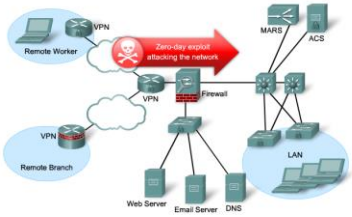
Implementing Intrusion Prevention

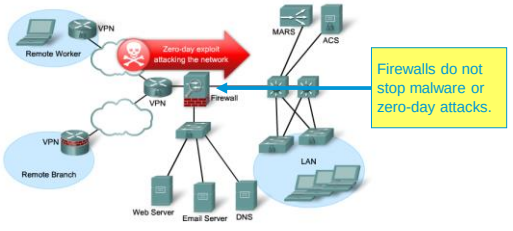
Zero-Day Exploits

- 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!



How do you protect your computer?

- Do you constantly:
  - Sit there looking at Task Manager for nefarious processes?
  - Look at the Event Viewer logs looking for anything suspicious?
- You rely on anti-virus software and firewall features.

How do you protect a network?

- Have someone continuously monitor the network and analyze log files.
- Obviously the solution is not very scalable.
  - Manually analyzing log file information is a time-consuming task.
  - It provides a limited view of the attacks being launched.
  - By the time that the logs are analyzed, the attack has already begun.

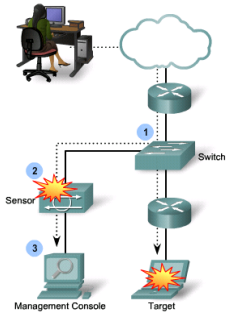
Solutions

- 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

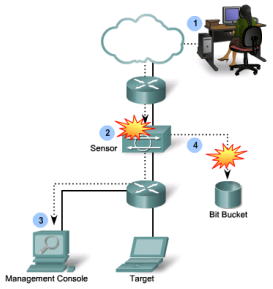
- IDS and IPS technology are deployed as a sensor in:
  - A router configured with Cisco IOS IPS Software.
  - A network module installed in router, an ASA, or a Catalyst switch.
  - An appliance specifically designed to provide dedicated IDS or IPS services.
  - Host software running on individual clients 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.

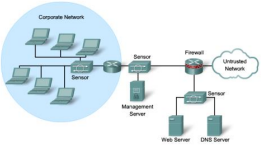
Which should be implemented?

- 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

Network-Based IPS

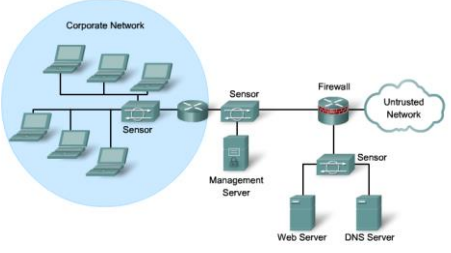
- Implementation analyzes network-wide activity looking for malicious activity.
  - Configured to monitor known signatures but can also detect abnormal traffic patterns.
- Configured on:
  - Dedicated IPS appliances
  - ISR routers
  - ASA firewall appliances
  - Catalyst 6500 network modules



Network-Based IPS Features

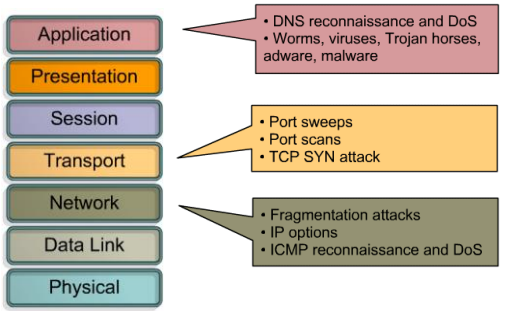
- Sensors are connected to network segments.
  - A single sensor can monitor many hosts.
- Sensors are network appliances tuned for intrusion detection analysis.
  - The operating system is “hardened.”
  - The hardware is dedicated to intrusion detection analysis.
- Growing networks are easily protected.
  - 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

