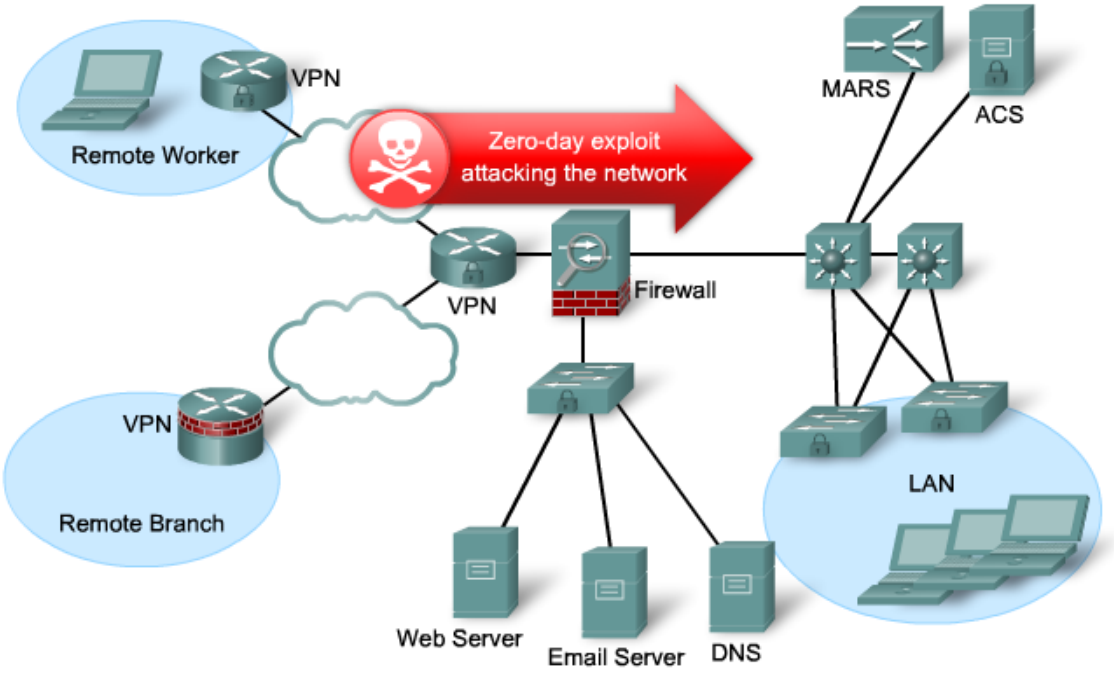
Implementing Intrusion Prevention

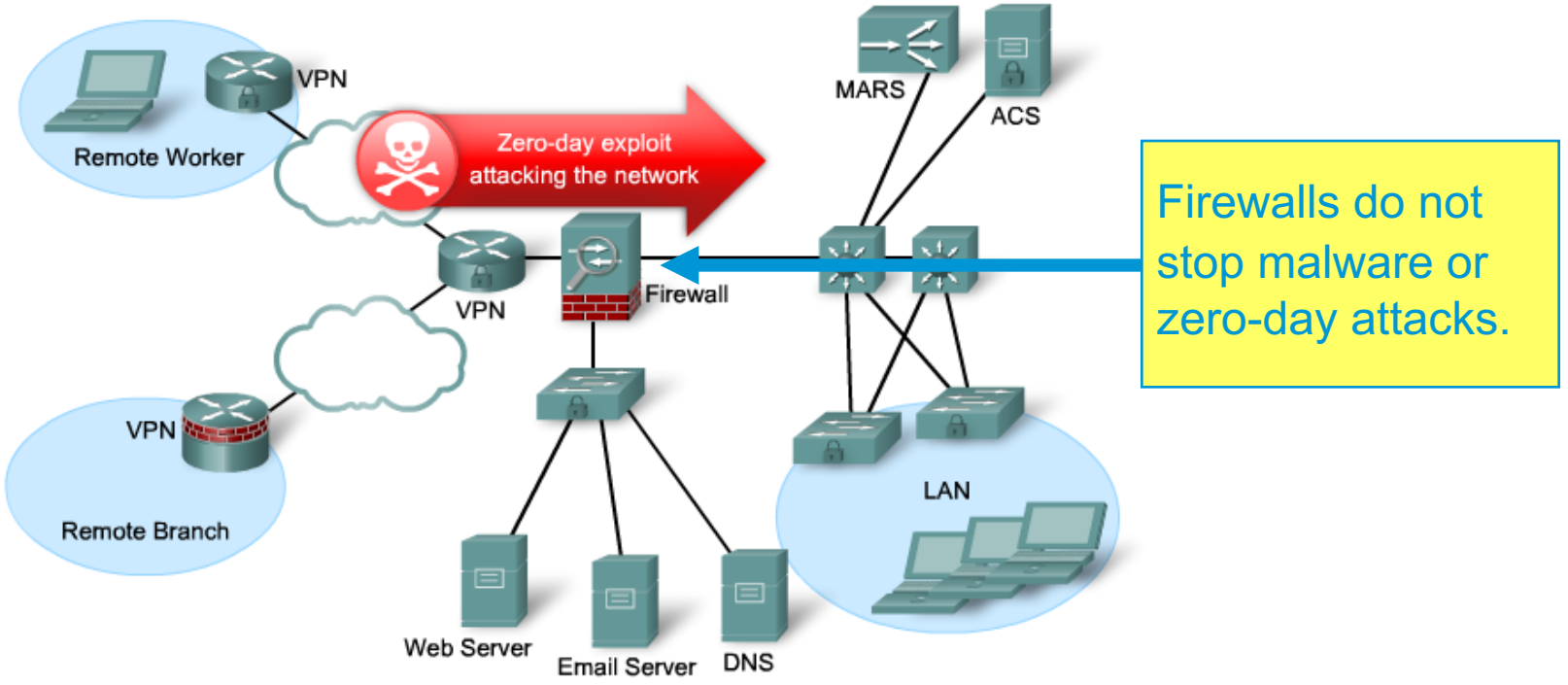
Zero-Day Exploits

- Worms and viruses can spread across the world in minutes.
  - **Zero-day attack** (zero-day threat), is a computer attack that tries to exploit software vulnerabilities.
  - **Zero-hour** describes the moment when the exploit is discovered.



Zero-Day Exploits

- How does an organization stop zero-day attacks?
