The Notebook
of
CCNA Security

Huy Bui

THE PUBLISHER

Contents

0.1 List of Codes

Chapter 1

Introduction to Network security

1.1 Network threats

1.1.1 Malware

A **virus** is malicious code that is attached to executable files which are often legitimate programs. A virus is triggered by an event and cannot automatically propagate itself to other systems. Viruses are spread by USB memory drives, CDs, DVDs, network shares, and email.

A **Trojan horse** carries out malicious operations under the guise of a desired function. This malicious operation exploits the privileges of the user. 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.

1.1.2 Network attacks

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

Access attacks gain access or control to sensitive information. Some examples of access attacks are listed as follow:

- 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

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

- 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.

1.2 Mitigating Threats

1.2.1 Mitigating common network attacks

Virus and Trojan horse: The primary means of mitigating virus and Trojan horse attacks is antivirus software. However, antivirus software cannot prevent viruses from entering the network.

Worms: 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

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: strong password policy, principle of minimum trust[2], cryptography, OS and app patches.

DoS attacks: a network utilization software and anti-spoofing technologies (port security, DHCP snooping, IP source guard, ARP inspection, and ACL).

1.2.2 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** is responsible for routing functions. We protect this plane using Routing protocol authentication, CoPP[3], and AutoSecure.
- **Management plane** is responsible for network security and management. Its security is implemented by password policy, RBAC[4], authorization, access reporting.

[2] a system or device should not trust another unconditionally
[3] prevents unnecessary traffic from overwhelming the route processor
[4] Role-based access control, restricts user access based on the role of the user.

- **Data plane** is responsible for forwarding data. Its security can be implemented using *ACLs*, antispoofing mechanisms, and port security.

Chapter 2

Router security

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 access, Disable unnecessary ports, interfaces and services

2.1 Administrative access

2.1.1 Virtual logins

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
```

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
end
show login
show login failures
```

The `login block-for` command disables logins for 60 seconds if more than 5 login failures occur within 15 seconds. Doing this can defend against DoS attacks. 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.

Note that these login enhancements do *not* apply to console connections and only available if local database is used for authentication. If the lines are configured for password authentication only, then the enhanced login features are not enabled.

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 privilege 15 algorithm-type scrypt secret cisco12345

line vty 0 4
        privilege 15
  login local
  transport input ssh
  exit
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. The default SSH timeouts and authentication parameters can be altered using `ip ssh time-out` and `ip ssh authentication-retries` commands.

2.1.2 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.

Privilege levels

There are 16 privilege levels (0 – 15) that can be applied to user accounts. Levels 0, 1, and 15 have predefined settings. Level 1 is the lowest user privileges and allows only commands available at the `router>` prompt. Level 15 provide the user full control.

The user SUPPORT in the following command can execute `ping` command and all commands available in level 1 to 4.

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.

Role-based CLI

Role-based CLI defines a set of CLI commands accessible by a specific user. Role-based CLI provides three types of views:

- **Root view:** Only a root view user can configure a new view and add or remove commands from the existing views.
- **CLI view:** This view is a set of commands. A CLI view does not inherit commands from any other view. However, the same commands can be used in multiple views.
- **Superview:** This view is a group of CLI views. Users who are logged into a superview can access all the commands of the member CLI views. Deleting a superview does not delete the associated CLI views, and those views remain available to be assigned to another superview. Commands cannot be configured for a superview. You must be in root view to configure a superview.

Note! AAA must be enabled before configuring any views.

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 (`exec`) mode. To access existing views, enter the `enable view view-name` command.

Listing 6: Superview configuration

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

To access the superview, use the `enable view` command followed by the name of the superview, and provide the password. From the root view, use the `show parser view all` command to see a summary of all views. Notice how the asterisk identifies superviews.

2.2 IOS security

2.2.1 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 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.

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. During boot process, 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 image using the `boot` .
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
```

2.2.2 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.

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.

2.2.3 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.

2.3 Syslog

2.3.1 Introduction

The syslog protocol allows networking devices to send their system messages across the network to syslog servers. 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 can be sent to either CLI or external server. Log messages on CLI are saved in RAM, therefore, they are lost after a reboot. To view syslog messages on an external server, an syslog application must be installed. Using syslog server, administrator can perform searches through the data and delete unimportant syslog messages.

2.3.2 Severity level and Facility

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 (interface up or down, system restart); Level 6 generates messages when the device is booting. By default, the severity level of Cisco routers and switches is 6.

2.3.3 Message format

Below is an example of syslog messages:

```
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

2.3.4 Configuration

Listing 9: Logging service

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

Above is an example showing logging service configuration. The first command enable timestamp to log messages. Log messages up to level 4 are sent by g0/0 to the syslog server at 192.168.1.3.

2.4 SNMP

2.4.1 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): provide access to the MIB
- **MIB** (Management Information Base): reside on each SNMP client device to store data about the device

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

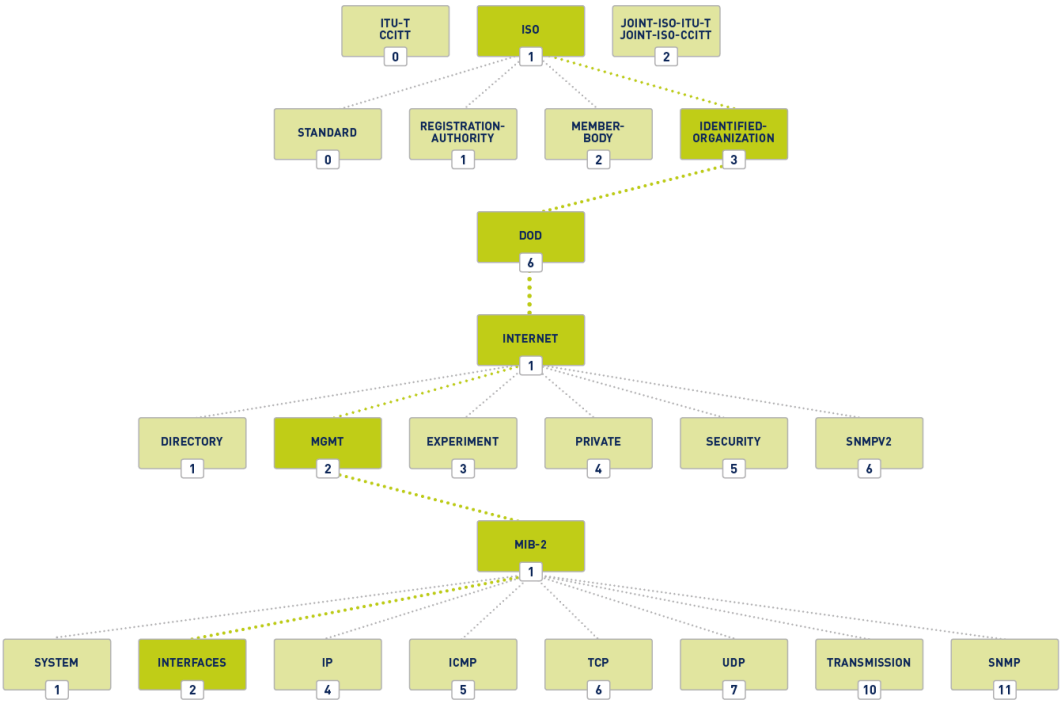
Polls: SNMP manager periodically *polls* the SNMP agents to monitor traffic loads and verify device configurations. This method has two drawbacks: (1) there is delay between the time that an event occurs and the time that it is noticed (via polling), (2) frequent polling consumes significant bandwidth.

Traps: *Agent traps* are used to mitigate disadvantages of polling. SNMP agents only send traps to SNMP manager only when events occur.

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, called Object ID (OID), and organizes them hierarchically (figure 2.1). 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 2.1: 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.

2.4.2 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` .

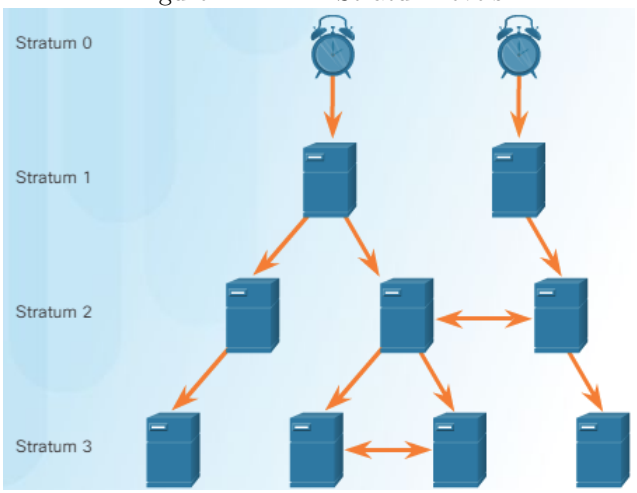
2.5 NTP

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 manually using `clock set` command, or by connecting NTP server via UDP port 123.

NTP networks use a hierarchical system of time sources. Each level in this hierarchical system is called a **stratum**. Smaller stratum numbers indicate that the server is closer to the authorized time source. Stratum 0 is the authoritative time sources (represented by the clock in the figure 2.2). Stratum 16, the lowest stratum level, indicates that a device is unsynchronized.

In the below configuration, the first command identifies NTP server. The second command periodically updates the hardware clock with the time learned from NTP. The next 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` .

Figure 2.2: NTP Stratum levels



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
```

2.6 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 (default), the router prompts with options to enable and disable security features. On the other hand, the non-interactive mode (configured with the `auto secure no-interact` command) will automatically execute security features with default settings.

2.7 Control plane security

2.7.1 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
```

2.7.2 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:** forward packets. Data plane are handled by CEF, which 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.
- **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.)

Chapter 3

AAA model

AAA controls 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 does not scale well for large enterprise. The local authentication only serves as a backup method for if authentication servers are not available.

