# The Notebook
# of
# CCNA

Huy Bui

PL

THE PUBLISHER

# Contents

## 0.1 List of Codes

# Chapter 1

# Introduction

## 1.1 Securing network

### 1.1.1 Introduction

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

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

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

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

### 1.1.2 Network topology

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

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

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

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

- **Hyperjacking:** An attacker could hijack a VM hypervisor and use it as a starting point to attack other devices.

- **Instant on activation:** A VM that has not been used for a long period of time can introduce security vulnerabilities when activated.
- **Antivirus storm:** Multiple VMs attempt to download antivirus file at the same time

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

- Data encryption
- PIN enforcement
- Data wipe (data in lost devices can be remotely wiped out)
- Data Loss Prevention (DLP): prevent unauthorized users from accessing, prevent authorized users from doing malicious things to critical data
- Detect password bypasses such as Jalibreaking (Apple iOS) or Rooting (Android) and restrict devices' access to network and corporate assets

## 1.2 Network threats

### 1.2.1 Who is a hacker?

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

- Script kiddies – inexperienced hackers running scripts, tools, programs, etc. to cause harm but not for profit
- Vulnerability broker – white hat hackers discover exploits for reward
- Hacktivists – protest against political or social ideas by leaking sensitive information
- Cyber criminals – black hat hackers
- State-sponsored – either white hat or black hat hacker, who steals government secrets, sabotage network, and intelligence; their targets are foreign government, terrorist group, and corporations

### 1.2.2 Malware

A **virus** is malicious code that is attached to executable files which are often legitimate programs. Most viruses require end user *activation*. A simple virus may install itself at the first line of code on an executable file. When activated, the virus might check the disk for other executables so that it can infect all the files it has not yet infected. Most viruses are now *spread* by USB memory drives, CDs, DVDs, network shares, and email. Email viruses are now the most common type of virus.

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

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

- **Enabling vulnerability:** A worm installs itself using an exploit mechanism, such as an email attachment, an executable file, or a Trojan horse.

- **Propagation mechanism:** After gaining access to a device, the worm replicates itself and locates new targets.
- **Payload:** Any malicious code that results in some action is a payload. Most often this is used to create a backdoor to the infected host or create a DoS attack.

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

Some other examples of modern malware:

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

### 1.2.3 Common network attacks

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

**Reconnaissance** is known as information gathering. Hackers use reconnaissance (or recon) attacks to do unauthorized discovery and mapping of systems, services, or vulnerabilities. Some examples of reconnaissance attacks: information query, ping sweep, port scan, Vulnerability Scanners, Exploitation tools.

**Access** attacks exploit known vulnerabilities in authentication services, FTP services, and web services to gain entry to sensitive information. There are five common types of access attacks: Password attack, Trust exploitation, Port redirection, Man-in-the-middle, Buffer overflow, IP, MAC, DHCP Spoofing.

**Social engineering** is an **access attack** that attempts to manipulate individuals into performing actions or divulging confidential information. Specific types of social engineering attacks include:

- Pretexting – a hacker calls an individual and lies to them in an attempt to gain access to privileged data
- Phishing – a malicious party sends a fraudulent email disguised as being from a legitimate, trusted source. The message intends to trick the recipient into installing malware on their device, or into sharing personal or financial information.
- Spam – use spam email to trick a user to click an infected link or download an infected file.
- Tailgating – This is when a hacker quickly follows an authorized person into a secure location. The hacker then has access to a secure area.
- Something for Something (Quid pro quo) – a hacker requests personal information from a party in exchange for something like a free gift.
- Baiting – a hacker leaves a malware-infected physical device, such as a USB flash drive in a public location such as a corporate washroom. The finder finds the device and loads it onto their computer, unintentionally installing the malware.

**Denial-of-Service (DoS)** attacks create interruption of service. They are popular and simple to conduct. There are two major sources of DoS attacks:

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

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

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

## 1.3 Mitigating Threats

### 1.3.1 Cisco SecureX architecture

The Cisco SecureX architecture is designed to provide effective security for any user, using any device, from any location, and at any time. This architecture includes the following five major components:

- **Scanning Engines:** examine the content, authenticate uses, and identify applications.
- **Delivery Mechanisms:** introduce scanning elements into the network, such as a module in switch or router, an image of Cisco security cloud
- **Security Intelligence Operations (SIO):** distinguish good traffic from malicious traffic
- **Policy Management Consoles:** span a single policy definition to multiple enforcement points; separated from the scanners
- **Next-Generation Endpoints:** ties all everything together

A **context-aware scanning element** is a network security device that examines packets on the wire, but also looks at external information to understand the full context of the situation. A context-aware policy uses a simplified descriptive business language to define security policies based on five parameters: person ID, application, device type, location, and access time.

To help keep the Cisco ESA, WSA, ASA, and IPS devices secure, Cisco designed the **Security Intelligence Operations (SIO)**. The SIO is a Cloud-based service that connects global threat information, reputation-based services, and sophisticated analysis, to Cisco network security devices.

### 1.3.2 Mitigating common network attacks

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

**Worms:** They are more network-based than viruses. Worm mitigation requires diligence and coordination on the part of network security professionals. 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:** We can detect Reconnaissance attacks and generate an alarm using *Anti-sniffer* software and hardware tools, Cisco ASA, Cisco ISR. *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:** In general, access attacks can be detected by reviewing logs, bandwidth utilization, and process loads. The use of encrypted or hashed authentication protocols, along with a strong password policy, greatly reduces the probability of successful access attacks. Educate employees about the risks of social engineering, and develop strategies to validate identities.

**DoS attacks:** One of the first signs of a DoS attack is a large number of user complaints about unavailable resources. To minimize the number of attacks, a network utilization software package should be running at all times.

### 1.3.3 Cisco Network Foundation Protection Framework

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

**Control plane** security can be implemented using the following features: *Routing protocol authentication*, *CoPP*, and *AutoSecure*. CoPP (Control Plane Policing) prevents unnecessary traffic from overwhelming the route processor. AutoSecure can lock down the management plane functions and the forwarding plane services and functions of a router.