  - Firewalls can't!



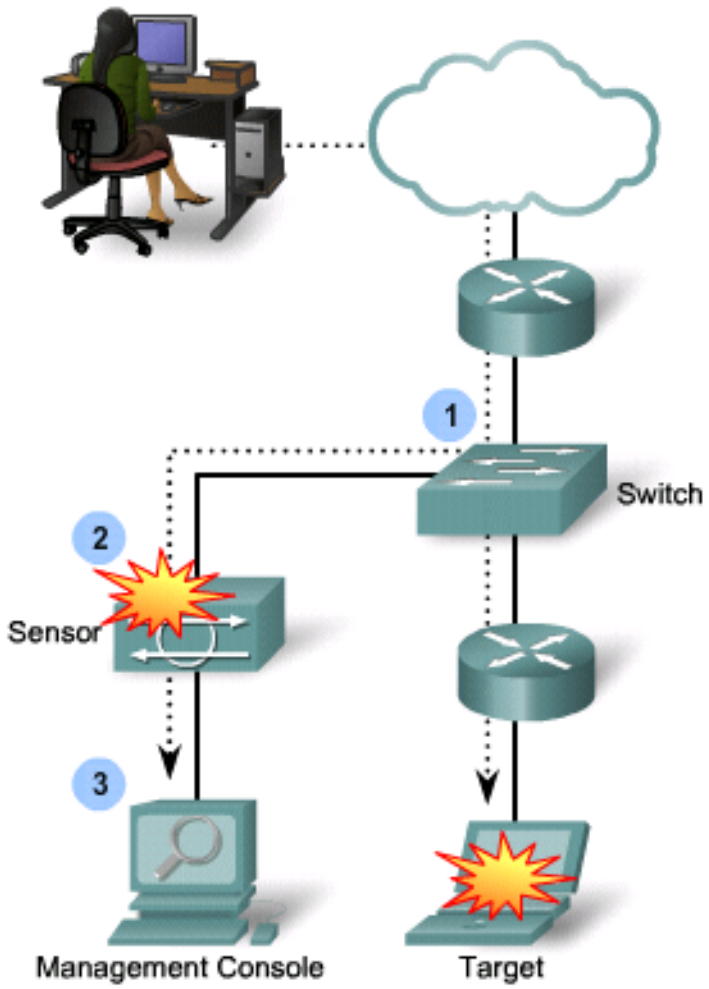
Solutions

- Networks must be able to instantly recognize and mitigate worm and virus threats.
- Two solution has evolved:
  - Intrusion Detection Systems (IDS) ❋ First generation
  - Intrusion Prevention Systems (IPS) ❋ Second generation
- IDS and IPS technologies use sets of rules, called signatures, to detect typical intrusive activity.