- 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 create two users ADMIN and JR-ADMIN, then uses local database to authenticate these users when they login the router (the last command). The `default` keyword means that the authentication method applies to all lines (console, vty, aux). Alternatively, you can name an authentication method and assign it to a particular line.

Listing 17: Local named authentication

```
aaa authentication login SSH-LOGIN local-case
line vty 0 4
login authentication SSH-LOGIN
```

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. The `sh aaa sessions` command can be used to show the unique ID of a session.

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)

Cisco Secure ACS for Windows Server is a single solution that offers AAA for both TACACS+ and RADIUS and is integrated to into Active Directory service. In this technology, Active Directory controller performs the authentication and authorization.

Listing 18: Server-based authentication

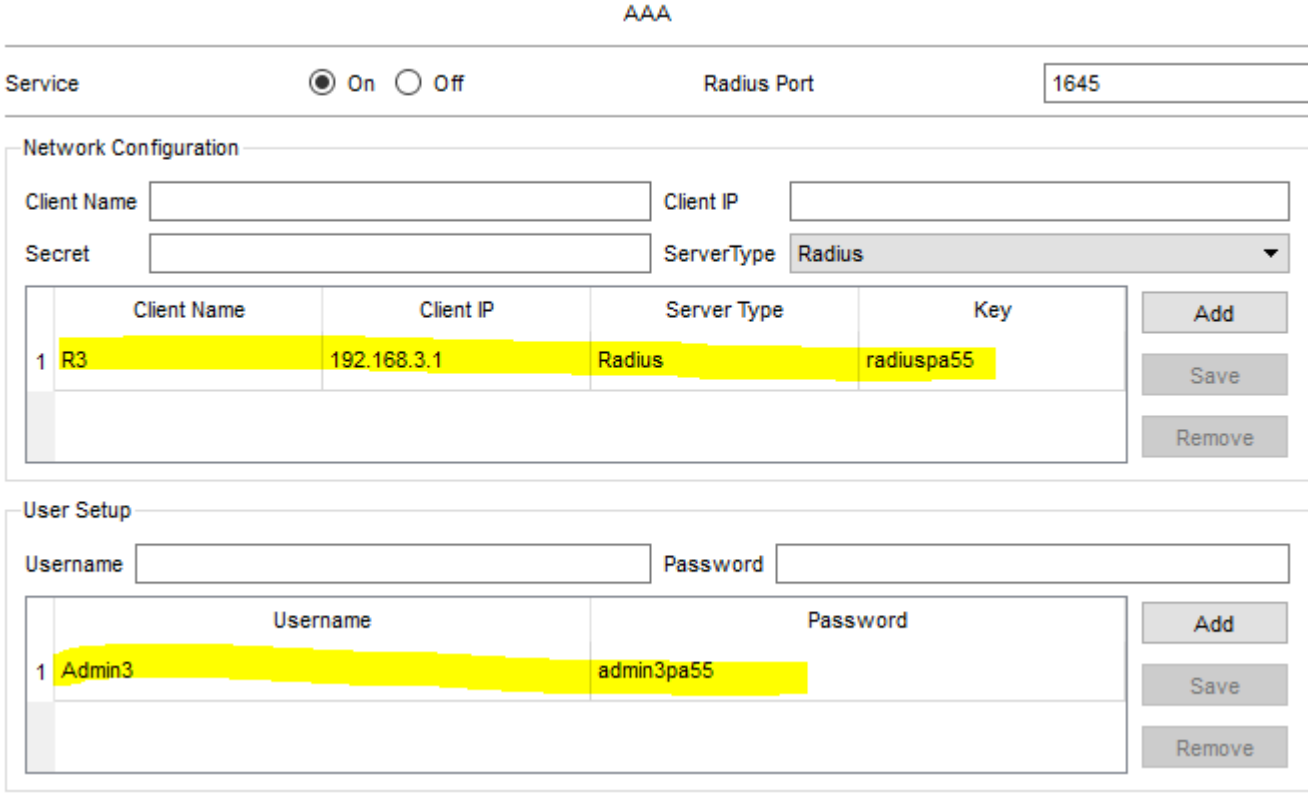
```
aaa new-models
username ADMIN algorithm-type scrypt secret Str0ng5rPa55w0rd

#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
  key RADIUS-Pa55w0rd

aaa authentication login default group tacacs+ group radius local-case

line con 0
        login authentication default
```

On TACACS+ or Radius server, you have to set up an entry as shown in figure 3.1. On router CLI, configure a corresponding entry with the server's address and the exact same encryption key with the server.

By default, TACACS+ establishes a new TCP session for every authorization request, which can lead to delays when users enter commands. To improve performance, Cisco Secure ACS supports persistent TCP sessions configured with the `single-connection` tacacs server configuration mode command.

We add AAA servers to the method list using the `group tacacs+` or `group radius` keywords. The above command configures a method list that first uses TACACS+ server for authentication. If TACACS+ server is unreachable, the RADIUS server takes over, and the last resort is local authentication (case-sensitive).

Figure 3.1: Add an entry for a router in a RADIUS server



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 an administrative user before authorization is enabled. Failure to do so immediately locks the administrator out of the system.

Listing 19: Authorization

```
aaa new-models
username ADMIN algorithm-type scrypt secret Str0ng5rPa55w0rd
aaa authorization exec default group tacacs+
line vty 0 4
        authorization exec default
```

Instead of `exec` (For starting an exec mode), you can specify another types of commands or services such as `network` (network services such as PPP), or `commands <level>` (exec commands).

Listing 20: Accounting Configuration

```
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.

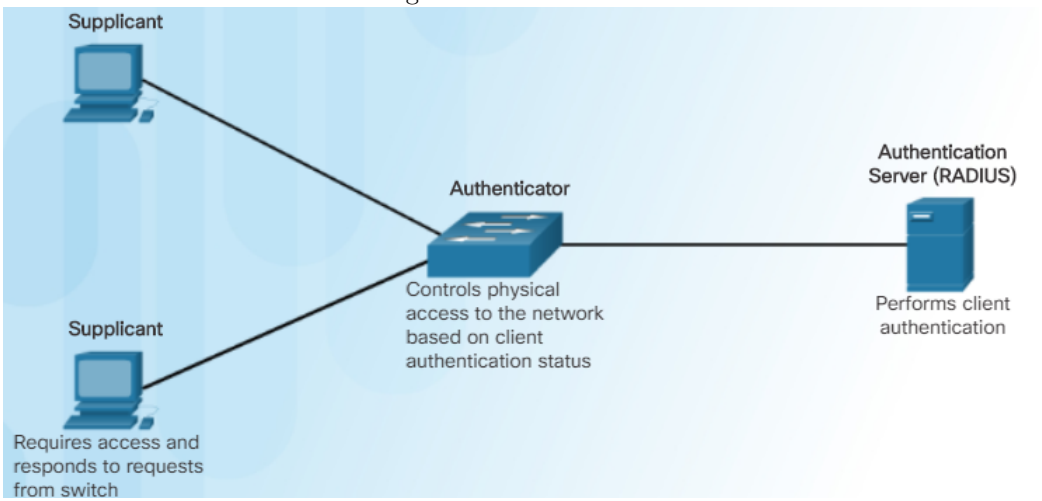
3.3 802.1X Port-Based Authentication

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 3.2 shows that with 802.1X port-based authentication roles:

- **Supplicants** are users' devices, which must have 802.1X-compliant client software.
- **Authenticators** are usually switches, which act as intermediary (proxy) between the supplicants and the authentication server. It uses a RADIUS software agent, which encapsulates and de-encapsulates the EAP frames to interact with the authentication server.
- **The authentication server** authenticates the client and notifies the switch to enable or disable access. Because the switch acts as the proxy, the authentication service is transparent to the client.

Figure 3.2: 802.1X roles



While in *unauthorized 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 link state of the switch port changes from up to down, the switch port transitions to the unauthorized 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.

Listing 21: 802.1X configuration

