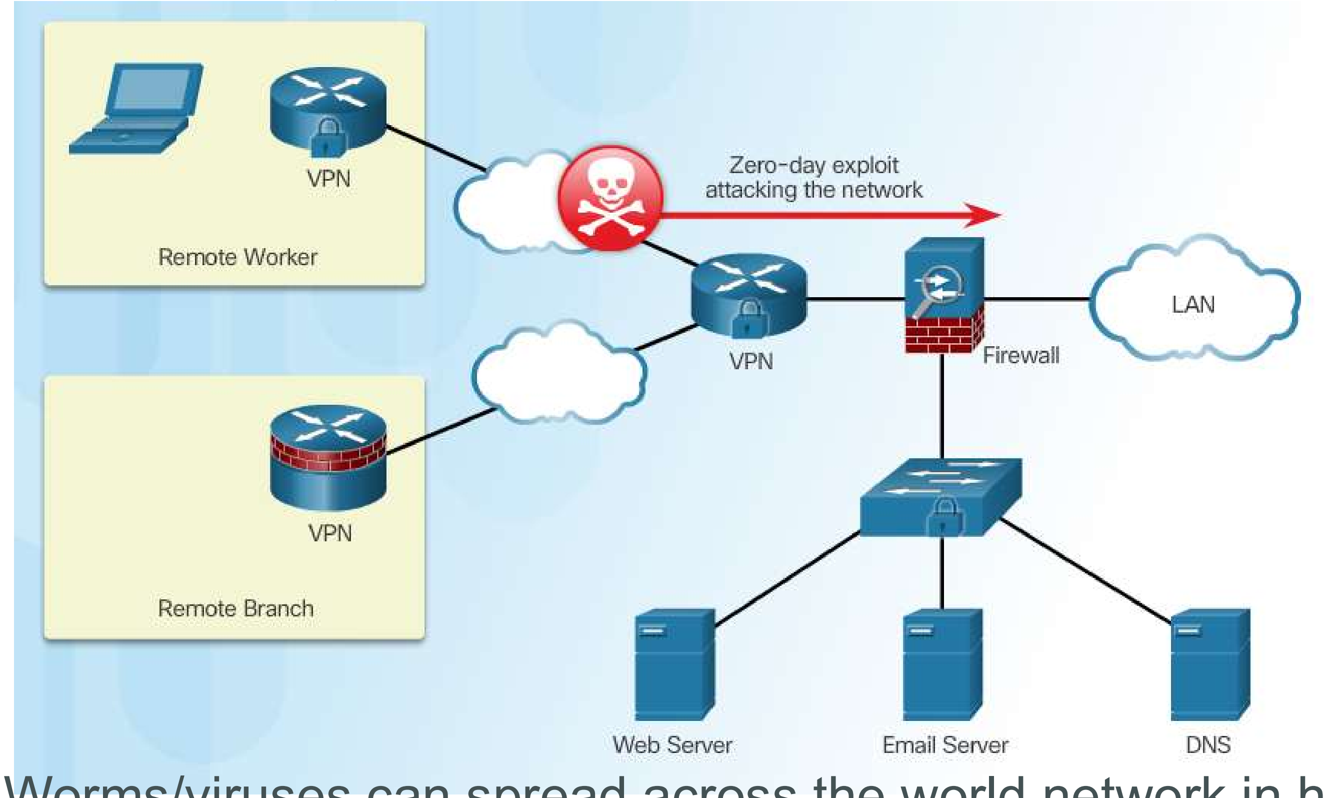
CCS6224 Network Security

Lecture 6
Intrusion Prevention System (IPS)

Outline

- Introduction to IPS
- IPS Technologies
- IPS Signatures
- IPS Implementation

Zero-Day Attacks



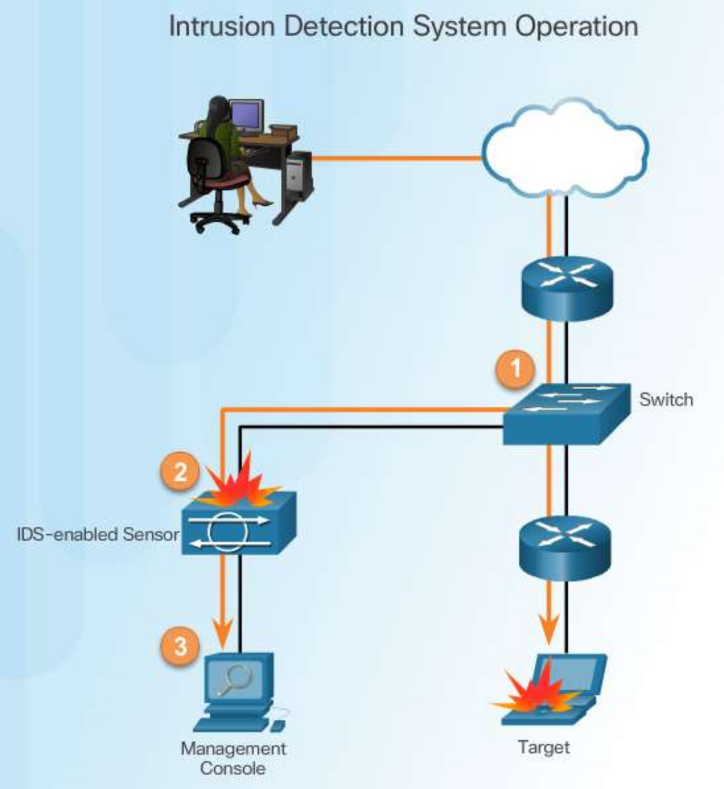
Worms/viruses can spread across the world network in hours or even minutes

Zero-Day Attacks – aka Zero-Day Threat, is a computer attack that attempts to exploit software vulnerabilities

Monitor for Attacks

Advantages of an IDS:

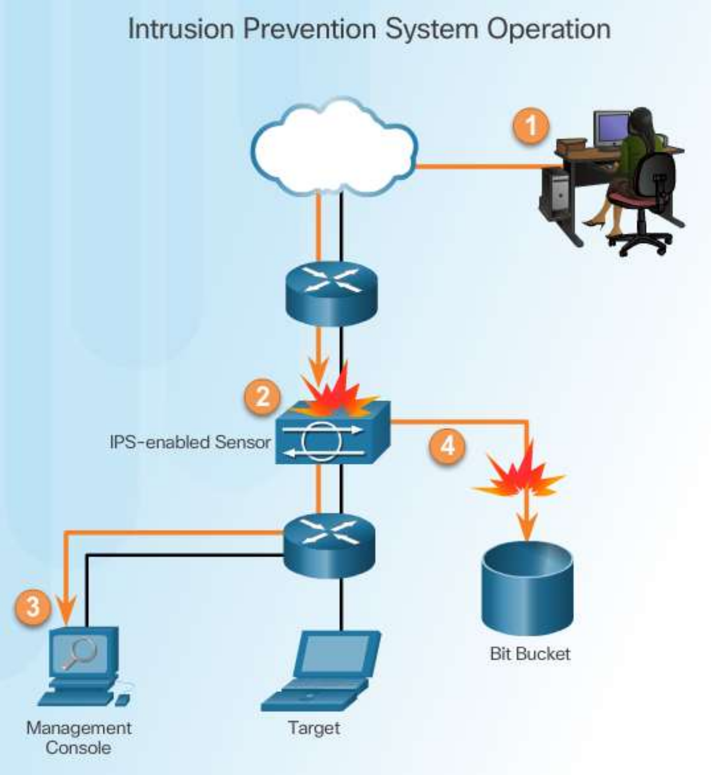
- Works passively
- Does not negatively affect the actual traffic flow
- Requires traffic to be mirrored in order to reach it
- Network traffic does not pass through the IDS unless it is mirrored



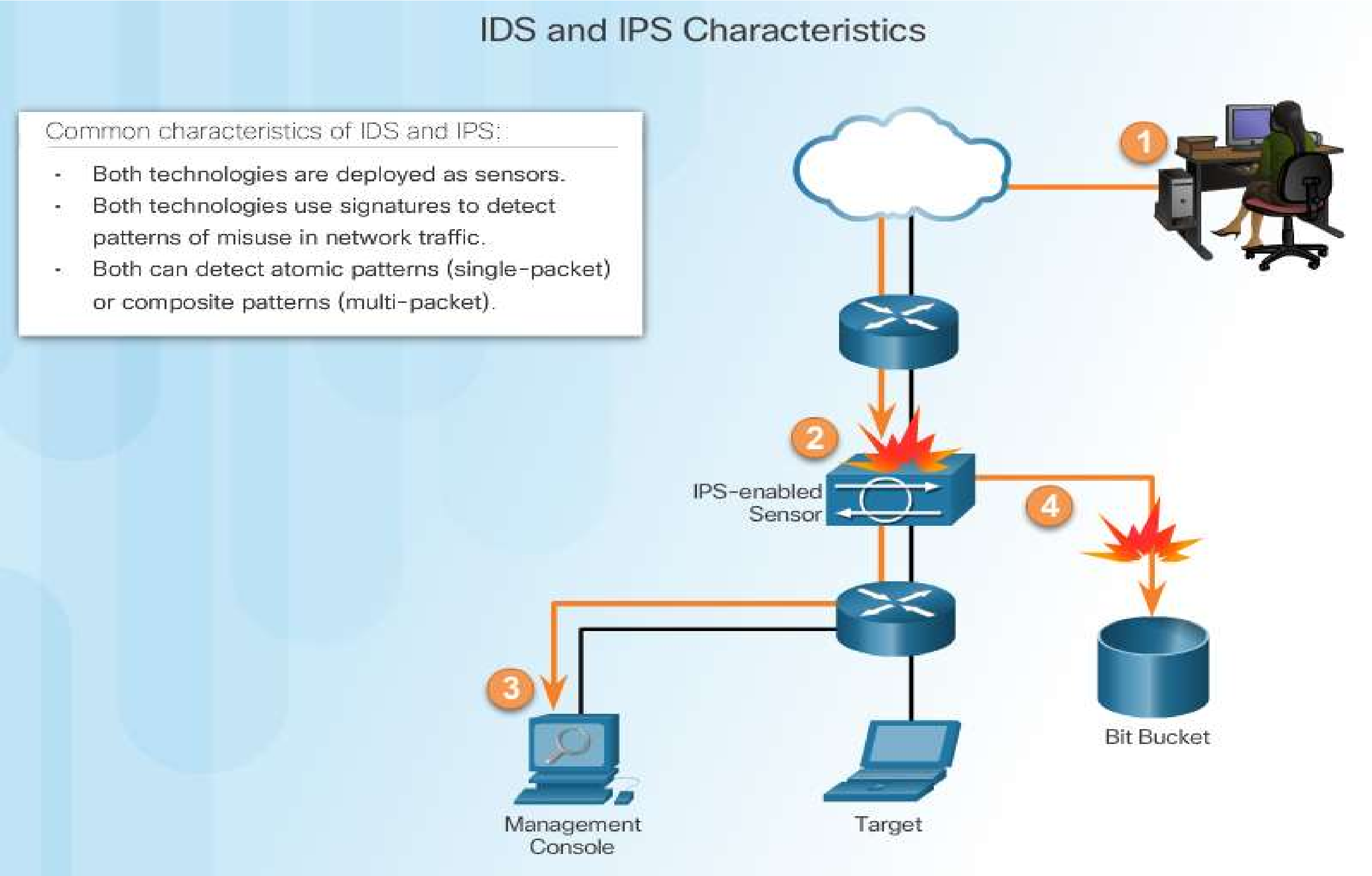
Detect and Stop Attacks

IPS:

- Implemented in an inline mode
- Monitors Layer 3 and Layer 4 traffic
- Can stop single packet attacks from reaching target
- Responds immediately, not allowing any malicious traffic to pass



Similarities between IDS and IPS



IDS and IPS Characteristics

Common characteristics of IDS and IPS:

- Both technologies are deployed as sensors.
- Both technologies use signatures to detect patterns of misuse in network traffic.
- Both can detect atomic patterns (single-packet) or composite patterns (multi-packet).

