS on a 3560 Multilayer switch



Listing 30: PVLAN

```
vtp mode transparent

vlan 60
private-vlan isolated
vlan 70
private-vlan community
vlan 50
private-vlan primary
private-vlan association 60,70
exit

int f0/5
sw mode private-vlan promiscuous
sw private-vlan mapping 50 60,70
int f0/6
sw mode private-vlan host
sw private-vlan host-association 50 70
int f0/7
sw mode private-vlan host
sw private-vlan host-association 50 70
int f0/18
sw mode private-vlan host
sw private-vlan host-association 50 60
exit
```

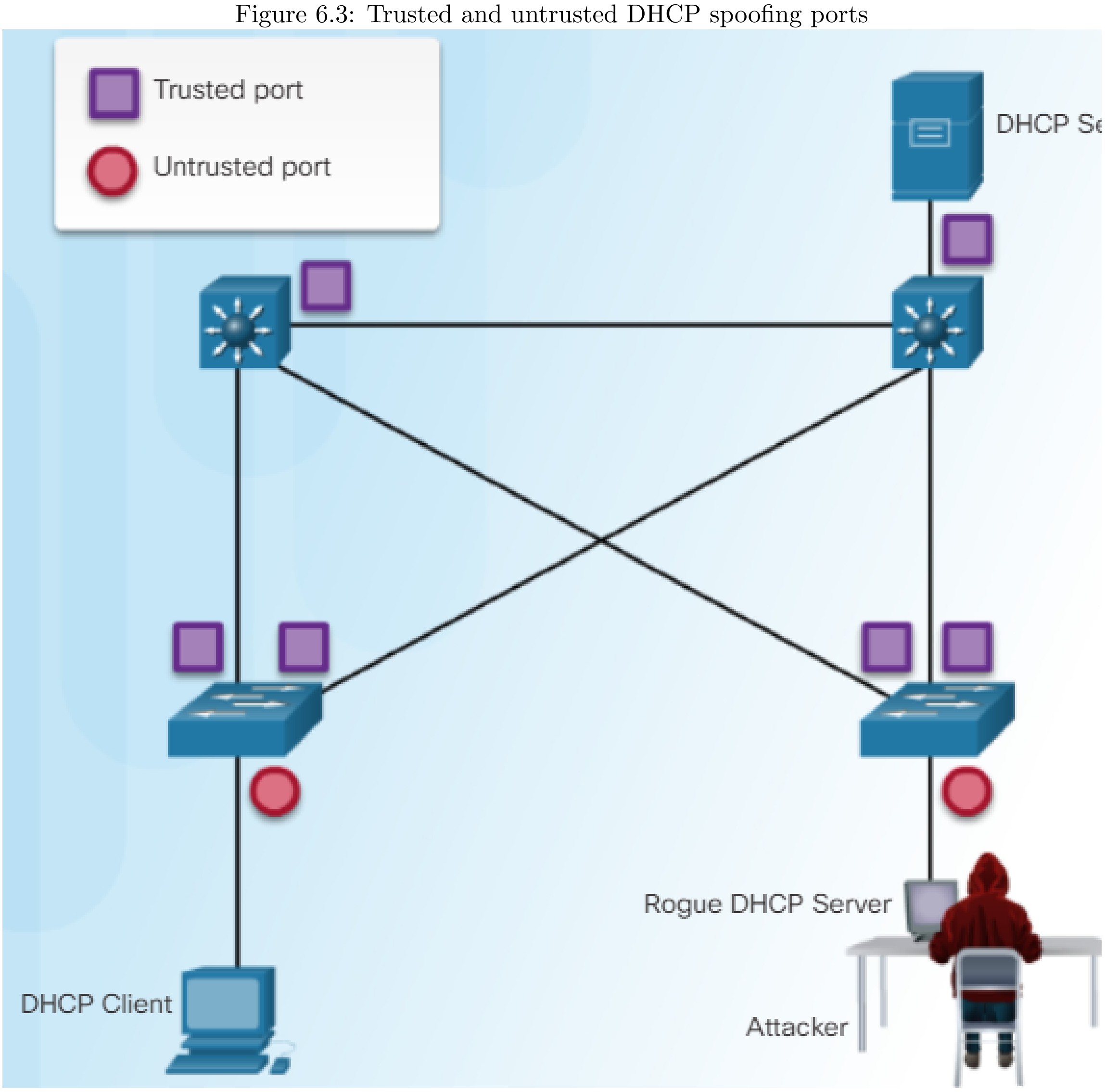
If you only have a 2960 series switch and you do not have a multilayer switch, you can use the `sw protected` interface configuration command to achieve a similar result. Ports configured with this command is called Protected ports. Hosts connected to Protected ports will not be able to communicate with each other, but can only talk with un-Protected ports.

6.4 DHCP snooping

DHCP starvation attack creates a DoS by leasing all available IP addresses. It is easy to mitigate DHCP starvation attacks using port security.

A **DHCP spoofing** attack occurs when a rogue DHCP server is connected to the network and provides false IP configuration parameters to legitimate clients. DHCP spoofing attacks can be mitigated using DHCP snooping on trusted ports. The general rule is that ports connected to hosts are untrusted, the other is trusted. Port connected to DHCP server must be trusted, otherwise DHCP service will not work.

Figure 6.3: Trusted and untrusted DHCP spoofing ports



Listing 31: DHCP snooping

```
ip dchp snooping

int f0/1
ip dchp snooping trust
int range f0/5-24
ip dchp snooping rate 6
exit

ip dchp snooping vlan 5,10,20
```

6.5 Dynamic ARP Inspection (DAI)

An attacker can send a gratuitous ARP message containing a spoofed MAC address to a switch (ARP spoofing). **Dynamic ARP Inspection (DAI)** will be configured to mitigate against ARP spoofing and ARP poisoning attacks.

Listing 32: Dynamic ARP Inspection (DAI) configuration

```
ip dhcp snooping
ip dhcp snooping vlan 10
ip arp inspection vlan 10

int f0/24
ip dhcp snooping trust
ip arp inspection trust
exit

ip arp inspection validate src-mac
ip arp inspection validate dest-mac
ip arp inspection validate ip
ip arp inspection validate src-mac dest-mac ip
```

DHCP snooping is enabled because DAI requires the DHCP snooping table to operate. Next, DHCP snooping and ARP inspection are enabled for the PCs on VLAN10. The uplink port to the router is trusted, and therefore, is configured as trusted for DHCP snooping and ARP inspection.

The `ip arp inspection validate` global configuration command is used to configure DAI to drop ARP packets when the `ip`, or `src-mac` (source MAC address), or `dest-mac` (destination MAC address) are invalid. Notice that entering multiple `ip arp inspection validate` commands overwrite the previous command. To include more than one validation method, enter them on the same command line as displayed in the output.

6.6 IP Source Guard (IPSG)

To protect against MAC and IP address spoofing, configure the IP Source Guard (IPSG) security feature. IPSG operates just like DAI, but it looks at every packet, not just the ARP packets. Like DAI, IPSG also requires that DHCP snooping be enabled.

Specifically, IPSG is deployed on untrusted Layer 2 access and trunk ports using the `ip verify source` interface configuration command. IPSG dynamically maintains per-port VLAN ACLs (PVACL) based on IP-to-MAC-to-switch-port bindings. For each untrusted port, there are two possible levels of IP traffic security filtering:

- IP addresses – only IP traffic with a source IP address that matches the IP source binding entry is permitted.
- IP and MAC address – Only IP traffic with source IP and MAC addresses that match the IP source binding entry are permitted.

6.7 Mitigating STP Attacks

6.7.1 PortFast

The spanning-tree PortFast feature causes an interface configured as a Layer 2 access port to transition from the blocking to the forwarding state immediately, bypassing the listening and learning states. PortFast can be used on Layer 2 access ports that connect to a single workstation or server. Because the purpose of PortFast is to minimize the time that access ports must wait for STP to converge, it should be used only on access ports.

PortFast can be configured globally on all non-trunking ports using the `spanning-tree portfast default` global configuration command. Alternatively, PortFast can be enabled on an interface using the `spanning-tree portfast` interface configuration command.