```
aaa new-models
radius server Server-R
  address ipv4 192.168.1.101 auth-port 1812 acct-port 1813
  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
```

We create an 802.1X port-based authentication method list using the `dot1x` key word. In interface configuration mode, the `authentication port-control auto` command enables 802.1X authentication. This command has two more options, `force-authorized` and `force-unauthorize`, which disable 802.1X authentication. The first option causes the port to remain authorized and allow normal traffic, while the second puts the port in unauthorized state and lock all authentication.

Chapter 4

Firewall

For ACL, take a look at chapter ACL in Notebook folder.

4.1 Background

4.1.1 Packet filtering

Basic packet filtering firewalls can only filter based on Layer 3 and sometimes basic Layer 4 information.

Benefits: Cheap, Simple implementation, Low impact on network performance.

Limitations: Cannot prevent IP spoofing, Complex ACLs, *Stateless* (examine each packet individually rather than in the context of the state of a connection).

4.1.2 Statefull firewall

Stateful firewall examine each packet in the context of the state of a connection. Stateful firewalls use a state table to keep track of the communication process.

Benefits: Prevent spoofing and DoS attacks.

Limitations: Cannot prevent UDP, ICMP, and layer 7 attacks; No authentication; Cannot detect dynamic port negotiation.

4.1.3 DMZ

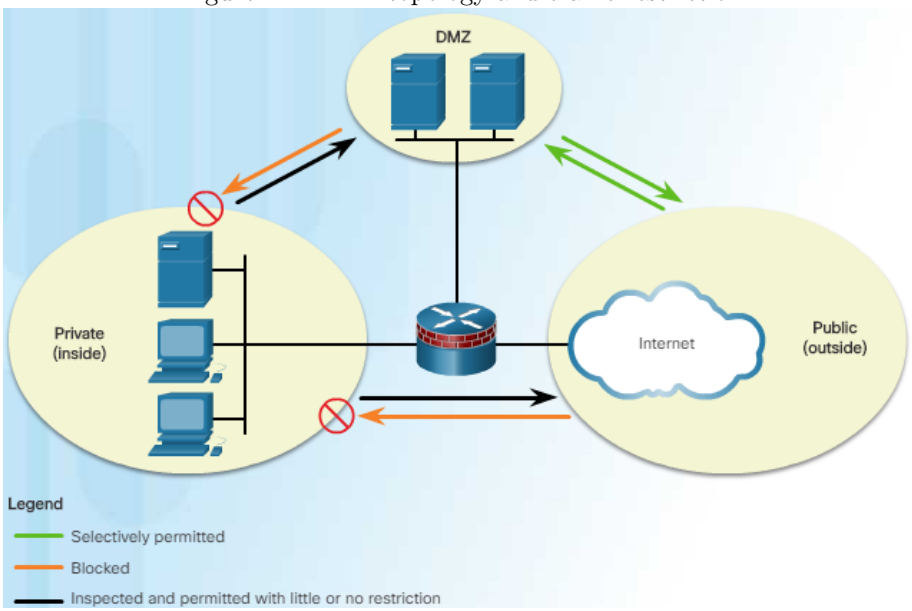
A demilitarized zone (DMZ) is a firewall design where there is typically one inside interface connected to the private network, one outside interface connected to the public network, and one DMZ interfac. As shown in the figure 4.1, all traffic towards internal network is denied, however, traffic originating from internal network can flow freely to other zones. Communication between the Internet and DMZ is selective permitted.

4.2 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. The Classic Firewall applies firewall policy to interfaces.

Classic Firewall creates temporary ACE 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

Figure 4.1: DMZ topology and traffic restriction



is reached.

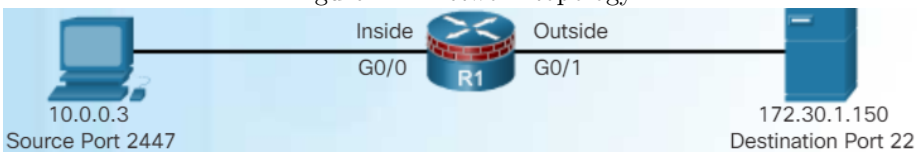
Take the topology in figure 4.2 as an example for configuration. Suppose that the administrator wants to allow SSH sessions (in one direction) from 10.0.0.0/24 network to 172.30.0.0/24 network:

1. You have to define the internal and external interfaces. In this case, g0/0 is the inside and g0/1 is the outside interface.

2. Each interface is configured with an access list. The INSIDE access list for inside interface g0/0 allows only SSH traffic initiated from the 10.0.0.0/24 network. The OUTSIDE access list denies all traffic go into outside interface.

3. Next we define a rule FWRULE that inspect SSH connection originating from 10.0.0.0/24 network, then apply it to inside interface g0/0. With this rule, whenever an SSH communication is initiated from a host in 10.0.0.0/24 network, an ACE is created on the outside interface to allow the return SSH traffic go through the firewall.

Figure 4.2: Network topology



Listing 22: Classic Firewall configuration

```
ip inspect name FWRULE ssh
ip access-list extended INSIDE
        permit tcp 10.0.0.0 0.0.0.255 any eq 22
        deny ip any any
        exit
ip access-list extended OUTSIDE
        deny ip any any
        exit
int g0/0
        ip access-group INSIDE in
        ip inspect FWRULE in
        exit
int g0/1
        ip access-group OUTSIDE in
```

4.3 Zone-based Policy Firewall (ZPF)

4.3.1 Introduction

Zone-Based Policy Firewall applies firewall policy to zones[1]. By default, the traffic between interfaces in the same zone passes freely. However, all zone-to-zone traffic is blocked or filtered by ZPF policies configured on each zone.

Self zone (the router itself) is a special zone that includes all the router interfaces. Any traffic is allowed to go through self-zone to reach another zone. Only packets destined to and sourced from the router (routing protocol messages, SSH packets, etc.) is restricted by policy.

An interface cannot belong to multiple zones. Traffic can never flow between an interface assigned to a zone and an interface without a zone assignment.

Table 4.1: Compare Classic Firewall and ZPF operation

Content	**Classic firewall**	**ZPF**
Only prevent attacks that travel through the firewall	•	
Require multiple ACLs and inspection actions	•	
Not dependent on ACLs		•
One policy affects any given traffic		•
Firewall policy is applied on interfaces	•	
Firewall policy is applied on zones		•
Examine connections for embedded NAT and PAT and perform address translation	•	
The default policy is to block unless explicitly allowed		•

[1] A zone is a group of one or more interfaces.

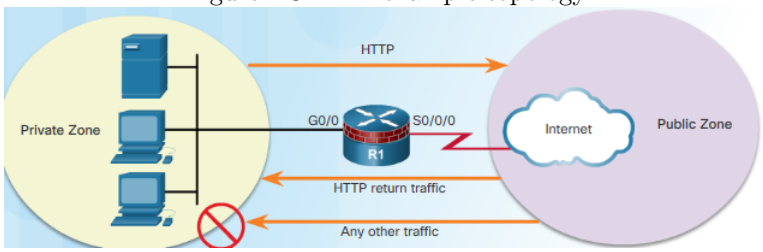
4.3.2 Configuration

We need to enable Security Technology package before configuring ZPF. This can be done by using the command `license boot module c1900 technology-package securityk9` . After the enabling the package, save the running configuration and reload the router. Verify that the Security Technology package has been enabled by using the `show version` command.

Take the topology in figure 4.3 as an example for configuration. The ZPF we are going to specify has to meet the following requirements:

- 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.
- Any HTTP, HTTPS, and DNS traffic from the PRIVATE zone to PUBLIC zone will be inspected.

Figure 4.3: ZPF example topology



Step 1. Create a policy

First of all, we need to specify which traffic between two zones we should inspect. To do this, we assign either pre-defined ACL or protocol port numbers or both to a class-map. In this example, all traffics originating from 192.168.3.0/24 network are defined in access list 100 and class-map PRIVATE-ACL-CLASS. Any traffic that utilizes HTTP, HTTPS, DNS protocol are assigned to the class-map PRIVATE-INTERNET-CLASS.

The next step is to create the policy that decides what to do witch each class-map. In this example, both class-maps we created are inspected.

Listing 23: Create a ZPF policy

```
access-list 100 permit ip 192.168.3.0 0.0.0.255 any
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
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
```

There are three action available for dealing with each traffic

- `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.

Step 2. Create zones

In this topology, we have two interfaces, two zones, and traffic flowing in one direction.

Listing 24: Create zones

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

Step 3. Match zone pair and policy

Listing 25: Match zone pair and policy

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

Verification

Listing 26: 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
```

Chapter 5

Intrusion Prevention System (IPS)

5.1 Introduction

5.1.1 Intrusion Detection Systems (IDSs)

IDS copies the actual traffic stream and analyzes the copied traffic. IDS works in offline mode, which means several things:

- IDS passively monitor network traffic without preventing attacks.
- 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

Advantage: No impact on the network (delay, jitter). **Disadvantage:** cannot stop malicious packets, cannot correct tuning required for response action.

5.1.2 Intrusion Prevention System (IPS)

Unlike IDS, IPS is implemented in inline mode. This means that all ingress and egress traffic must flow through it for processing. IPS can detect and immediately solve a network problem.

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

5.1.3 Compare IDS and IPS

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. However, IDS and IPS 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.

5.1.4 IPS technologies

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

Network-based IPS devices are implemented at designated network points that enable security managers to monitor network activity while it is occurring, regardless of the location of the attack target. 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 has to install HIPS.

5.2 Signatures

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

To make the scanning of signatures more efficient, Cisco IOS software relies on signature micro-engines (SMEs), which categorize common signatures in groups. When IDS or IPS is enabled, an SME is loaded to the router. SME then scans atomic and composite packets, then extracts values from those packets and uses them to search for multiple patterns at the same time.

Signatures have three distinctive attributes: Type, Trigger (alarm), Action.

5.2.1 Type

Signature types are generally categorized as atomic or composite.

An **atomic signature** can be matched on a single event. Examining theses signatures does not require a state information (stateless) and consumes minimal resources.

A **composite signature** is a stateful signature which identifies a sequence of events. Maintaining state, therefore, is required. The length of time that the signatures must maintain state is known as the event horizon.

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

SME (signature micro-engine) categorizes signatures in group and scans 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[3] found in a signature.

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 Trigger

A signature trigger could be anything that signals an intrusion or security policy violation. There are four types of triggering mechanisms listed below:

- **Pattern-based detection** (signature-based detection) compares the network traffic to a database of known attacks.
- **Anomaly-based detection** (profile-based detection) involves first defining a profile of what is considered normal traffic, then detecting malicious operations based on this predefined profile. **Advantage:** unknown attacks can be detected. **Disadvantage:** Attack activity may be defined as normal traffic.

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

- **Policy-based detection** (behavior-based detection) defines suspicious behaviors based on historical analysis. This technique 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. Antivirus and other security vendors tend to use them for research.

- **Protocol decodes** breaks down a packet into the fields of a protocol, and then searches for specific patterns in each field. **Advantage**: more granular inspection of traffic and small number of false positives.

Triggering mechanisms mentioned above can generate alarms (table 5.1). A true alarm is the expected outcome. In other words, we would like that intrusion system can generate an alarm in response to known attack traffic (**true positive**) and be silent when the network is safe (**true negative**). However, there may be some undesired result. For example, intrusion system fails to generate an alarm after processing attack traffic (**false negative**), or mistakes normal traffic from malicious and generates alarm (**false positive**).

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

When a signature detects the activity for which it is configured, the signature triggers one or more actions.