Exploit Signatures



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 Attributes

- Signatures have three distinctive attributes:
  - Signature Type
    - Atomic (one packet required)
    - Composite (many packets required)
  - Trigger (alarm)
  - Action

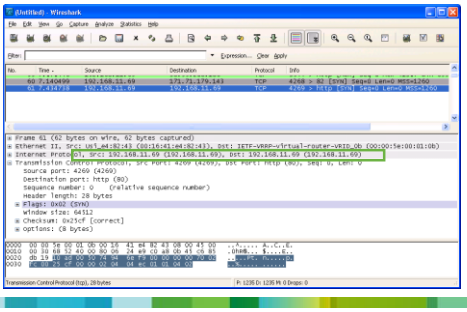
Signature Type

Signature Type – Atomic Signature

- Simplest form of an attack as it consists of a single packet, activity, or event that is examined to determine if it matches a configured signature.
  - If it does, an alarm is triggered, and a signature action is performed.
  - It does not require any knowledge of past or future activities (No state information is required).

Signature Type – Atomic Signature Example

- A LAND attack contains a spoofed TCP SYN packet with the IP address of the target host as both source and destination causing the machine to reply to itself continuously.



Signature Type – Composite Signature

- Also called a stateful signature, it identifies a sequence of operations distributed across multiple hosts over an arbitrary period of time (event horizon).
  - Event horizon: The length of time that the signatures must maintain state.
- Usually requires several pieces of data to match an attack signature, and an IPS device must maintain state.

Signature Type – Composite Signature

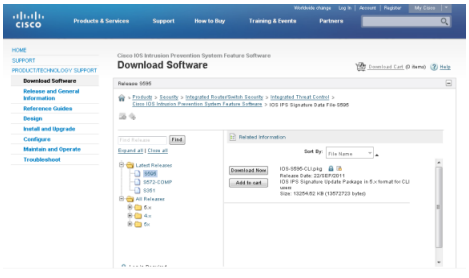
- The length of an event horizon varies from one signature to another.
  - An IPS cannot maintain state information indefinitely without eventually running out of resources.
- Therefore, an IPS uses a configured event horizon to determine how long it looks for a specific attack signature when an initial signature component is detected.
  - Configuring the length of the event horizon is a tradeoff between consuming system resources and being able to detect an attack that occurs over an extended period of time.

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 File

- For example, the LAND attack is identified in the Impossible IP Packet signature (signature 1102.0).
  - A signature file contains that signature and many more.



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.

Signature Micro - Engines

- To make the scanning of signatures more efficient, Cisco IOS software relies on signature micro-engines (SME), which categorize common signatures in groups.
  - Cisco IOS software can then scan for multiple signatures based on group characteristics, instead of one at a time.
- The available SMEs vary depending on the platform, Cisco IOS version, and version of the signature file.

Signature Micro - Engines

- SMEs are constantly being updated.
  - For example, before Release 12.4(11T), the Cisco IPS signature format used version 4.x.
- Since IOS 12.4(11)T, Cisco introduced version 5.x, an improved IPS signature format.
  - The new version supports encrypted signature parameters and other features such as signature risk rating, which rates the signature on security risk.

Signature Micro - Engines

- Cisco IOS Release 12.4(6)T defines five micro-engines:

Signature	Description
Atomic	• Signatures that examine simple packets, such as ICMP and UDP
Service	• Signatures that examine the many services that are attacked.
String	• Signatures use regular expression patterns to detect intrusions.
Multi-string	• Supports flexible pattern matching and Trend Labs signatures.
Other	• Internal engine that handles miscellaneous signatures.