6.7.2 BPDU Guard

Even though PortFast is enabled, the interface will listen for BPDUs. The receipt of unexpected BPDUs might be accidental, or part of an unauthorized attempt to add a switch to the network. BPDU Guard protects the integrity of ports that are PortFast-enabled. If any BPDU is received on a BPDU Guard enabled port, that port is put into error-disabled state.

Use the `spanning-tree portfast bpduguard` default global configuration command to globally enable BPDU guard on all PortFast-enabled ports. If PortFast is not configured, then BPDU Guard is not activated. Alternatively, BPDU Guard can be enabled per interface using the `spanning-tree bpduguard enable` interface configuration command.

Note! Always enable BPDU Guard on all PortFast-enabled ports.

6.7.3 Root Guard

On a network, there are some switches that should never, under any circumstances, become the STP root bridge. Root Guard provides a way to enforce the placement of root bridges on the network by limiting which switch can become the root bridge.

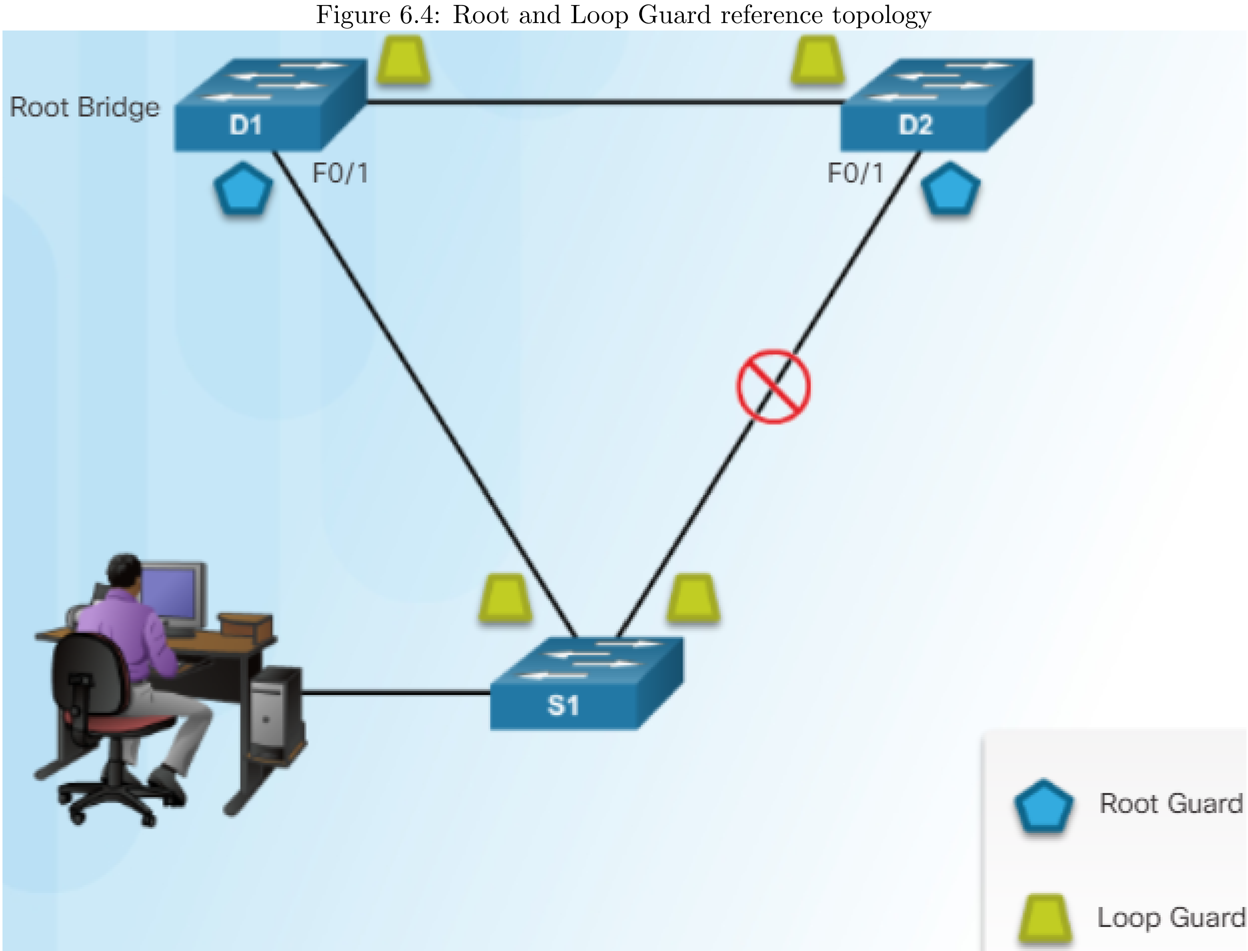
Root guard is deployed on ports that *toward* the unsecure switches (switches that should not be the root bridge). Look at figure 6.4, we don't want S1 to be root bridge, so that F0/1 on both S2 and S3, which are towards S1, should be configured with Root Guard.
If a root-guard-enabled port receives BPDUs that are superior to those that the current root bridge is sending, that port is moved to a *root-inconsistent state*. Recovery occurs as soon as the offending device ceases to send superior BPDUs.

Use the `spanning-tree guard root` interface configuration command to configure root guard on an interface. To view Root Guard ports that have received superior BPDUs and are in a root-inconsistent state, use the `show spanning-tree inconsistent ports` command.

6.7.4 Loop Guard

Traffic on bidirectional links flows in both directions. If for some reason one direction traffic flow fails, this creates a unidirectional link which can result in a Layer 2 loop. If BPDUs are not received on a non-designated Loop Guard-enabled port, the port transitions to a loop-inconsistent blocking state, instead of the listening / learning / forwarding state.

Figure 6.4: Root and Loop Guard reference topology



Loop Guard is enabled on all *non-Root guard* ports (figure 6.4) using the `spanning-tree guard loop` interface configuration command.

Chapter 7

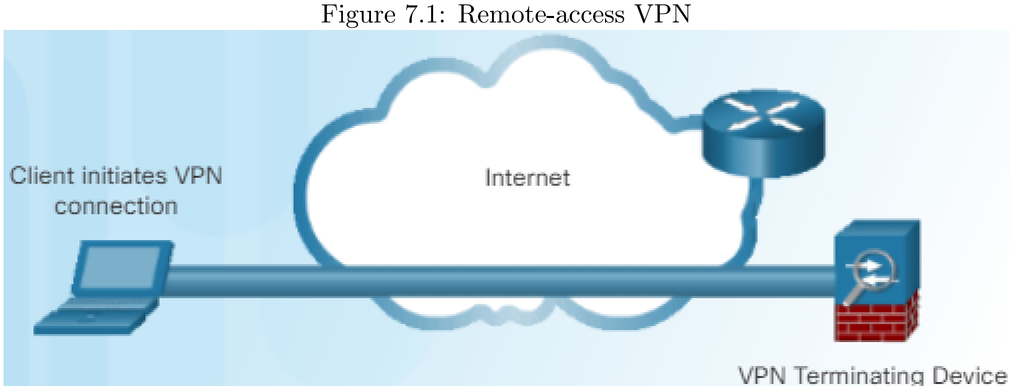
Virtual Private Networks (VPN) and IPsec

7.1 VPN introduction

A VPN is a private network that is created over a public network, usually the Internet. A VPN is virtual in that it carries information within a private network, but that information is actually transported over a public network. A VPN is private in that the traffic is encrypted to keep the data confidential while it is transported across the public network.

In the simplest sense, a VPN connects two endpoints, such as two remote offices, over a public network to form a logical connection. The logical connections can be made at either Layer 2 or Layer 3. This chapter focuses on Layer 3 VPN technology. Common examples of Layer 3 VPNs are GRE, Multiprotocol Label Switching (MPLS), and IPsec (This course focuses on IPsec VPNs).

Figure 7.1: Remote-access VPN



There are two basic types of VPNs: remote-access and site-to-site. A **remote-access VPN** is created when VPN information is not statically set up, but instead allows for dynamically changing connection information, which can be enabled and disabled when needed (Figure 7.1). A **site-to-site VPN** is created when devices on both sides of the VPN connection are aware of the VPN configuration in advance. The VPN remains static, and internal hosts have no knowledge that a VPN exists (Figure 7.2).