**Management plane** security can be implemented using the following features:

- Login and password policy
- Present legal notification
- **RBAC** (Role-based access control) restricts user access based on the role of the user. In Cisco IOS, the role-based CLI access feature implements RBAC for router management access.
- Authorize actions
- Enable management access reporting

**Data plane** security can be implemented using *ACLs*, *antispoofing mechanisms*, and *Layer 2 security* features.

- ACLs are used to secure the data plane in a variety of ways: Blocking unwanted traffic or users, Reducing the chance of DoS attacks, Mitigating spoofing attacks, Providing bandwidth control, Classifying traffic to protect the Management and Control planes.
- Layer 2 security tools are integrated into the Cisco Catalyst switches: Port security, DHCP snooping, Dynamic ARP Inspection (DAI), and IP Source Guard.

# Chapter 2

# Securing the network infrastructure

## 2.1 Securing device access

### 2.1.1 Edge router

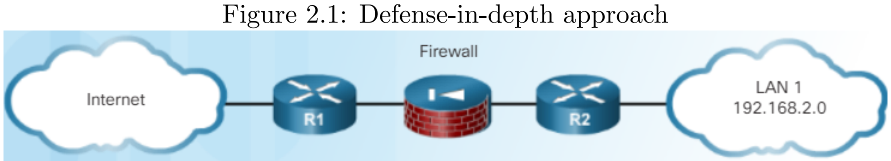
There are many approaches to secure the edge router:

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

Three areas of router security must be maintained:

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

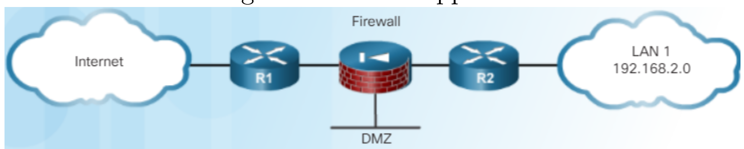
Figure 2.1: Defense-in-depth approach




A router can be accessed for administrative purposes locally or remotely. Local access to a router requires a direct connection to a console port, and using a computer that is running terminal emulation software. The most common remote access method involves allowing SSH, HTTPS, or SNMP connections to the router from a computer. Precautions should be taken when accessing the network remotely:

- Encrypt all traffic between the administrator computer and the router. Use SSH version 2 and HTTPS.

Figure 2.2: DMZ approach




- Establish a dedicated management network
- Configure a packet filter to allow only the identified administration hosts and preferred protocols to access the router.
- Configure and establish a VPN connection to the local network before connecting to a router management interface.

### 2.1.2 Administrative access

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

**Strong password:** On Cisco devices, password-leading spaces are ignored but spaces after the first character are not ignored. One method to create a strong password is to use a blank space in the password or create a phrase made of many words. This is called a *passphrase*. A passphrase is often easier to remember than a complex password and more difficult to guess.

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

**Listing 1: Secret password type 9**

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

### 2.1.3 Virtual logins

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

**Listing 2: Login security commands**

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

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

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

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

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

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

### 2.1.4 Configuring SSH

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

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

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

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

**Listing 3: Configuring SSH**

```
ip domain-name cisco.com

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

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

line vty 0 4
  login local
  transport input ssh

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

sh crypto key mypubkey rsa
sh ssh
```

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

## 2.2 Administrative roles

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

### 2.2.1 Privilege levels

By default, the Cisco IOS software CLI has two levels of access to commands:

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

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

**Listing 4: Privilege level configuration**

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

The use of privilege levels has its limitations:

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

### 2.2.2 Role-based CLI

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

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

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

The following commands show how to create a CLI view:

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

**Listing 6: Superview configuration**

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

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

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

## 2.3 IOS image and Configuration files

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

To secure the IOS image and enable Cisco IOS image resilience, use the `secure boot-image` command. The Cisco IOS image resilience feature can only be disabled through a console session using the no form of the command. This command functions properly only when the system is configured to run an image from a flash drive with an ATA interface. Additionally, the running image must be loaded from secured storage. Images that are loaded from a remote location, such as a TFTP server, cannot be secured.

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

Secured files do not appear in the output of a dir command that is issued from the CLI. This is because the Cisco IOS file system prevents secure files from being listed. Use the `show secure bootset` command to verify the existence of the archive.

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

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

**Listing 7: Restore a primary bootset**

```
Router# reload

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

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

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

**Listing 8: Configure SCP with local AAA**

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

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

ip scp server enable
```

With the above configuration, R1 is now an SCP server and will use SSH connections to accept secure copy transfers from authenticated and authorized users. Transfers can originate from any SCP client (router, switch, or workstation).

For example, you want to transfer a backup file from R2 to R1. On R2, use the copy command. Specify the source file location first `flash0:R2backup.cfg` and then the destination `scp:`. Answer the series of prompts to establish a connection to the SCP server on R1. On R1, you can enter the `debug ip scp` command to watch the transfer proceed.

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

## 2.4 Syslog

### 2.4.1 Introduction

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

- Gather logging information
- Select the type of logging information
- Specify the destination of captured syslog messages

Syslog messages may be sent to an internal buffer. Messages sent to the internal buffer (RAM) are only viewable through the CLI of the device (console line, terminal line). Alternatively, syslog messages may be sent across the network to an external syslog server.

To view syslog messages, a syslog server must be installed on a workstation. One advantage of viewing syslog messages on a syslog server is the ability to perform granular searches through the data. Also, a network administrator can quickly delete unimportant syslog messages from the database.

### 2.4.2 Severity level and Facility

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

Table 2.1: Syslog Severity level

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

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

### 2.4.3 Message format

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

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

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

Table 2.2: Syslog message format

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

### 2.4.4 Configuration

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

**Listing 9: Logging service**

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

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

## 2.5 SNMP

### 2.5.1 Introduction

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

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

**SNMP requests** The SNMP manager uses the get and set actions to perform the operations, as described in the Figure 2.3.