Generate an alert. There are two categories of alert: atomic and summary alert. 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 (drop): this action can be expanded to drop all packets for a specific connection or even all packets from a specific host for a certain amount of time. By dropping traffic for a connection or host, the IPS conserves resources without having to analyze each packet separately.

Resetting a TCP connection: Many IPS devices use the TCP reset action to abruptly end a TCP connection that is performing unwanted operations.

Blocking future activity 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.

Allowing the Activity: this action is necessary so that an administrator can define exceptions to configured signatures. For example, suppose that the IT department routinely scans its network to find security hole.

5.3 Monitoring and management

5.3.1 Monitoring strategy

There are four factors to consider when implementing a monitoring strategy: Management method, Event correlation, Security staff, and Incident response plan. Event correlation refers to the process of correlating events happening at different points across a network based on time stamp.

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

Alarms are generated when an enabled signature is triggered. These alarms are stored on the sensor and sent to the administrator using either Syslog or Secure Device Event Exchange (SDEE) protocol. A message generated by SDEE protocol will look like as follow:

```
%IPS-4-SIGNATURE:Sig:1107 Subsig:0 Sev:2 RFC1918 address [192.168.121.1:137 ->192.168.121.255:137]
```

5.3.2 Global Correlation and SensorBase Network

Cisco Global Correlation provides regular threat updates to IPS sensors from a database called the Cisco SensorBase Network, which has information about IP addresses with a reputation. The sensor uses this information to determine harmful traffic.

Communication between sensors and the SensorBase Network involves an HTTPS request and response over TCP/IP. There are three modes for sensor to participate SensorBase Network: off, partial participation, and full participation.

The SensorBase Network is part of a Cisco Security Intelligence Operation (SIO), a security intelligence ecosystem that baselines the current state of threats on a worldwide basis. SIO provides live threat prevention based on malware outbreaks, current vulnerabilities, and zero-day attacks.

5.4 IPS configuration on CLI

Preparation

Prior to configuring IPS, it is necessary to download the signature files `IOS-Sxxx-CLI.pkg`, and a public crypto key `realm-cisco.pub.key.txt` from cisco.com. Only registered customers can download the package files and key.

Next, we use `mkdir <dir-name>` command to create a directory in flash, for example `flash:IPS`, to store the signature file. After that, we paste the content of `realm-cisco.pub.key.txt` file to the router at the global configuration prompt. This 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.

If you want to use SDEE for logging notification, the HTTP or HTTPS server must first be enabled (`ip http server` or `ip https server` command), then use 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. The number of events stored in RAM can be altered with the `ip sdee events <num>` command. If you prefer traditional syslog, use the `ip ips notify log` command.

The location of signature files is required so that IPS knows where to search for threat patterns. IPS configuration first involves creating a rule associated with an optional access list. All traffic that is permitted by the ACL is subject to inspection by the IPS.

Listing 27: IPS preparation

```
mkdir flash:IPS
no crypto key pubkey-chain rsa
no named-key realm-cisco.pub signature

<Script from realm-cisco.pub.key.txt>

ip https server
ip ips notify sdee
ip ips config location flash:IPS
ip ips name IOSIPS list ALLOW-HTTP
```

Signature category

All signatures are grouped into three categories: `all`, `basic`, and `advanced`. These signatures can be retired or unretired. **Retiring** a signature means that IPS does not compile that signature into memory for scanning. **Unretiring** a signature instructs IPS to compile the signature into memory and use it to scan traffic.

Do not unretire the `all` category, because IPS cannot compile and use all the signatures at one time because it will run out of memory. Instead, you should retire `all` category before selecting any desired category.

IPS processes the signature category commands in the order listed in the configuration. If multiple categories are configured and a signature belongs to more than one of them, only the last configured category matters.

Listing 28: IPS category

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

interface g0/0
  ip ips IOSIPS in
interface g0/1
  ip ips IOSIPS in
  ip ips IOSIPS out
  end
show ip ips all
show ip ips signature count
```

5.4.1 Modification

The command `ip ips signature-definition` is used to modify a specific signature, including retire/unretire and event action.

Listing 29: Retire a specific signature

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

Listing 30: 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
```

Listing 31: 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
```

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.

Chapter 6

Endpoint security

6.1 Endpoint security solutions

Protecting endpoints in a borderless network can be accomplished using the following modern security solutions: Advanced Malware Protection (AMP), Email Security Appliance (ESA), Web Security Appliances (WSA), and Network Admission Control (NAC).
AMP defeats malware across the extended network before, during, and after an attack. AMP for Endpoints integrates with AMP for Networks to deliver comprehensive protection across extended networks and endpoints.

ESA fights spam, viruses, and blended threats. The Cisco ESA is constantly updated by real-time feeds from the Cisco Talos. Some of the main features and benefits of ESA: Global threat intelligence, Spam blocking, integrated with AMP, and Outbound message control.

WSA controls over how users access the Internet. It performs blacklisting, URL-filtering, malware scanning, Web application filtering, and TLS/SSL encryption and decryption. These are some of the main features and benefits of WSA: AMP, Data Loss Prevention (DLP), Talos security intelligence, and Web usage control.

Cloud Web Security (CWS) is a cloud-based security service that uses web proxies in Cisco's cloud environment to scan traffic. Cisco devices can connect to CWS using a proxy autoconfiguration (PAC) file or through connectors integrated into four Cisco products: ISR G2 routers, ASA, WSA, and AnyConnect Secure Mobility Client.

NAC allows only authorized and compliant systems to access the network by providing authentication, authorization, and posture assessment. NACs are evolving to become more sophisticated endpoint visibility, access, and security (EVAS) controls.

There are two categories of Cisco NAC products: NAC framework and NAC appliance. The NAC framework uses the existing network infrastructure and third-party software to enforce security policy. The NAC Appliance incorporates NAC functions into an appliance.

NAC has three components: Manager, Server, and Agent. NAC Manager defines role-based user access and endpoint security policies. NAC Server (NAS) assesses and enforces security policy compliance. NAC Agent (NAA), which runs on an endpoint device, performs deep inspection of the device's security profile.

These are two additional TrustSec Policy enforcement tools for NAC: guest server and profiler. Guest server enforces guest network policy to either NAC appliance or Wireless LAN controller. It also provides the ability to create guest accounts.

On the other hand, NAC profiler enables the dynamic discovery, identification, and monitoring of all network-attached endpoints. It has two components: Collector and Server. Profiler server aggregates information from Collector and stores it in a database, then provisions the appropriate access decisions.

- Advanced Malware Protection (AMP) d

- Email Security Appliance (ESA) = SPAM filtering

- Web Security Appliances (WSA) = Blacklisting and URL filtering. WSA is a secure web gateway which combines AMP, application visibility and control, acceptable use policy controls, reporting, and secure mobility functions.

- Network Admission Control (NAC) = Data loss prevention.

- Cisco Cloud Web Security (CWS) is a cloud-based security service that uses web proxies in Cisco's cloud environment to scan traffic for malware and policy enforcement. Cisco customers can connect to the Cisco CWS service through connectors integrated into four Cisco products: ASA, WSA, ISR G2 routers, and AnyConnect Secure Mobility Client.

6.2 CAM table attack

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. When this occurs, the switch treats the frame as an unknown unicast and begins to flood all incoming traffic to all ports. We prevent CAM table overflow using **port security** on access port.

The type of secure address can be Static, or Dynamic, or Sticky. Static secure MAC addresses are manually configured by the administrator and they are stored in both CAM table and running configuration. On the other hand, switches learn Dynamic addresses automatically but only keeps them in CAM table. Because CAM table locates in RAM, Dynamic addresses are removed when the switch restarts.

Sticky is the combination of static and dynamic types. Like static addresses, sticky addresses are stored in the address table and running configuration. Sticky learning is dynamic just like Dynamic type. Additionally, the switch converts all learned MAC addresses into sticky addresses. If sticky learning is disabled, the sticky secure MAC addresses remain part of the address table but are removed from the running configuration.

Listing 32: Enable port security

```
int g0/0
        sw mode access
        sw port-security
        sw port-security mac-address sticky
        end
show port-security
show port-security interface g0/0
```

A security **violation** describes a situation when an unknown MAC address attempts to access an interface with port security configured. Whenever a violation occurs, the switch drops all frames associated with malicious MAC addresses. There are three violation modes: Protect, Restrict, and Shutdown. Only Shutdown mode is capable of putting port into error-disabled state. A detection of violation forces both Shutdown and Restrict mode send syslog message and increase violation counter. However, this is not the case for Protect mode.

You can bring a port in error-disabled state back to normal by entering `shutdown` followed by `no shutdown` command.

Listing 33: Additional port security