Advantages and Disadvantages of IDS and IPS

Advantages IDS:

- No impact on network
- No network impact if there is a sensor failure
- No network impact if there is a sensor overload

Disadvantages IDS:

- Response action cannot stop trigger
- Correct tuning required for response actions
- More vulnerable to network security evasion techniques

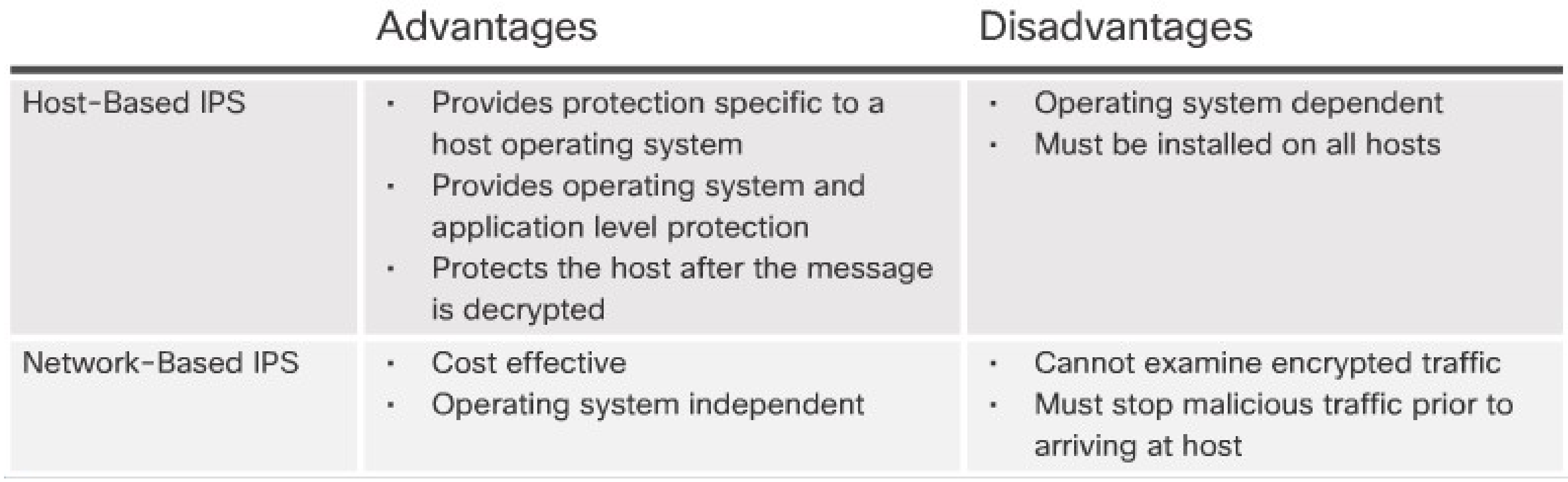
Advantages IPS:

- Stops trigger packets
- Can use stream normalization techniques

Disadvantages IPS:

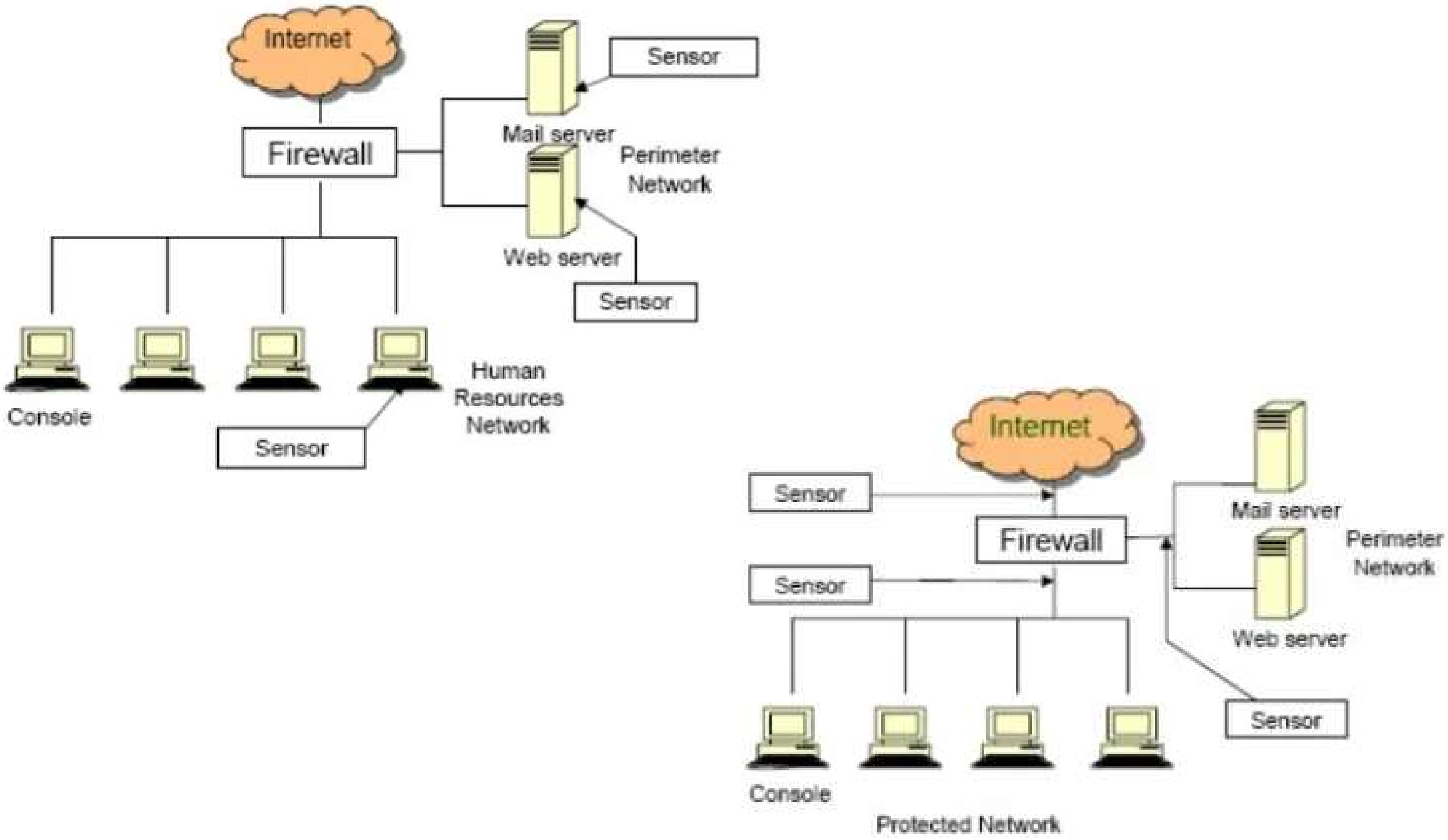
- Sensor issues might affect network traffic
- Sensor overloading impacts the network
- Some impact on network

Host-Based vs Network-Based



	Advantages	Disadvantages
Host-Based IPS	- Provides protection specific to a host operating system - Provides operating system and application level protection - Protects the host after the message is decrypted	- Operating system dependent - Must be installed on all hosts
Network-Based IPS	- Cost effective - Operating system independent	- Cannot examine encrypted traffic - Must stop malicious traffic prior to arriving at host

Host-Based vs Network-Based IPS Sensors



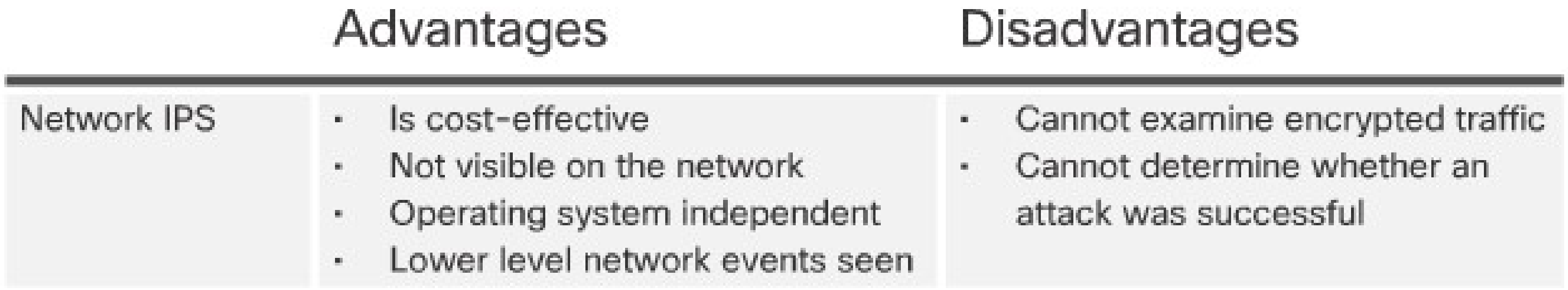
Network IPS Sensors

- Looking for possible malicious activity by analyzing network-wide activity
- Configured to detect known signatures, but can also used to discover abnormal traffic patterns
- A single sensor can monitor many hosts
- Sensors are network appliances that are customized for intrusion detection analysis. Hardware e.g. processor, RAM, NIC, etc. is dedicated for the analysis. Also, unnecessary services are stripped off from OS
- Network is scalable – new hosts/devices can be added without adding sensors

Network IPS

Selection and deployment of Network IPS. Several factors to consider:

- Amount of network traffic
- Network topology
- Security budget
- Available security staff to manage IPS



	Advantages	Disadvantages
Network IPS	▪ Is cost-effective ▪ Not visible on the network ▪ Operating system independent ▪ Lower level network events seen	▪ Cannot examine encrypted traffic ▪ Cannot determine whether an attack was successful

IPS Signature Attributes

- IPS sensors are configured to look for matching signatures or abnormal traffic patterns
- When a sensor matches a signature with data flow, it takes action, such as logging or send an alarm to IDS or IPS
- A signature is a set of rules that an IDS and an IPS use to detect typical intrusion activity.
- Signatures have three distinct attributes:

- Type
- Trigger (alarm)
- Action

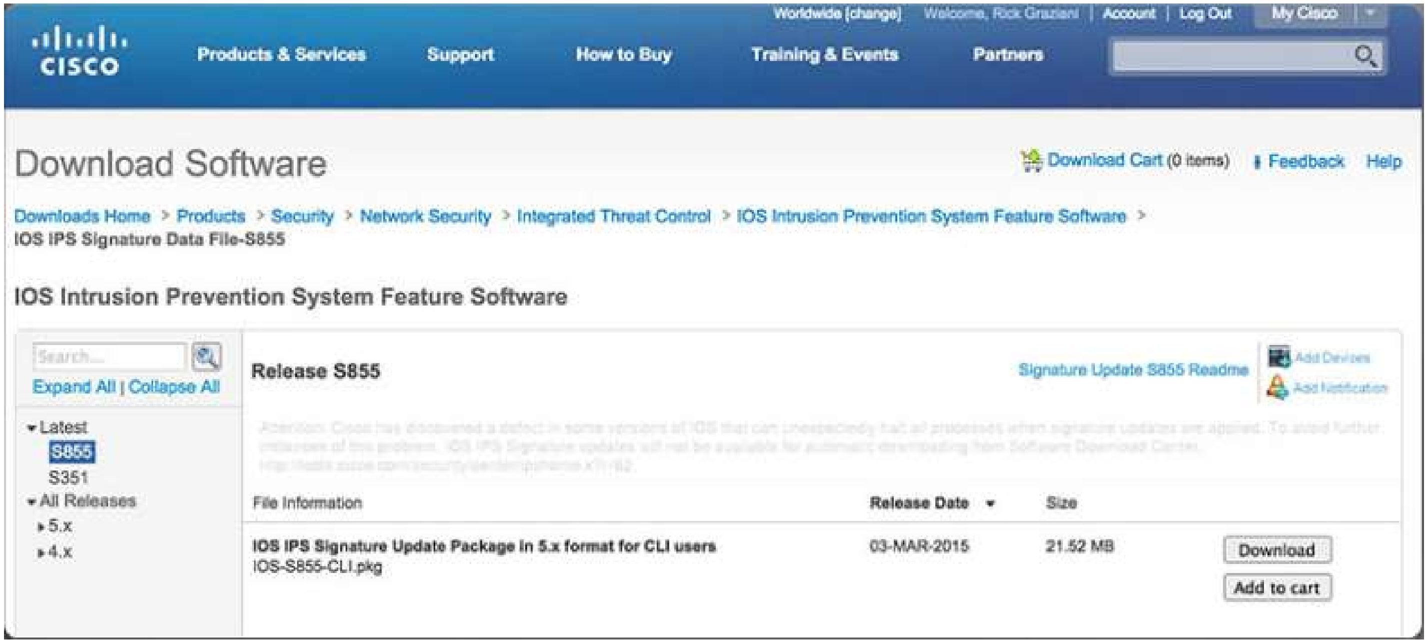
Signature Types

Signatures are categorized as either:

- Atomic – this simplest type of signature consists of a single packet, activity, or event that is examined to determine if it matches a configured signature. If yes, an alarm is triggered and a signature action is performed.
- Composite – this type of signature identifies a sequence of operations distributed across multiple hosts over an arbitrary period of time.

Signature File

- As new threats are identified, new signatures must be created and uploaded to an IPS.
- A signature file contains a package of network signatures.



Download Software

Downloads Home > Products > Security > Network Security > Integrated Threat Control > IOS Intrusion Prevention System Feature Software >
IOS IPS Signature Data File-S855

IOS Intrusion Prevention System Feature Software

Release S855

Attention: Cisco has discovered a defect in some versions of IOS that can unexpectedly halt all processes when signature updates are applied. To avoid further instances of this problem, IOS IPS Signature updates will not be available for automatic downloading from Software Download Center. http://tools.cisco.com/security/center/[illegible]

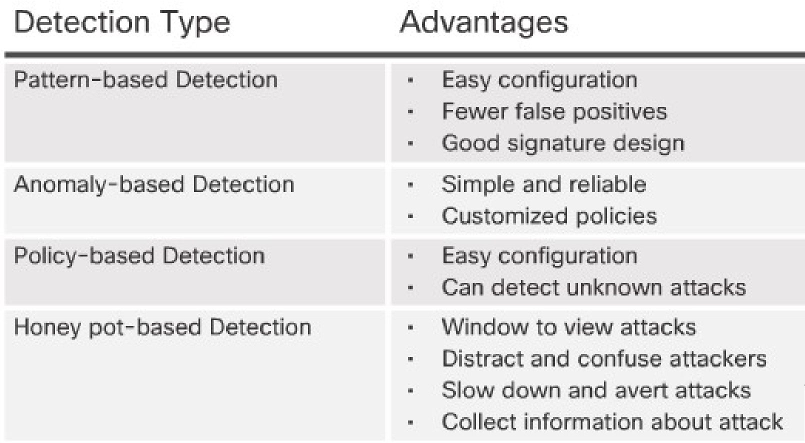
File Information	Release Date	Size
IOS IPS Signature Update Package in 5.x format for CLI users IOS-S855-CLI.pkg	03-MAR-2015	21.52 MB

Signature Micro-Engines

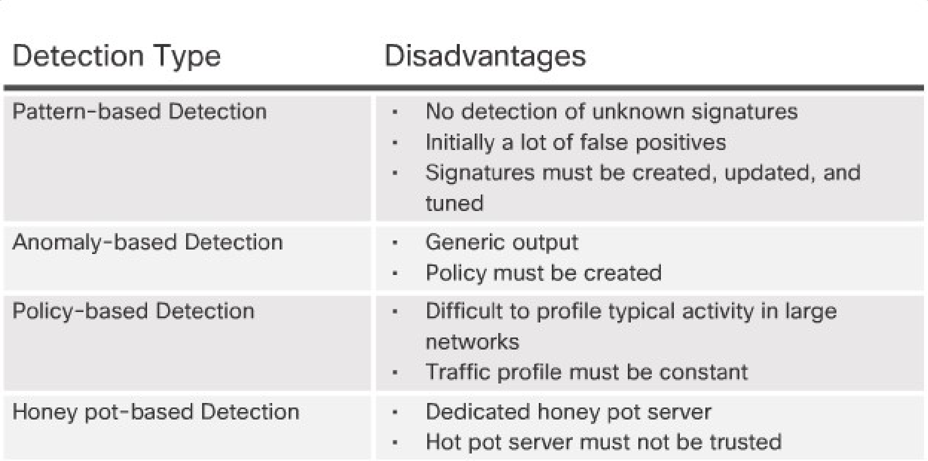
Cisco IOS defines five micro-engines:

- Atomic – Signatures that examine simple packets.
- Service – Signatures that examine the many services that are attacked.
- String - Signatures that use regular expression-based patterns to detect intrusions.
- Multi-string – Supports flexible pattern matching and Trend Labs signatures.
- Other – Internal engine that handles miscellaneous signatures.

IPS Signature Alarm



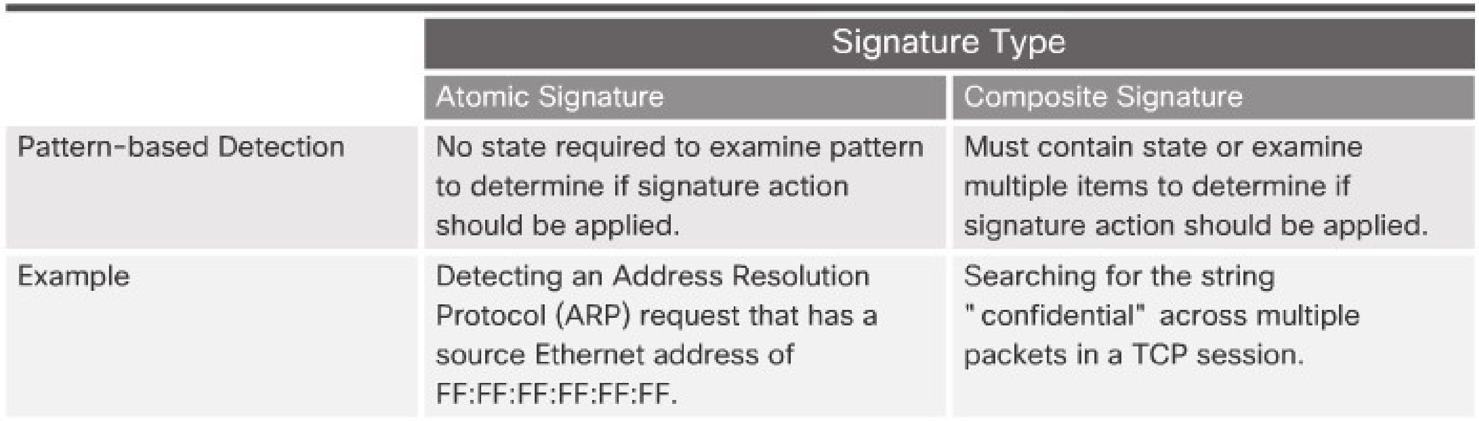
Detection Type	Advantages
Pattern-based Detection	- Easy configuration - Fewer false positives - Good signature design
Anomaly-based Detection	- Simple and reliable - Customized policies
Policy-based Detection	- Easy configuration - Can detect unknown attacks
Honey pot-based Detection	- Window to view attacks - Distract and confuse attackers - Slow down and avert attacks - Collect information about attack



Detection Type	Disadvantages
Pattern-based Detection	- No detection of unknown signatures - Initially a lot of false positives - Signatures must be created, updated, and tuned
Anomaly-based Detection	- Generic output - Policy must be created
Policy-based Detection	- Difficult to profile typical activity in large networks - Traffic profile must be constant
Honey pot-based Detection	- Dedicated honey pot server - Hot pot server must not be trusted

Pattern-Based Detection

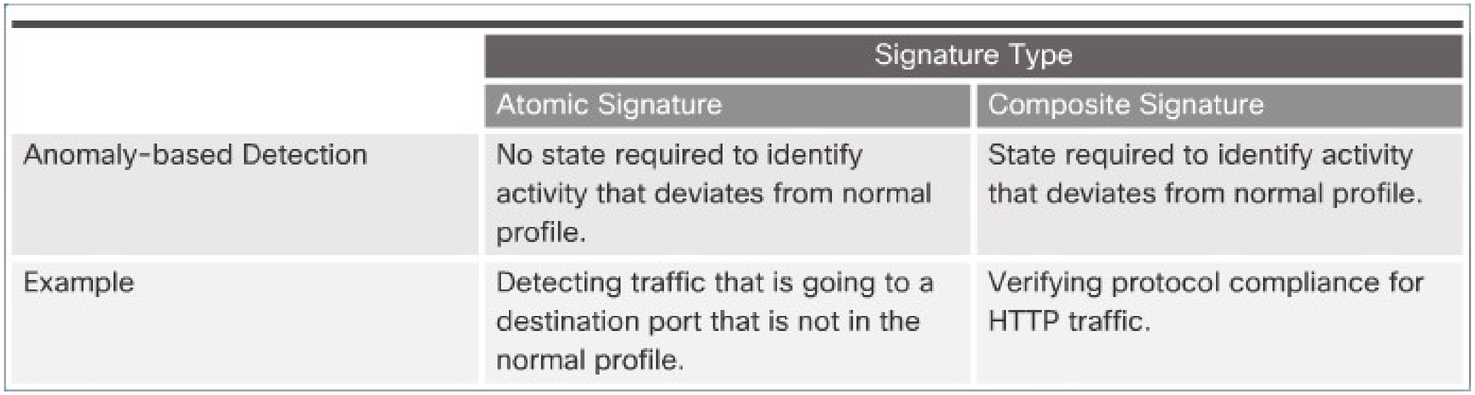
Also known as signature-based detection, compares the network traffic to a database of known attacks and triggers an alarm, or prevents communication if a match is found.