Table 2.3: SNMP operations

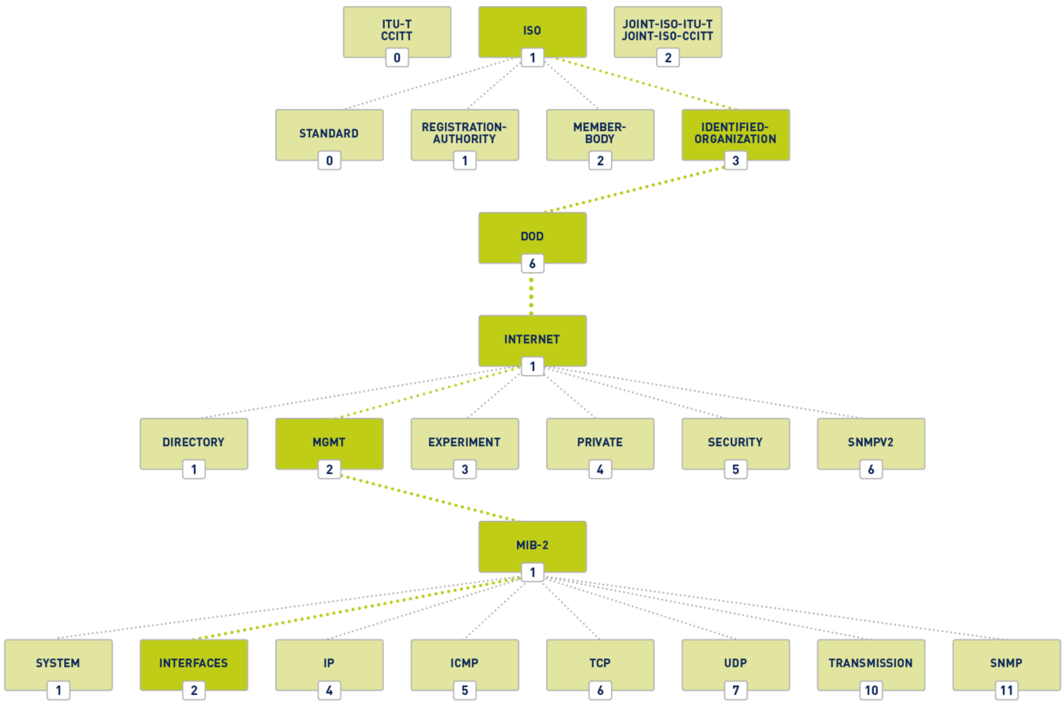
| **Operation** | **Description** |
|---|---|
| `get-request` | Retrieves a value from a specific variable |
| `get-next-request` | Retrieves a value from a variable within a table |
| `get-bulk-request` | Retrieve large block of data such as multiple rows in a table |
| `get-response` | Replies to a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

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

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

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

Figure 2.3: OID tree




### SNMPv2 configuration

Listing 10: SNMPv2 configuration

```
snmp-server community batonaug ro SNMP_ACL

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

show snmp
```

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

## 2.5.2 SNMPv3 configuration

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

**Listing 11: SNMPv3 configuration**

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

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

## 2.6 NTP

### 2.6.1 System clock

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

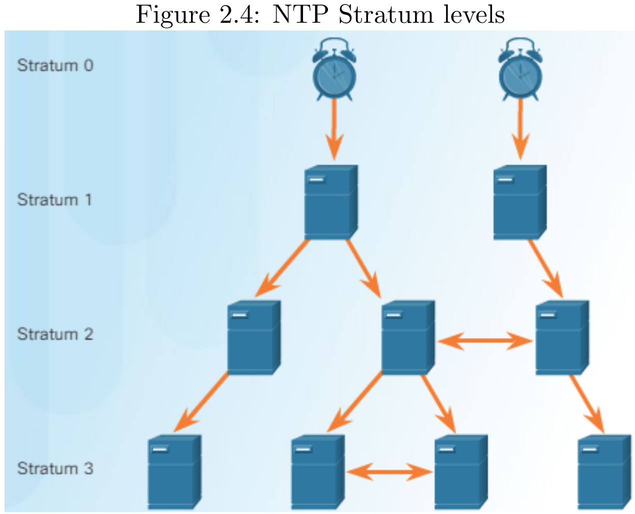
- Manually configure the date and time. For example, `clock set 20:36:00 aug 30 2016`
- Configure the NTP

### 2.6.2 Operation

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

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

Figure 2.4: NTP Stratum levels




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

### 2.6.3 Configuration

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

**Listing 12: NTP authentication**

```
ntp server 192.168.1.5
ntp update-calendar

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

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

## 2.7 Cisco AutoSecure

AutoSecure makes recommendations for fixing security vulnerabilities and then modifies the security configuration of the router. It can lock down the management plane functions and the forwarding plane services and functions of a router. There are several management plane services and functions: firewall inspection, traffic filtering with ACLs, Secure password and login functions, Secure SSH access, Secure NTP, etc.

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

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

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

## 2.8 Control plane security

### 2.8.1 Routing protocol authentication

**Routing Protocol Spoofing:** Routing systems can be attacked by disrupting peer network routers, or by falsifying or spoofing the information carried within the routing protocols. Spoofing routing information may generally be used to cause systems to misinform (lie to) each other, cause a DoS attack, or cause traffic to follow a path it would not normally follow.

**OSPF MD5 Authentication:** OSPF supports routing protocol authentication using MD5 enabled globally for all interfaces or on a per interface basis.

**Listing 13: OSPF interface authentication**

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

**Listing 14: OSPF 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.

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

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

**Listing 15: OSPF SHA authentication**

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

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

### 2.8.2 Control plane policing

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

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

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

# Chapter 3

# AAA model

## 3.1 Introduction

AAA network security services provide the primary framework to set up access control on a network device. AAA is a way to control who is permitted to access a network (authenticate), what they can do while they are there (authorize), and to audit what actions they performed while accessing the network (accounting).
**Authentication:** Cisco provides two common methods of implementing AAA authentication: Local AAA Authentication and Server-Based AAA Authentication. **Local AAA Authentication** uses a local database for authentication. This method stores usernames and passwords locally in the Cisco router. With **Server-Based AAA Authentication**, the central AAA server contains the usernames and password for all users.
**Authorization** is typically implemented using a AAA server-based solution. Authorization uses a created set of attributes that describes the user's access to the network. These attributes are compared to the information contained within the AAA database, and a determination of restrictions. Authorization is implemented immediately and automatically after the user is authenticated.
**Accounting** is implemented using a AAA server-based solution. This service reports usage statistics back to the ACS server.

## 3.2 Local AAA authentication

### 3.2.1 Configuration

Before enabling AAA, at least a local database entry must be configured. To enable AAA, the `aaa new-model` global configuration command must *first* be configured. No other AAA commands are available until this command is entered. The `aaa authentication login` command allows the HUY users to log into the router vty terminal lines. The `default` keyword means that the authentication method applies to all lines (including vty line). However, when the method list `SSH-LOGIN` is applied to vty lines, it overrides the default method. If you want to erase these custom methods `SSH-LOGIN` , use `no authentication login` command.

**Listing 16: Local AAA authentication example**