Hairpinning is a situation in which the VPN terminating device at the corporate network is the hub and the remote-access VPN clients are spokes (Figure 7.3). In **Split tunneling**, if traffic is destined for a corporate subnet, it is sent through the VPN tunnel; otherwise, it is sent as unencrypted traffic (untrusted) to the Internet.

Figure 7.2: Site-to-site VPN

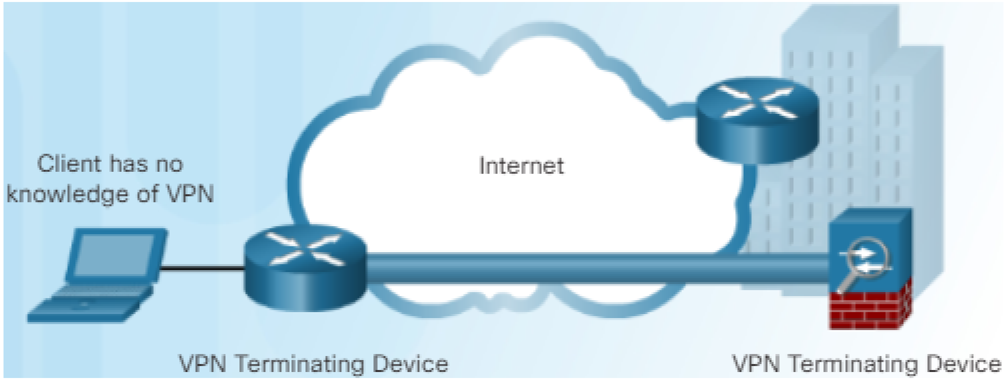


Figure 7.3: Hairspinning

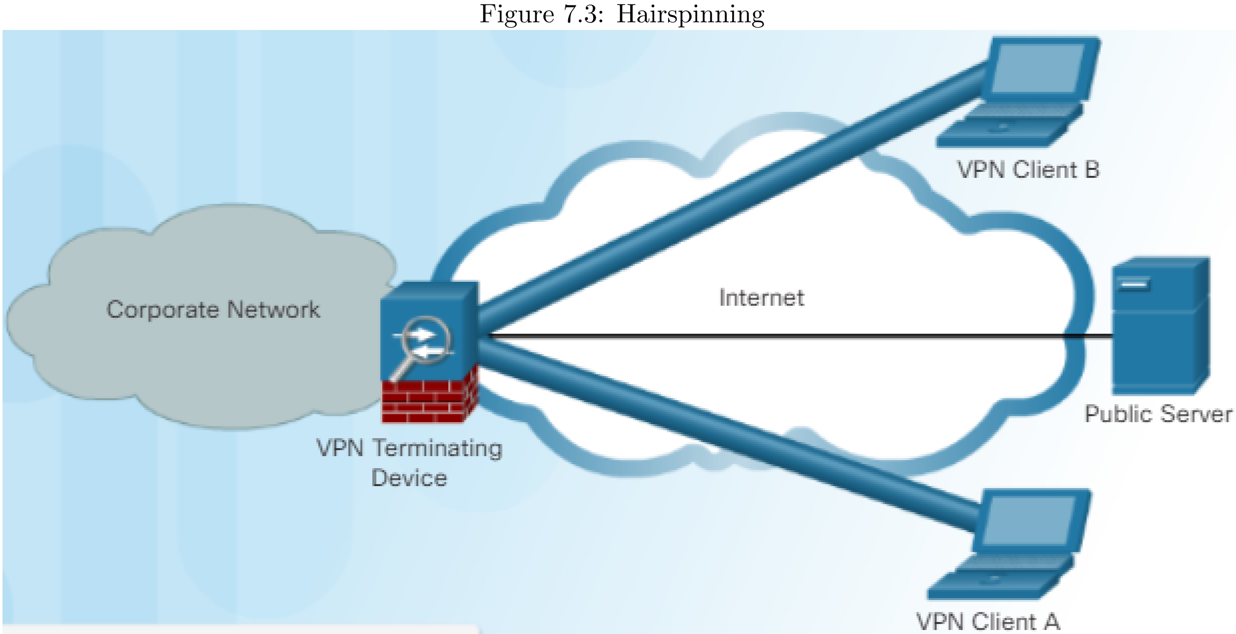
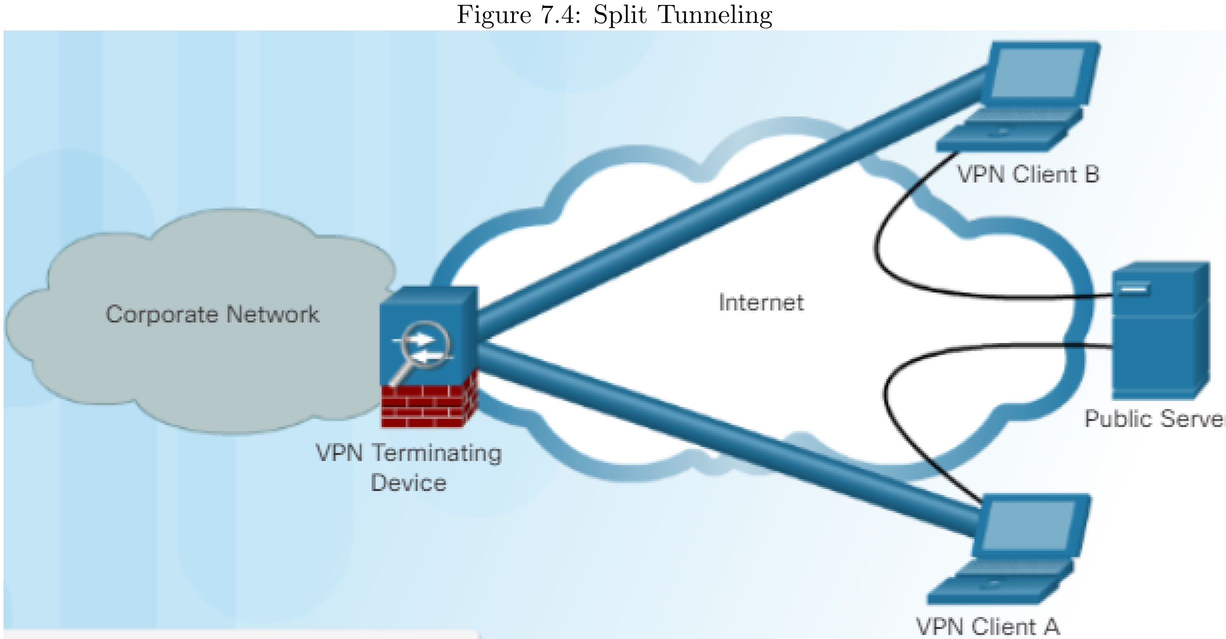


Figure 7.4: Split Tunneling



7.2 IPsec introduction

IPsec is an IETF standard that defines how a VPN can be secured across IP networks. IPsec is not bound to any specific rules for secure communications (Figure 7.5). This flexibility of the framework allows IPsec to easily integrate new security technologies without updating the existing IPsec standards. The level of security and reliability is increased from left to right, meaning that the right-most is the most secure and reliable.