Signature Micro - Engines

Version 4.x SME Prior 12.4(11)T	Version 5.x SME 12.4(11)T and later	Description
ATOMIC.IP	ATOMIC.IP	Provides simple Layer 3 IP alarms.
ATOMIC.ICMP	ATOMIC.IP	Provides simple Internet Control Message Protocol (ICMP) alarms based on the following parameters: type, code, sequence, and ID.
ATOMIC.IPOPTIONS	ATOMIC.IP	Provides simple alarms based on the decoding of Layer 3 options.
ATOMIC.UDP	ATOMIC.IP	Provides simple User Datagram Protocol (UDP) packet alarms based on the following parameters: port, direction, and data length.
ATOMIC.TCP	ATOMIC.IP	Provides simple TCP packet alarms based on the following parameters: port, destination, and flags.
SERVICE.DNS	SERVICE.DNS	Analyzes the Domain Name System (DNS) service.
SERVICE.RPC	SERVICE.RPC	Analyzes the remote-procedure call (RPC) service.
SERVICE.SMTP	STATE	Inspects Simple Mail Transfer Protocol (SMTP).
SERVICE.HTTP	SERVICE.HTTP	Provides HTTP protocol decode-based string engine that includes ant evasive URL de-obfuscation.
SERVICE.FTP	SERVICE.FTP	Provides FTP service special decode alarms.

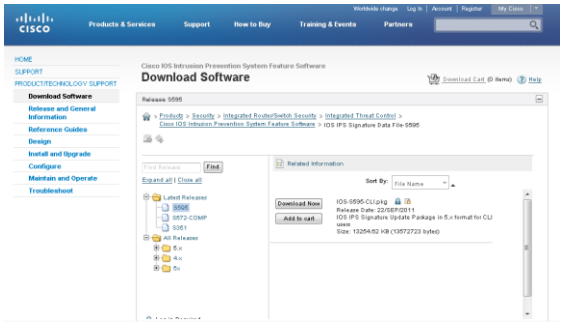
Signature Micro - Engines

Version 4.x SME Prior 12.4(11)T	Version 5.x SME 12.4(11)T and later	Description
STRING.TCP	STRING.TCP	Offers TCP regular expression-based pattern inspection engine services
STRING.UDP	STRING.UDP	Offers UDP regular expression-based pattern inspection engine services
STRING.ICMP	STRING.ICMP	Provides ICMP regular expression-based pattern inspection engine services
MULTI-STRING	MULTI-STRING	Supports flexible pattern matching and supports Trend Labs signatures
OTHER	NORMALIZER	Provides internal engine to handle miscellaneous signatures

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.

Updating Signatures



Signature Trigger

Signature Trigger (Signature Alarm)

- The signature trigger for an IPS sensor is anything that can reliably signal an intrusion or security policy violation.
  - E.g., a packet with a payload containing a specific string going to a specific port.
- The Cisco IPS 4200 Series Sensors and Cisco Catalyst 6500 - IDSM can use four types of signature triggers:
  - Pattern-based detection
  - Policy-based detection
  - Anomaly-based detection
  - Honey pot-based detection

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.

Tuning IPS Signature Alarms

- A signature is tuned to one of four levels, based on the perceived severity of the signature:

Tuning IPS Signature Alarms

- Low
  - Abnormal network activity is detected that could be perceived as malicious, but an immediate threat is not likely.
- Medium
  - Abnormal network activity is detected that could be perceived as malicious, and an immediate threat is likely.
- High
  - Attacks used to gain access or cause a DoS attack are detected, and an immediate threat is extremely likely.
- Informational
  - Activity that triggers the signature is not considered an immediate threat, but the information provided is useful information.

Signature Action

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.

IPS Signature Actions

Category	Specific Alert	Description
Generating an alert	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.
Logging the activity	Log attacker packets	• This action starts IP logging on packets that contain the attacker address and sends an alert.
	Log pair packets	• This action starts IP logging on packets that contain the attacker and victim address pair.
	Log victim packets	• This action starts IP logging on packets that contain the victim address and sends an alert.
Dropping or preventing the activity	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 wait for the timer to expire. • 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.