```
username HUY algorithm-type scrypt secret cisco12345

aaa new-model
aaa authentication login default local-case enable
aaa authentication login SSH-LOGIN local-case

line vty 0 4
login authentication SSH-LOGIN

aaa local authentication attempts max-fail 3
```

Below is the syntax of `aaa authentication login` command. This command lists authentication methods (four methods at the maximum) in the order of execution. In other words, the next listed authentication method is executed only when there is no response or an error from the previous method occurs. The name of this list is specified by the user as `<list-name>` . Table 3.1 shows the command syntax and all available method type keywords.

Table 3.1: AAA login authentication methods

| `aaa authentication login default \| list-name method1 ... method4` | |
|---|---|
| **Keywords** | **Description** |
| `enable` | Use the enable password |
| `local` | Use local username database |
| `local-case` | Use case-sensitive local username database |
| `none` | Ensure that the authentication succeeds even if all methods return an error |
| `group radius` | Use the lists of all RADIUS servers |
| `group tacacs+` | Use the lists of all TACACS+ servers |
| `group <group-name>` | Use a subset of RADIUS or TACACS+ servers |

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

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

## 3.3 Server-based AAA authentication

### 3.3.1 RADIUS vs TACACS+

The Cisco Secure Access Control System (ACS) is a centralized solution that ties together an enterprise's network access policy and identity strategy. Cisco Secure ACS supports both TACACS+ and RADIUS protocols (Table 3.2).

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

**Microsoft Active Directory (AD)** is a directory service for Windows domain networks, and is part of most Windows Server operating systems. The AD domain controller is used to enforce security policies by authenticating and authorizing users when they log into the Windows domain. **Cisco Secure ACS** can be integrated to use the AD service. It supports both TACACS+ and RADIUS. Instead of Cisco Secure ACS, Windows Server can also be configured as a AAA server using RADIUS, known as **NPS (Network Policy Server)**.

### 3.3.2 Identity Services Engine (ISE)

Cisco Identity Services Engine (ISE) is an identity and access control policy platform that enables enterprises to enforce compliance (including *BYOD*), enhance infrastructure security, and streamline their service operations. The architecture of this engine allows administrator to gather real-time information to make proactive governance

Table 3.2: 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) |

decisions by tying identity to various network elements. Cisco ISE combines policy definition, control, and reporting in *one* appliance.

Cisco ISE is the main policy component for **Cisco TrustSec**, which protects end devices from unauthorized access. There are four features in the ISE toolset: AAA, Device profiling, Posture assessment, and Guest assessment.

### 3.3.3 Configuration

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

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

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

**Listing 17: Create a TACACS+ server**

```
aaa new-models

tacacs server Server-T
  address ipv4 192.168.1.101
  single-connection
  key TACACS-Pa55w0rd
```

**Listing 18: Create a RAIDUS server**

```
aaa new-models

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

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

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

When the AAA servers have been identified as shown in the above commands, the servers must be included in the method list of the `aaa authentication login` command. AAA servers are identified using the `group tacacs+` or `group radius` keywords.

**Listing 19: Configure Authentication to Use the AAA Server**

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

The above commands configure a method list for the default login to authenticate first using a TACACS+ server, second with a RADIUS server, and finally with a local username database. It is important to realize that R1 will only attempt to authenticate using RADIUS if the TACACS+ server is not reachable. Likewise, R1 would only attempt to authenticate using the local database if the TACACS+ and RADIUS servers are unavailable.

Troubleshoot Server-based AAA authentication using the following commands: `debug radius` , `debug tacacs` , `debug tacacs events` , and `debug aaa authentication` .

