

CCNA Security 2.0 Study Material – Chapter 5: Implementing Intrusion Prevention

 itexamanswers.net/ccna-security-2-0-study-material-chapter-5-implementing-intrusion-prevention.html

October 7, 2017

Chapter Outline:

5.0 Introduction

5.1 IPS Technologies

5.2 IPS Signatures

5.3 Implement IPS

5.4 Summary

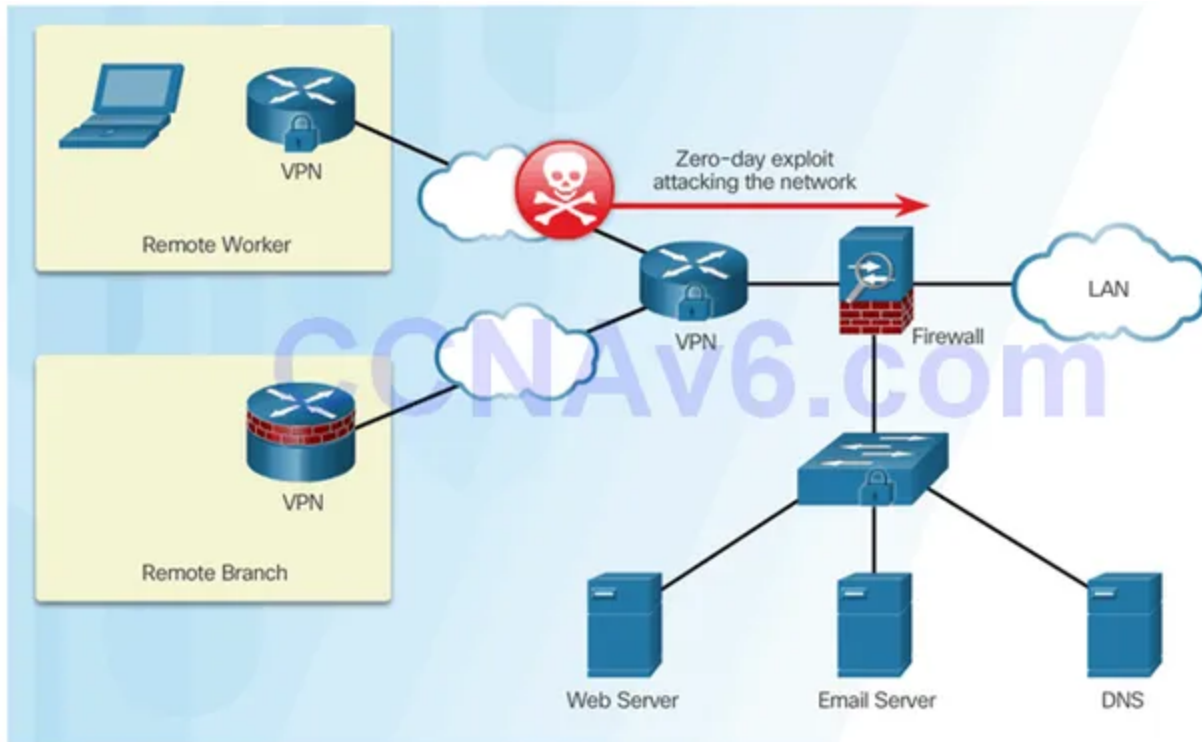
Section 5.1: IPS Technologies

Upon completion of this section, you should be able to:

- Explain zero-day attacks.
- Understand how to monitor, detect and stop attacks.
- Describe the advantages and disadvantages of IDS and IPS.

Topic 5.1.1: IDS and IPS Characteristics

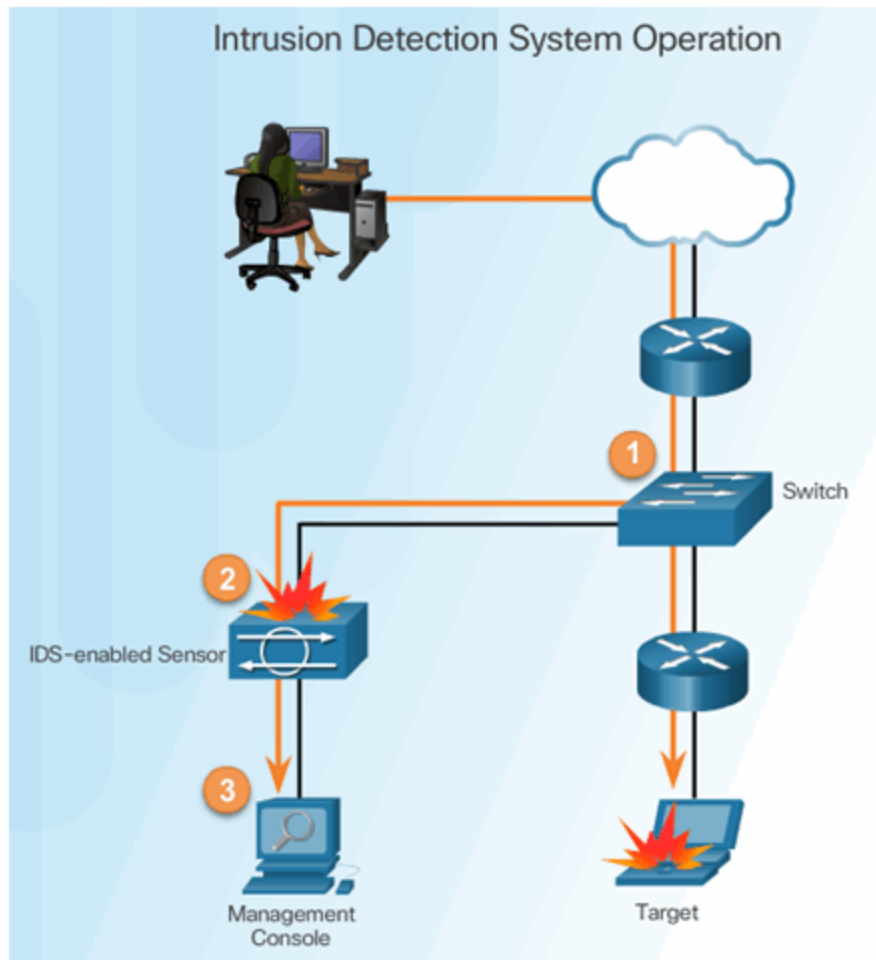
Zero-Day Attacks



Monitor for Attacks

Advantages of an IDS:

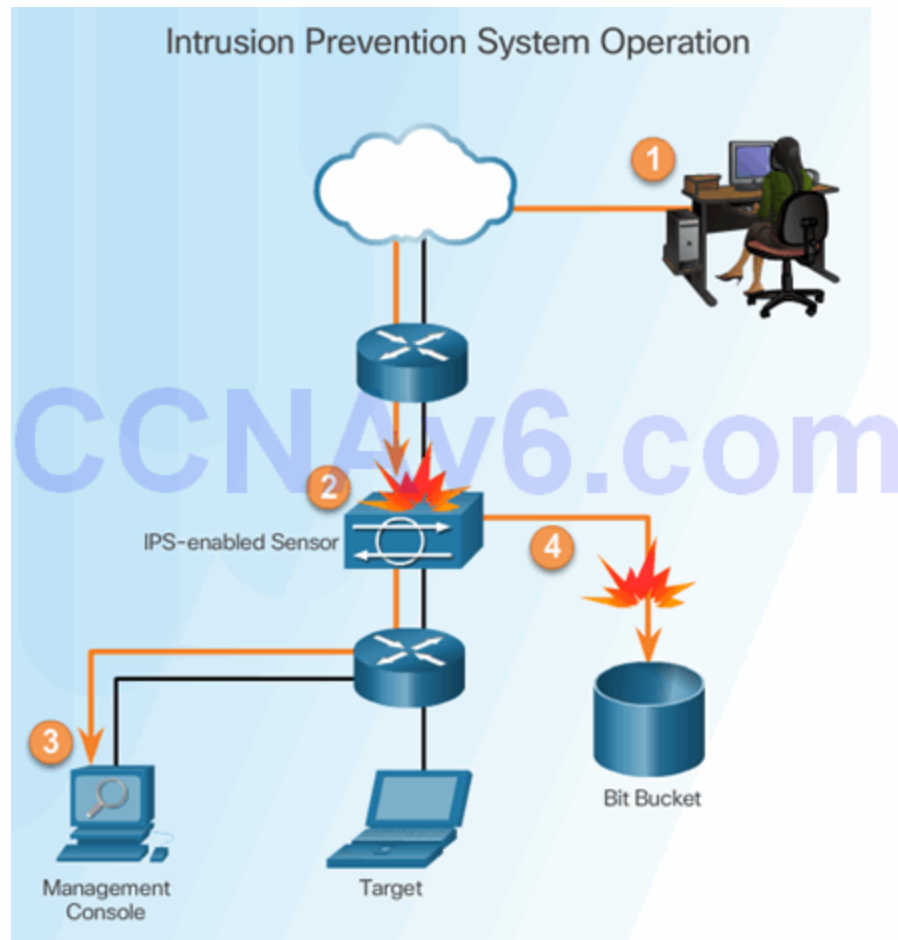
- Works passively
- Requires traffic to be mirrored in order to reach it
- Network traffic does not pass through the IDS unless it is mirrored



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

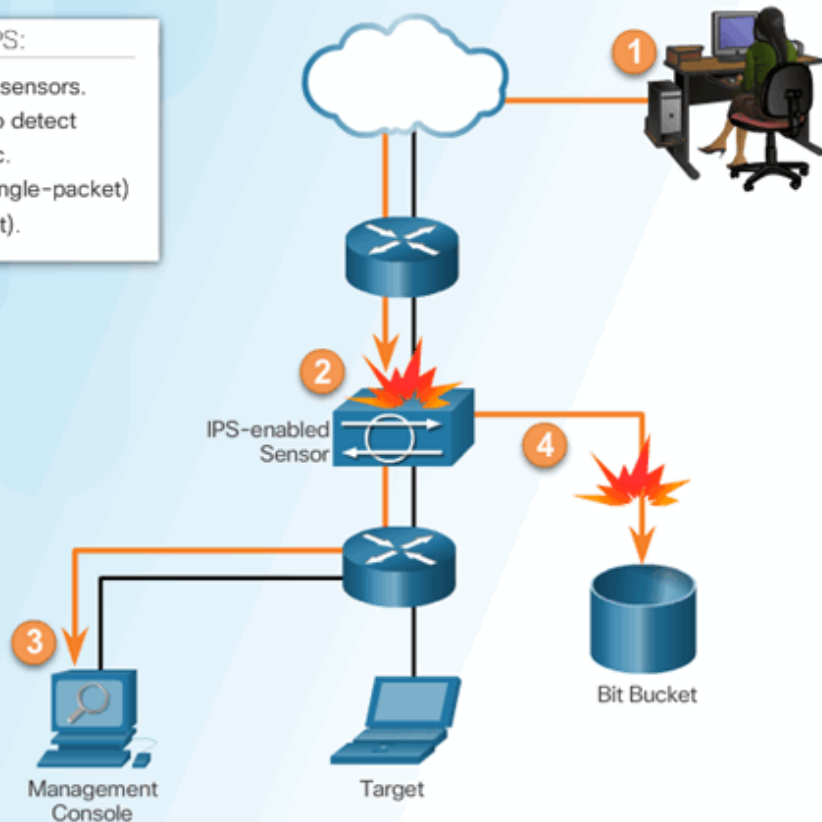


Similarities Between IDS and IPS

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

Advantages IPS:

- Stops trigger packets
- Can use stream normalization techniques

Disadvantages IDS:

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

Disadvantages IPS:

- Sensor issues might affect network traffic

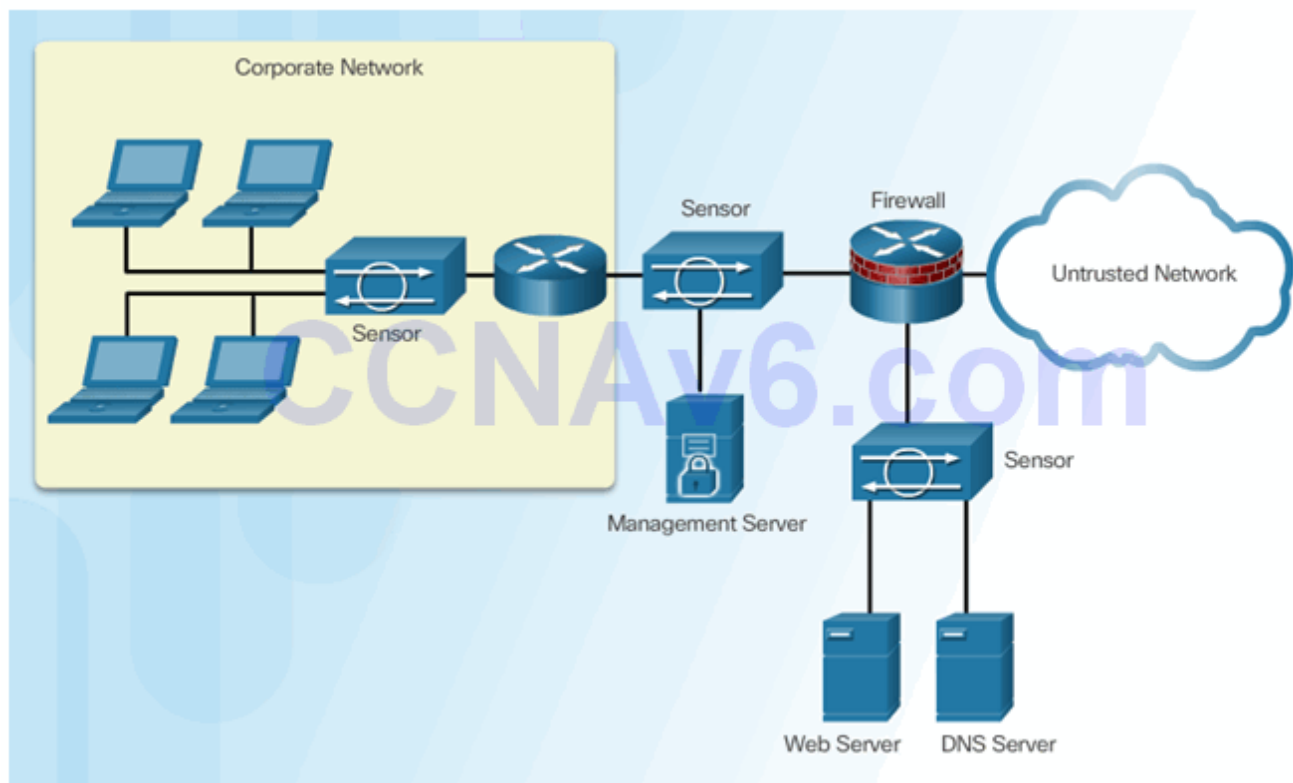
- Sensor overloading impacts the network
- Some impact on network

Topic 5.1.2: Network-Based IPS Implementations

Host-Based and Network-Based IPS

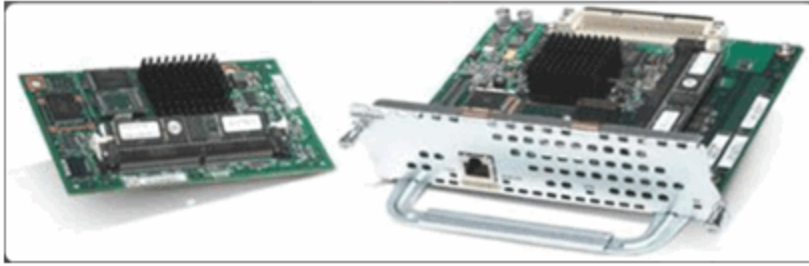
	Advantages	Disadvantages
Host-Based IPS	<ul style="list-style-type: none"> • Provides protection specific to a host operating system • Provides operating system and application level protection • Protects the host after the message is decrypted 	<ul style="list-style-type: none"> • Operating system dependent • Must be installed on all hosts
Network-Based IPS	<ul style="list-style-type: none"> • Cost effective • Operating system independent 	<ul style="list-style-type: none"> • Cannot examine encrypted traffic • Must stop malicious traffic prior to arriving at host

Network-Based IPS Sensors



Cisco's Modular and Appliance-Based IPS Solutions

Cisco IPS AIM and Network Module Enhanced (IPS NME)



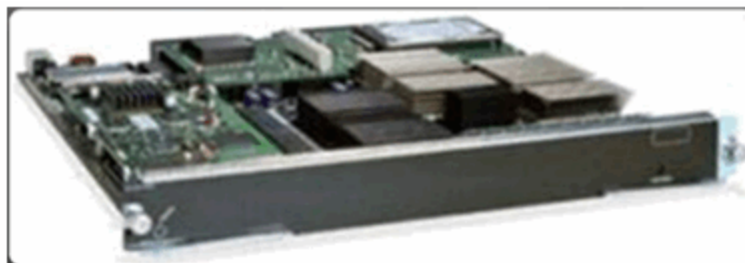
Cisco ASA AIP-SSM



Cisco IPS 4300 Series Sensors



Cisco Catalyst 6500 Series IDS Module



Choose an IPS Solution

Factors affecting the IPS sensor selection and deployment:

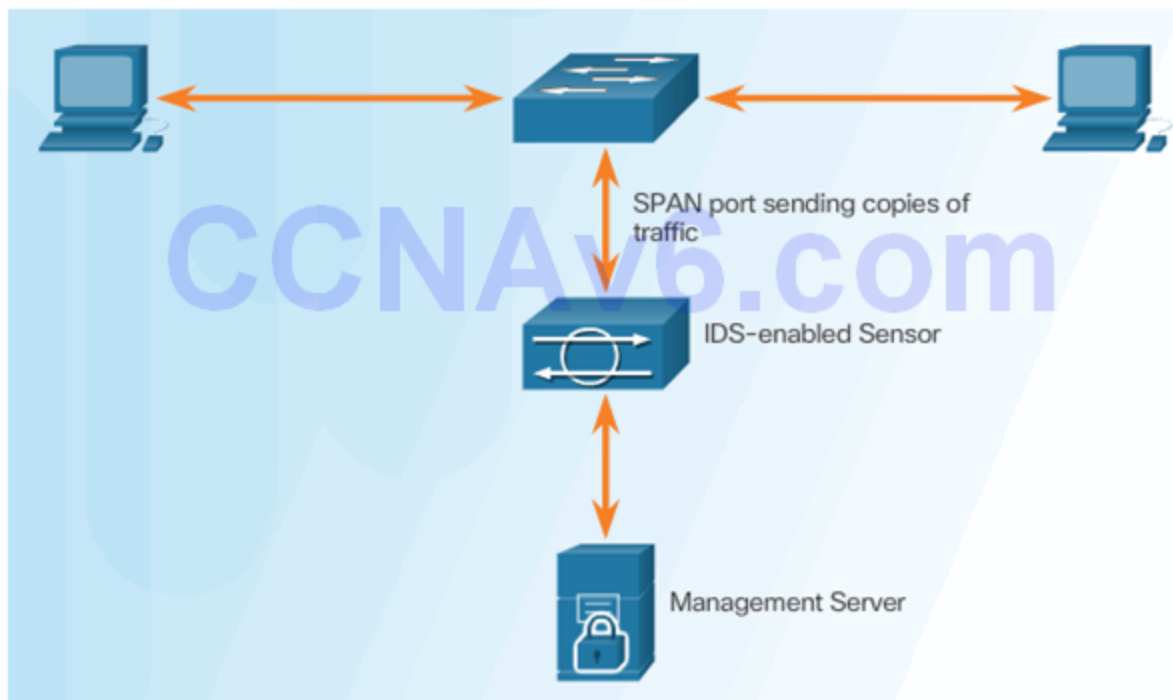
- Amount of network traffic
- Network topology
- Security budget
- Available security staff to manage IPS