```
int g0/0
        sw port-security max 2
        sw port-security violation mode shutdown
        sw port-security aging time 10
        sw port-security aging type inactivity
        exit
mac address-table notification
```

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

We use Port aging to remove secure MAC addresses on a secure port without manually deleting the existing secure MAC addresses. Two types of aging are supported per port: Absolute and Inactivity. Absolute aging deletes an address after the specified time, while Inactivity aging removes ports that is sleeping more than a specified of time.

The **MAC address notification** feature sends SNMP trap whenever a new MAC address is added to, or an old address is deleted from the CAM tables. This feature is only available for dynamic and secure MAC addresses.

6.3 VLAN attacks

6.3.1 VLAN hopping and double-tagging

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 or Introducing a rogue switch. Another type of VLAN attack is double-tagging. This attack method adds a hidden 802.1Q tag inside the frame which allows the frame to go to another VLAN. This attack works even if trunk ports are disabled.

The best way to prevent basic these attacks:

- Manually enable trunking and access ports
- Disable DTP on trunking ports using the `sw non-negotiate` , on non-trunking port using `sw mode access` .
- Set the native VLAN to be something other than VLAN 1
- Be sure that native VLAN is only used for trunk lines.
- Disable unused ports and put them in an unused VLAN.
- Implement Private VLAN

6.3.2 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): promiscuous, isolated, and community. A promiscuous port (often connected to the router) can talk to everyone. Community ports can talk to ports in the same community and promiscuous ports. An isolated port can only talk to promiscuous 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 6.1: PVLANs – promiscuous ports, isolated ports, community ports

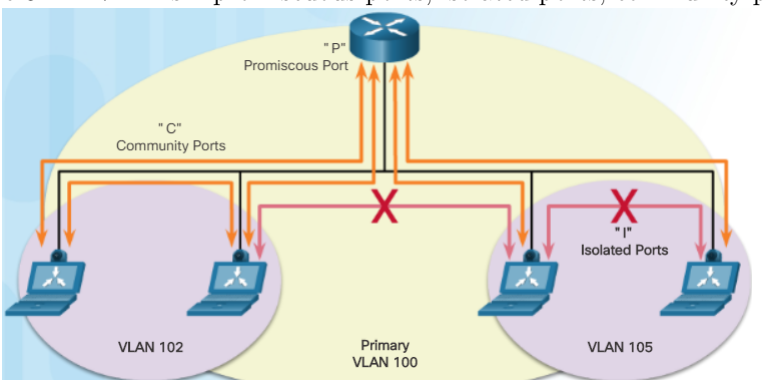
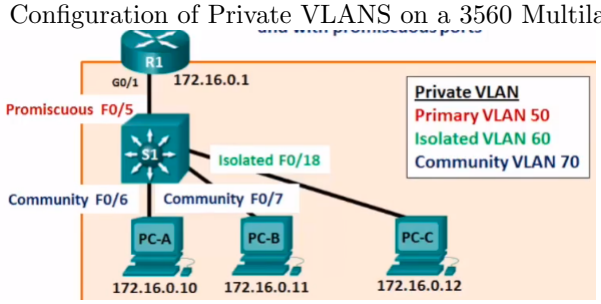


Figure 6.2: Configuration of Private VLANS on a 3560 Multilayer switch



Listing 34: 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

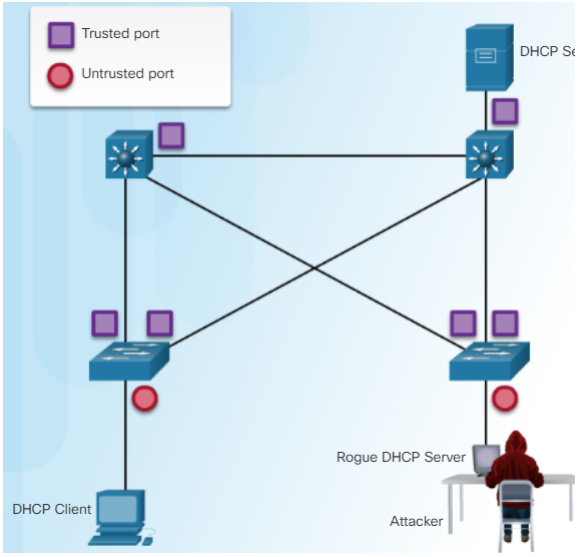
ports. Hosts connected to Protected ports will not be able to communicate with each other, but can only talk with un-Protected ports.

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 35: 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 36: 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.

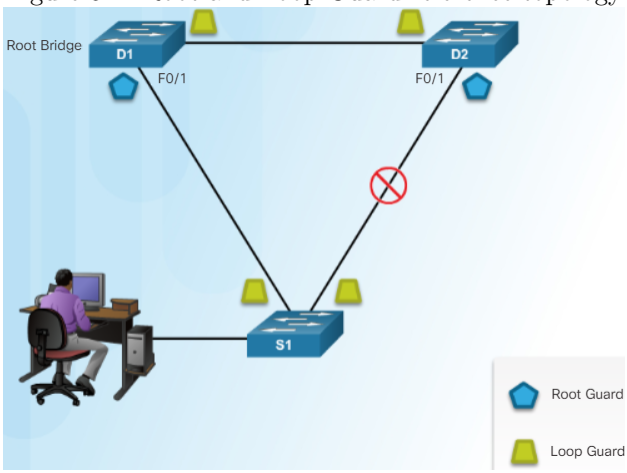
6.7.3 Root Guard

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.

Figure 6.4: Root and Loop Guard reference topology



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.

Root guard in conjunction with PortFast, and BPDU guard is used to prevent an STP manipulation attack.

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.

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

Chapter 7

Cryptography

Authentication, Integrity, and Confidentiality are the three objectives of secure communications. Authentication guarantees that a message comes from the source that it claims to come from. Integrity ensures that messages are not altered in transit. Confidentiality ensures so that only the receiver can read the message.

Encryption and hashing are used to make certain that only authorized entities can read the message (Confidentiality). The receiver can verify that the received message is identical to the sent message and that no manipulation occurred (Integrity).

7.1 Hash function

A hash function takes the message and produces a fixed-length and condensed bit string, called the hash value or message digest. Hashing is based on a one-way mathematical function that is relatively easy to compute, but significantly harder to reverse. The cryptographic hashing function can provide proof of authenticity (IPsec, routing protocol, CHAP) and message integrity check proof.

MD5 produces a 128-bit hashed message digest and is now considered a legacy algorithm.

The SHA-1 algorithm produces a 160-bit message digest and is slightly slower than MD5, but the larger message digest makes it more secure against brute-force collision and inversion attacks. SHA-1 is now considered to be a legacy algorithm. It is recommended to use the SHA-2 family of hash functions, which are SHA-224 (224 bit), SHA-256 (256 bit), SHA-384 (384 bit), SHA-512 (512 bit).

A keyed-hash message authentication code (HMAC or KHMAC) use a secret key as input to the hash function. This adds authentication to integrity assurance. The mechanism of HMAC is that two parties share a secret key and use HMAC functions for authentication. Only parties who have access to that secret key can compute the digest of an HMAC function. This characteristic defeats man-in-the-middle attacks. Cisco technologies use two well-known HMAC functions: legacy Keyed MD5 (HMAC-MD5) and Keyed SHA-1 (HMAC-SHA-1).

Two terms that are used to describe keys are: Key length (key size) and Keyspace (the number of possibilities that can be generated by a specific key length). As key length increase, the keyspace increases exponentially, which affects the time it takes to crack the code. Longer keys are more secure; however, they are also more resource intensive.

7.2 Encryption

Cryptographic encryption can provide confidentiality at several layers of the OSI model. For example, the IPsec for network layer protocols. Secure Sockets Layer (SSL) or Transport Layer Security (TLS), provide session layer confidentiality. MD5, Keyed MD5, and Secure Hash Algorithm 1 are examples of hash functions. They provide data integrity but not data confidentiality.

There are two classes of encryption algorithms: Symmetric algorithms and Asymmetric algorithms.

7.2.1 Symmetric algorithms

Symmetric algorithms use the same pre-shared key on both parties and the key is shorter, meaning faster execution. The encryption and decryption keys are the same. The sender and the receiver must exchange the secret key using a secure channel before any encryption can occur. By obtaining the key, anyone can encrypt and decrypt messages. DES, 3DES, AES, Software Encryption Algorithm (SEAL), and the Rivest ciphers (RC) series are all well-known encryption algorithms that use symmetric keys.

The most commonly used techniques in symmetric encryption cryptography are block ciphers and stream ciphers. Block ciphers transform a fixed-length block of plaintext into a common block of ciphertext of 64 or 128 bits. Unlike block ciphers, stream ciphers encrypt plaintext one byte or one bit at a time.

Two main criteria that should be considered when selecting an encryption algorithm for an organization: The algorithm is trusted by the cryptographic community, The algorithm adequately protects against brute-force attacks.

One way to increase the DES effective key length is to use the same algorithm with different keys several times in a row. The technique of applying DES three times in a row to a plaintext block is called 3DES. The Cisco IPsec implementation uses DES and 3DES in CBC mode.

Although 3DES is very secure, it is also resource intensive. To better manage resources, AES was chosen to replace DES. It has stronger key and runs faster than DES. Despite these advantages, AES is a relatively young algorithm. A mature algorithm, like 3DES, is always more trusted.

The Software-Optimized Encryption Algorithm (SEAL) is a stream cipher that uses a 160-bit encryption key. Because it is a stream cipher, data to be encrypted is continuously encrypted, which makes it much faster than block ciphers. SEAL has several restrictions: IPsec and Security version IOS are required, The router and the peer must not have hardware IPsec encryption.

The stream cipher RC4 is often used in file encryption products and for secure communications, such as within SSL. It can be implemented insecurely, as in Wired Equivalent Privacy (WEP). RC5 is a fast block cipher that can be used as a drop-in replacement for DES if the block size is set to 64-bit. RC6 is a 128-bit to 256-bit block cipher that is based on RC5 and was designed to meet the requirement of AES.

7.2.2 Asymmetric algorithms

Asymmetric algorithms use different keys to encrypt and decrypt data. One key is called the private key, and the other is the public key. The private key is secret and known only to the user. The public key is openly shared and easily distributed. Secure messages can be exchanged without having to have a pre-shared key. Because neither party has a shared secret, very long key lengths must be used. These algorithms are resource intensive and slower to execute. Some well-known asymmetric algorithms: DH, RSA, DSS, DSA. Asymmetric algorithms are slow, so they are commonly used in low-volume transactions such as making online purchases or logging into a financial website.

Diffie-Hellman (DH) Algorithm allows two computers to generate an identical shared secret on both systems, without having communicated before. To start a DH exchange, both hosts must agree on two nonsecret numbers. The first number is a base number, also called the generator. The second number is a prime number that is used as the modulus. DH is commonly used in IKE (fundamental component of IPsec VPNs), SSL, TLS, and SSH. It is common to use DH algorithm to create and exchange pre-shared keys for symmetric algorithm (3DES or AES).

Digital signatures are commonly used in Code signing and Digital certificate. Code signing verifies the integrity of executable files downloaded from a vendor website. Digital certificates verify the identity of a vendor website and establish an encrypted connection. Digital signatures provide three basic security services: Authenticity, Integrity,

and Nonrepudiation of the transaction[1].

The **Public Key Infrastructure (PKI)** identifies a certificate authority which issues public key (certificates) for asymmetric algorithm. The PKI also identifies the encryption algorithms, levels of security, and distribution policy to users. **X.509** is a well-known standard that defines basic PKI formats. The X.509 version 3 (X.509v3) standard defines the format of a digital certificate. Another important set of PKI standards are the **Public-Key Cryptography Standards (PKCS**). PKCS defines the low-level formats for the secure exchange of arbitrary data, such as an encrypted piece of data or a signed piece of data.

[1]Nonrepudiation uses the unique characteristics of the sender of a message to confirm that the reputed sender is in fact the actual sender.

Chapter 8

IPsec

8.1 VPN

A VPN is a private network that is created over a public network, usually the Internet. A VPN is virtual because 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.

A remote-access VPN is not statically set up, but instead allows for dynamically creating, changing, and terminating connection. Using remote-access VPN, remote host has to install a special VPN software. A site-to-site VPN is statically set up and always active even if network communication is terminated. Site-to-site VPN is transparent to internal hosts.

There are two kinds of VPN topology: Hairpinning and Split tunneling. Hairpinning allows VPN traffic received on a single interface to be routed back out that same interface. Split tunneling allows traffic that originates from a remote-access client to be split according to traffic that must cross a VPN and traffic that is destined for the public Internet.

8.2 IPsec protocols

IPsec is a layer-3 VPN technology which is often used for site-to-site VPN. The IPsec framework uses various protocols and algorithms:

- IPsec protocol: AH, ESP, AH+ESP
- Confidentiality (encryption): DES, 3DES, AES, SEAL
- Integrity (hash): MD5, SHA
- Authentication: PSK, RSA
- Key exchange: DH family

Authentication Header (AH) is IP protocol 51 and does not provide data confidentiality because the data payload is not encrypted. However, AH achieves authenticity applying a keyed one-way hash function (MD5 or SHA) to the packet. The AH function is applied to the entire packet, except for any IP header fields that normally change in transit. That is why AH will not work with NAT.

Encapsulating Security Payload (ESP) is IP protocol 50 and provides data confidentiality, integrity, and authentication. ESP encrypts entire original IP datagram and ESP trailer. Optionally, ESP can also enforce anti-replay protection, which 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.

ESP and AH can be applied to IP packets in two different modes, transport mode and tunnel mode. In 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 not IP address. 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 Internet Key Exchange (IKE) is a key management protocol, which negotiates IPsec security associations (SAs) and enables IPsec secure communications. IKE uses **UDP port 500** to implement key exchange protocols inside the Internet Security Association Key Management Protocol (ISAKMP) framework[1]. Instead of transmitting keys directly across a network, IKE calculates shared keys based on the exchange of a series of data packets.

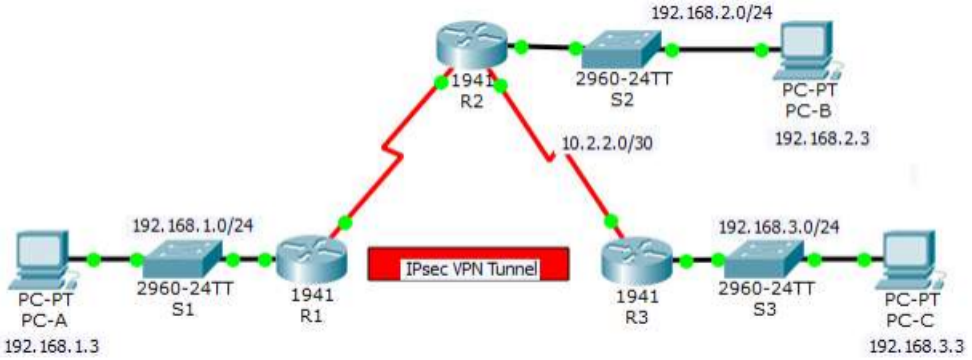
8.3 Operation

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

1. **ISAKMP tunnel:** When host A sends "interesting" traffic to host B, an ISAKMP tunnel is initiated. Traffic is considered interesting when it travels between the peers and meets the criteria that are defined in an ACL.
2. **IKE Phase 1:** The peers negotiate the ISAKMP policy. When the peers agree on the policy and are authenticated, a secure tunnel is created.
3. **IKE Phase 2:** The peers negotiate the IPsec policy using the tunnel in phase 1. In this phase, a separate key exchange is required for each data flow.
4. The IPsec tunnel is created.
5. The IPsec tunnel terminates manually by the user, or when their lifetime expires.

8.4 Site-to-site VPN using IPsec configuration

Figure 8.1: Site-to-site VPN topology



The configuration tasks for the topology in figure 8.1 and addressing table in figure 8.2 are shown in order as below:

1. Enable the Security Technology package and ISAKMP
2. Identify interesting traffic: Configure ACL to permit the traffic from the R1-LAN to R3-LAN. Whenever this traffic is active, VPN is triggered.
3. ISAKMP policy: Use the mnemonic **HAGLE** to remember the five SAs to configure: Hash, Authentication, Group, Lifetime, and Encryption. Note that the address of the peer router R3 is the address of serial interface connected to the Internet (s0/0/0).

[1]ISAKMP defines the message format, key exchange mechanism, and the negotiation process for IPsec.

Figure 8.2: Adressing table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/0	192.168.1.1	255.255.255.0	N/A	S1 F0/1
	S0/0/0 (DCE)	10.1.1.2	255.255.255.252	N/A	N/A
R2	G0/0	192.168.2.1	255.255.255.0	N/A	S2 F0/2
	S0/0/0	10.1.1.1	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.1	255.255.255.252	N/A	N/A
R3	G0/0	192.168.3.1	255.255.255.0	N/A	S3 F0/5
	S0/0/1	10.2.2.2	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/2
PC-B	NIC	192.168.2.3	255.255.255.0	192.168.2.1	S2 F0/1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

4. Transform set: This step is to configure the set of encryption and hashing algorithms that will be used to transform the data sent through the IPsec tunnel. This is called the transform set. In this situation, we create a transform set named VPN-SET that uses an ESP transform with an AES 256 for encryption and SHA for hash. The transform sets on R1 and R3 must match.

5. Create a crypto map VPN-MAP to bind all policy 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 37: Site-to-site IPsec