IDS and IPS Sensors

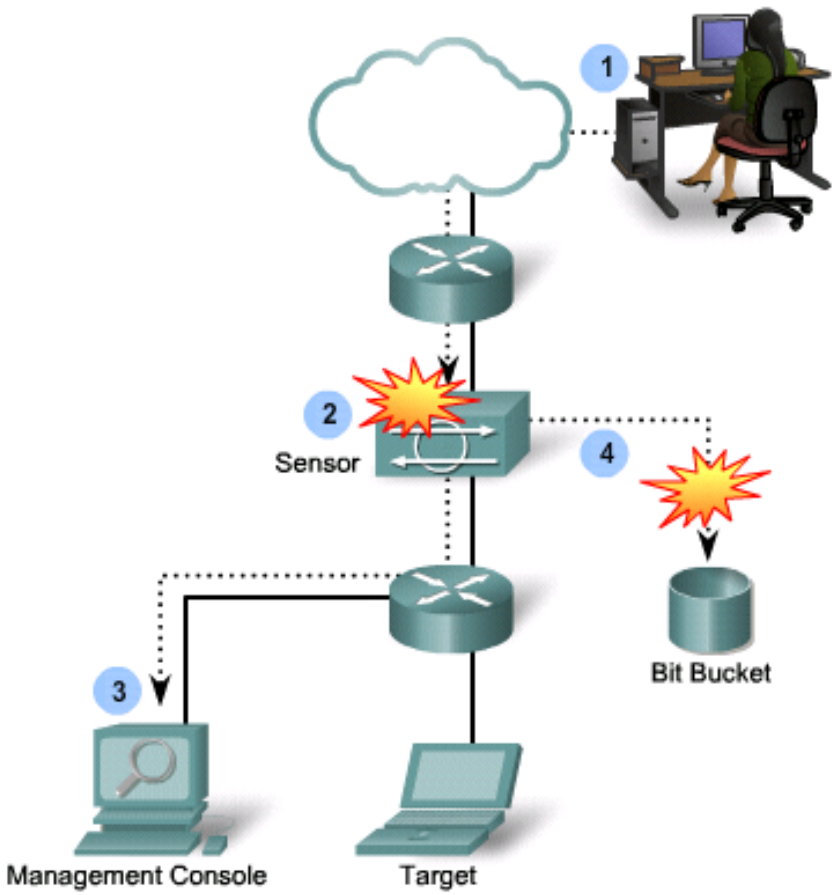
- IDS and IPS technology are deployed as a sensor in:
  - A router configured with Cisco IOS IPS Software.
  - A network module installed in router, an ASA, or a Catalyst switch.
  - An appliance specifically designed to provide dedicated IDS or IPS services.
  - Host software running on individual clients and servers.
- Note:
  - Some confusion can arise when discussing IPS.
  - There are many ways to deploy it and every method differs slightly from the other.
  - The focus of this chapter is on Cisco IOS IPS Software.

Intrusion Detection System



- An IDS monitors traffic offline and generates an alert (log) when it detects malicious traffic including:
  - Reconnaissance attacks
  - Access attacks
  - Denial of Service attacks
- It is a passive device because it analyzes copies of the traffic stream traffic.
  - Only requires a promiscuous interface.
  - Does not slow network traffic.
  - Allows some malicious traffic into the network.

Intrusion Prevention System



- It builds upon IDS technology to detect attacks.
  - However, it can also immediately address the threat.
- An IPS is an active device because all traffic must pass through it.
  - Referred to as “inline-mode”, it works inline in real time to monitor Layer 2 through Layer 7 traffic and content.
  - It can also stop single-packet attacks from reaching the target system (IDS cannot).