IPS Signature Actions

Category	Specific Alert	Description
Resetting a TCP connection	Reset TCP connection	• This action sends TCP resets to hijack and terminate the TCP flow.
Blocking future activity	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.

cisco

Managing and Monitoring IPS

Event Monitoring and Management

- There are two key functions of event monitoring and management:
  - Real-time event monitoring and management.
  - Analysis based on archived information (reporting).
- Event monitoring and management can be hosted on a single server or on separate servers for larger deployments.
  - It is recommended that a maximum of 25 well-tuned sensors report to a single IPS management console.

Cisco IOS IPS

- The Cisco IOS IPS feature can send a syslog message or an alarm in Secure Device Event Exchange (SDEE) format.
- An SDEE system alarm message has this type of format:
  - `%IPS-4-SIGNATURE:Sig:1107 Subsig:0 Sev:2 RFC1918 address [192.168.121.1:137 ->192.168.121.255:137]`

Event Monitoring and Management

- Several Cisco device management software solutions are available to help administrators manage an IPS solution.
  - Cisco Router and Security Device Manager (SDM)
  - Cisco IPS Manager Express (IME)
  - Cisco Security Manager (CSM)

Cisco Configuration Professional (CCP)

- Cisco IOS IPS monitors and prevents intrusions by comparing traffic against signatures of known threats and blocking the traffic when a threat is detected.
- CCP allows administrators to control the application of Cisco IOS IPS on interfaces, import and edit signature definition files (SDF) from Cisco.com, and to configure the action that Cisco IOS IPS is to take if a threat is detected.

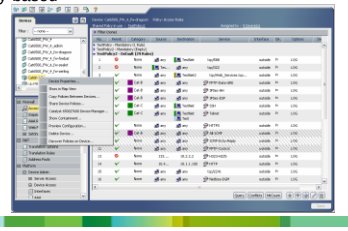
Cisco IPS Manager Express (IME)

- Cisco IME is a GUI-based configuration and management tool for IPS appliances.

- All-in-one IPS management application to provision, monitor, troubleshoot and generate reports for up to five sensors.
- Supports live RSS feed for most recent security intelligence.
- After downloading and installing the approximately 120MB setup.exe file, two desktop shortcuts are created: one for actual sensor use and the second for demo mode only.

Cisco Security Manager (CSM)

- Cisco Security Manager is a powerful, but very easy-to-use solution to centrally provision all aspects of device configurations and security policies for Cisco firewalls, VPNs, and IPS.
- Supports automatic policy-based IPS sensor software and signature updates.
- Includes a signature update wizard allowing easy review and editing prior to deployment.
- Provides support for IPS sensors and Cisco IOS IPS.

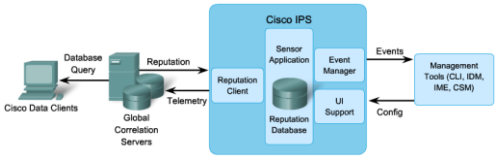


Cisco SensorBase Network

- With global correlation, Cisco IPS devices receive regular threat updates from a centralized Cisco threat database called the Cisco SensorBase Network.
- The Cisco SensorBase Network contains real-time, detailed information about known threats on the Internet.
- Participating IPS devices are part of the SensorBase Network, and receive global correlation updates that include information on network devices with a reputation for malicious activity.

IPS Global Correlation

- When participating in global correlation, the Cisco SensorBase Network provides information to the IPS sensor about IP addresses with a reputation.
- The sensor uses this information to determine which actions, if any, to perform when potentially harmful traffic is received from a host with a known reputation.



Configuring Cisco IOS IPS

Cisco IOS IPS

- Cisco IOS IPS enables administrators to manage intrusion prevention on routers that use Cisco IOS Release 12.3(8)T4 or later.
- Cisco IOS IPS monitors and prevents intrusions by comparing traffic against signatures of known threats and blocking the traffic when a threat is detected.
- Several steps are necessary to use the Cisco IOS CLI to work with IOS IPS 5.x format signatures.
  - Cisco IOS version 12.4(10) or earlier used IPS 4.x format signatures and some IPS commands have changed.

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.