## 3.4 Server-based AAA authorization

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

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

**Listing 20: AAA Authorization Configuration**

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

aaa authorization exec default group tacacs+
```

## 3.5 Server-based AAA accounting

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

**Listing 21: AAA Authorization Configuration**

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

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

The following three parameters are commonly used aaa accounting keywords:

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

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

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

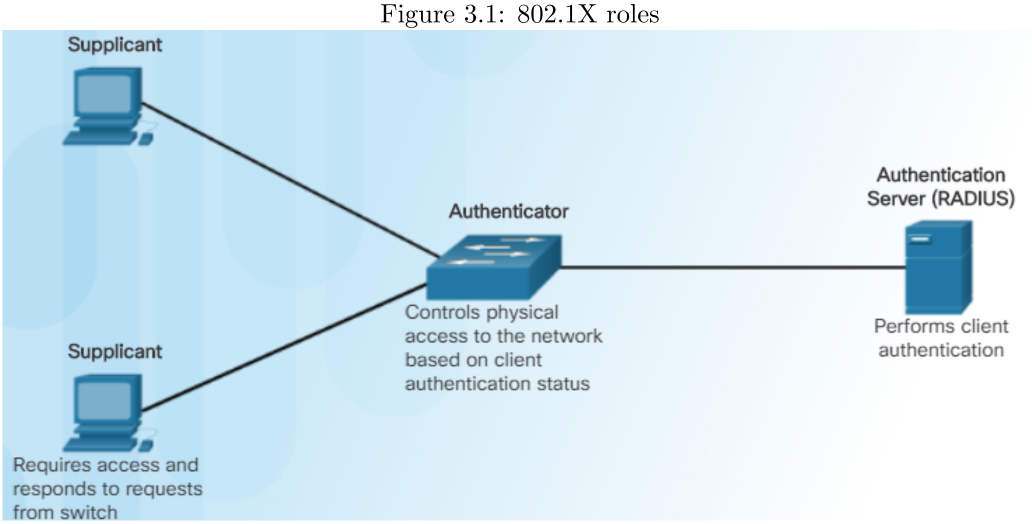
## 3.6 802.1X Port-Based Authentication

### 3.6.1 Operation

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

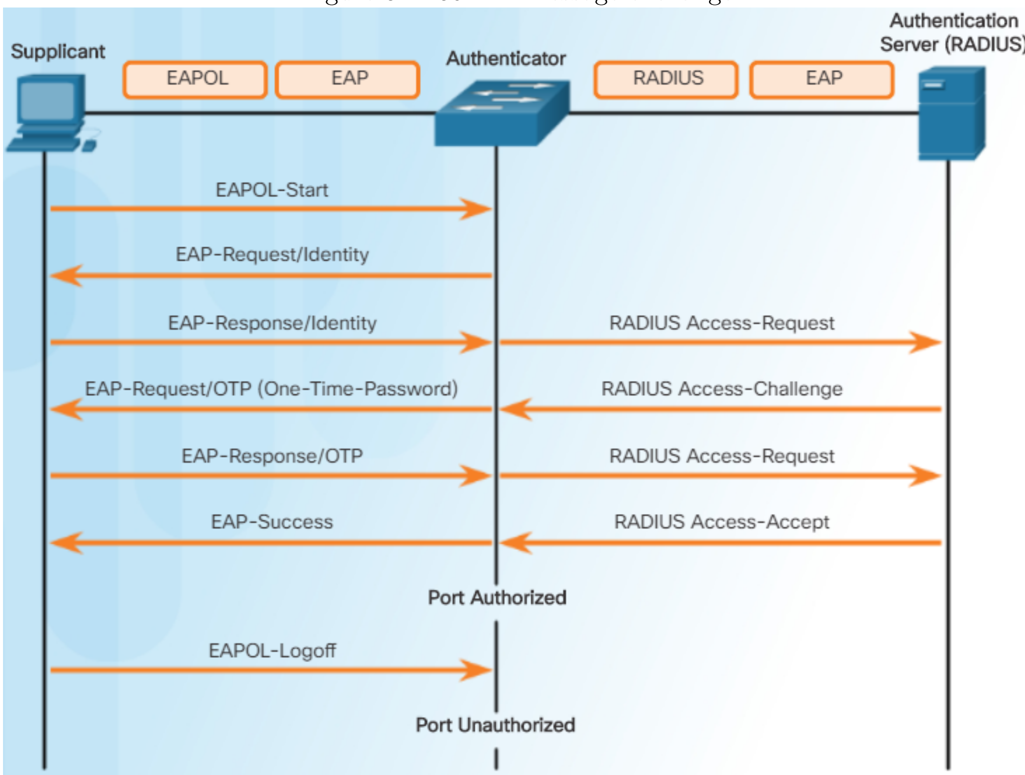
- **Supplicant (Client)** – The device that requests access to LAN. The workstation must be running 802.1X-compliant client software.
- **Authenticator (Switch)** – Controls physical access to the network based on the authentication status of the client. The switch acts as an intermediary (proxy) between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

Figure 3.1: 802.1X roles




If the Supplicant is successfully authenticated (receives an Accept frame from the authentication server), the port state changes to authorized, and all frames from the authenticated client are allowed through the port. If the authentication fails, the port remains in the unauthorized state, but authentication can be retried. If the authentication server cannot be reached, the switch can resend the request. If no response is received from the server after the specified number of attempts, authentication fails, and network access is not granted.

Figure 3.2: 802.1X message exchange




**Message exchange** Until the workstation is authenticated, 802.1X access control enables only EAPOL (EAP over LAN) traffic through the port to which the workstation is connected. After authentication succeeds, normal traffic can pass through the port. Figure 3.2 shows the complete message exchange between the supplicant, authenticator, and the authentication server. The encapsulation occurs as follows:

- Between the supplicant and the authenticator - EAP data is encapsulated in EAPOL frames.

- Between the authenticator and the authentication server - EAP data is encapsulated using RADIUS.

### 3.6.2 Port Authorization State

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

When a client logs out, it sends an EAPOL-logout message, causing the switch port to transition to the unauthorized state. If the link state of a port changes from up to down, or if an EAPOL-logoff frame is received, the port returns to the unauthorized state.

If the supplicant does not support 802.1X, the port remains in the unauthorized state. In contrast, if a switch that is not running the 802.1X protocol, the client begins sending frames as if the port is in the authorized state.

### 3.6.3 Configuration

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

**Listing 22: 802.1X configuration**

```
aaa new-models

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

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

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

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

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

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

# Chapter 4

# Firewall

## 4.1 ACL

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

- All zeros addresses
- Broadcast addresses
- Local host addresses (127.0.0.0/8)
- Reserved private addresses (RFC 1918)
- IP multicast address range (224.0.0.0/4)

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

- Echo reply – Allows users to ping external hosts.
- Source quench - Requests that the sender decrease the traffic rate of messages.
- Unreachable - Generated for packets that are administratively denied by an ACL.

Several ICMP messages are required for proper network operation and should be allowed to exit the network:

- Echo – Allows users to ping external hosts.
- Parameter problem – Informs the host of packet header problems.
- Packet too big – Enables packet maximum transmission unit (MTU) discovery.
- Source quench – Throttles down traffic when necessary.

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

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

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

## 4.2 Firewall

### 4.2.1 Introduction

All firewalls share some common properties: resistant to attacks, the only transit point between networks because all traffic flows through the firewall, enforce the access control policy. There are many types of firewalls: Packet filtering firewall, Stateful firewall, Application gateway firewall (proxy firewall), etc.

There are two configuration models for Cisco IOS Firewall: Classic Firewall and Zone-based Policy Firewall (ZPF). These models can be enabled concurrently on a router. However, the models cannot be combined on a single interface.

Table 4.1: Packet Filtering Firewall Benefits and Limitations

| **Advantages** | **Disadvantages** |
|---|---|
| Simple implementation | Susceptible to IP spoofing |
| Low impact on network performance | Not reliably filter fragmented packets |
| Initial degree of security at the network layer | Use complex ACLs, which can be difficult to implement and maintain |
| Almost all the tasks of a high-end firewall at a much lower cost | Stateless: examine each packet individually rather than in the context of the state of a connection. |

**Stateful firewalls** are the most versatile and the most common firewall technologies in use. Unlike a stateless firewall that uses static packet filtering, stateful filtering tracks each connection and confirms that they are valid. Stateful firewalls use a state table to keep track of the actual communication process. Benefits: prevent spoofing and DoS attacks, provide more stringent control over security. Limitations: cannot prevent Application Layer attacks, does not filter UDP and ICMP packets, cannot track connections that use dynamic port negotiation, not support authentication.