	Signature Type	
	Atomic Signature	Composite Signature
Pattern-based Detection	No state required to examine pattern to determine if signature action should be applied.	Must contain state or examine multiple items to determine if signature action should be applied.
Example	Detecting 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.

Anomaly-Based Detection

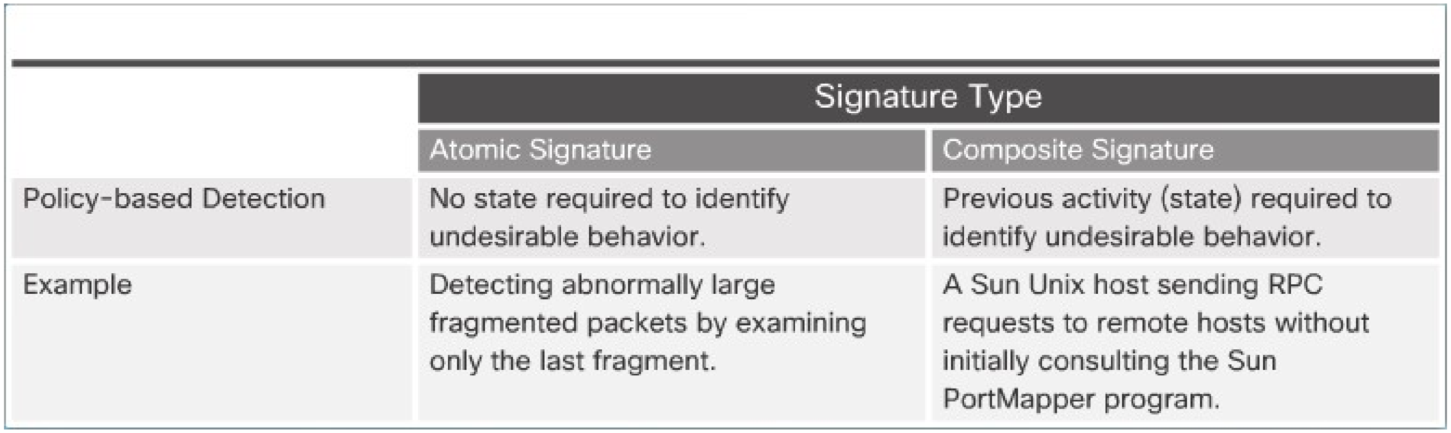
- Also known as profile-based detection, at first the network administrator has to define a profile what is considered normal for the network/host
- The signature triggers an action if excessive activity occurs which are deviated from normal profile



	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.

Policy-Based and Honey Pot-Based Detection

- Policy-based also known as behavior-based detection, the network administrator defines behaviors that are suspicious based on historical analysis
- Honeypot-based uses a dummy server to attract attacks. It is to distract attacks away from the real network devices.



	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.

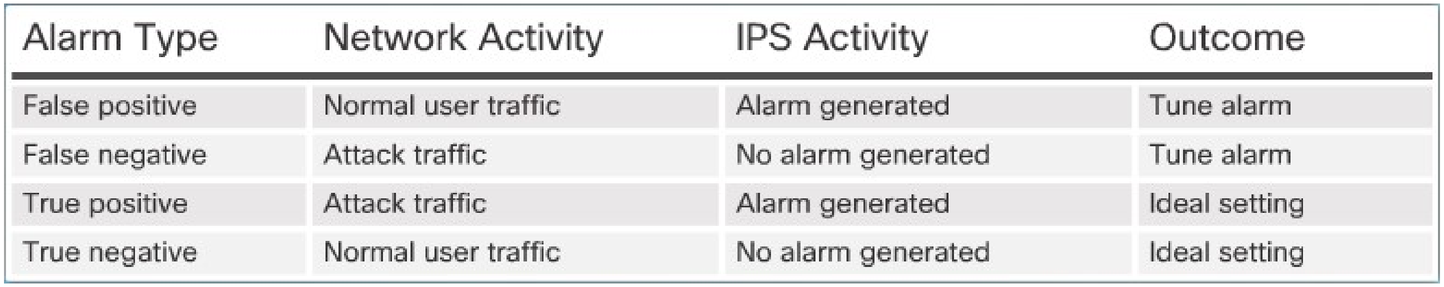
Benefits of installing an IPS

Benefits:

- It uses underlying routing infrastructure to provide an additional layer of security.
- It is inline and is supported on a broad range of routing platforms.
- It provides threat protection at all entry points to the network when used in combination with Cisco IDS, Cisco IOS Firewall, VPN, and NAC solutions
- The size of the signature database used by the devices can be adapted to the amount of available memory in the router.

Alarm Triggering Mechanisms

Understanding Alarm Types:



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

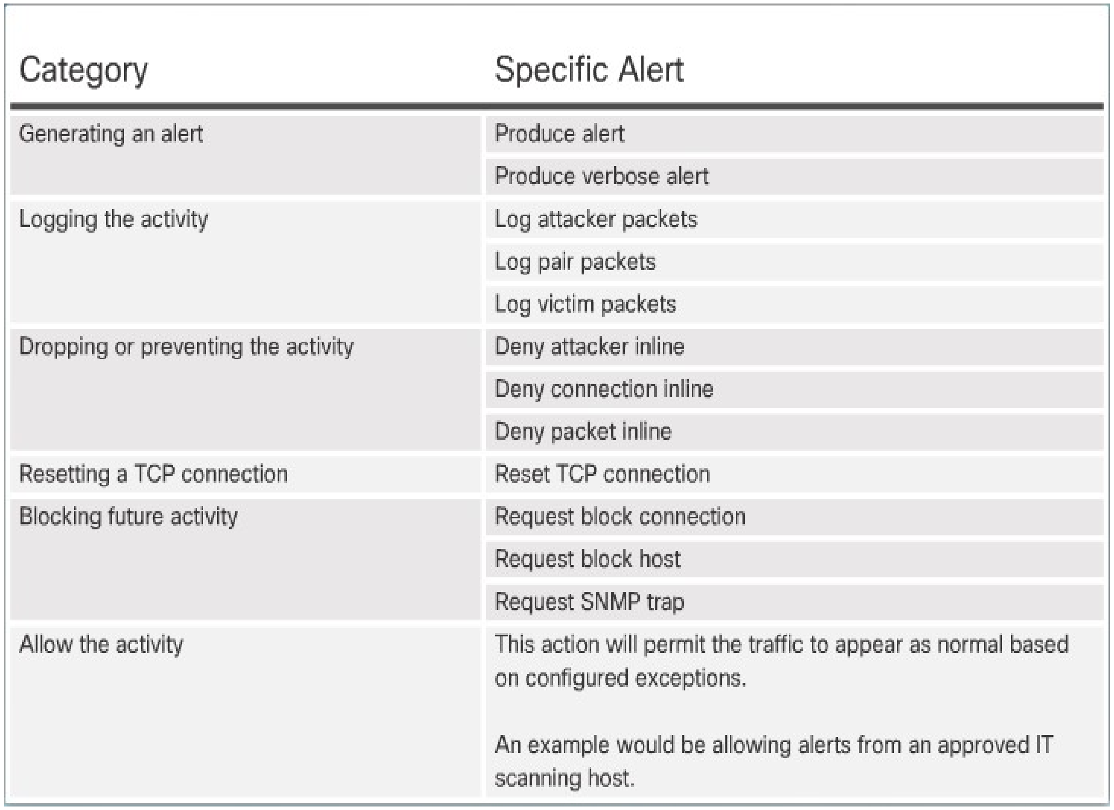
- Tune Alarm

- An administrator must balance the number of incorrect alarms that can be tolerated with the ability of the signature to detect actual intrusions
- If IPS systems use untuned signatures, they produce many false positive alarms

IPS Signature Actions

When a signature detects the activity which it is configured, the following actions can be triggered:

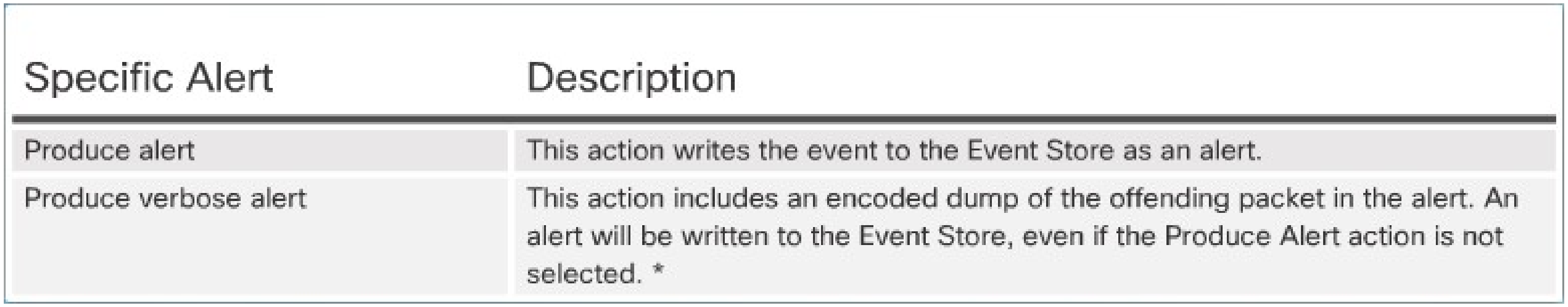
- Generating an alert
- Log the activity
- Drop or prevent the activity
- Reset a TCP connection
- Block future activity
- Allow the activity



Category	Specific Alert
Generating an alert	Produce alert
	Produce verbose alert
Logging the activity	Log attacker packets
	Log pair packets
	Log victim packets
Dropping or preventing the activity	Deny attacker inline
	Deny connection inline
	Deny packet inline
Resetting a TCP connection	Reset TCP connection
Blocking future activity	Request block connection
	Request block host
	Request SNMP trap
Allow the activity	This action will permit the traffic to appear as normal based on configured exceptions. An example would be allowing alerts from an approved IT scanning host.