Figure 7.5: IPsec framework

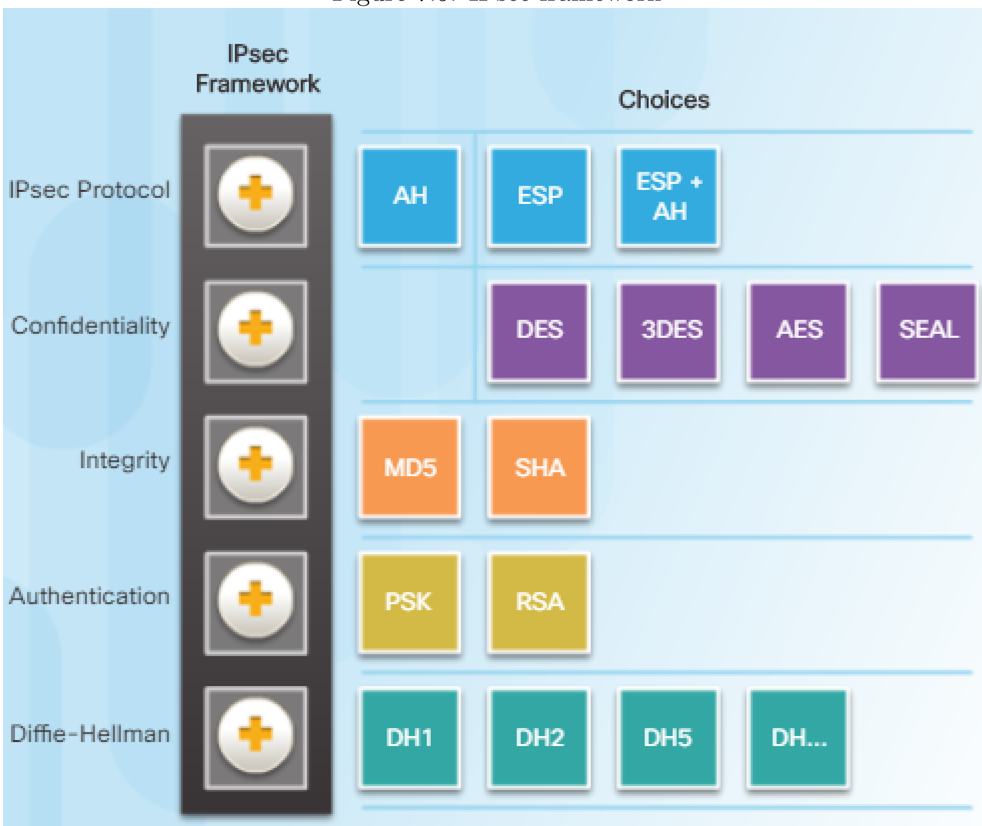


Figure 7.6 shows examples of security associations (SAs) for two different implementations. An SA is the basic building block of IPsec. When establishing a VPN link, the peers must share the same SA.

7.3 IPsec protocols

Having said that IPsec framework contains a variety of protocols. This section introduce Authentication Header (AH) protocol and Encapsulation Security Protocol (ESP). Refer to figure 7.5, you can see that AH and ESP are both IPsec protocols, the first layer of IPsec framework.

7.3.1 Authentication Header (AH) protocol

AH achieves **authenticity** by applying a **keyed one-way** hash function to the packet to create a hash or message digest. AH supports MD5 and SHA algorithms. AH may not work if the environment uses NAT. The AH process occurs in this order:

1. The IP header and data payload are hashed using the shared secret key.
2. The hash builds a new AH header, which is inserted into the original packet (Figure 2).
3. The new packet is transmitted to the IPsec peer router.

Figure 7.6: IPsec implementations

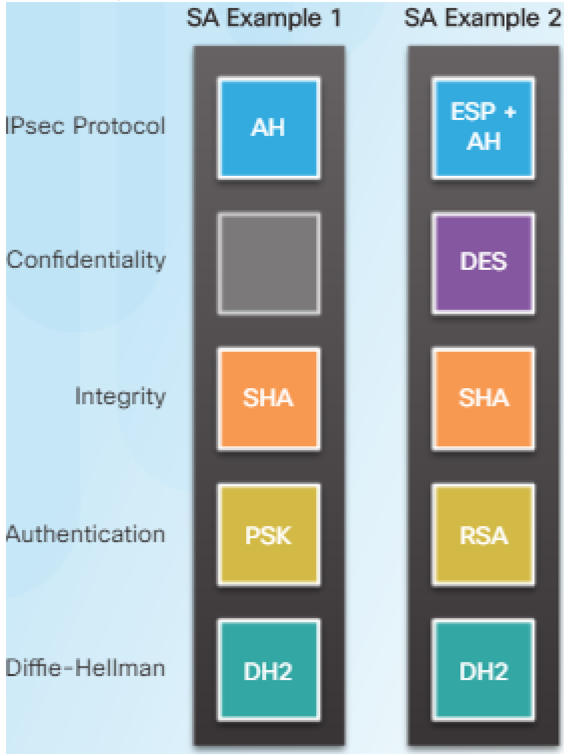
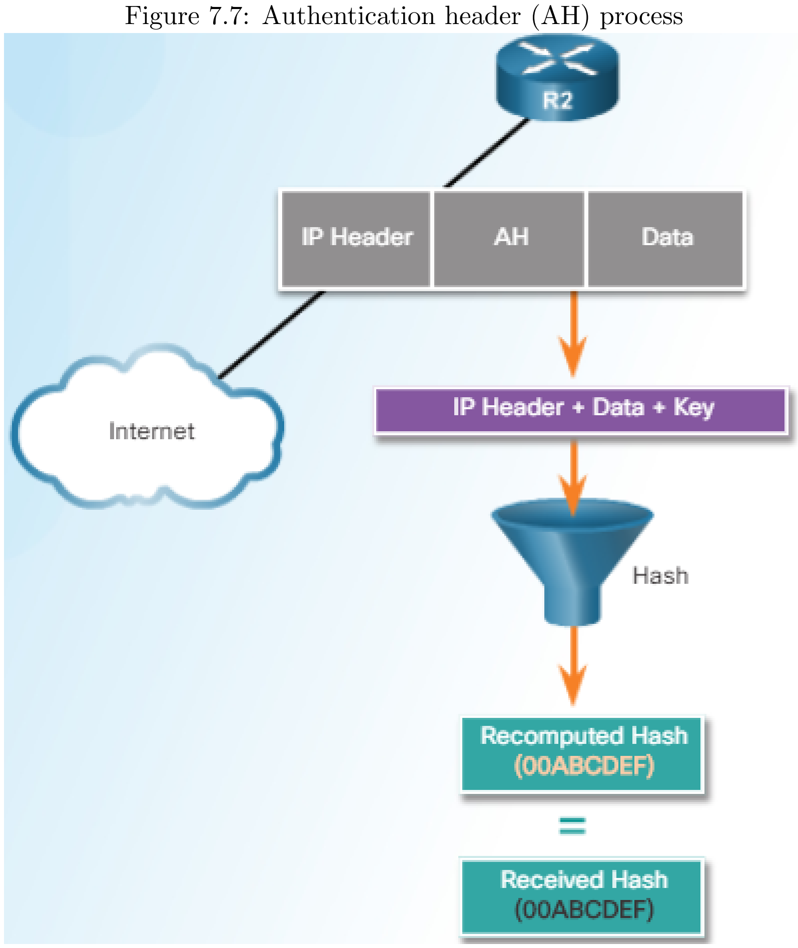