IPS Advantages and Disadvantages

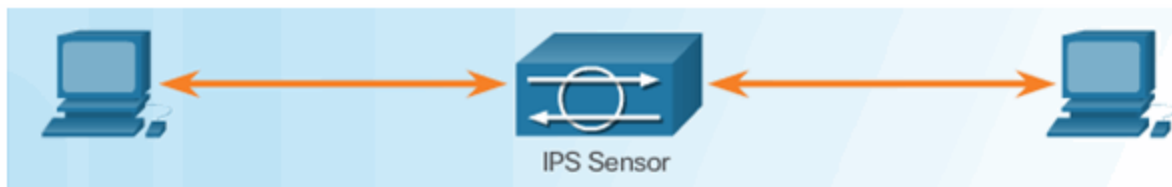
Advantages		Disadvantages
Network IPS	<ul style="list-style-type: none">• Is cost-effective• Not visible on the network• Operating system independent• Lower level network events seen	<ul style="list-style-type: none">• Cannot examine encrypted traffic• Cannot determine whether an attack was successful

Modes of Deployment

Promiscuous Mode



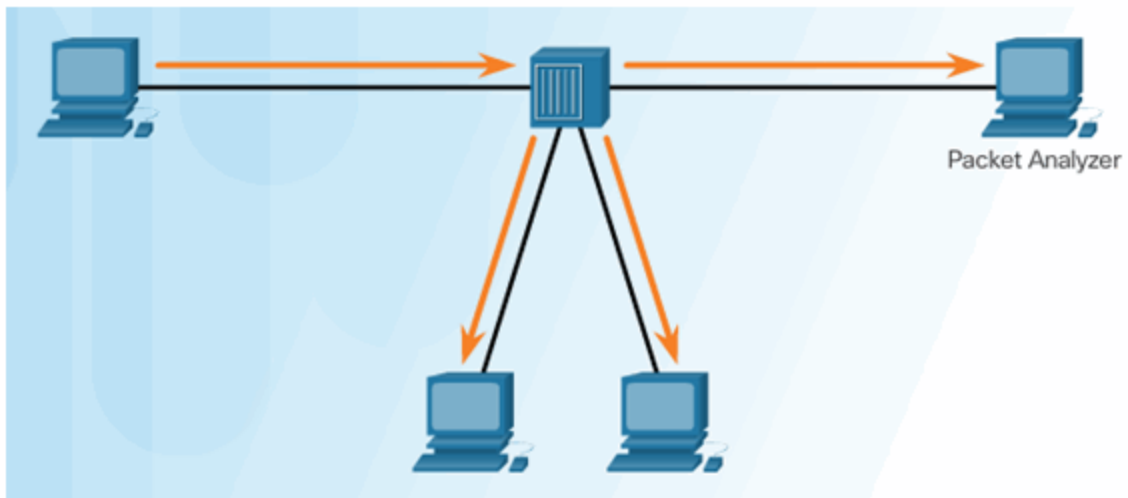
Inline Mode



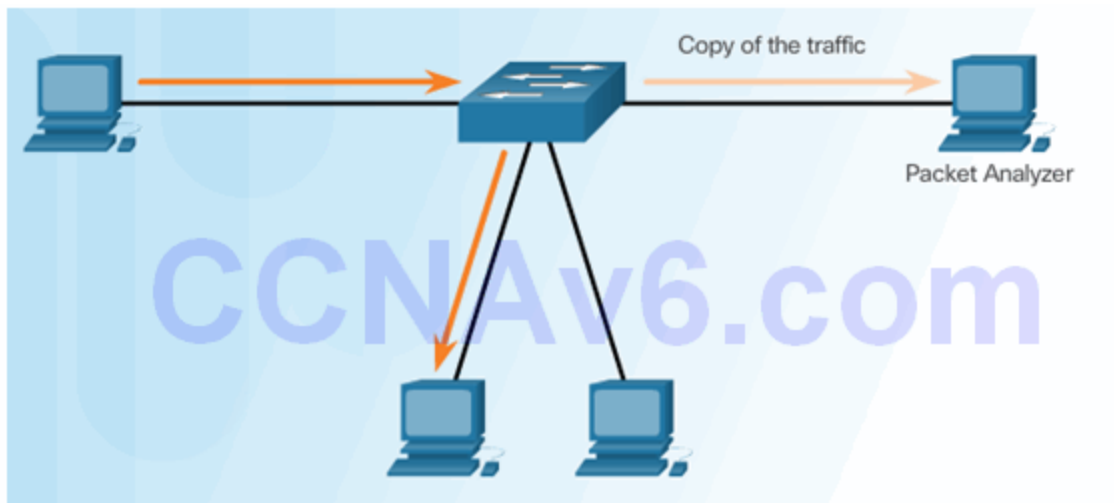
Topic 5.1.3: Cisco Switched Port Analyzer