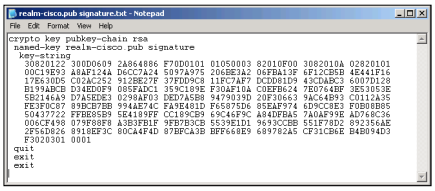
```
R1# mkdir ips
Create directory filename [ips]?
Created dir flash:ips
R1#
R1# dir flash:
Directory of flash:/
   5 -rw-   51054864 Jan 10 2009 15:46:14 -08:00
                     c2800nm-advipservicesk9-mz.124-20.T1.bin
   6 drw-      0 Jan 15 2009 11:36:36 -08:00 ips
64016384 bytes total (12693504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


3. Configure an IOS IPS crypto key

- Configure the crypto key to verify the digital signature for the master signature file (sigdef-default.xml).
  - The file is signed by a Cisco to guarantee its authenticity and integrity.
- To configure the IOS IPS crypto key, open the text file, copy the contents of the file, and paste it in the global configuration prompt.
  - The text file issues the various commands to generate the RSA key.

3. Configure an IOS IPS crypto key

- Highlight and copy the text in the public key file.



- Paste the copied text at the global config prompt.

```
R1# conf t
R1(config)#
```


3. Configure an IOS IPS crypto key

- Issue the **`show run`** command to verify that the key was copied.

```
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 D34EDDF9 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>
```


3. Configure an IOS IPS crypto key

- At the time of signature compilation, an error message is generated if the public crypto key is invalid.
  - If the key is configured incorrectly, the key must be removed and then reconfigured using the **`no crypto key pubkey-chain rsa`** and the **`no named-key realm-cisco.pub signature`** commands.

4a. 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)#
```

4b. 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)#
```


4c. 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.

4c. 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)#
```


4d. 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
```

5. Load the IOS IPS signature

- Upload the signature package to the router using either FTP or TFTP.
  - To copy the downloaded signature package from the FTP server to the router, make sure to use the **idconf** parameter at the end of the command.
  - **copy ftp://ftp_user:password@Server_IP_address/signature_package idconf**

```
R1# copy ftp://cisco:cisco@10.1.1.1/IOS-S376-CLI.pkg idconf
Loading IOS-S310-CLI.pkg !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 7608873/4096 bytes]
*Jan 15 16:44:47 PST: %IPS-6-ENGINE_BUILDS_STARTED: 16:44:47 PST Jan 15 2008
*Jan 15 16:44:47 PST: %IPS-6-ENGINE_BUILDING: multi-string - 8 signatures - 1 of
13 engines
*Jan 15 16:44:47 PST: %IPS-6-ENGINE_READY: multi-string - build time 4 ms -
packets for this engine will be scanned
*Jan 15 16:44:47 PST: %IPS-6-ENGINE_BUILDING: service-http - 622 signatures - 2 of
13 engines
*Jan 15 16:44:53 PST: %IPS-6-ENGINE_READY: service-http - build time 6024 ms -
packets for this engine will be scanned

<Output omitted>
```


5. Load the IOS IPS signature

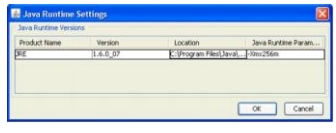
- Verify that the signature package is properly compiled using the **show ip ips signature count** command.

```
R1# show ip ips signature count
Cisco SDF release version S310.0 ← signature package release version
Trend SDF release version V0.0
Signature Micro-Engine: multi-string: Total Signatures 8
multi-string enabled signatures: 8
multi-string retired signatures: 8