```
#ENABLE SECURITY FEATURE
license boot module c1900 technology-package securityk9
crypto isakmp enable

#INTERESTING TRAFFIC
access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255

#ISAKMP POLICY
crypto isakmp policy 10
        hash sha
        authentication pre-share
        group 14
        lifetime 3600
        encryption aes 256
        exit
crypto isakmp key vpnpa55 address 10.2.2.2

#TRANSFORM SET
crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac

#CRYPTO MAP
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

#APPLY TO INTERFACE
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 9

ASA Firewall Models

9.1 Introduction

An IOS router firewall solution is appropriate for small network. The Cisco ASA provides dedicated firewall services in one device, which scales well and typically suitable for a large enterprise.

The ASA CLI has a similar look and feel to the Cisco router IOS. Although it shares some common features with the router IOS, it has its unique features. For example, an ASA CLI command can be executed regardless of the current configuration mode prompt. The IOS `do` command is not required or recognized. Different from the router IOS, the ASA provides a `help` command that provides a brief command description and syntax for certain commands.

There are two firewall modes of operation available on ASA devices: Routed and Transparent mode. In routed mode, the ASA is considered to be a router hop and supports multiple interfaces, NAT and applies policy to traffic as they transit a firewall. In transparent mode, ASA functions like a Layer 2 device and is only assigned an IP address on the local network for management purposes. In this mode, ASA does not support QoS, dynamic routing protocols, VPNs, etc.

The ASA assigns **security levels** to distinguish between inside and outside interfaces. The higher the level, the more trusted the interface. The security level numbers range from 0 to 100. Therefore, the interface connecting to the Internet should be assigned the lowest level. The interface connecting to the internal network should be assigned the highest level. The interface connecting to the DMZ network should be assigned a level between them.

When traffic moves from inside interface to outside interface, it is considered outbound traffic. Outbound traffic and return traffic (originating on the inside network) is allowed and inspected by default. Conversely, traffic moving from outside interface to inside interface is considered inbound traffic, which is denied by default. Connectivity between interfaces with the same security levels is blocked by default and only enabled by executing the `same-security-traffic permit inter-interface` global configuration command.

9.2 Basic configuration on ASA 5505

9.2.1 VLAN

With the ASA 5505, the eight integrated switch ports are Layer 2 ports. Therefore, there are two kinds of interfaces that need to be configured: Logical VLAN interfaces and Physical switch ports.

Logical VLAN interfaces are configured with the Layer 3 information including a name, security level, and IP address. The IP address can be configured using one of the following options: manually, DHCP, and PPPoE.

Listing 38: VLAN interfaces

```
int vlan 1
        nameif inside
        security-level 100
        ip address 192.168.1.1 255.255.255.0
int vlan 2
        nameif outside
        security-level 100
        ip address 209.165.200.226 255.255.255.248
        exit
```

By default, all Layer 2 switch ports are assigned to VLAN 1. Therefore, we need to assign all ports connected to internal network to VLAN 1 (inside interface) and the other to VLAN 2 (outside interface). This is done using `sw access vlan vlan-id` interface configuration command.

An ASA 5505 with a Base license does not allow three *fully* functioning VLAN interfaces to be created, but a third *limited* VLAN interface can be created if it is first configured with the `no forward interface vlan` command before the `nameif` command. The Security Plus license is required to have more than two VLANs with full functionality.