Port Mirroring

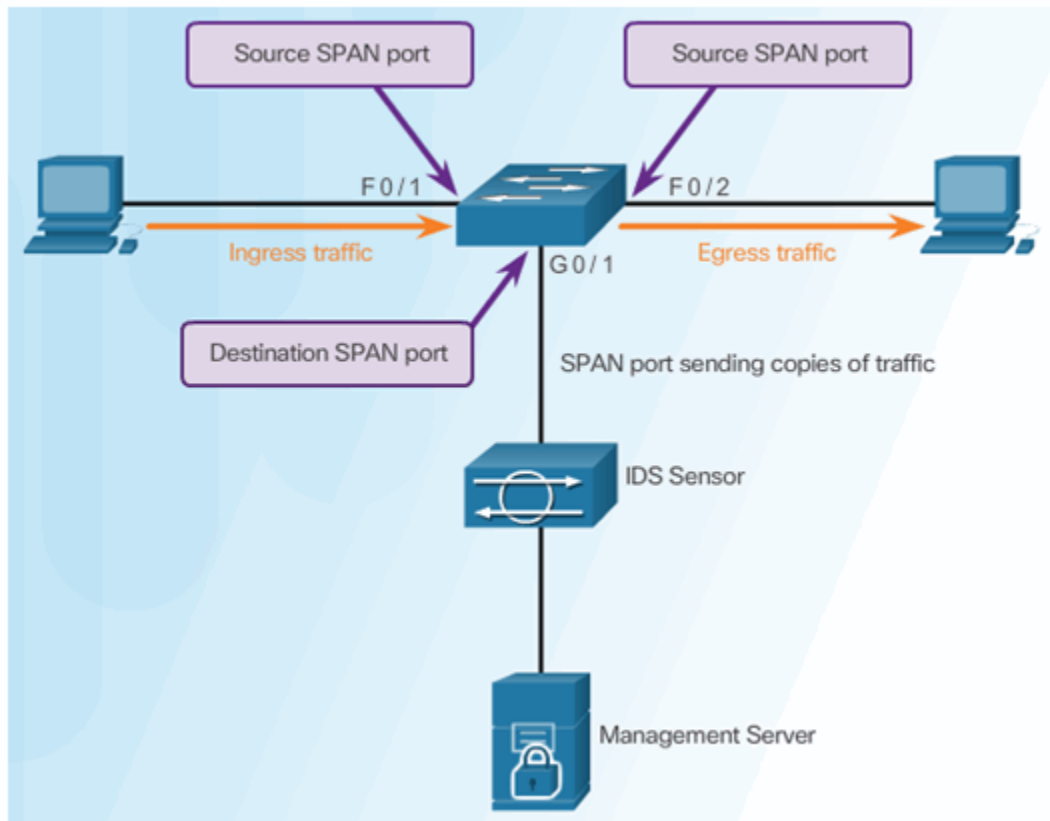
Traffic Sniffing Using a Hub



Traffic Sniffing Using a Switch



Cisco SPAN



Configuring Cisco SPAN Using Intrusion Detection

Cisco SPAN Commands:

Monitor session command – used to associate a source port and a destination port with a SPAN session.

Associate a SPAN session with a source port

```
Switch(config)# monitor session number source [ interface interface | vlan vlan ]
```

Associate a SPAN session with a destination port

```
Switch(config)# monitor session number destination [ interface interface | vlan vlan ]
```

Show monitor command – used to verify the SPAN session.

Section 5.2: IPS Signatures

Upon completion of the section, you should be able to:

- Understand IPS signature characteristics

- Explain IPS signature alarms
- Manage and monitor IPS
- Understand the global correlation of Cisco IPS devices

Topic 5.2.1: IPS Signature Characteristics

Signature Attributes

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.

The screenshot shows the Cisco Software Download Center interface. The top navigation bar includes links for Products & Services, Support, How to Buy, Training & Events, and Partners. The main heading is "Download Software". Below this, the breadcrumb trail reads: Downloads Home > Products > Security > Network Security > Integrated Threat Control > IOS Intrusion Prevention System Feature Software > IOS IPS Signature Data File-S855.

The main content area is titled "IOS Intrusion Prevention System Feature Software". It features a search bar, a "Release S855" section, and a "Signature Update S855 Readme" link. A large watermark "CCNAv6.com" is overlaid on the page.

Under the "Release S855" section, there is a table with the following information:

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

Buttons for "Download" and "Add to cart" are visible next to the table entry.

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.

Download a Signature File

The screenshot shows the Cisco Software Download Center interface. At the top is the Cisco logo and navigation links: Products & Services, Support, How to Buy, Training & Events, and Partners. Below this is a search bar and a 'Download Software' heading. The breadcrumb trail indicates the path: Downloads Home > Products > Security > Network Security > Integrated Threat Control > IOS Intrusion Prevention System Feature Software > IOS IPS Signature Data File-S855. The main content area is titled 'IOS Intrusion Prevention System Feature Software'. On the left, there's a sidebar with a search box and a list of releases: Latest (S855, S351) and All Releases (5.x, 4.x). The main content shows 'Release S855' with a warning about a defect in some IOS versions. Below the warning is a table with columns: File Information, Release Date, and Size. The table lists 'IOS IPS Signature Update Package in 5.x format for CLI users' (IOS-S855-CLI.pkg) with a release date of 03-MAR-2015 and a size of 21.52 MB. There are 'Download' and 'Add to cart' buttons next to the entry.

Topic 5.2.2: IPS Signature Alarms

Signature Alarm

Detection Type	Advantages
Pattern-based Detection	<ul style="list-style-type: none">• Easy configuration• Fewer false positives• Good signature design
Anomaly-based Detection	<ul style="list-style-type: none">• Simple and reliable• Customized policies
Policy-based Detection	<ul style="list-style-type: none">• Easy configuration• Can detect unknown attacks
Honey pot-based Detection	<ul style="list-style-type: none">• Window to view attacks• Distract and confuse attackers• Slow down and avert attacks• Collect information about attack

Detection Type

Disadvantages

Pattern-based Detection	<ul style="list-style-type: none">• No detection of unknown signatures• Initially a lot of false positives• Signatures must be created, updated, and tuned
Anomaly-based Detection	<ul style="list-style-type: none">• Generic output• Policy must be created
Policy-based Detection	<ul style="list-style-type: none">• Difficult to profile typical activity in large networks• Traffic profile must be constant
Honey pot-based Detection	<ul style="list-style-type: none">• Dedicated honey pot server• Hot pot server must not be trusted

Pattern-Based Detection

	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

	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

	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 the Cisco IOS IPS Solution

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

Topic 5.2.3: IPS Signature Actions

Signature Actions

Summary of Action Categories:

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	<p>This action will permit the traffic to appear as normal based on configured exceptions.</p> <p>An example would be allowing alerts from an approved IT scanning host.</p>

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.

Deny the Activity

Dropping or Preventing the Activity:

Specific Alert	Description
Deny attacker inline	<ul style="list-style-type: none"> 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.