Intrusion Prevention

- The ability to stop attacks against the network and provide the following active defense mechanisms:
  - Detection – Identifies malicious attacks on network and host resources.
  - Prevention – Stops the detected attack from executing.
  - Reaction – Immunizes the system from future attacks from a malicious source.
- Either technology can be implemented at a network level, host level, or both for maximum protection.

Comparing IDS and IPS Solutions

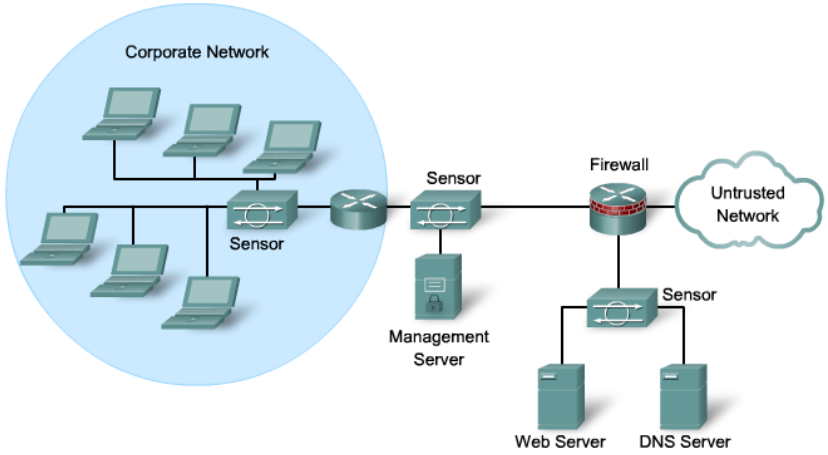
	IDS (Promiscuous Mode)	IPS (Inline Mode)
Advantages	• No impact on network (latency, jitter). • No network impact if there is a sensor failure or a sensor overload.	• Stops trigger packets. • Can use stream normalization techniques.
Disadvantages	• Response action cannot stop trigger packets. • Correct tuning required for response actions. • More vulnerable to network evasion techniques.	• Some impact on network (latency, jitter). • Sensor failure or overloading impacts the network.

Which should be implemented?

- The technologies are not mutually exclusive.
- IDS and IPS technologies can complement each other.
  - For example, an IDS can be implemented to validate IPS operation, because IDS can be configured for deeper packet inspection offline allowing the IPS to focus on fewer but more critical traffic patterns inline.
- Deciding which implementation is used should be based on the security goals stated in the network security policy.