9.2.2 DHCP

The ASA 5505 Base license is a 10-user license and therefore the maximum number of DHCP clients supported is 32. To enable an ASA as a DHCP server and provide DHCP services to hosts, use the commands listed below:

Listing 39: DHCP configuration in ASA

```
dhcpd enable inside
dhcpd address 192.168.1.10-192.168.1.54 inside
dhcpd release 1800
show dhcpd ?
```

The `dhcpd auto-config outside` command was issued to enable the DHCP client for outside interface.

9.2.3 Other configurations

A default static route must be configured using the `route outside 0.0.0.0 0.0.0.0 next-hop-ip-address` command.

SSH is required to manage the ASA 5505 remotely, using the CLI. In the following example, AAA authentication is enabled referencing the local database, the RSA crypto key is generated using 2048 bits. Two inside hosts and an outside host are being permitted to access the ASA and SSH version 2 is enabled. The `aaa authentication ssh console LOCAL` command overrides the password set with the password command and authenticates the Telnet access against the local database.

Listing 40: SSH configuration in ASA

```
username ADMIN password class
aaa authentication ssh console LOCAL

crypto key generate rsa modulus 2048

ssh 192.168.1.3 255.255.255.255 inside
ssh 172.16.1.3 255.255.255.255 outside

ssh version 2
end

show ssh
```

Network Time Protocol (NTP) services can be enabled on an ASA to obtain the date and time from an NTP server. To enable NTP, use the global configuration mode commands as follow

Listing 41: NTP in ASA

```
ntp authenticate
ntp trusted-key 1
ntp authentication-key 1 md5 cisco123
ntp server 192.168.1.254
end

show ntp status
show ntp associations
```

9.3 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. In other words, defining object is similar to defining variables in programming. There are two types of objects that can be configured:

- Network object: a single IP address and subnet mask and there are three types: host, subnet, or range. A network object is configured using the `object network <name>` command.
- Service object: a protocol and optional source and/or destination port. A service object is configured using the `object service <name>` command.

Note! Note: A network object is required to configure NAT in ASA image versions 8.3 and higher.

9.3.1 Network object

There can only be one statement in the network object. Entering a second IP address/mask pair replaces the existing configuration. To erase all network objects, use the clear config object network command.

Listing 42: Network object

```
object network ADMIN-HOST
        host 192.168.1.3
        exit
object network INTERNAL
        subnet 192.168.1.0 255.255.255.224
        exit
object network PUBLIC-ADDR
        range 209.165.200.240 209.165.200.248
        exit
show run object network
```

9.3.2 Service object

A service object name can only be associated with one protocol and port (or ports). If an existing service object is configured with a different protocol and port, the new configuration replaces the existing protocol and port with the new ones.

Listing 43: Service object

```
object service WEB
        service tcp destination eq ftp
        service tcp destination eq www
        exit
show run object service
```

9.3.3 Object group

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.

Note! A network object group cannot be used to implement NAT. A network object is required to implement NAT.

Listing 44: Network object group

```
object network LEAD-ADMIN
        host 192.168.1.3
        exit
object-group network ADMIN-HOST
        description Administrative hosts
        network-object LEAD-ADMIN
        network-object host 192.168.1.4
        exit
object-group network INSIDE
        description All inside hosts
        network-object host 192.168.1.32 255.255.255.240
        group-object ADMIN-HOST
        exit
show run object-group
```

Listing 45: ICMP object group

```
object-group icmp-type ICMP-ALLOWED
        icmp-object echo
        icmp-object time-exceeded
        exit
```

Listing 46: Service object group

```
object-group service WEB-PAGE
        service-object tcp destination www
        service-object tcp destination https
        exit
object-group service MAIL tcp
        port-object eq www
        port-object eq smtp
        exit
object-group service DOWNLOAD
        group-object MAIL
        port-object eq ftp
        port-object range 2000 2005
        exit
```

9.4 ACL in ASA

ASA standard ACLs are used to identify the destination IP addresses, unlike IOS ACLs where a standard ACL identifies the source host/network. They are typically only used for OSPF routes and can be used in a route map for OSPF redistribution. Standard ACLs cannot be applied to interfaces to control traffic.

ASA ACLs use the subnet mask in defining a network, whereas IOS ACLs use the wildcard mask.

The ASA supports five types of access lists: Extended, Standard, EtherType, WebType, and IPv6 access lists. An EtherType ACL can be configured only if the security appliance is running in transparent mode. The Webtype ACLs are used in a configuration that supports filtering for clientless SSL VPN users.

Listing 47: Simple ACL in ASA

```
access-list ACL-IN extended permit ip 192.168.1.0 255.255.255.0 209.165.201.0 255.255.255.2
access-group ACL-IN in interface inside
```

Listing 48: ACL with object groups

```
object-group network NET-HOSTS
        network-object host 209.165.201.1
        network-object host 209.165.201.2
        exit
object-group network SERVERS
        network-object host 209.165.202.131
        network-object host 209.165.202.132
        exit
object-group service HTTP-SMTP tcp
        port-object eq smtp
        port-object eq www
        exit
access-list ACL-IN extended permit tcp object-group NET-HOSTS object-group SERVERS object-g
```

9.5 NAT in ASA

Besides normal form of NAT (dynamic NAT, static NAT, PAT), ASA also supports Policy NAT. This kink of NAT is based on a set of rules. These rules can specify that only certain source addresses intended for specific destination addresses and/or specific ports will be translated. For example, policy NAT would be used on an ASA where 10.0.1.0/24 inside addresses are to be translated only if traffic from these addresses is destined for the 198.133.219.0/24 network.

NAT can be deployed on an ASA using one of these methods:

- inside NAT: when a host from a higher-security interface has traffic destined for a lower-security interface and the ASA translates the internal host address to a global address
- outside NAT: when traffic from a lower-security interface destined for a host on the higher-security interface is translated
- bidirectional NAT: when both inside NAT and outside NAT are used together

To configure network object dynamic NAT, two network objects are required. A network object identifying the pool of public IP addresses. The other identifies the internal addresses to be translated and then binds the two objects together. Use the `show xlate` and `show nat detail` commands to verify translations.

Listing 49: Dynamic NAT in ASA

```
object network PUBLIC
        range 209.165.200.240 209.165.200.248
        exit
object network DYNAMIC-NAT
        subnet 192.168.1.0 255.255.255.224
        nat (inside,outside) dynamic PUBLIC
        exit
show xlate
show nat detail
```

When configuring Dynamic PAT, Only one network object is required when overloading the outside interface.

Listing 50: PAT in ASA

```
object network INSIDE-NET
        subnet 192.168.1.0 255.255.255.224
        nat (inside,outside) dynamic interface
```

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

Listing 51: Static NAT in ASA

```
object network DMZ-SERVER
        host 192.168.2.3
        nat (dmz,outside) static 209.165.200.227
        exit

access-list OUTSIDE-DMZ extended permit ip any host 192.168.2.3
access-group OUTSIDE-DMZ in interface outside

access-list ICMPACL extended permit ip any any
access-group ICMPACL in interface dmz

policy-map global_policy
        inspect inspection_default
```

9.6 AAA in ASA

To create a TACACS+ or RADIUS server, use the commands listed below:

Listing 52: Create authentication server in ASA

```
aaa-server TACACS-SEVER protocol tacacs+
        aaa-server TACACS-SEVER (dmz) host 192.168.2.3
        exit
```

To authenticate users who access the ASA CLI over a console, SSH, HTTPS (ASDM), or to authenticate users who access privileged EXEC mode using the following command.

Listing 53: Authenticate users

```
aaa authentication http console TACACS-SERVER LOCAL
aaa authentication enable console TACACS-SERVER LOCAL
aaa authentication ssh console TACACS-SERVER LOCAL
```

9.7 Modular Policy Framework (MPF)

A Modular Policy Framework (MPF) configuration defines a set of rules for applying firewall features, such as traffic inspection and QoS. There are three configuration objects in the MPF; class maps, policy maps, and service policy. The class maps configuration object uses match criteria to identify interesting traffic.

There are four steps to configure MPF on an ASA:

- Configure extended ACLs to identify granular traffic that can be specifically referenced in the class map. For example, ACLs can be used to match TCP traffic, UDP traffic, HTTP traffic, or all traffic to a specific server.
- Configure the class map to identify traffic (figure 9.1.
- Configure a policy map to apply actions to those class maps.
- Configure a service policy to attach the policy map to an interface.