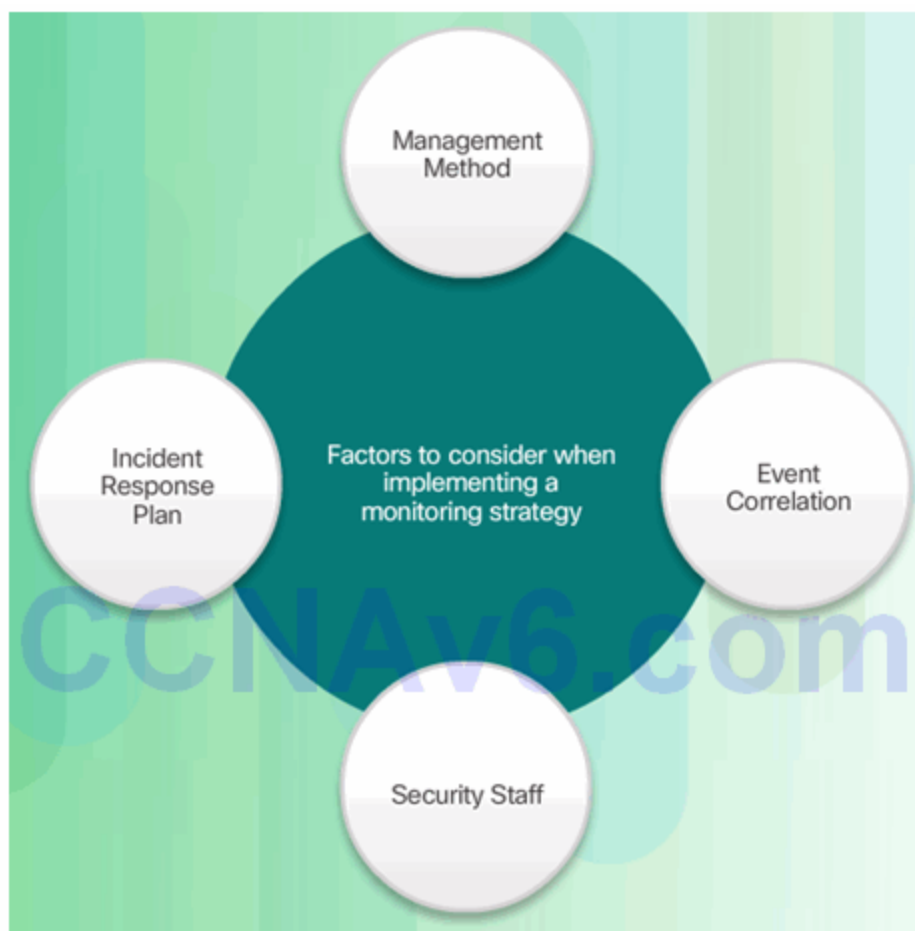
Topic 5.2.4: Manage and Monitor IPS

Monitor Activity

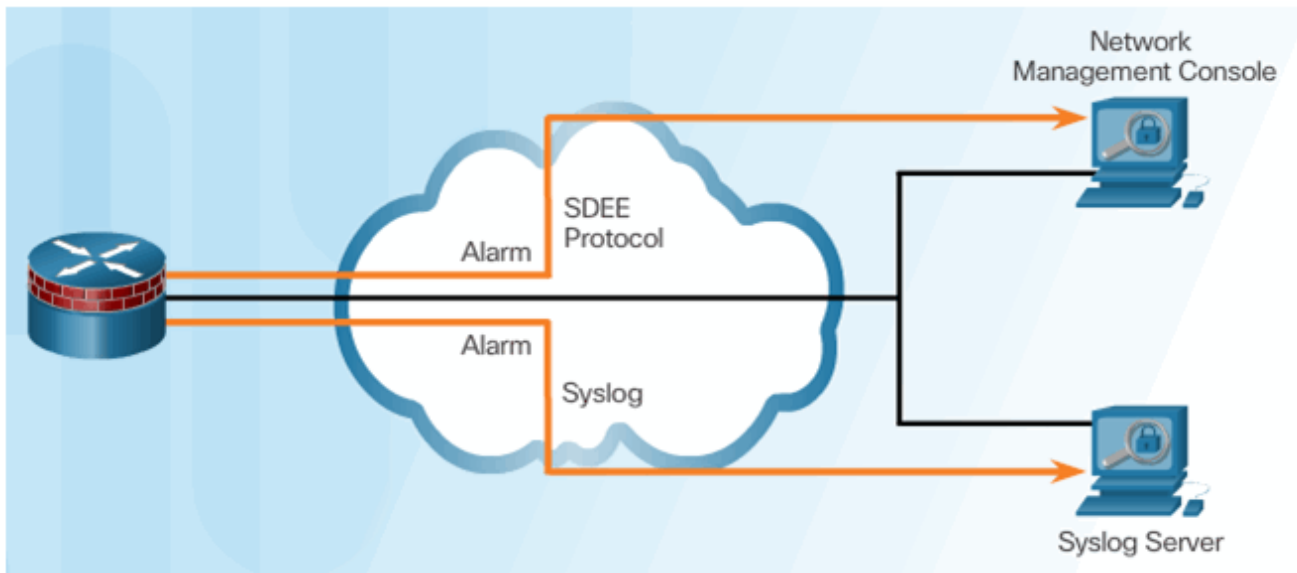
IPS Planning and Monitoring Considerations:

- Management method
- Event correlation
- Security staff
- Incident response plan