Manage Generated Alerts

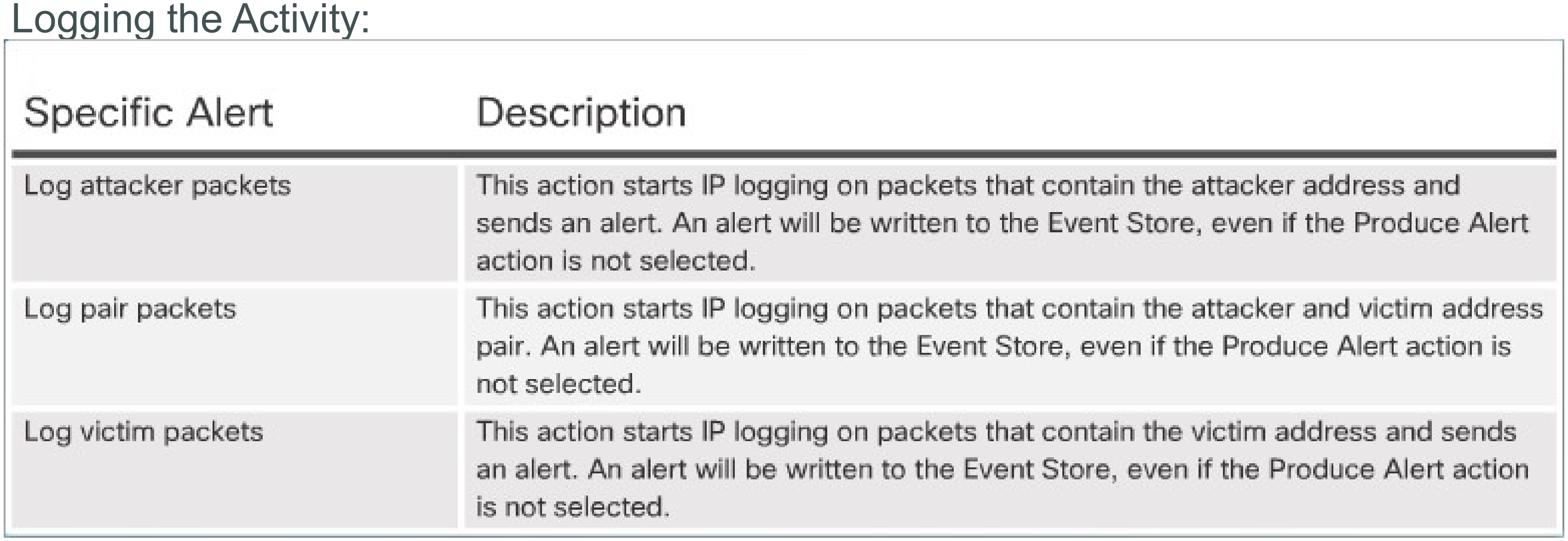
Generating an Alert:



Specific Alert	Description
Produce alert	This action writes the event to the Event Store as an alert.
Produce verbose alert	This action includes an encoded dump of the offending packet in the alert. An alert will be written to the Event Store, even if the Produce Alert action is not selected. *

Log Activities for Later Analysis

Logging the Activity:

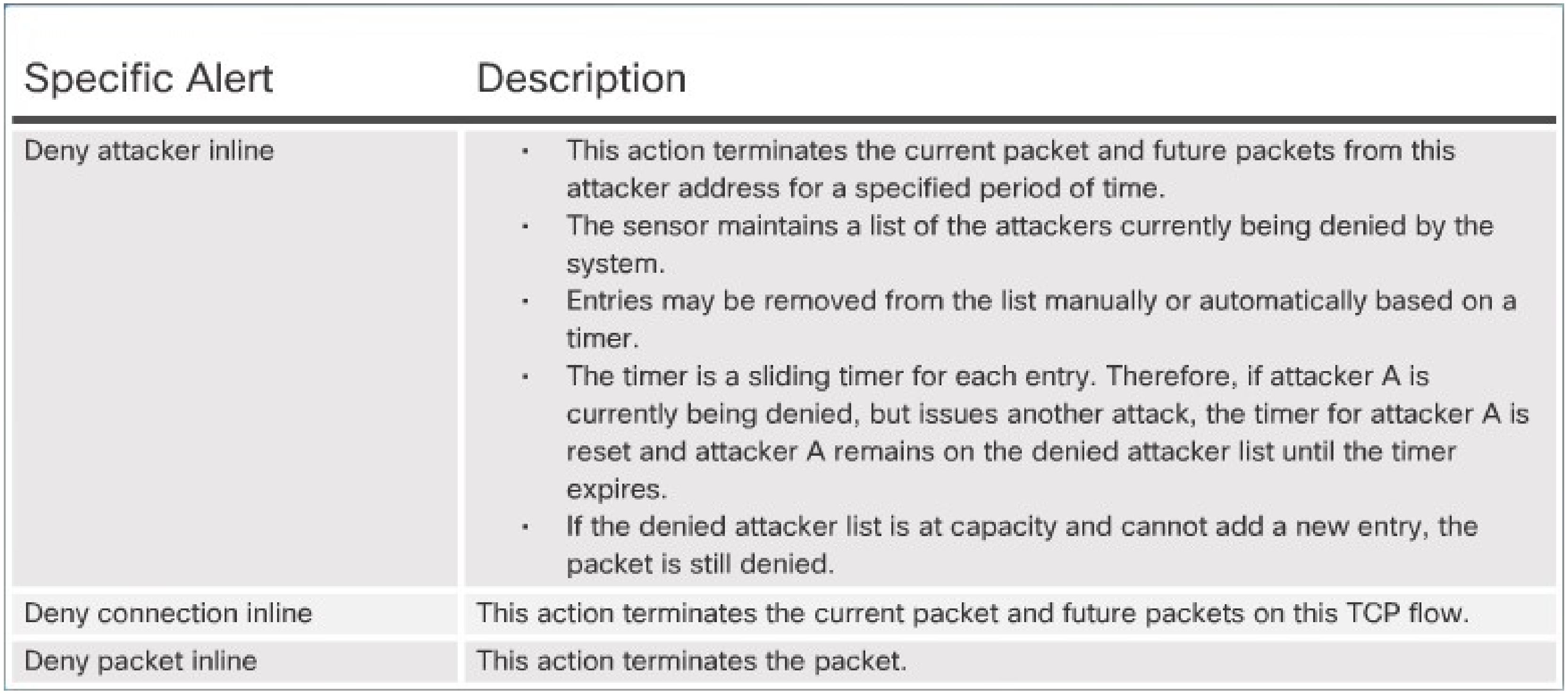


Specific Alert	Description
Log attacker packets	This action starts IP logging on packets that contain the attacker address and sends an alert. An alert will be written to the Event Store, even if the Produce Alert action is not selected.
Log pair packets	This action starts IP logging on packets that contain the attacker and victim address pair. An alert will be written to the Event Store, even if the Produce Alert action is not selected.
Log victim packets	This action starts IP logging on packets that contain the victim address and sends an alert. An alert will be written to the Event Store, even if the Produce Alert action is not selected.

- When an administrator has no sufficient information to stop the activity, he logs the activity. The logging can be attacker packets, victim packets or both
- The administrator can then perform a detailed analysis, and make a decision as to allow or deny it in the future

Deny the Activity

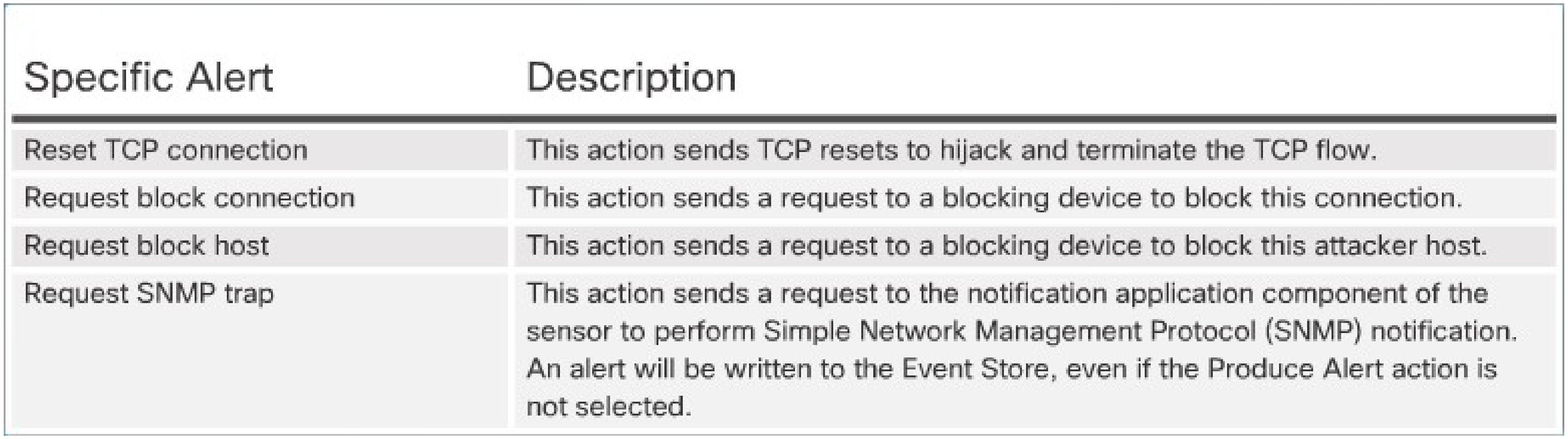
Dropping or Preventing the Activity:



Specific Alert	Description
Deny attacker inline	• This action terminates the current packet and future packets from this attacker address for a specified period of time. • The sensor maintains a list of the attackers currently being denied by the system. • Entries may be removed from the list manually or automatically based on a timer. • The timer is a sliding timer for each entry. Therefore, if attacker A is currently being denied, but issues another attack, the timer for attacker A is reset and attacker A remains on the denied attacker list until the timer expires. • If the denied attacker list is at capacity and cannot add a new entry, the packet is still denied.
Deny connection inline	This action terminates the current packet and future packets on this TCP flow.
Deny packet inline	This action terminates the packet.

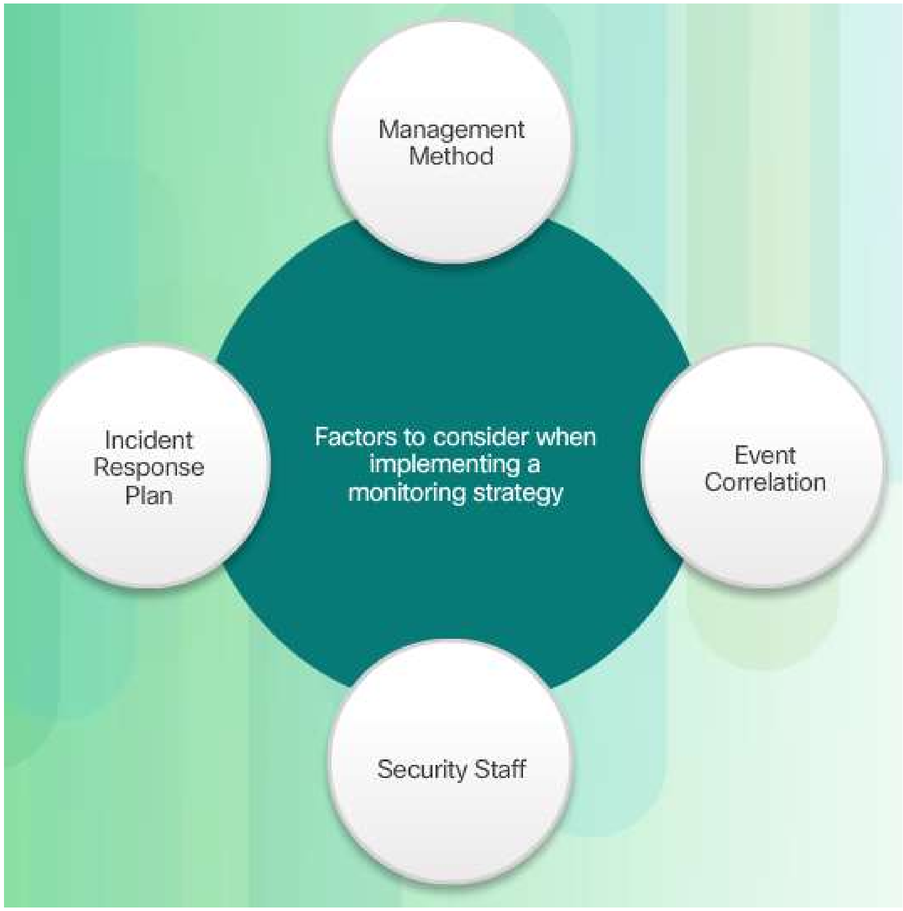
Reset, Block, and Allow Traffic

Resetting the Connection and Blocking the Activity:

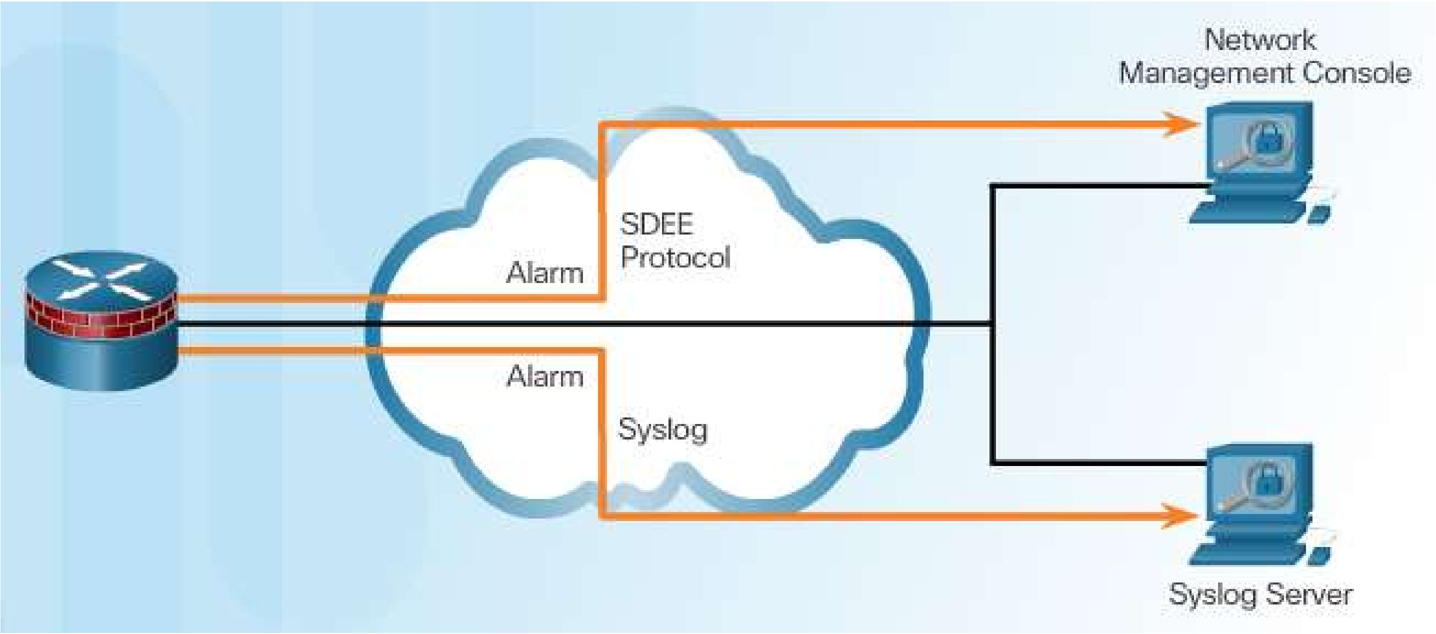


Specific Alert	Description
Reset TCP connection	This action sends TCP resets to hijack and terminate the TCP flow.
Request block connection	This action sends a request to a blocking device to block this connection.
Request block host	This action sends a request to a blocking device to block this attacker host.
Request SNMP trap	This action sends a request to the notification application component of the sensor to perform Simple Network Management Protocol (SNMP) notification. An alert will be written to the Event Store, even if the Produce Alert action is not selected.

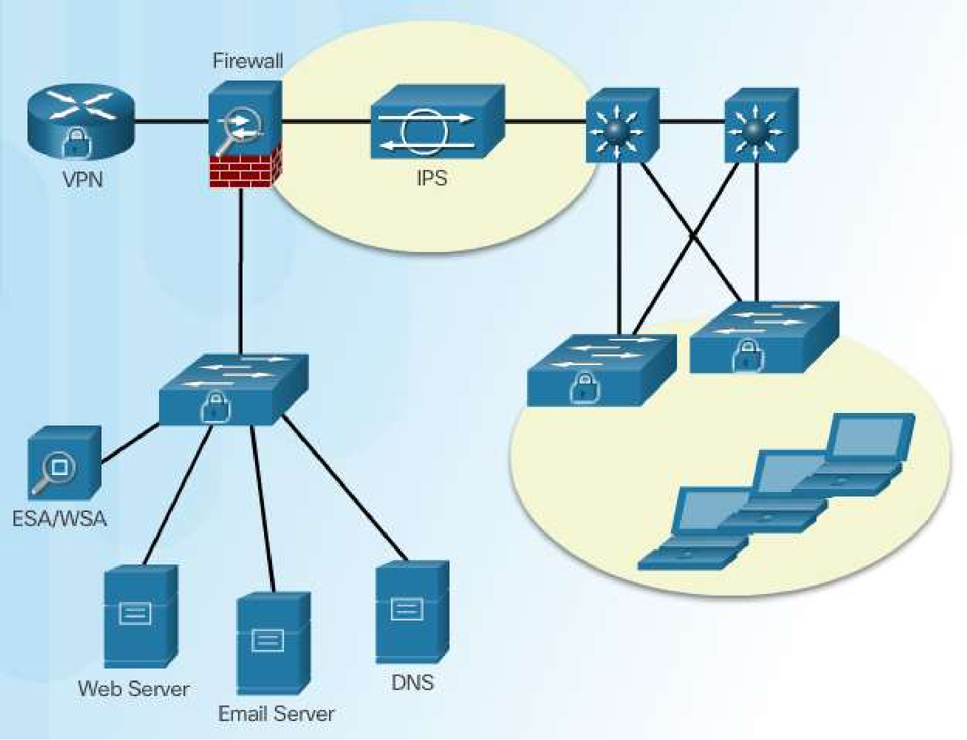
Monitor Activity



Secure Device Event Exchange



IPS Configuration Best Practices



- Need to upgrade sensors with the latest signature packs
- Update signature packs automatically
- Download new signatures to a secure server (SFTP) within the management network
- Configure the sensors to regularly check the SFTP server for new signature packs
- Synchronize the signature levels supported on the management console with the signature packs on the sensors

Configure Cisco IOS IPS with CLI

Step 1. Download the IOS IPS files.

Step 2. Create an IOS IPS configuration directory in Flash.

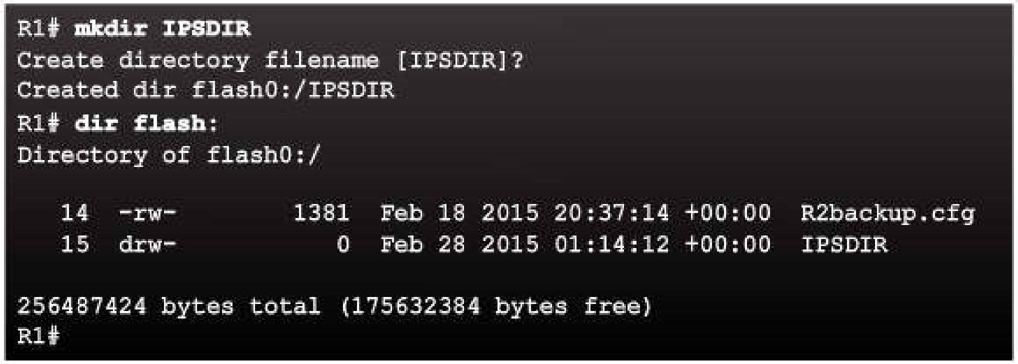
Step 3. Configure an IOS IPS crypto key.

Step 4. Enable IOS IPS.

Step 5. Load the IOS IPS signature package to the router.

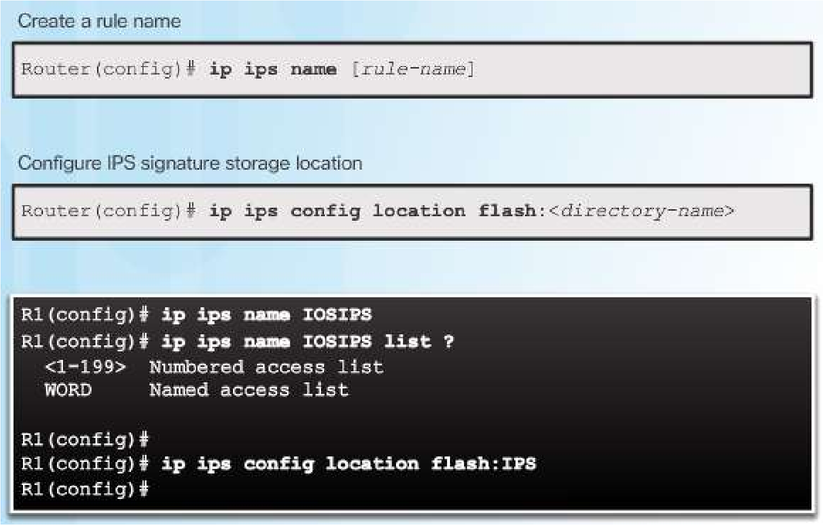
Download the IOS IPS Files

- Step 1: Download the IOS IPS signature package files and a public crypto key from Cisco website
- Step 2: Create an IOS IPS configuration directory in flash
- Step 3: Configure an IOS IPS crypto key



```
R1# mkdir IPSDIR
Create directory filename [IPSDIR]?
Created dir flash0:/IPSDIR
R1# dir flash:
Directory of flash0:/

   14  -rw-       1381  Feb 18 2015 20:37:14 +00:00  R2backup.cfg
   15  drw-          0  Feb 28 2015 01:14:12 +00:00  IPSDIR

256487424 bytes total (175632384 bytes free)
R1#
```

Step 4: Enable IOS IPS



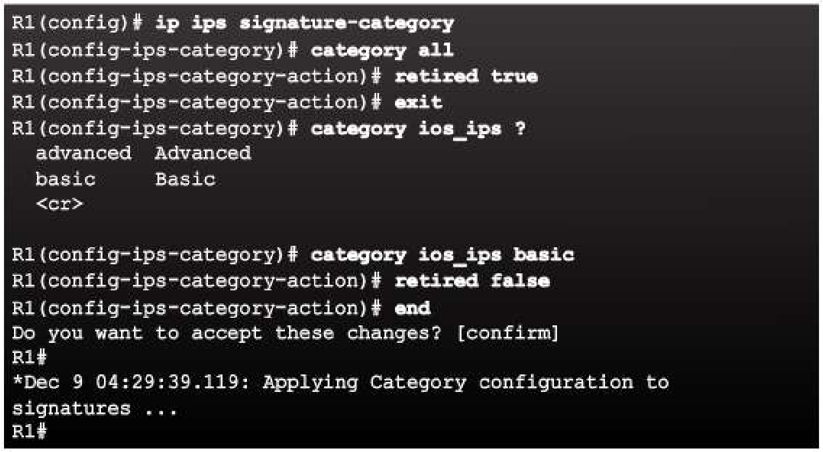
Create a rule name

```
Router(config)# ip ips name [rule-name]
```