Figure 9.1: Configure the class map to identify traffic

```
CCNAS-ASA(config)# access-list UDP permit udp any any
CCNAS-ASA(config)# access-list TCP permit tcp any any
CCNAS-ASA(config)# access-list SERVER permit ip any host 10.1.1.1
CCNAS-ASA(config)#
CCNAS-ASA(config)# class-map ALL-TCP
CCNAS-ASA(config-cmap)# description "This class-map matches all TCP traffic"
CCNAS-ASA(config-cmap)# match access-list TCP
CCNAS-ASA(config-cmap)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# class-map ALL-UDP
CCNAS-ASA(config-cmap)# description "This class-map matches all UDP traffic"
CCNAS-ASA(config-cmap)# match access-list UDP
CCNAS-ASA(config-cmap)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# class-map ALL-HTTP
CCNAS-ASA(config-cmap)# description "This class-map matches all HTTP traffic"
CCNAS-ASA(config-cmap)# match port TCP eq http
CCNAS-ASA(config-cmap)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# class-map TO-SERVER
CCNAS-ASA(config-cmap)# description "Class map matches traffic  10.1.1.1"
CCNAS-ASA(config-cmap)# match access-list SERVER
CCNAS-ASA(config-cmap)# exit
CCNAS-ASA(config)#
```

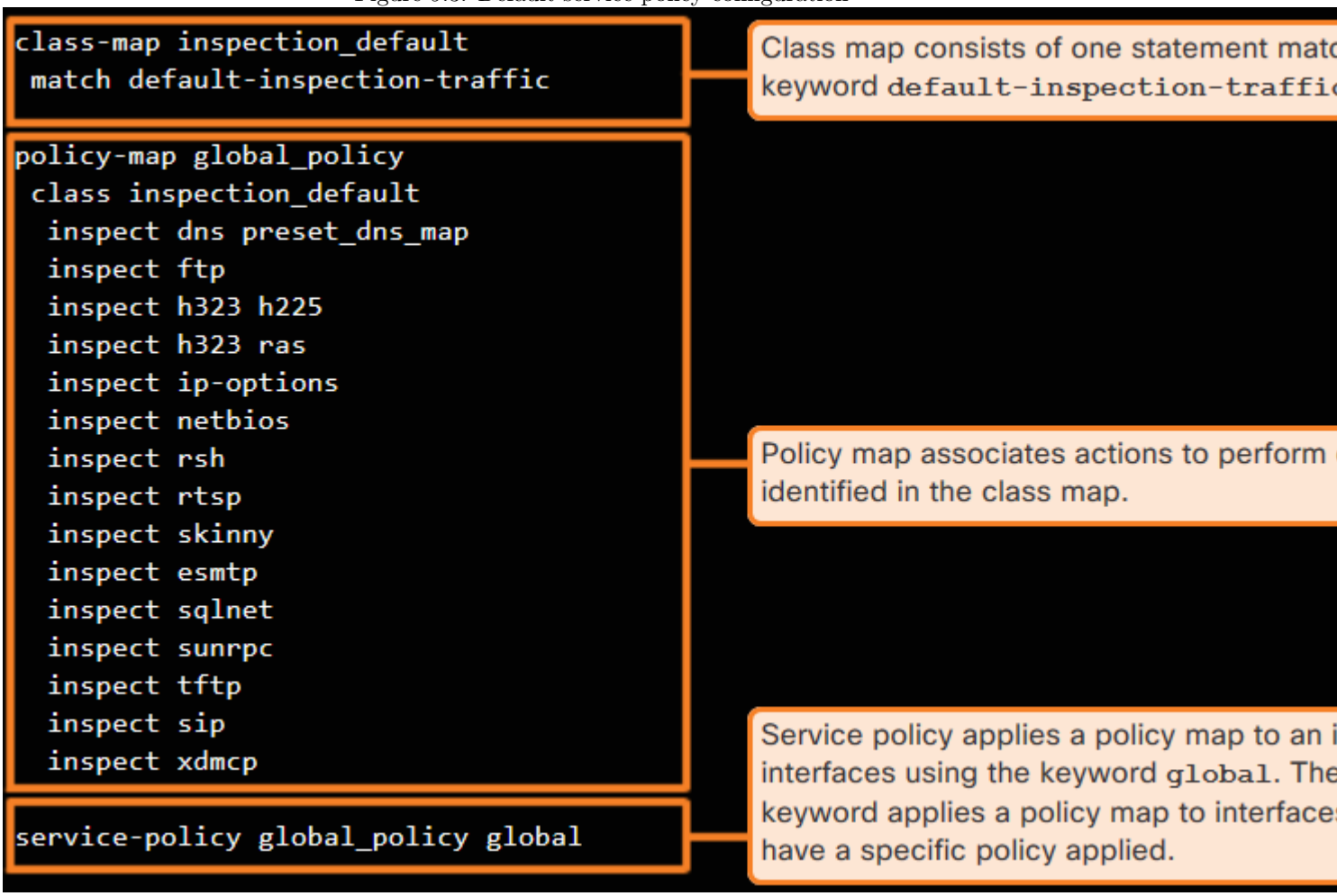
The names `class-default` and any name that begins with `_internal` or `_default` are reserved. The class map name must be unique and can be up to 40 characters in length.

The ASA also automatically defines a default Layer 3/4 class map identified in the configuration by `class-map inspection_defaul`
Identified in this class map is the `match default-inspection-traffic` which matches the default ports for all inspections. When used in a policy map, this class map ensures that the correct inspection is applied to each packet, based on the destination port of the traffic.
Policy maps are used to bind class maps with actions (figure 9.2). The default configuration includes a default Layer 3/4 policy map is called `global_policy` (figure 9.3). This policy performs an inspection on the default inspection traffic. There can only be one global policy. Therefore, to alter the global policy, either edit it or replace it.

Figure 9.2: Create policy map for MPF

```
CCNAS-ASA(config)# access-list TFTP-TRAFFIC permit udp any any eq 69
CCNAS-ASA(config)#
CCNAS-ASA(config)# class-map CLASS-TFTP
CCNAS-ASA(config-cmap)# match access-list TFTP-TRAFFIC
CCNAS-ASA(config-cmap)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# policy-map POLICY-TFTP
CCNAS-ASA(config-pmap)# class CLASS-TFTP
CCNAS-ASA(config-pmap-c)# inspect tftp
CCNAS-ASA(config-pmap-c)# exit
CCNAS-ASA(config-pmap)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# service-policy POLICY-TFTP global
CCNAS-ASA(config)#
```

Figure 9.3: Default service policy configuration



Chapter 10

ASA Security Device Manager (ASDM)

10.1 Starting ASDM

The Cisco ASA can be configured and managed using either the command line interface (CLI) or by using the graphical user interface (GUI) ASA Security Device Manager (ASDM). The CLI is fast but requires more time to learn while ASDM is intuitive and simplifies the ASA configuration. It works with SSL to ensure secure communication with the ASA. It also provides quick-configuration wizards and logging and monitoring functionality that is not available using the CLI.

10.1.1 Password Recovery Procedure

To recover passwords for the ASA, perform the following steps:

1. Connect to the ASA console port and restart the ASA (Power off, and then power it on).
2. After startup, press the Escape key when you are prompted to enter ROMMON mode.
3. In the ROMMON mode, enter the `confreg 0x41` command to update the configuration register value.
4. To set the ASA to ignore the startup configuration, enter `confreg` .

10.1.2 Preparing for ASDM

To enable access to the ASDM, the ASA requires some minimal configurations. Specifically, to prepare for ASDM access on an ASA 5505, the following must be configured:

- Inside logical VLAN interface – Assign the Layer 3 address and the security level.
- Ethernet 0/1 physical port – By default it is assigned to VLAN 1, but must be enabled.
- Enable the ASA Web Server – Disabled by default.
- Permit access to the ASA Web Server – By default, the ASA operates in a closed policy; therefore, all connections to the HTTP server are denied.

The example in Figure 10.1 configures the logical management inside interface with IP address 192.168.1.1. It enables Ethernet 0/1, enables the ASA HTTP server, and permits access from an inside host with IP address 192.168.1.3. To remove and disable the ASA HTTP server service, use the `clear configure http` global configuration mode command.

10.1.3 Install ASDM

To start ASDM, enter the management IP address of the ASA in a web browser from a PC. The ASDM launch window is displayed, as shown in Figure 2, providing two options:

Figure 10.1: Preparing ASDM

```
ciscoasa(config)# interface vlan 1
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
ciscoasa(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
ciscoasa(config-if)# exit
ciscoasa(config)#
ciscoasa(config)# interface Ethernet0/1
ciscoasa(config-if)# no shut
ciscoasa(config-if)# exit
ciscoasa(config)#
ciscoasa(config)# http server enable
ciscoasa(config)# http 192.168.1.3 255.255.255.255 inside
ciscoasa(config)#
```

- **Run Cisco ASDM as a local application** – This provides the **Install ASDM Launcher** option to connect to the ASA from the host's desktop using SSL. The advantage of doing so is that one application can be used to manage several ASA devices, and an Internet browser is not required to start ASDM.
- **Run Cisco ASDM as a Java Web Start application** – This provides the **Run ASDM** option to run the ASDM application. Using an Internet browser is required to establish a connection. ASDM is not installed on the local host. The Run Startup Wizard option can be selected instead. It provides a step-by-step initial configuration similar to the CLI Setup Initialization wizard.

In this example, **Run ASDM** is selected. If security warning appears, click **Continue**. Next a security warning is displayed stating that ASDM could be a security risk. Accept the risk and then click **Run**. ASDM then displays the Cisco ASDM-IDM Launcher. The launcher requests a username and password. Because none were initially configured, leave these fields blank and click **OK**.

Cisco ASDM offers several wizards to help simplify the configuration of the appliance:

- Startup Wizard: Modify existing configuration or to Reset configuration to factory defaults
- VPN Wizards
- Other wizard: High Availability and Scalability Wizard, Unified Communication Wizard, ASDM Identity Certificate Wizard, Packet Capture Wizard

10.2 Basic configuration

The ASDM Configuration view is required to configure most device settings using the following two main tabs:

- **Device Setup:** this tab can be used to configure the hostname, passwords, system time, interface settings, and routing.
- **Device Management:** this tab can be used to configure management access, users and AAA access, DHCP, and more. Specifically, this tab can be used to configure basic management features including legal notification and to create a master passphrase.

Basic ASA settings include a device hostname, enable password, master passphrase, and banner. To configure the ASA hostname, domain name, and enable password, click Configuration ¿ Device Setup ¿ Device Name/Password. To configure a master passphrase and encrypt all passwords, click Configuration ¿ Device Management ¿ Advanced ¿ Master Passphrase. On this page, the master passphrase can be created and enabled to use AES encryption. To configure legal notification, click Configuration ¿ Device Management ¿ Management Access ¿ Command Line (CLI) ¿ Banner. On this page, various banners can be created and edited.

10.2.1 Basic settings

10.3 Advanced configuration

Chapter 11

VPN in ASA