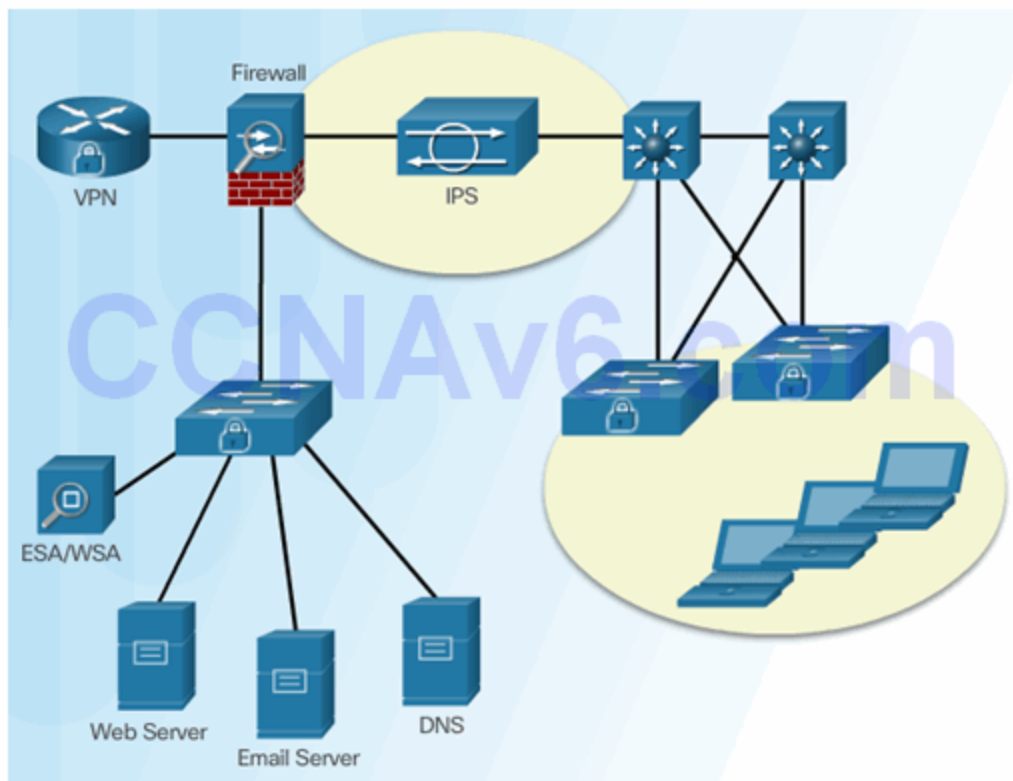
Monitoring Considerations



Secure Device Event Exchange



IPS Configuration Best Practices



Topic 5.2.5: IPS Global Correlation

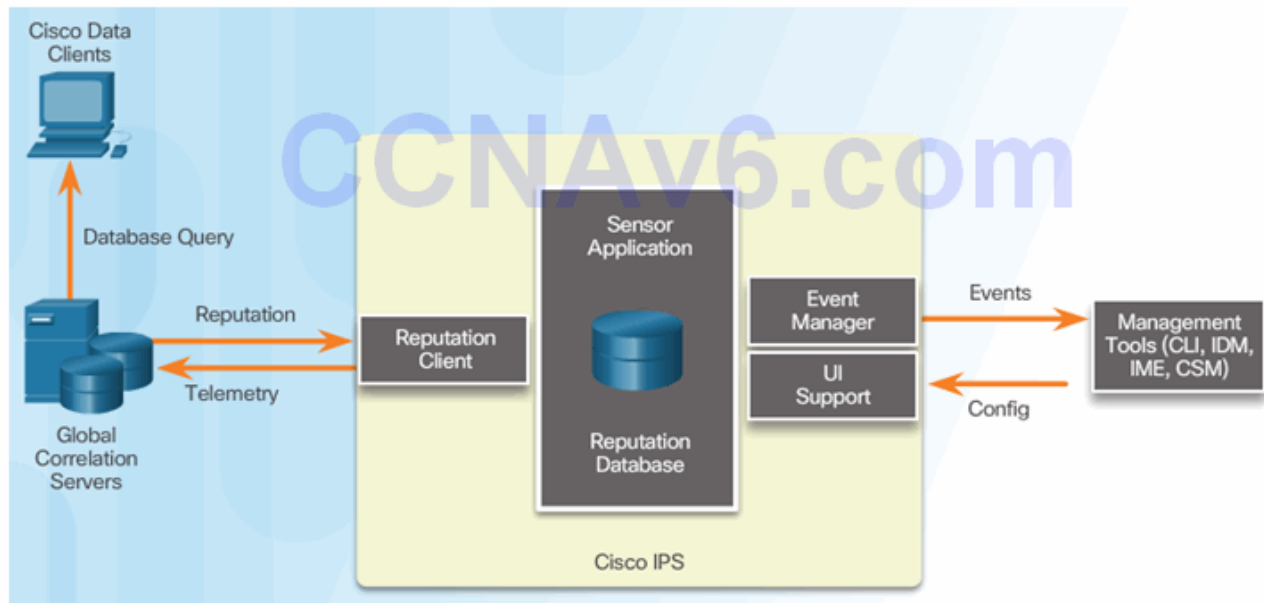
Cisco Global Correlation

Goals of global correlation:

- Dealing intelligently with alerts to improve effectiveness

- Improving protection against known malicious sites
- Sharing telemetry data with the SensorBase Network to improve visibility of alerts and sensor actions on a global scale
- Simplifying configuration settings
- Automatic handling of security information uploads and downloads

Cisco SensorBase Network



Cisco Security Intelligence Operation

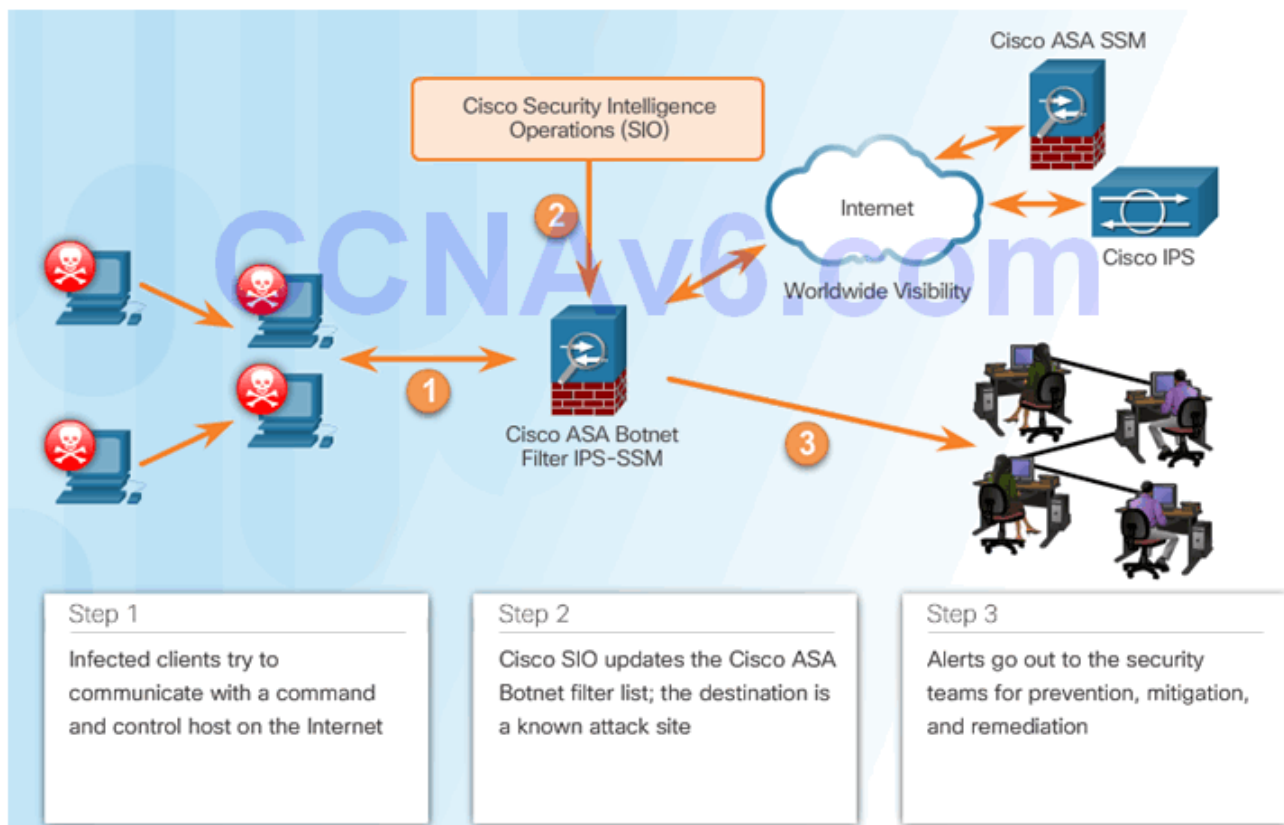
Network participation gathers the following data:

- Signature ID
- Attacker IP address
- Attacker port
- Maximum segment size
- Victim IP address
- Victim port
- Signature version
- TCP options string
- Reputation score
- Risk rating

Reputations, Blacklists, and Traffic Filters



Reputations, Blacklists, and Traffic Filters



Section 5.3: Implement IPS

Upon completion of this section, you should be able to:

- Understand how to configure Cisco IOS IPS with CLI
- Explain how to verify and monitor IPS

Topic 5.3.1: Configure Cisco IOS IPS with CLI

Implement IOS IPS

- 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

The screenshot shows the Cisco Software Download Center interface. The top navigation bar includes links for Products & Services, Support, How to Buy, Training & Events, and Partners. The main heading is "Download Software". Below this, the breadcrumb trail reads: Downloads Home > Products > Security > Network Security > Integrated Threat Control > IOS Intrusion Prevention System Feature Software >. The page title is "IOS IPS Signature Data File-S855". The main content area is titled "IOS Intrusion Prevention System Feature Software". On the left, there is a search bar and a list of releases under "Latest" (S859, S351) and "All Releases" (5.x, 4.x). The main content area displays "Release S855" with a "Signature Update S855 Readme" link. A warning message states: "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/home.x?hw=2". Below the warning, a table lists the file information:

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

Buttons for "Download" and "Add to cart" are located to the right of the file information.

Make a directory

```
Router# mkdir directory-name
```

Rename a directory

```
Router# rename current-name new-name
```

Display a directory

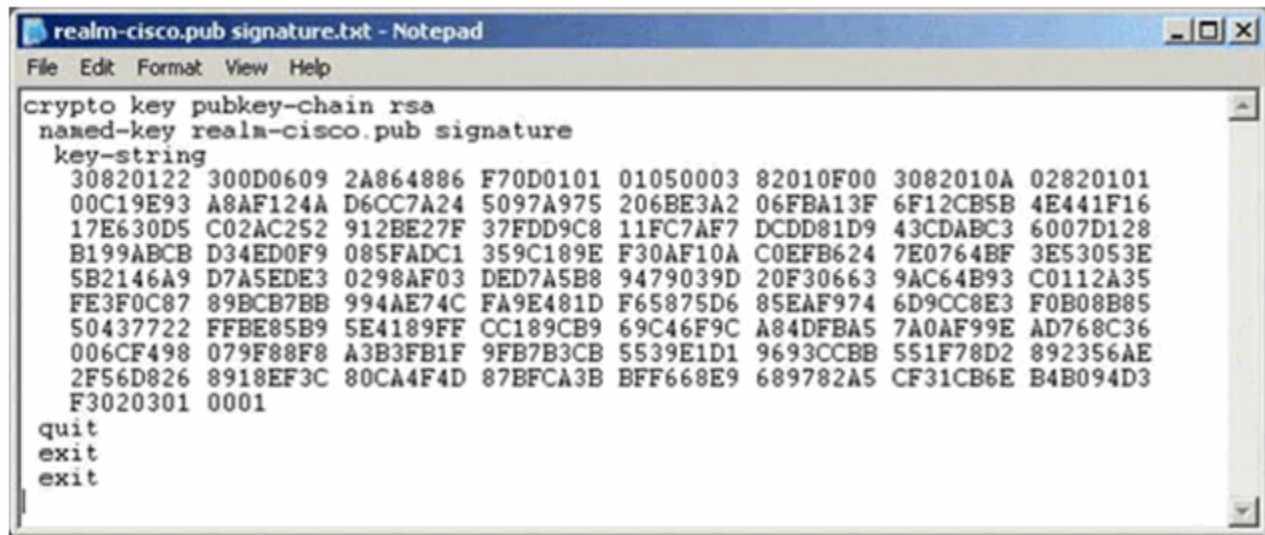
```
Router# dir [/all] [filesystem: ][file-url]
```

```
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#
```

IPS Crypto Key



```
realm-cisco.pub signature.txt - Notepad
File Edit Format View Help
crypto key pubkey-chain rsa
named-key realm-cisco.pub signature
key-string
30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
00C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CBBB 4E441F16
17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128
B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E
5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35
FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85
50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36
006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE
2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3
F3020301 0001
quit
exit
exit
```

```
R1# show run
```

```
<output omitted>
```

```
crypto key pubkey-chain rsa  
named-key realm-cisco.pub signature  
key-string
```

```
30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101  
00C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16  
17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128  
B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E  
5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35  
FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85  
50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36  
006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE  
2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3  
F3020301 0001
```

```
<output omitted>
```

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)#
```


Specify the method of event notification

```
Router(config)# ip ips notify [ sdee | log ]
```

Parameter	Description
sdee	Sends messages in SDEE format.
log	Sends messages in syslog format.Note: If an option is not specified, alert messages are sent in syslog format.

```
R1(config)# ip http server
R1(config)# ip ips notify ?
    SDEE  Send events to SDEE
    log   Send events as syslog messages
```

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

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#
```

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

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)#

```

Topic 5.3.2: Modifying Cisco IOS IPS Signatures

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.

Topic 5.3.3: Verify and Monitor IPS

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

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

Enable SDEE

```
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)#
```

Clear the SDEE events or buffer:

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

Modify the SDEE buffer size:

```
Router(config)# ip sdee events events
```

Section 5.4: Summary

Chapter Objectives:

- Describe IPS technologies and how they are implemented.
- Explain IPS Signatures.
- Describe the IPS implementation process.

Download Slide PowerPoint (pptx):

[sociallocker id="54558"]



CCNASv2_InstructorPPT_CH5.pptx

3.87 MB

2100 downloads

...

[Download](#)

[/sociallocker]