Figure 7.7: Authentication header (AH) process

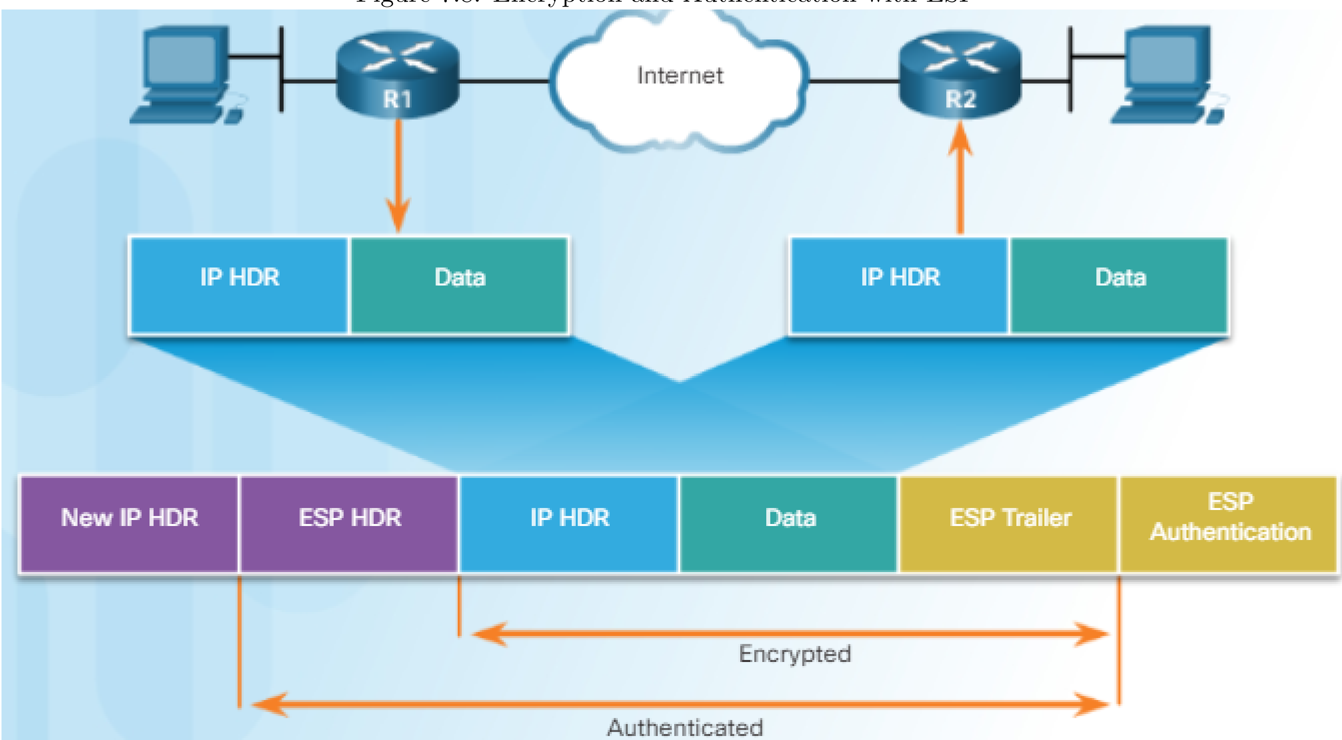


4. The peer router hashes the IP header and data payload using the shared secret key, extracts the transmitted hash from the AH header, and compares the two hashes (Figure 7.7). The hashes must match exactly.

7.3.2 Encapsulation Security Protocol (ESP)

ESP provides **confidentiality** by encrypting the entire original IP datagram and ESP trailer. If ESP is selected as the IPsec protocol, an encryption algorithm must also be selected. The default algorithm for IPsec is 56-bit DES. ESP can also provide **integrity** and **authentication**.

Figure 7.8: Encryption and Authentication with ESP



Optionally, ESP can also enforce anti-replay protection. **Anti-replay protection** verifies that each packet is unique and is not duplicated. This protection ensures that a hacker cannot intercept packets and insert changed packets into the data stream. Anti-replay works by keeping track of packet sequence numbers and using a sliding window on the destination end.
Looking at figure 7.8, ESP process starts with encrypting the payload (IP datagram and ESP trailer). Then, the newly encrypted data and the ESP header are included in the hashing process. Next, a new IP header is attached to the authenticated payload. The new IP address is used to route the packet through the Internet.

7.3.3 Transport and Tunnel modes

ESP and AH can be applied to IP packets in two different modes, transport mode and tunnel mode.

In **ESP transport mode**, security is provided only for the transport layer of the OSI model and above. Transport mode protects the payload of the packet but leaves the original IP address in plaintext. The original IP address is used to route the packet through the Internet. ESP transport mode is used between hosts.

ESP tunnel mode provides security for the complete original IP packet. The original IP packet is encrypted and then it is encapsulated in another IP packet. This is known as IP-in-IP encryption. The IP address on the outside IP packet is used to route the packet through the Internet. ESP tunnel mode is used between a host and a security gateway, or between two security gateways.

AH transport mode provides authentication and integrity for the entire packet. It does not encrypt the data, but it is protected from modification.

AH tunnel mode encapsulates the IP packet with an AH and a new IP header, and signs the entire packet for integrity and authentication.

7.4 IPsec key exchange

7.4.1 IKE protocol

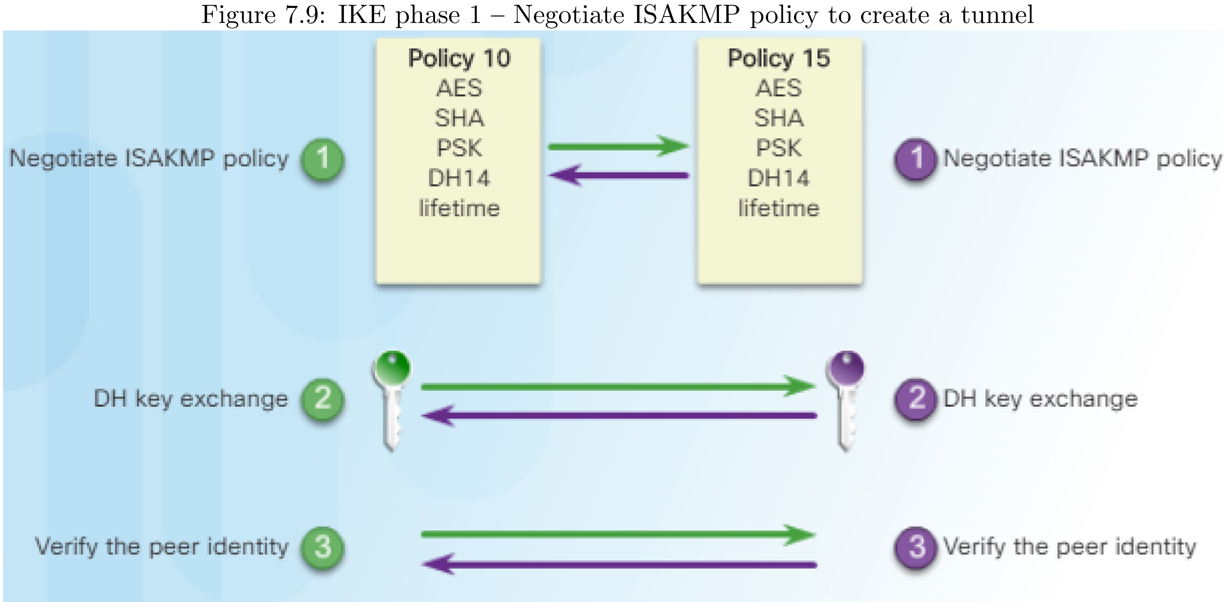
The Internet Key Exchange (IKE) protocol is a key management protocol standard. IKE is used in conjunction with the IPsec standard. IKE automatically negotiates IPsec security associations and enables IPsec secure communications.

Instead of transmitting keys directly across a network, IKE calculates shared keys based on the exchange of a series of data packets. This disables a third party from decrypting the keys even if the third party captured all of the exchanged data that was used to calculate the keys.

IKE uses **UDP port 500** to exchange IKE information between the security gateways. UDP port 500 packets must be permitted on any IP interface that is connecting a security gateway peer.

7.4.2 IKE phase 1

Figure 7.9: IKE phase 1 – Negotiate ISAKMP policy to create a tunnel



IKE uses ISAKMP for phase 1 and phase 2 of key negotiation. In Phase 1 (figure 7.9), the following tasks are performed in order:

1. IPsec peers authenticate each other.
2. Negotiate a matching IKE SA policy to protect the exchange
3.

two IPsec peers perform the initial negotiation to ensure that SAs (ISAKMP policy) on both sides are matched. This phase also authenticates the peers, and sets up a secure tunnel between the peers. This tunnel will then be used in Phase 2 to negotiate the IPsec policy.

Phase 1 can be implemented in main mode or aggressive mode. When **main mode** is used, the identities of the two IKE peers are hidden. **Aggressive mode** takes less time than main mode to negotiate keys between peers. However, since the authentication hash is sent unencrypted before the tunnel is established, aggressive mode is vulnerable to brute-force attacks.

7.4.3 IKE phase 2

The purpose of IKE Phase 2 is to negotiate the IPsec security parameters (figure 7.10). IKE Phase 2 is called quick mode and can only occur after IKE has established a secure tunnel in Phase 1. In this phase, the SAs that IPsec uses are unidirectional; therefore, a separate key exchange is required for each data flow.

Figure 7.10: IKE phase 2 – Negotiate IPsec policy for sending secure traffic accross the tunnel

Quick mode also renegotiates a new IPsec SA when the IPsec SA lifetime expires. Basically, quick mode refreshes the keying material that creates the shared secret key. This is based on the keying material that is derived from the DH exchange in Phase 1.