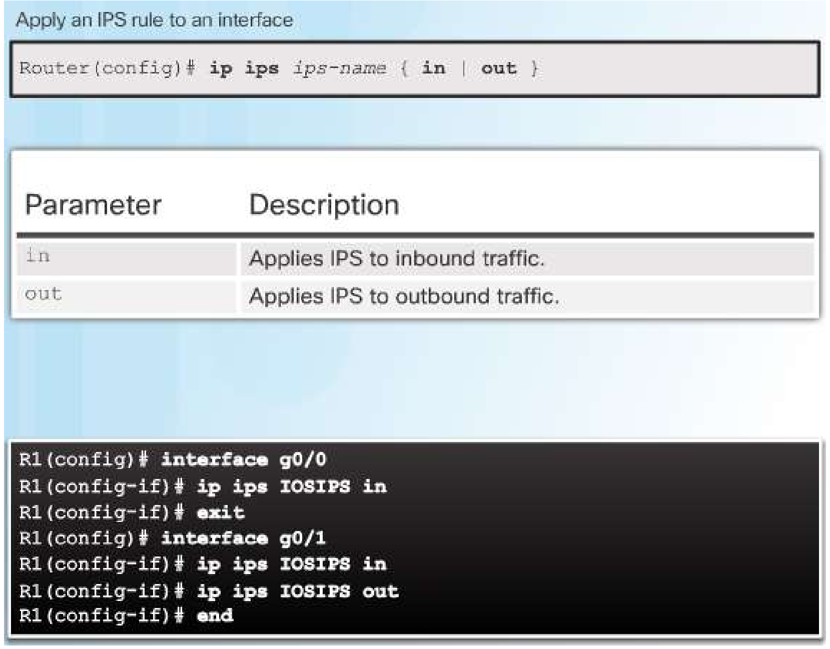
Configure IPS signature storage location

```
Router(config)# ip ips config location flash:<directory-name>
```

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

R1(config)#
R1(config)# ip ips config location flash:IPS
R1(config)#
```



```
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)# category ios_ips ?
  advanced  Advanced
  basic     Basic
  <cr>

R1(config-ips-category)# category ios_ips basic
R1(config-ips-category-action)# retired false
R1(config-ips-category-action)# end
Do you want to accept these changes? [confirm]
R1#
*Dec 9 04:29:39.119: Applying Category configuration to
signatures ...
R1#
```



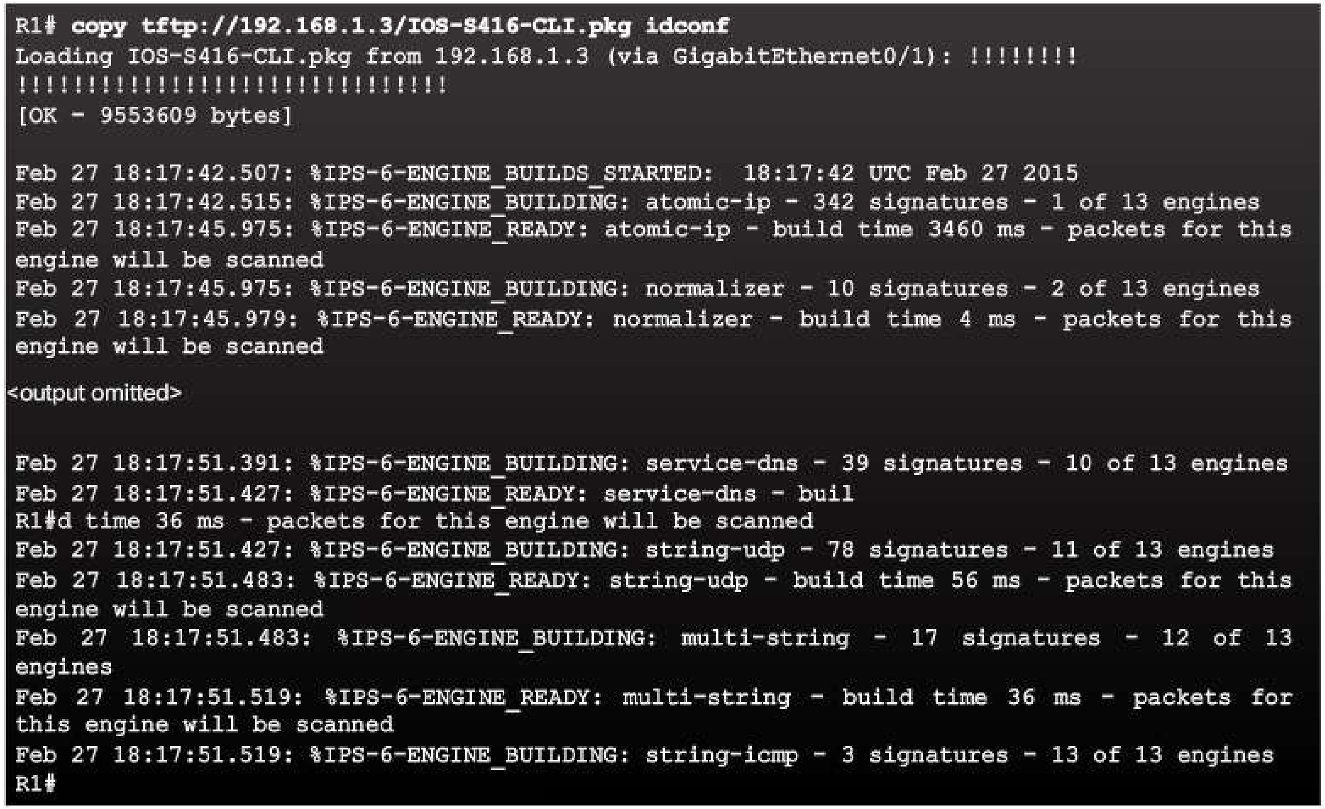
Apply an IPS rule to an interface

```
Router(config)# ip ips ips-name { in | out }
```

Parameter	Description
in	Applies IPS to inbound traffic.
out	Applies IPS to outbound traffic.

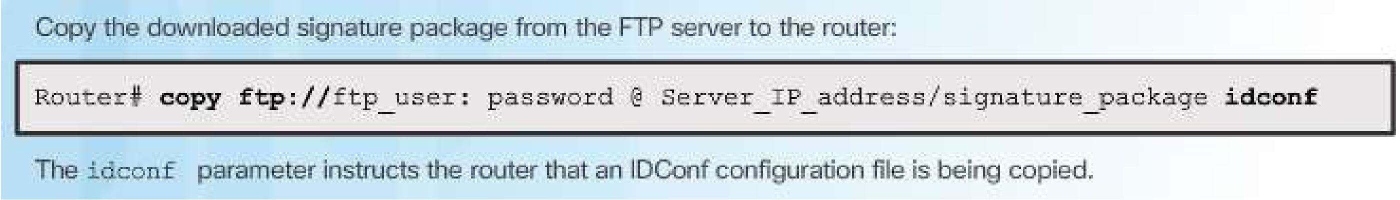
```
R1(config)# interface g0/0
R1(config-if)# ip ips IOSIPS in
R1(config-if)# exit
R1(config)# interface g0/1
R1(config-if)# ip ips IOSIPS in
R1(config-if)# ip ips IOSIPS out
R1(config-if)# end
```

Step 5: Load the IPS Signature Package in RAM



```
R1# copy tftp://192.168.1.3/IOS-S416-CLI.pkg idconf
Loading IOS-S416-CLI.pkg from 192.168.1.3 (via GigabitEthernet0/1): !!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 9553609 bytes]

Feb 27 18:17:42.507: %IPS-6-ENGINE_BUILDS_STARTED:  18:17:42 UTC Feb 27 2015
Feb 27 18:17:42.515: %IPS-6-ENGINE_BUILDING: atomic-ip - 342 signatures - 1 of 13 engines
Feb 27 18:17:45.975: %IPS-6-ENGINE_READY: atomic-ip - build time 3460 ms - packets for this
engine will be scanned
Feb 27 18:17:45.975: %IPS-6-ENGINE_BUILDING: normalizer - 10 signatures - 2 of 13 engines
Feb 27 18:17:45.979: %IPS-6-ENGINE_READY: normalizer - build time 4 ms - packets for this
engine will be scanned
<output omitted>

Feb 27 18:17:51.391: %IPS-6-ENGINE_BUILDING: service-dns - 39 signatures - 10 of 13 engines
Feb 27 18:17:51.427: %IPS-6-ENGINE_READY: service-dns - buil
R1#d time 36 ms - packets for this engine will be scanned
Feb 27 18:17:51.427: %IPS-6-ENGINE_BUILDING: string-udp - 78 signatures - 11 of 13 engines
Feb 27 18:17:51.483: %IPS-6-ENGINE_READY: string-udp - build time 56 ms - packets for this
engine will be scanned
Feb 27 18:17:51.483: %IPS-6-ENGINE_BUILDING: multi-string - 17 signatures - 12 of 13
engines
Feb 27 18:17:51.519: %IPS-6-ENGINE_READY: multi-string - build time 36 ms - packets for
this engine will be scanned
Feb 27 18:17:51.519: %IPS-6-ENGINE_BUILDING: string-icmp - 3 signatures - 13 of 13 engines
R1#
```

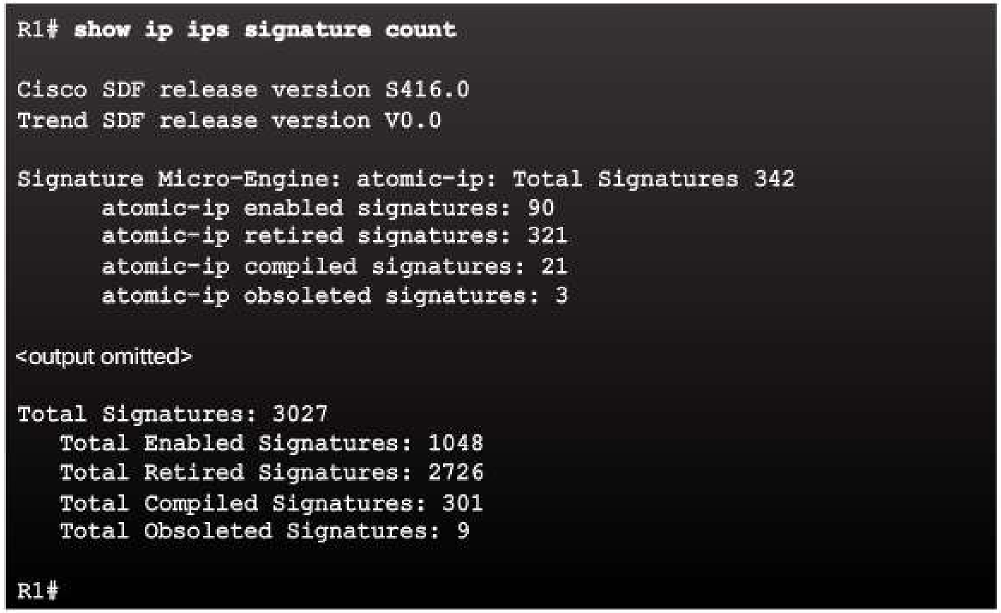
Load the IPS Signature Package in RAM



Copy the downloaded signature package from the FTP server to the router:

```
Router# copy ftp://ftp_user: password @ Server_IP_address/signature_package idconf
```

The `idconf` parameter instructs the router that an IDConf configuration file is being copied.

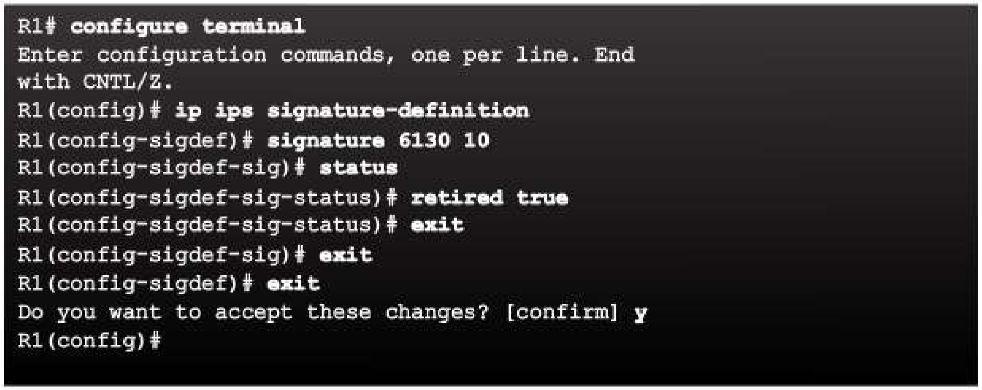


```
R1# show ip ips signature count

Cisco SDF release version S416.0
Trend SDF release version V0.0

Signature Micro-Engine: atomic-ip: Total Signatures 342
      atomic-ip enabled signatures: 90
      atomic-ip retired signatures: 321
      atomic-ip compiled signatures: 21
      atomic-ip obsoleted signatures: 3

<output omitted>

Total Signatures: 3027
   Total Enabled Signatures: 1048
   Total Retired Signatures: 2726
   Total Compiled Signatures: 301
   Total Obsoleted Signatures: 9

R1#
```

Retire and Unretire Signatures

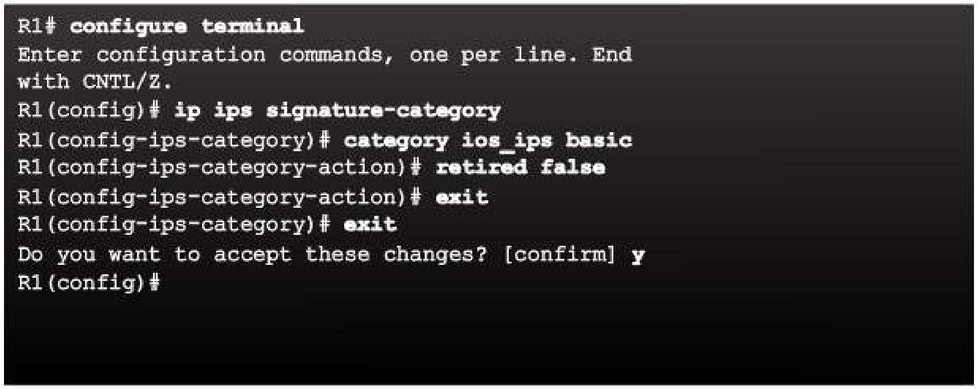
A network administrator can retire or unretired individual signatures or a group of signatures that belong to a signature category

Retiring an Individual Signature:



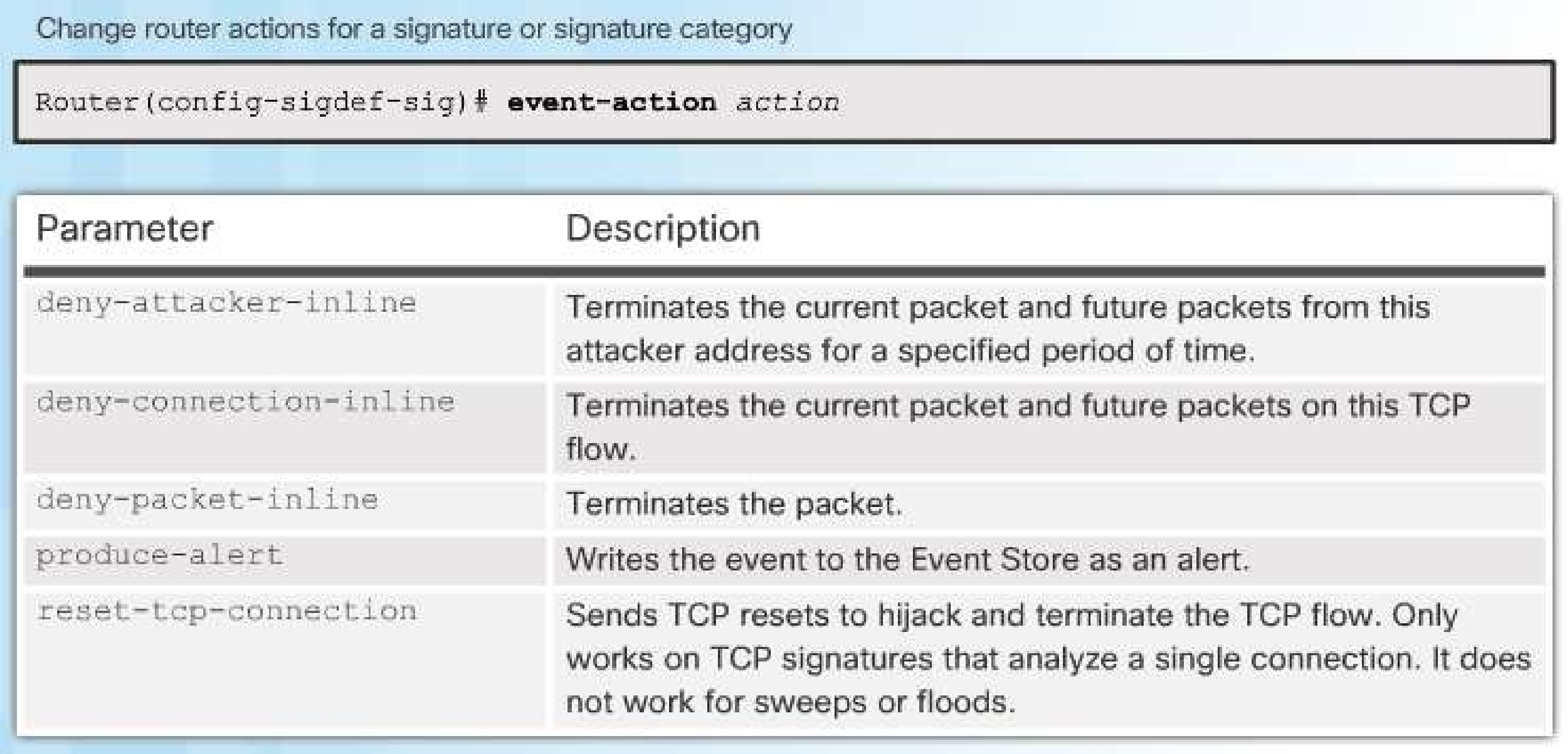
```
R1# configure terminal
Enter configuration commands, one per line. End
with CNTL/Z.
R1(config)# ip ips signature-definition
R1(config-sigdef)# signature 6130 10
R1(config-sigdef-sig)# status
R1(config-sigdef-sig-status)# retired true
R1(config-sigdef-sig-status)# exit
R1(config-sigdef-sig)# exit
R1(config-sigdef)# exit
Do you want to accept these changes? [confirm] y
R1(config)#
```

Retiring a Signature Category:



```
R1# configure terminal
Enter configuration commands, one per line. End
with CNTL/Z.
R1(config)# ip ips signature-category
R1(config-ips-category)# category ios_ips 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)#
```

Change Signature Actions



Change router actions for a signature or signature category

```
Router(config-sigdef-sig)# event-action action
```

Parameter	Description
deny-attacker-inline	Terminates the current packet and future packets from this attacker address for a specified period of time.
deny-connection-inline	Terminates the current packet and future packets on this TCP flow.
deny-packet-inline	Terminates the packet.
produce-alert	Writes the event to the Event Store as an alert.
reset-tcp-connection	Sends TCP resets to hijack and terminate the TCP flow. Only works on TCP signatures that analyze a single connection. It does not work for sweeps or floods.

Verify IOS IPS

Show commands to verify the IOS IPS configuration:

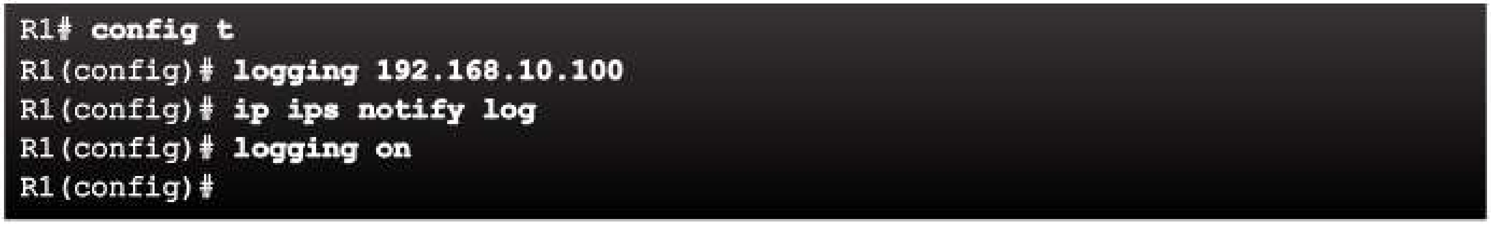
- show ip ips
- show ip ips all
- show ip ips configuration
- show ip ips interfaces
- show ip ips signatures
- show ip ips statistics

Clear commands to disable IPS:

- clear ip ips configuration
- clear ip ips statistics

Report IPS Alerts

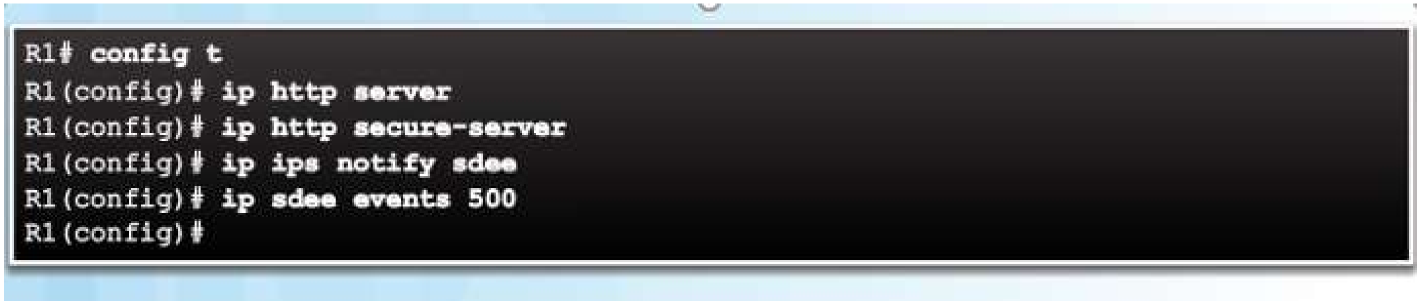
- Cisco IOS logging via syslog – the `log` keyword sends messages in syslog format



```
R1# config t
R1(config)# logging 192.168.10.100
R1(config)# ip ips notify log
R1(config)# logging on
R1(config)#
```

Enable SDEE

- SDEE uses HTTP and XML to provide standardized approach
- Enable an IOS IPS router using the `ip ips notify sdee` command



```
R1# config t
R1(config)# ip http server
R1(config)# ip http secure-server
R1(config)# ip ips notify sdee
R1(config)# ip sdee events 500
R1(config)#
```