Network-Based IPS

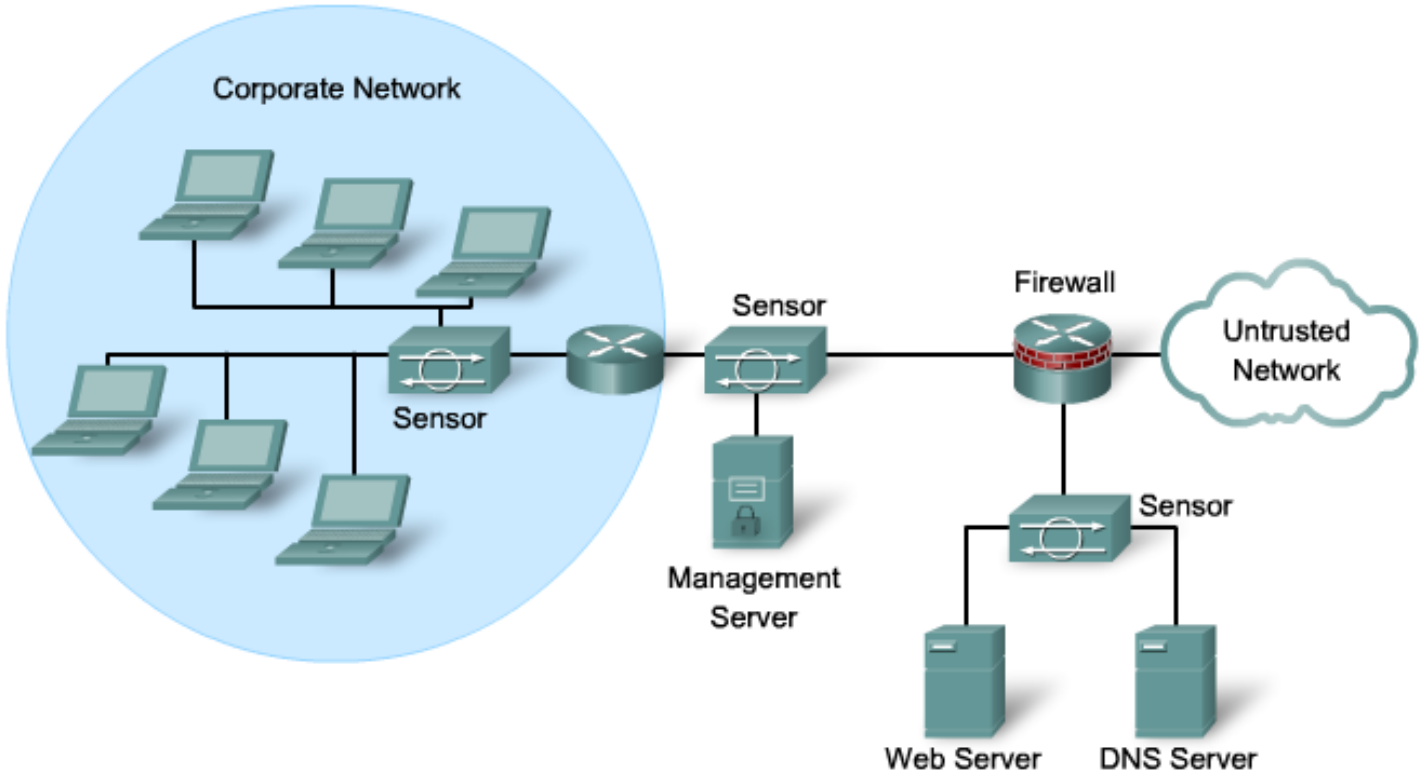
- Implementation analyzes network-wide activity looking for malicious activity.
  - Configured to monitor known signatures but can also detect abnormal traffic patterns.
- Configured on:
  - Dedicated IPS appliances
  - ISR routers
  - ASA firewall appliances
  - Catalyst 6500 network modules



Network-Based IPS Features

- Sensors are connected to network segments.
  - A single sensor can monitor many hosts.
- Sensors are network appliances tuned for intrusion detection analysis.
  - The operating system is “hardened.”
  - The hardware is dedicated to intrusion detection analysis.
- Growing networks are easily protected.
  - New hosts and devices can be added without adding sensors.
  - New sensors can be easily added to new networks.

Cisco Network IPS Deployment



IPS Signatures

- To stop incoming malicious traffic, the network must first be able to identify it.
  - Fortunately, malicious traffic displays distinct characteristics or "signatures."
- A signature is a set of rules that an IDS and an IPS use to detect typical intrusive activity, such as DoS attacks.
  - Signatures uniquely identify specific worms, viruses, protocol anomalies, or malicious traffic.
  - IPS sensors are tuned to look for matching signatures or abnormal traffic patterns.
- IPS signatures are conceptually similar to the virus.dat file used by virus scanners.

Signature File

- As new threats are identified, new signatures must be created and uploaded to an IPS.
- To make this process easier, all signatures are contained in a signature file and uploaded to an IPS on a regular basis.
  - Networks deploying the latest signature files are better protected against network intrusions.

Signature Examples

ID	Name	Description
1101	Unknown IP Protocol	This signature triggers when an IP datagram is received with the protocol field set to 134 or greater.
1307	TCP Window Size Variation	This signature will fire when the TCP window varies in a suspect manner.
3002	TCP SYN Port Sweep	This signature triggers when a series of TCP SYN packets have been sent to a number of different destination ports on a specific host.
3227	WWW HTML Script Bug	This signature triggers when an attempt is made to view files above the HTML root directory.

Updating Signatures

- Cisco investigates / creates signatures for new threats as they are discovered and publishes them regularly.
  - Lower priority IPS signature files are published biweekly.
  - If the threat is severe, Cisco publishes signature files within hours of identification.
- Update the signature file regularly to protect the network.
  - Each update includes new signatures and all the signatures in the previous version.
    - For example, signature file IOS-S361-CLI.pkg includes all signatures in file IOS-S360-CLI.pkg plus signatures created for threats discovered subsequently.
- New signatures are downloadable from CCO.
  - Requires a valid CCO login.