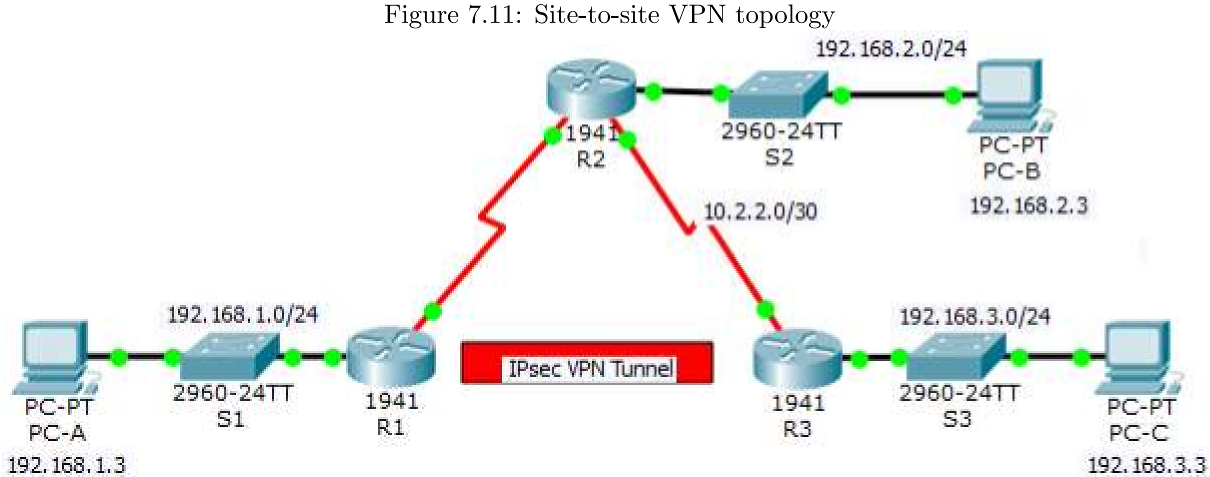
7.4.4 IPsec negotiation

IPsec negotiation to establish a VPN involves five steps, which include IKE Phase 1 and Phase 2:

1. An ISAKMP tunnel is initiated when host A sends "interesting" traffic to host B. Traffic is considered interesting when it travels between the peers and meets the criteria that are defined in an ACL.
2. IKE Phase 1 begins. The peers negotiate the ISAKMP SA policy. When the peers agree on the policy and are authenticated, a secure tunnel is created.
3. IKE Phase 2 begins. The IPsec peers use the authenticated secure tunnel to negotiate the IPsec SA policy. The negotiation of the shared policy determines how the IPsec tunnel is established.
4. The IPsec tunnel is created, and data is transferred between the IPsec peers based on the IPsec SAs.
5. The IPsec tunnel terminates when the IPsec SAs are manually deleted, or when their lifetime expires.

7.5 Site-to-site IPsec configuration

Figure 7.11: Site-to-site VPN topology



The configuration tasks for the topology in figure 7.11 are shown in order as below:

1. Test connectivity
2. Enable the Security Technology package
3. Identify interesting traffic: Configure ACL to identify the traffic from the LAN on R1 to the LAN on R3 as interesting. This interesting traffic will trigger the IPsec VPN to be implemented when there is traffic between the R1 to R3 LANs.
4. Configure the IKE Phase 1 ISAKMP policy on R1 (encryption method, key exchange method, and DH method)
5. Configure the IKE Phase 2 IPsec policy on R1. First, we create the transform-set VPN-SET to use esp-aes and esp-sha-hmac. Next, a crypto map VPN-MAP is created to bind all of the Phase 2 parameters together. Use sequence number 10 and identify it as an ipsec-isakmp map. In the following commands, the perfect forwarding secrecy type is set using the `set pfs` command.
6. Configure the crypto map on the outgoing interface.
7. Repeat the above steps on R3.

Listing 33: Site-to-site IPsec

```
#STEP 2
license boot module c1900 technology-package securityk9

#STEP 3
access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255

#STEP 4
crypto isakmp policy 10
        hash sha
        encryption aes 256
        authentication pre-share
        group 14
        exit
crypto isakmp key vpnpa55 address 10.2.2.2

#STEP 5
crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
crypto map VPN-MAP 10 ipsec-isakmp
        description VPN connection to R3
        set peer 10.2.2.2
        set transform-set VPN-SET
        set pfs group14
        set security-association lifetime seconds 900
        match address 110
        exit

#STEP 6
interface s0/0/0
        crypto map VPN-MAP
        exit

#VERIFICATION
show crypto ipsec transform-set
show crypto map
show crypto isakmp sa
show crypto ipsec sa
```

Chapter 8

ASA Firewall Models

8.1 Introduction

8.1.1 What is ASA?

Modern network design must include proper placement of one or more firewalls to protect resources. Cisco provides two firewall solutions: the firewall-enabled ISR and the Cisco Adaptive Security Appliance (ASA). This chapter will provide an introduction to the ASA platform.

The ASA software combines firewall, VPN concentrator, and intrusion prevention functionality into one software image. There are four advanced ASA firewall features:

- ASA virtualization – A single ASA can be partitioned into multiple virtual devices
- High availability with failover – two identical ASAs can be paired into an active / standby failover configuration to provide device redundancy.
- Identity firewall - The ASA provides access control based on an association of IP addresses to Windows Active Directory login information.
- Support basic IPS features.

There are two firewall modes of operation available on ASA devices:

- The ASA is considered to be a router in the network and can perform NAT between connected networks. The focus of this chapter is on the routed mode.
- The ASA functions like a Layer 2 device and is not considered a router. It is only assigned an IP address on the local network for management purposes.

A **license** specifies the options that are enabled on a given ASA. To verify the license information on an ASA device, use the `show version` command, as shown in Figure 3, or the `show activation-key` command.

8.1.2 Security levels

The ASA assigns **security levels** to distinguish between inside and outside networks. Security levels define the level of trustworthiness of an interface. The higher the level, the more trusted the interface. The security level numbers range from 0 (untrustworthy) to 100 (very trustworthy). Each operational interface must have a name and a security level from 0 (lowest) to 100 (highest) assigned.

When traffic moves from an interface with a higher security level to an interface with a lower security level, it is considered outbound traffic. Conversely, traffic moving from an interface with a lower security level to an interface with a higher security level is considered inbound traffic.

Outbound traffic is allowed and inspected by default. Returning traffic is allowed because of stateful packet inspection. However, traffic that is coming from the outside network and going into either the DMZ or the inside network, is denied by default. Return traffic, originating on the inside network and returning via the outside interface, would be allowed.

8.1.3 ASA Interactive Setup Initialization Wizard

You can erase ASA configuration using `write erase` and `reload` privileged EXEC commands. When the device is rebooted, the ASA wizard displays the prompt "Pre-configure Firewall now through interactive prompts [yes]" To cancel and display the ASA default user EXEC mode prompt, enter `no`. Otherwise, enter `yes` or simply press `Enter`. This initiates the wizard and the ASA interactively guides an administrator to configure the default settings.

8.2 Configuration

8.2.1 Basic configurations

The default ASA user prompt of `ciscoasa>` is displayed when an ASA configuration is erased, the device is rebooted, and the user does not use the interactive setup wizard. To enter privileged EXEC mode, use the `enable` user EXEC mode command. Initially, an ASA does not have a password configured; therefore when prompted, leave the enable password prompt blank and press Enter.

The ASA date and time should be set either manually or by using Network Time Protocol (NTP). To set the date and time, use the `clock set` privileged EXECcommand. Enter global configuration mode using the `conf t` privileged EXEC command. An ASA must be configured with basic management settings. The table in Figure 8.1 displays the commands to accomplish this task.

Figure 8.1: ASA basic configuration commands

ASA Command	Description
hostname *name*	• Specifies a hostname up to 63 characters. • A hostname must start and end with a letter or digit, and have as interior characters only letters, digits, or a hyphen.
domain-name *name*	• Sets the default domain name.
enable password *password*	• Sets the enable password for privileged EXEC mode. • Sets the password as a case-sensitive string of 3 to 32 alphanumeric and special characters (not including a question mark or a space).
banner motd *message*	• Provides legal notification and configures the system to display a message-of-the-day banner when connecting to the ASA.
key config-key password-encryption [*new-pass* [*old-pass*]]	• Sets the passphrase between 8 and 128 character long. • Used to generate the encryption key.
password encryption aes	• Enables password encryption and encrypts all user passwords.