<output omitted>

Signature Micro-Engine: service-msrpc: Total Signatures 25
service-msrpc enabled signatures: 25
service-msrpc retired signatures: 18
service-msrpc compiled signatures: 1
service-msrpc inactive signatures - invalid params: 6
Total Signatures: 2136
Total Enabled Signatures: 807
Total Retired Signatures: 1779
Total Compiled Signatures:
      351 ← total compiled signatures for the IOS IPS Basic category
Total Signatures with invalid parameters: 6
Total Obsoleted Signatures: 11
R1#
```

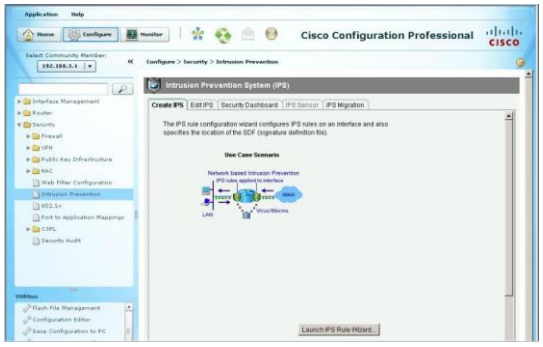

Configuring IPS using CCP

Increase the Java Memory Heap Size

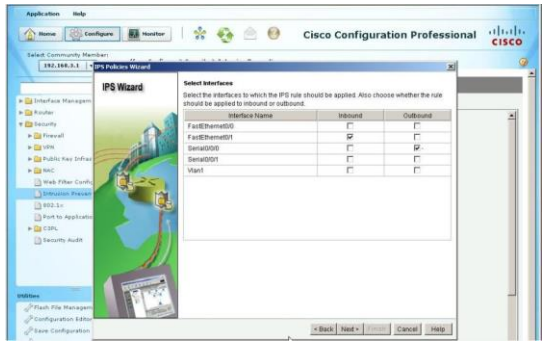
- CCP needs a minimum Java memory heap size of 256MB to support IOS IPS.
  - Exit CCP and open the Windows Control Panel.
  - Click on the Java option which opens the Java Control Panel.
  - Select the **Java** tab and click on the **View** button under the Java Applet Runtime Settings.
  - In the Java Runtime Parameter field enter **-Xmx256m** and click **OK**.



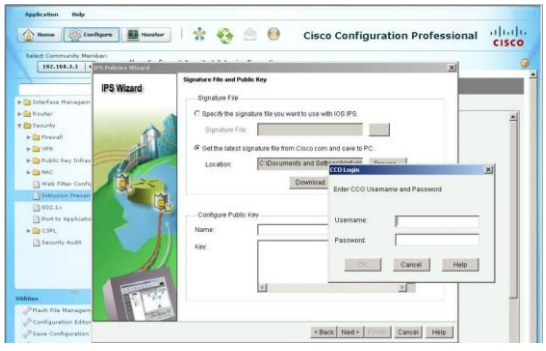
Configuring IOS IPS using CCP



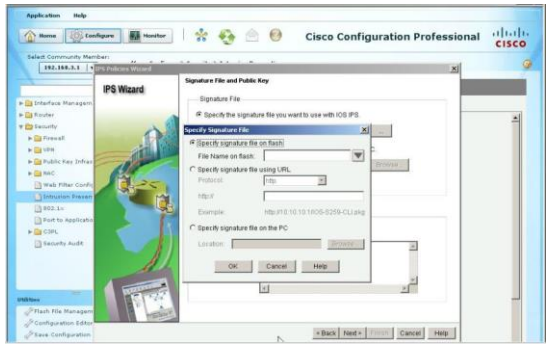
Select the Interfaces



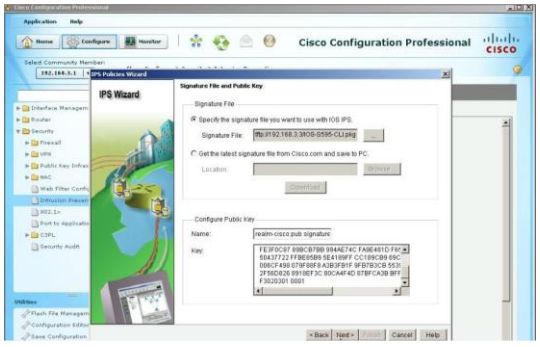
Download the Signature File



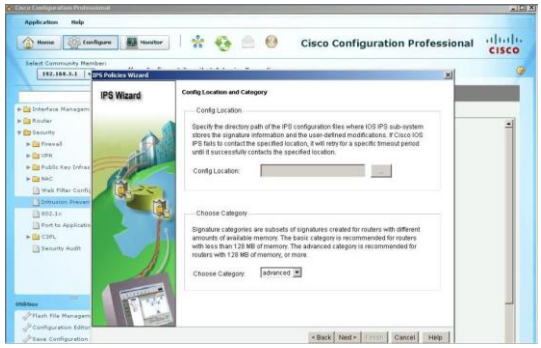
Select the Signature File



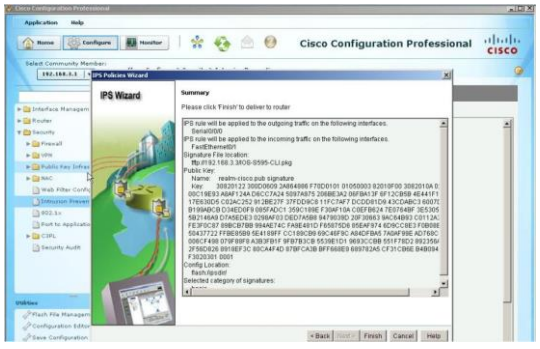
Configure the Public Key



Specify Location of Signature Files



Summary



Modifying Signatures

- This example shows how to retire individual signatures.
  - In this example, signature 6130 with subsig ID of 10 is retired.