Pattern-Based Detection

- Pattern-based detection (signature-based detection), is the simplest triggering mechanism because it searches for a specific, pre-defined pattern.
- The IPS sensor compares the network traffic to a database of known attacks and triggers an alarm or prevents communication if a match is found.

Signature Trigger	Signature Type	
	Atomic Signature	Composite Signature
Pattern-based Detection	No state required to examine pattern to determine if signature action should be applied	Must maintain state or examine multiple items to determine if signature action should be applied
Example	Detecting for an Address Resolution Protocol (ARP) request that has a source Ethernet address of FF:FF:FF:FF:FF:FF	Searching for the string "confidential" across multiple packets in a TCP session

Policy-Based Detection

- Similar to pattern-based detection, but instead of trying to define specific patterns, the administrator defines behaviors that are suspicious based on historical analysis.

Signature Trigger	Signature Type	
	Atomic Signature	Composite Signature
Policy-based Detection	No state required to identify undesirable behavior.	Previous activity (state) required to identify undesirable behavior.
Example	Detecting abnormally large fragmented packets by examining only the last fragment.	A SUN Unix host sending RPC requests to remote hosts without initially consulting the SUN PortMapper program.

Anomaly-Based Detection

- It can detect new and previously unpublished attacks.
- Normal activity is defined and any activity that deviates from this profile is abnormal and triggers a signature action.
  - Note that an alert does not necessarily indicate an attack since a small deviation can sometimes occur from valid user traffic.
  - As the network evolves, the definition of normal usually changes, so the definition of normal must be redefined.

Signature Trigger	Signature Type	
	Atomic Signature	Composite Signature
Anomaly-based Detection	No state required to identify activity that deviates from normal profile	State required to identify activity that deviates from normal profile
Example	Detecting traffic that is going to a destination port that is not in the normal profile	Verifying protocol compliance for HTTP traffic

Types of Signature Triggers

	Advantages	Disadvantages
Pattern detection (Signature-based)	• Easy configuration • Fewer false positives • Good signature design	• No detection of unknown signatures • Initially a lot of false positives • Signatures must be created, updated, and tuned
Policy-based detection (Behavior-based)	• Simple and reliable • Customized policies • Can detect unknown attacks	• Generic output • Policy must be created
Anomaly detection (Profile-based)	• Easy configuration • Can detect unknown attacks	• Difficult to profile typical activity in large networks • Traffic profile must be constant
Honey Pot-based	• Window to view attacks • Distract and confuse attackers • Slow down and avert attacks • Collect information about attack	• Dedicated honey pot server • Honey pot server must not be trusted

Tuning Alarms

- Triggering mechanisms can generate various types of alarms including:

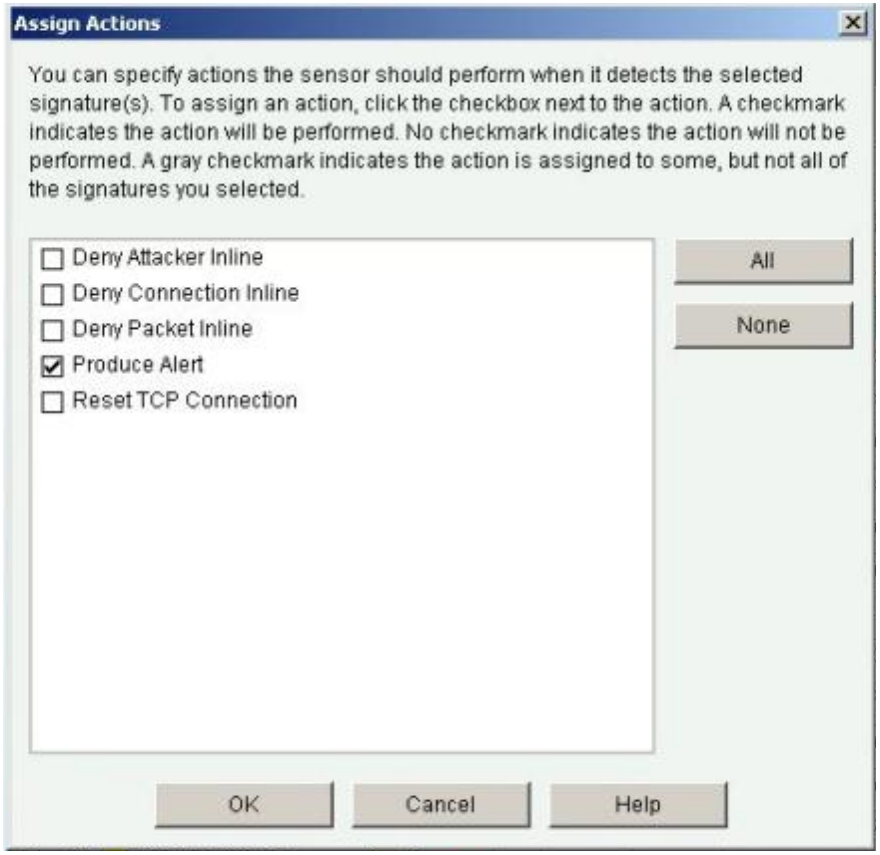
Alarm Type	Network Activity	IPS Activity	Outcome
True positive	Attack traffic	Alarm generated	Ideal setting
True negative	Normal user traffic	No alarm generated	Ideal setting
False positive	Normal user traffic	Alarm generated	Tune alarm
False negative	Attack traffic	No alarm generated	Tune alarm