8.2.2 Configuring Logical VLAN Interfaces

When configuring an ASA 5505, there are two kinds of interfaces that need to be configured:

- Logical VLAN interfaces – These interfaces are configured with the Layer 3 information including a name, security level, and IP address.
- Physical switch ports – These are Layer 2 switch ports which are assigned to the logical VLAN interfaces.

An ASA 5505 with a Base license does not allow three fully functioning VLAN interfaces to be created. However, a third "limited" VLAN interface can be created if it is first configured with the `no forward interface vlan <num>` command (figure 8.2). This command limits the interface from initiating contact with another VLAN. Therefore, when the inside and outside VLAN interfaces are configured, the no forward interface vlan number command must be entered before the `nameif` command is entered on the third interface. The `<num>` argument specifies the VLAN ID to which this VLAN interface cannot initiate traffic. The Security Plus license is required to achieve full

Figure 8.2: Logical VLAN interface command

ASA Command	Description
interface vlan *vlan-number*	• Enters VLAN interface configuration mode.
nameif *if_name*	• Names the interface using a text string of up to 48 characters. • The name is not case-sensitive. • You can change the name by re-entering this command with a new value. • Do not enter the no form, because that command causes all commands that refer to that name to be deleted.
security-level *value*	• Sets the security level, where number is an integer between 0 (lowest) and 100 (highest).

functionality.

8.2.3 Static routes and IP addresses

Switch ports on the same VLAN can communicate with each other using hardware switching. But when a switch port on VLAN 1 wants to communicate with a switch port on VLAN 2, then the ASA applies the security policy to the traffic and routes between the two VLANs. If an ASA is configured as a DHCP client, then it can receive and install a default route from the upstream device. Otherwise, a default static route must be configured using the `route <ifname> 0.0.0.0 0.0.0.0 next-hop-ip-address` command. To verify the route entry, use the show route command.

The IP address of an interface can be configured using one of the following options: DHCP, PPPoE, or manually. The table in Figure 8.3 lists the commands to configure an IP address on an interface.

Figure 8.3: Configure IP addresses on logical VLAN interfaces

Manually	**ip address** *ip-address netmask*	• Assigns an IP address to the interface.
Using DHCP	**ip address dhcp**	• Used to have the interface request an IP address configuration from the upstream device.
	ip address dhcp setroute	• Used to have the interface request and install a default route to the upstream device.
Using PPP0E	**ip address pppoe**	• Interface configuration mode command that requests an IP address from the upstream device.
	ip address pppoe setroute	• Same command but it also requests and installs a default route to the upstream device.

8.2.4 Remote access

Figure 8.4: ASA Telnet configuration commands

ASA Command	Description
{passwd | password} *password*	• Sets the login password up to 80 characters in length for Telnet.
telnet {*ipv4_address mask* | *ipv6_address/prefix* } *if_name*	• Identifies which inside host or network can Telnet to the ASA interface. • Use the **clear configure telnet** command to remove the Telnet connection.
telnet timeout *minutes*	• By default, Telnet sessions left idle for five minutes are closed by the ASA. • The command alters the default exec timeout of five minutes.
aaa authentication telnet console LOCAL	• Configures Telnet to refer to the local database for authentication. • The **LOCAL** keyword is case sensitive and is a predefined server tag.
clear configure telnet	• Removes the Telnet connection from the configuration.

Figure 8.5: Sample ASA Telnet configuration

```
CCNAS-ASA(config)# password cisco
CCNAS-ASA(config)# telnet 192.168.1.3 255.255.255.255 inside
CCNAS-ASA(config)# telnet timeout 3
CCNAS-ASA(config)#
CCNAS-ASA(config)# show run telnet
telnet 192.168.1.3 255.255.255.255 inside
telnet timeout 3
CCNAS-ASA(config)#
```

Figure 8.6: ASA ssh configuraiton commands

ASA Command	Description
username *name* **password** *password*	• Creates a local database entry.
aaa authentication ssh console LOCAL	• Configures SSH to refer to the local database for authentication. • The **LOCAL** keyword is case sensitive and is a predefined server tag.
crypto key generate rsa modulus *modulus_size*	• Generates the RSA key required for SSH encryption. • The **modulus_size** (in bits) can be 512, 768, 1024, or 2048. • A value of 2048 is recommended.
ssh {*ip_address mask* | *ipv6_address/prefix* } *if_name*	• Identifies which inside host or network can SSH to the ASA interface. • Multiple commands can be in the configuration. • If the **if_name** is not specified, SSH is enabled on all interfaces except the outside interface. • Use the **clear configure ssh** command to remove the SSH connection.
ssh version *version_number*	• (Optional) By default, the ASA allows both SSH Version 1 (less secure) and Version 2 (more secure). • Enter this command in order to restrict the connections to a specific version.
ssh timeout *minutes*	• Alters the default exec timeout of five minutes.
clear configure ssh	• Removes the SSH connection from the configuration.

8.2.5 NTP configuration

Figure 8.7: NTP authentication commands

ASA Command	Description
ntp authenticate	• Enables authentication with an N
ntp trusted-key *key_id*	• Specifies an authentication key I key, which is required for auther NTP server.
ntp authentication-key *key_id* **md5** *key*	• Sets a key to authenticate with a
ntp server *ip_address* [**key** *key_id*]	• Identifies an NTP server.

8.2.6 DHCP configuration

The example in Figure 8.9 enables the DHCP service for inside clients on an ASA 5505. The ASA 5505 Base license can provide IP configuration information for up to 32 DHCP clients. If the ASA outside interface was configured as a DHCP client, then the `dhcpd auto outside` global configuration mode command can be used to pass the DHCP-obtained information to the DHCP inside clients.

8.2.7 Objects and Object Groups

The ASA supports objects and object groups. An object can be a particular IP address, an entire subnet, a range of addresses, a protocol, or a specific port or range of ports. The object can then be re-used in several configurations.

Figure 8.8: DHCP server commands

ASA Command	Description
`dhcpd address IP_address1 [-IP_address2 ] if_name`	• Creates a DHCP address pool in which IP_address1 is the start of the pool and IP_address2 is the end of the pool, separated by a hyphen. • The address pool must be on the same subnet as the ASA interface.
`dhcpd dns dns1 [dns2 ]`	• (Optional) Specifies the IP address(es) of the DNS server(s).
`dhcpd lease lease_length`	• (Optional) Changes the lease length granted to the client which is the amount of time in seconds that the client can use its allocated IP address before the lease expires. • The lease_length defaults to 3600 seconds (1 hour) but can be a value from 0 to 1,048,575 seconds.
`dhcpd domain domain_name`	• (Optional) Specifies the domain name assigned to the client.
`dhcpd enable if_name`	• Enables the DHCP server service (daemon) on the interface (typically the inside interface) of the ASA.

Figure 8.9: Sample configuration ASA as an DHCP server

```
CCNAS-ASA(config)# dhcpd address 192.168.1.10-192.168.1.100
ERROR: % Incomplete command
CCNAS-ASA(config)# dhcpd address 192.168.1.10-192.168.1.100 inside
Warning, DHCP pool range is limited to 32 addresses, set address range as:
192.168.1.10-192.168.1.41
CCNAS-ASA(config)# dhcpd address 192.168.1.10-192.168.1.41 inside
CCNAS-ASA(config)# dhcpd lease 1800
CCNAS-ASA(config)#
```

The advantage is that when an object is modified, the change is automatically applied to all rules that use the specified object. There are two types of objects that can be configured:

- Network object – Contains a single IP address and subnet mask. Network objects can be of three types: host, subnet, or range.
- Service object – Contains a protocol and optional source and/or destination port.

To create a network object, use the `object network <name>` global configuration mode command. The prompt changes to network object configuration mode. A network object name can contain only one IP address and mask pair. Therefore, there can only be one statement in the network object. Entering a second IP address/mask pair replaces the existing configuration (figure 8.10).