```
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)#
```

Modifying Signatures

- This example shows how to unretire all signatures that belong to the IOS IPS Basic 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 Actions for a Signature

- This example shows how to change signature actions to alert, drop, and reset for signature 6130 with subsig ID of 10.

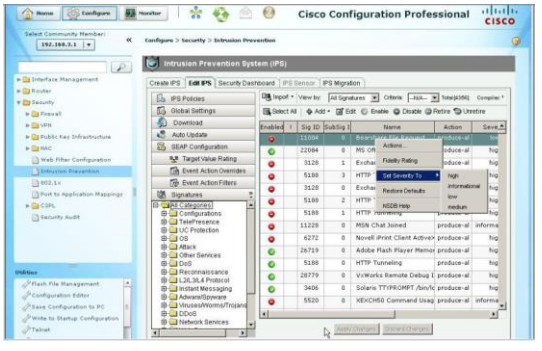
```
R1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# ip ips signature-definition
R1(config-sigdef)# signature 6130 10
R1(config-sigdef-sig)# engine
R1(config-sigdef-sig-engine)# event-action produce-alert
R1(config-sigdef-sig-engine)# event-action deny-packet-inline
R1(config-sigdef-sig-engine)# event-action reset-tcp-connection
R1(config-sigdef-sig-engine)# exit
R1(config-sigdef-sig)# exit
R1(config-sigdef)# exit
Do you want to accept these changes? [confirm] y
R1(config)
```


Change Actions for a Category

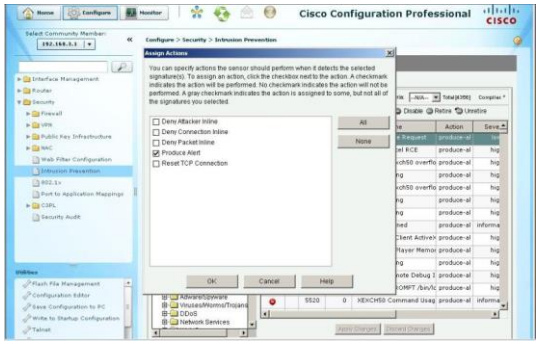
- This example shows how to change event actions for all signatures that belong to the signature IOS IPS Basic category.