Tuning Alarms

- False Positive:
  - False positive alarm is an expected but undesired result.
  - It occurs when an intrusion system generates an alarm after processing normal user traffic that should not have resulted in the alarm.
  - The administrator must be sure to tune the IPS to change these alarm types to true negatives.
- False Negative:
  - The IPS fails to generate an alarm after processing attack traffic that it is configured to detect.
  - It is imperative that the IPS does not generate false negatives, because it means that known attacks are not being detected.
  - The goal is to render these alarm types as true positive.

IPS Signature Actions

- Whenever a signature detects the activity for which it is configured, the signature triggers one or more actions.
- Several actions can be performed:
  - Allow the activity.
  - Drop or prevent the activity.
  - Block future activity.
  - Generate an alert.
  - Log the activity.
  - Reset a TCP connection.



Steps to implement Cisco IOS IPS

1. Download the IOS IPS files.
2. Create an IOS IPS configuration directory in flash.
3. Configure an IOS IPS crypto key.
4. Enable IOS IPS (consists of several substeps).
5. Load the IOS IPS signature package to the router.

1. Download the IOS IPS files.

- Download the IOS IPS signature file and public crypto key.
  - IOS-Sxxx-CLI.pkg - This is the latest signature package.
  - realm-cisco.pub.key.txt - This is the public crypto key used by IOS IPS.
- The specific IPS files to download vary depending on the current release.
  - Only registered customers can download the package files and key.

2. Create an IOS IPS directory in Flash

- Create a directory in flash to store the signature files and configurations.
  - Use the **`mkdir`** *`directory-name`* privileged EXEC command to create the directory.
  - Use the **`rename`** *`current-name new-name`* command to change the name of the directory.
- To verify the contents of flash, enter the **`dir flash:`** privileged EXEC command.

```
R1# mkdir ips
Create directory filename [ips]?
Created dir flash:ips
R1#
R1# dir flash:
Directory of flash:/
   5 -rw-   51054864 Jan 10 2009 15:46:14 -08:00
                     c2800nm-advipservicesk9-mz.124-20.T1.bin
   6 drw-       0 Jan 15 2009 11:36:36 -08:00 ips
64016384 bytes total (12693504 bytes free)
R1#
```

3a. Enable IOS IPS

- Identify the IPS rule name and specify the location.
  - Use the **ip ips name** [*rule name*] [*optional ACL*] command to create a rule name.
  - An optional extended or standard ACL can be used to filter the traffic.
  - Traffic that is denied by the ACL is not inspected by the IPS.
- Use the **ip ips config location flash:***directory-name* command to configure the IPS signature storage location.
  - Prior to IOS 12.4(11)T, the **ip ips sdf location** command was used.

```
R1(config)# ip ips name IOSIPS
R1(config)# ip ips name ips list ?
<1-199> Numbered access list
WORD Named access list
R1(config)#
R1(config)# ip ips config location flash:ips
R1(config)#
```