Figure 8.10: Network object configuration

```
CCNAS-ASA(config)# object network EXAMPLE-1
CCNAS-ASA(config-network-object)# host 192.168.1.3
CCNAS-ASA(config-network-object)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# show running-config object
object network EXAMPLE-1
 host 192.168.1.3
CCNAS-ASA(config)#
CCNAS-ASA(config)# object network EXAMPLE-1
CCNAS-ASA(config-network-object)# host 192.168.1.4
CCNAS-ASA(config-network-object)# range 192.168.1.10 192.168.1.20
CCNAS-ASA(config-network-object)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# show running-config object
object network EXAMPLE-1
 range 192.168.1.10 192.168.1.20
CCNAS-ASA(config)#
```

To create a service object, use the object service object-name global configuration mode command. The prompt changes to service object configuration mode. The service object can contain a protocol, ICMP, ICMPv6, TCP, or UDP port (or port ranges).
Objects can be grouped together to create an object group. By grouping like objects together, an object group can be used in an access control entry (ACE) instead of having to enter an ACE for each object separately.
To configure a network object group, use the `object-group network <name>` global configuration mode command. After entering the command, add network objects to the network group using the `network-object` and

Figure 8.11: Service object configuration

```
CCNAS-ASA(config)# object service SERV-1
CCNAS-ASA(config-service-object)# service tcp destination eq ftp
CCNAS-ASA(config-service-object)# service tcp destination eq www
CCNAS-ASA(config-service-object)# exit
CCNAS-ASA(config)# show running-config object service
object service SERV-1
 service tcp destination eq www
CCNAS-ASA(config)#
```

Figure 8.12: Create a network object group

```
CCNAS-ASA(config)# object-group network ALL-HOSTS
CCNAS-ASA(config-network-object-group)# description All inside hosts
CCNAS-ASA(config-network-object-group)# network-object 192.168.1.32 255.255.255.240
CCNAS-ASA(config-network-object-group)# group-object ADMIN-HOST
CCNAS-ASA(config-network-object-group)# exit
```

`group-object` commands (figure 8.12). **Note:** A network object group cannot be used to implement NAT. A network object is required to implement NAT.

Figure 8.13: ICMP-type object group

```
CCNAS-ASA(config)# object-group icmp-type ICMP-ALLOWED
CCNAS-ASA(config-icmp-object-group)# icmp-object echo
CCNAS-ASA(config-icmp-object-group)# icmp-object time-exceeded
CCNAS-ASA(config-icmp-object-group)# exit
```

To configure an ICMP object group, use the object-group icmp-type grp-name global configuration mode command (figure 8.13). After entering the command, add ICMP objects to the ICMP object group using the icmp-object and group-object commands.

8.2.8 Restricting traffic with ACL

To allow connectivity between interfaces with the same security levels, the `same-security-traffic permit inter-interface` global configuration mode command is required. To enable traffic to enter and exit the same interface, such as when encrypted traffic enters an interface and is then routed out the same interface unencrypted, use the `same-security-traffic permit intra-interface` global configuration mode command.

Object grouping is a way to group similar items together to reduce the number of ACEs (comparing figure 8.14 and 8.15). By grouping like objects together, object groups can be used in an ACL instead of having to enter an ACE for each object separately.

8.2.9 NAT configuration in ASA

Static NAT

Static NAT is configured when a single inside address is mapped to only one outside address. For instance, static NAT can be used when a server must be accessible from the outside.

Dynamic NAT

In figure 8.16, the inside hosts on the 192.168.1.0/27 network will be dynamically assigned a range of public IP address from 209.165.200.240 to 209.165.200.248. The PUBLIC network object identifies the public IP addresses to be translated to while the DYNAMIC-NAT identifies the internal addresses to be translated. The name `inside` is the interface connected to the private network, while `outside` interface connected to the Internet.

Figure 8.17 displays the configuration to allow return ICMP traffic from outside hosts.
After the inside host pings the outside host, verify the network address translation using the `show xlate` command. Additional information can be gathered using the `show nat` and `show nat detail` commands.

Figure 8.14: ACL configuration without Object groups

```
CCNAS-ASA(config)# access-list ACL-IN remark Permit PC-1 -> Server A for HTTP / SMTP
CCNAS-ASA(config)# access-list ACL-IN extended permit tcp host 209.165.201.1 host 209.165.202.131 eq http
CCNAS-ASA(config)# access-list ACL-IN extended permit tcp host 209.165.201.1 host 209.165.202.131 eq smtp
CCNAS-ASA(config)# access-list ACL-IN remark Permit PC-1 -> Server B for HTTP / SMTP
CCNAS-ASA(config)# access-list ACL-IN extended permit tcp host 209.165.201.1 host 209.165.202.132 eq http
CCNAS-ASA(config)# access-list ACL-IN extended permit tcp host 209.165.201.1 host 209.165.202.132 eq smtp
CCNAS-ASA(config)# access-list ACL-IN remark Permit PC-2 -> Server A for HTTP / SMTP
CCNAS-ASA(config)# access-list ACL-IN extended permit tcp host 209.165.201.2 host 209.165.202.131 eq http
CCNAS-ASA(config)# access-list ACL-IN extended permit tcp host 209.165.201.2 host 209.165.202.131 eq smtp
CCNAS-ASA(config)# access-list ACL-IN remark Permit PC-2 -> Server B for HTTP / SMTP
CCNAS-ASA(config)# access-list ACL-IN extended permit tcp host 209.165.201.2 host 209.165.202.132 eq http
CCNAS-ASA(config)# access-list ACL-IN extended permit tcp host 209.165.201.2 host 209.165.202.132 eq smtp
CCNAS-ASA(config)# access-list ACL-IN extended deny ip any any log
CCNAS-ASA(config)#
CCNAS-ASA(config)# access-group ACL-IN in interface outside
CCNAS-ASA(config)#
```

Figure 8.15: ACL configuration using Network object group

```
CCNAS-ASA(config)# object-group network NET-HOSTS
CCNAS-ASA(config-network-object-group)# description OG matches PC-A and PC-B
CCNAS-ASA(config-network-object-group)# network-object host 209.165.201.1
CCNAS-ASA(config-network-object-group)# network-object host 209.165.201.2
CCNAS-ASA(config-network-object-group)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# object-group network SERVERS
CCNAS-ASA(config-network-object-group)# description OG matches Web / Email Servers
CCNAS-ASA(config-network-object-group)# network-object host 209.165.202.131
CCNAS-ASA(config-network-object-group)# network-object host 209.165.202.132
CCNAS-ASA(config-network-object-group)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# object-group service HTTP-SMTP tcp
CCNAS-ASA(config-service-object-group)# description OG matches SMTP / WEB traffic
CCNAS-ASA(config-service-object-group)# port-object eq smtp
CCNAS-ASA(config-service-object-group)# port-object eq www
CCNAS-ASA(config-service-object-group)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# access-list ACL-IN remark Only permit PC-A / PC-B -> Internal Servers
CCNAS-ASA(config)#  access-list ACL-IN extended permit tcp object-group NET-HOSTS
object-group SERVERS object-group HTTP-SMTP
```

Figure 8.16: Dynamic NAT configuration on ASA

```
CCNAS-ASA(config)# object network PUBLIC
CCNAS-ASA(config-network-object)# range 209.165.200.240 209.165.200.248
CCNAS-ASA(config-network-object)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# object network DYNAMIC-NAT
CCNAS-ASA(config-network-object)# subnet 192.168.1.0 255.255.255.224
CCNAS-ASA(config-network-object)# nat (inside,outside) dynamic PUBLIC
CCNAS-ASA(config-network-object)# end
CCNAS-ASA#
```

Figure 8.17: Enable return traffic

```
CCNAS-ASA(config)# policy-map global_policy
CCNAS-ASA(config-pmap)# class inspection_default
CCNAS-ASA(config-cmap)# access-list ICMPACL extended permit icmp any any
CCNAS-ASA(config)# access-group ICMPACL in interface outside
CCNAS-ASA(config)#
```

PAT

Only one network object is required when overloading the outside interface. To enable inside hosts to overload the outside address, use the commands in figure

Figure 8.18: PAT configuration in ASA

```
CCNAS-ASA(config)# object network INSIDE-NET
CCNAS-ASA(config-network-object)# subnet 192.168.1.0 255.255.255.224
CCNAS-ASA(config-network-object)# nat (inside,outside) dynamic interface
CCNAS-ASA(config-network-object)# end
CCNAS-ASA#
```