```
R1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# ip ips signature-definition
R1(config-ips-category)# category ios_ips basic
R1(config-ips-category-action)# event-action produce-alert
R1(config-ips-category-action)# event-action deny-packet-inline
R1(config-ips-category-action)# event-action reset-tcp-connection
R1(config-ips-category-action)# exit
R1(config-ips-category)# exit

Do you want to accept these changes? [confirm] y
R1(config)#
```


Modifying IOS IPS Signatures

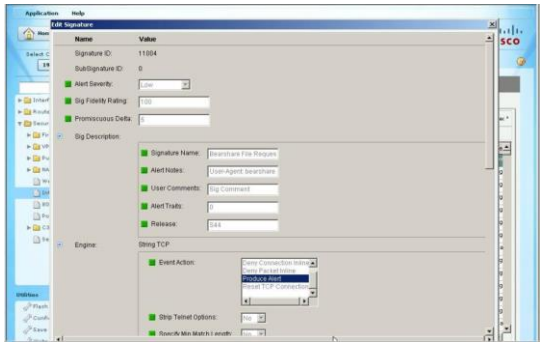


Tuning a Signature



Edit a Signature

Signature Parameters



Verifying IOS IPS

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#
```

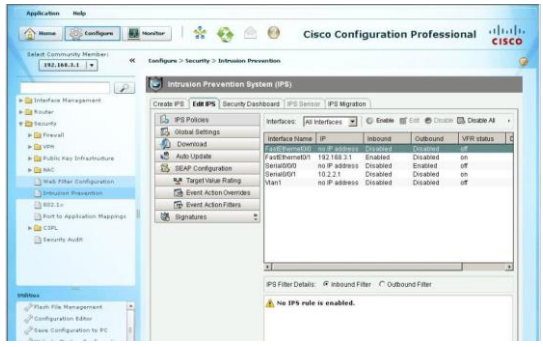

Show Signature Status

```
R1# show ip ips signature | include 5000
SigID:SubID   On   Action   Sev   Trait   MH   AI   CT   TI   AT FA  WF Version
-----------   --   ------   ---   -----   --   --   --   --   -----  ----------

50000:0       N    A        HIGH  0       0    0    0    0    FA  N   OPACL
50000:1       N    A        HIGH  0       0    0    0    0    FA  N   OPACL
50000:2       N    A        HIGH  0       0    0    0    0    FA  N   OPACL

R1#
```

View Alarm and Packet Statistics

```
R1# show ip ips statistics
Signature audit statistics [process switch:fast switch]
  signature 2000 packets audited: [0:2]
  signature 2001 packets audited: [9:9]
  signature 2004 packets audited: [0:2]
  signature 3151 packets audited: [0:12]
Interfaces configured for audit 2
Session creations since subsystem startup or last reset 11
Current session counts (estab/half-open/terminating) [0:0:0]
Maxever session counts (estab/half-open/terminating) [2:1:0]
Last session created 19:18:27
Last statistic reset never
HID:1000 OID:100 S:218 A:3 H:14085 HA:7114 DA:0 R:0
R1#
```


Verify the IPS Configuration

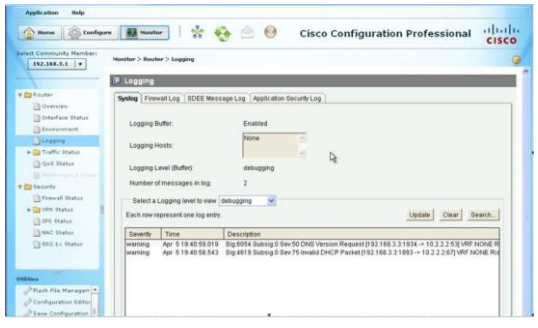


Monitoring IOS IPS

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

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


CCP Syslog



Extra Stuff

- Cisco IPS
  - www.cisco.com/go/ips
- Shields Up! Time to Start Blocking with your Cisco IPS Sensors
  - http://www.networkworld.com/community/node/45922
- Cisco IPS Sensor Tuning Timesavers
  - http://www.networkworld.com/community/node/55244?source=NWWNLE_nlt_cisco_2010-01-18

© 2012 Cisco and/or its affiliates. All rights reserved.