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

### 4.2.2 DMZ

A demilitarized zone (DMZ) is a firewall design where there is typically one inside interface connected to the private network, one outside interface connected to the public network, and one DMZ interface, as shown in the figure 4.1.

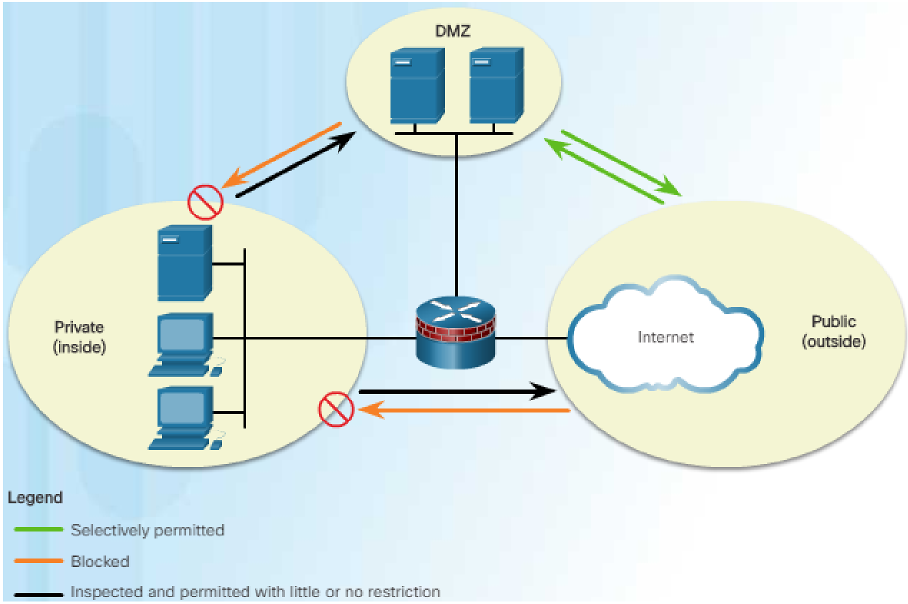
- Private network → DMZ: Inspected
- DMZ → Private network: Blocked
- Public network ↔ DMZ: selectively permitted
- Private network → Public network: Inspected
- Public network → Private network: Blocked

### 4.2.3 Layered Defense

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

1. Edge router (packet filtering)

Figure 4.1: DMZ topology and traffic restriction




2. Bastion host (hardened computer located in the DMZ[1]) or Screened firewall

3. Interior screening router

## 4.3 Classic firewall

### 4.3.1 Introduction

Classic Firewall (CBAC) is a *stateful* firewall that provides four main functions: traffic filtering, traffic inspection, intrusion detection, and generation of audits and alerts. It can also examine NAT, PAT information, P2P connections. Classic Firewall only provides filtering for those protocols that are specified by an administrator. It can only detects and protects against external attacks that travel through the firewall, but not attacks originating from within the protected network.

Classic Firewall creates *temporary* openings in the ACL to allow returning traffic. These entries are created as inspected traffic leaves the network and are removed when the connection terminates or the idle timeout period for the connection is reached. Figure 4.2 shows how Classic Firewall inspects SSH traffic.

### 4.3.2 Configuration

Take the topology in figure 4.3 as an example for configuration. Suppose that the administrator wants to allow SSH sessions between the 10.0.0.0 and 172.30.0.0 networks. However, only hosts from the 10.0.0.0 network are allowed to initiate SSH sessions. All other access is denied.

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

Figure 4.2: Classic Firewall inspects SSH traffic

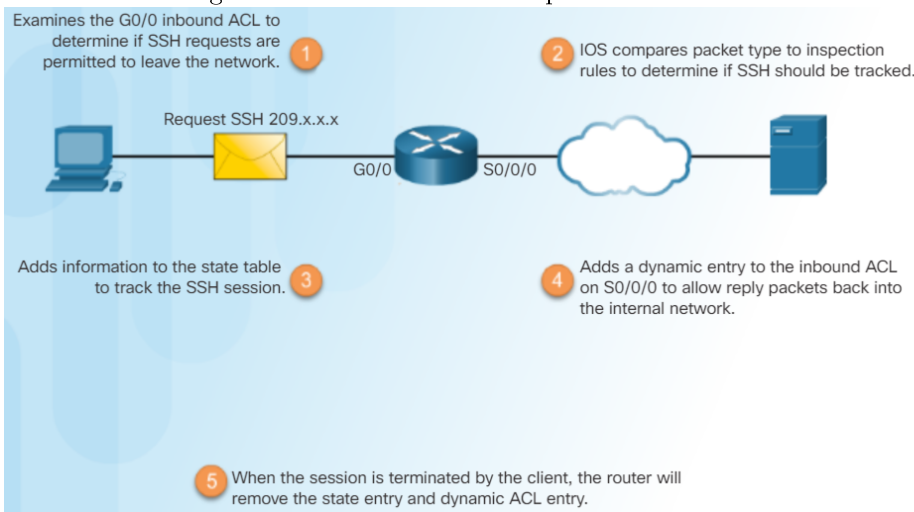
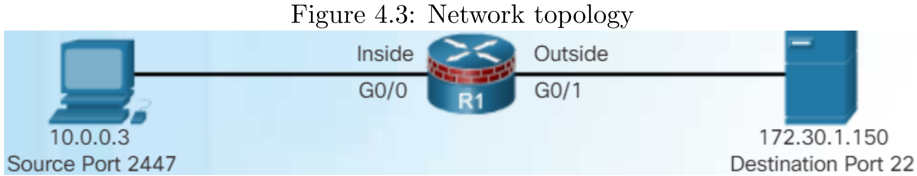



Figure 4.3: Network topology




**Listing 23: Classic Firewall configuration**

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

ip inspect name FWRULE ssh

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

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

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

## 4.4 Zone-based Policy Firewall (ZPF)

### 4.4.1 Overview

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

There are several benefits of a ZPF:

- Not dependent on ACLs.
- The router security posture is to block unless explicitly allowed.
- Policies are easy to read and troubleshoot with the Cisco Common Classification Policy Language (C3PL). C3PL can create traffic policies based on events and affect any given traffic with only one policy, instead of needing multiple ACLs and inspection actions.