3b. Enable IOS IPS

- Enable SDEE and logging event notification.
  - The HTTP server must first be enabled using the **ip http server** command.
  - SDEE notification must be explicitly enabled using the **ip ips notify sdee** command.
- IOS IPS also supports logging to send event notification.
  - SDEE and logging can be used independently or simultaneously.
  - Logging notification is enabled by default.
  - Use the **ip ips notify log** command to enable logging.

```
R1(config)# ip http server
R1(config)# ip ips notify sdee
R1(config)# ip ips notify log
R1(config)#
```

3c. Configure the Signature Category

- All signatures are grouped into three common categories:
  - All
  - Basic
  - Advanced
- Signatures that IOS IPS uses to scan traffic can be retired or unretired.
  - Retired means that IOS IPS does not compile that signature into memory.
  - Unretired instructs the IOS IPS to compile the signature into memory and use it to scan traffic.

3c. Configure the Signature Category

- When IOS IPS is first configured, all signatures in the **`all`** category should be retired, and then selected signatures should be unretired in a less memory-intensive category.
  - To retire and unretired signatures, first enter IPS category mode using the **`ip ips signature-category`** command.
  - Next use the **`category`** *`category-name`* command to change a category.

```
R1(config)# ip ips signature-category
R1(config-ips-category)# category all
R1(config-ips-category-action)# retired true
R1(config-ips-category-action)# exit
R1(config-ips-category)#
R1(config-ips-category)# category IOSIPS basic
R1(config-ips-category-action)# retired false
R1(config-ips-category-action)# exit
R1(config-ips-category)# exit
Do you want to accept these changes? [confirm] y
R1(config)#
```

3d. Configure the Signature Category

- Apply the IPS rule to a desired interface, and specify the direction.
- Use the **ip ips** *rule-name* **[in | out]** interface configuration command to apply the IPS rule.
  - The **in** argument means that only traffic going into the interface is inspected by IPS.
  - The **out** argument specifies that only traffic going out of the interface is inspected.

```
R1(config)# interface GigabitEthernet 0/1
R1(config-if)# ip ips IOSIPS in
R1(config-if)# ip ips IOSIPS out
R1(config-if)# exit
R1(config)# exit
```

Verify IOS IPS

```
R1# show ip ips all
IPS Signature File Configuration Status
    Configured Config Locations: flash:/ipsdir/
    Last signature default load time: 04:39:33 UTC Jan 15 2009
    Last signature delta load time: -none-
    Last event action (SEAP) load time: -none-

    General SEAP Config:
    Global Deny Timeout: 3600 seconds
    Global Overrides Status: Enabled
    Global Filters Status: Enabled

IPS Auto Update is not currently configured

IPS Syslog and SDEE Notification Status
    Event notification through syslog is enabled
    Event notification through SDEE is enabled

IPS Signature Status
    Total Active Signatures: 693
    Total Inactive Signatures: 1443

IPS Packet Scanning and Interface Status
    IPS Rule Configuration
      IPS name myips
    IPS fail closed is disabled
    IPS deny-action ips-interface is false
    Fastpath ips is enabled
    Quick run mode is enabled
    Interface Configuration
      Interface FastEthernet0/1
        Inbound IPS rule is not set
        Outgoing IPS rule is myips
 <output omitted>
```

View Configuration

```
R1# show ip ips configuration
Event notification through syslog is enabled
Event notification through Net Director is enabled
Default action(s) for info signatures is alarm
Default action(s) for attack signatures is alarm
Default threshold of recipients for spam signature is 25
PostOffice:HostID:5 OrgID:100 Addr:10.2.7.3 Msg dropped:0
HID:1000 OID:100 S:218 A:3 H:14092 HA:7118 DA:0 R:0
    CID:1 IP:172.21.160.20 P:45000 S:ESTAB (Curr Conn)
Audit Rule Configuration
 Audit name AUDIT.1
    info actions alarm

<output omitted>
```

View IPS Interface Configuration

```
R1# show ip ips interfaces
Interface Configuration
      Interface FastEthernet0/0
        Inbound IPS rule is sdm_ips_rule
        Outgoing IPS rule is not set
      Interface FastEthernet0/1
        Inbound IPS rule is sdm_ips_rule
        Outgoing IPS rule is not set
R1#
```