### 4.4.2 Operation

The Cisco IOS ZPF can take three possible actions: Inspect, Drop and Pass. ZPF Rules for Transit Traffic depends on the zone that an interface belongs to:

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

The *self zone* is a special zone which is the router itself and includes all the router interface IP addresses. By default, if the router (self zone) is the source or the destination, then all traffic is permitted. The only exception is if the source and destination are a zone-pair with a specific service-policy. In that case, the policy is applied to all traffic.

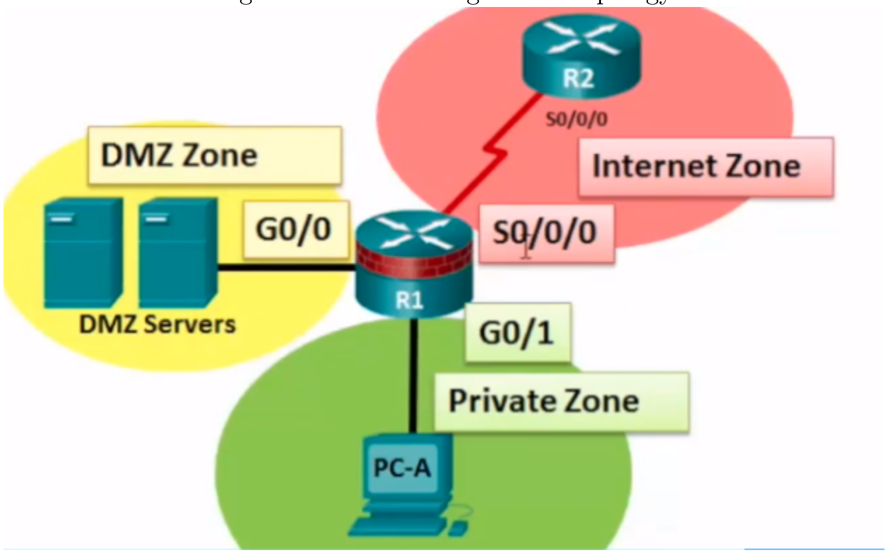
### 4.4.3 Configuration

There are five steps to configure a ZPF zone:

1. Create the zones and Assign zones to appropriate interfaces
2. Identify traffic with class-map
3. Define an action with policy-map
4. Identify a zone-pair and match it to a policy-map

Take the topology in figure 4.4 as an example.

Figure 4.4: ZPF configuration topology




**Listing 24: ZPF configuration**

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

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

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

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

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

The second step is to use a class-map to identify the traffic. A class is a way of identifying a set of packets based on its contents using `match` conditions. Packets must meet one of the match criteria `match-any` or all of the match criteria `match-all` to be considered a member of the class. Table 4.2 shows the syntax for the `class-map` and its sub-commands.

Table 4.2: The syntax of class-map command

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

The third step is to assign class-maps (PRIVATE-ACL-CLASS and PRIVATE-INTERNET-CLASS) to a policy-map and define what action (Inspect, Drop, or Pass) should be taken for traffic that is a member of a class.

- `inspect` – This action offers state-based traffic control. It tracks UDP or TCP connections and permit the return traffic.
- `drop` – This is the default action for all traffic. Similar to the implicit deny any at the end of every ACL, , there is an explicit `drop` applied to the end of every policy-map.
- `pass` – This action allows *one-direction* traffic between two zones, and does not track the state of connections. A corresponding policy must be applied to allow return traffic to pass in the opposite direction. This action is ideal for secure protocols, such as IPsec.

The fourth step is to identify a zone pair (PRIVATE-2-INTERNET) using `zone-pair security` command, and associate that zone pair to a policy-map (PRIV-TO-PUB-POLICY) using `service-policy type inspect` command.

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

### 4.4.4 ZPF Configuration Considerations

- The router never filters the traffic between interfaces in the same zone.
- An interface cannot belong to multiple zones. ZPF can coexist with Classic Firewall although they cannot be used on the same interface. Remove the `ip inspect` interface configuration command before applying the `zone-member security` command.

- Traffic can never flow between an interface assigned to a zone and an interface without a zone assignment. Applying the zone-member configuration command always results in a temporary interruption of service until the other zone-member is configured.

- Communication between zones are, by default, dropped. Unless there exits a service-policy configured for the zone-pair.

- The `zone-member` command does not protect the router itself (traffic to and from the router is not affected) unless the zone-pairs are configured using the predefined self zone.

# Chapter 5

# Intrusion Prevention System (IPS)

## 5.1 Introduction

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

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

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

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

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

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

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

IDS and IPS technologies share several characteristics:

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

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

## 5.2 IPS Signatures

### 5.2.1 Characteristics

Signatures have three distinctive attributes: Type, Trigger (alarm), Action. Signature types are generally categorized as atomic or composite.
An **atomic signature** consists of a single packet, activity, or event that is examined to determine if it matches a configured signature. Because these signatures can be matched on a single event, they do not require an intrusion system to maintain state[3] information. Detecting atomic signatures consumes minimal resources. For example, a LAND attack has an atomic signature because it sends a spoofed TCP SYN packet, therefore, one packet is enough to identify this type of attack.

A **composite signature** is a stateful signature which identifies a sequence of operations distributed across multiple hosts over an arbitrary period of time. The length of time that the signatures must maintain state is known as the event horizon. An IPS uses a configured event horizon to determine how long it will look for a specific attack signature when an initial signature component is detected.

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

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

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

### 5.2.2 Alarms

The heart of any IPS signature is the signature alarm (signature trigger). Anything that can reliably signal an intrusion or security policy violation can be used as a triggering mechanism. Cisco IDS and IPS sensors can use four types of signature triggers:

- **Pattern-based detection** (signature-based detection) is the simplest triggering mechanism. It compares the network traffic to a database of known attacks, and triggers an alarm or prevents communication if a match is found. The mechanism is only suitable for the suspect packets that are associated with services or ports. However, it cannot deal with protocols and attacks that do not use well-defined ports.

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

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

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

[3]State refers to situations in which multiple packets of information are required, but the packets of information are not necessarily received at the same time.
[4]A regular expression is a systematic way to specify a search for a pattern in a series of bytes.

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

The table shows four types of IPS alarms

Table 5.1: Alarm types

| **Alarm type** | **Status** | **Alarm** | **Outcome** |
|---|---|---|---|
| False positive | normal | • | tune alarm |
| False negative | dangerous | | tune alarm |
| True positive | dangerous | • | ideal setting |
| True negative | normal | | ideal setting |

- A false positive alarm occurs when an intrusion system generates an alarm after processing normal traffic. If this occurs, the administrator must be sure to tune the IPS to change these alarm types to true negatives.
- A false negative is when an intrusion system fails to generate an alarm after processing attack traffic. The goal of the administrator is for these alarm types to generate true positive alarms.
- A true positive alarm is when an intrusion system generates an alarm in response to known attack traffic.
- A true negative describes a situation in which normal network traffic does not generate an alarm.

### 5.2.3 Actions

**Alerts:** Should an attacker cause a flood of bogus alerts, examining these alerts can overwhelm the security analysts. IPS solutions incorporate two types of alerts to enable an administrator to efficiently monitor the operation of the network: atomic alerts and summary alerts. **Atomic alerts** are generated every time a signature triggers. A **summary alert** is a single alert that indicates multiple occurrences of the same signature from the same source address or port.

**Log activities for later analysis:** an IPS can be enabled to log the attacker packets, pair packets, or just the victim packets. **Logging attacker packets** is the action that starts IP logging on the packets that contain attacker's address and sends an alert.**Logging pair packets** is the action that starts IP logging on the packets that contain attacker-victim address pair and sends an alert. **Logging victim packets** is the action that starts IP logging on the packets that contain victim address and sends an alert. Note that the alerts are stored in Event Store.

**Deny the Activity:** an IPS can be enabled to deny the specific packets, or the attacker packets, or connection. **Denying the attacker packets** is the action that terminates the current and future packets from a particular attacker address for a period of time. There is a sliding timer for each attacker. If attacker A is currently denied, but issues another attack, then the timer for attacker A is reset and this attacker remain denied until the timer expires. **Denying the connection** is the action that terminates packets come from a particular TCP port. **Denying**

**Reset, Block, and Allow Traffic:** The **TCP Reset** Signature Action terminates TCP connections by generating a packet for the connection with the TCP RST flag set. Deny packet and deny flow actions do not automatically cause TCP reset actions to occur. **Blocking** is the action that updates ACL on *one* of the infrastructure devices. After a configured period of time, the IPS device removes the ACL. One advantage of the blocking action is that a single IPS device can stop traffic at multiple locations throughout the network, regardless of the location of the IPS device. The **Allow Signature** action define exceptions to configured signatures. Configuring exceptions enables administrators to take a more restrictive approach to security because they can first deny everything and then allow only the activities that are needed.

### 5.2.4 Manage and monitor

There are four factors to consider when planning a monitor strategy: Management method, Event correlation, Security staff, and Incident response plan. There are three GUI-based IPS device managers available: Cisco Configuration Professional, Cisco IPS Manager Express (IME), and Cisco Security Manager.

**Management method:** IPS sensors can be managed individually (small network) or centrally (large network). In a larger network, a centralized management system that allows the administrator to configure and manage all IPS devices from a single central system should be deployed.

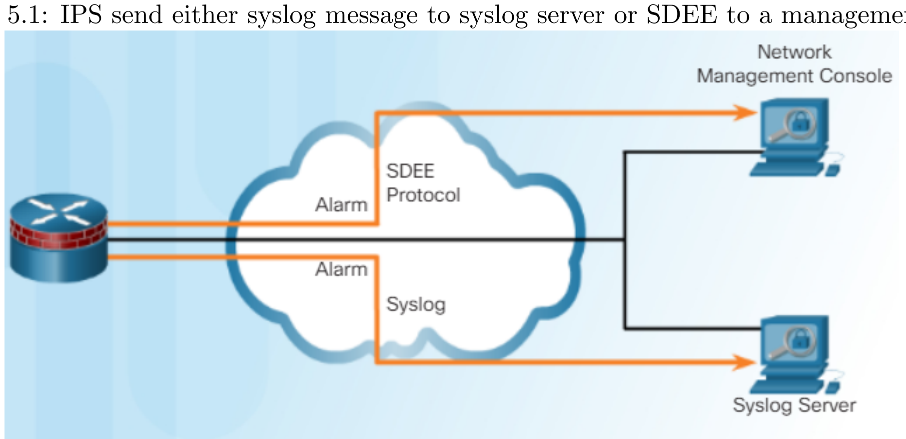
**Event correlation:** Event correlation refers to the process of correlating attacks and other events that are happening simultaneously at different points across a network. A correlation tool correlates the alerts based on their time-stamps. Therefore, the administrator should enable NTP on all network devices with a common system time. Another factor that facilitates event correlation is deploying a centralized monitoring facility on a network. By monitoring all IPS events at a single location, an administrator greatly improves the accuracy of event correlation.

**Security staff:** IPS devices tend to generate numerous alerts and other events during network traffic processing. Large enterprises require appropriate security staff to analyze this activity and determine how well the IPS is protecting the network.

**Incident response plan:** If a system is compromised on a network, a response plan must be in place. The compromised system should be restored to the state it was in before the attack.

**SDEE:** When an attack signature is detected, the Cisco IOS IPS feature can send a syslog message or an alarm in Secure Device Event Exchange (SDEE) format, as shown in the figure 5.1. The SDEE protocol was developed to improve communication of events generated by security devices. It primarily communicates IDS events, but the protocol is intended to be extensible and allows additional event types to be included as they are defined.

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




### 5.2.5 Global correlation

## 5.3 Implementation

### 5.3.1 Configuration

### 5.3.2 Modification

### 5.3.3 Verification