Cisco IOS IPS

Q. What is the difference between Cisco IOS® Intrusion Prevention System (IPS) and Cisco® IPS sensors?

A. Cisco IOS IPS acts as an inline intrusion prevention sensor that can be turned on in Cisco IOS Software router platforms with security feature images. Cisco IPS sensors are dedicated, stand-alone IPS platforms that run on the Cisco IPS 4200 Series Sensor appliances and AIP-SSM modules on the Cisco ASA 5500 series Security Appliances.

Q. What is the IPS subsystem version? How can I find it?

A. The IPS subsystem version is a version number used to keep track of Cisco IOS IPS feature changes. You can use the command **show subsys name ips** to show the detailed Cisco IOS IPS subsystem version.

Q. Where can I download Cisco IPS Version 5.x/6.x format signature files for Cisco IOS IPS in Cisco IOS Software Release 12.4(11)T and later releases?

A. You can download Cisco IPS 5.x/6.x format signature files for Cisco IOS IPS from Cisco.com at: http://tools.cisco.com/support/downloads/go/Model.x?mdfid=281442967&mdfLevel=Software%20Family&treeName=Security&modelName=Cisco%20IOS%20Intrusion%20Prevention%20System%20Feature%20Software&treeMdfId=268438162.

Users can also access to this link from Cisco Software Download page by clicking on "Security" followed by "Integrated Router/Switch Security" link followed by "Integrated Threat Control" link and finally clicking on "Cisco IOS Intrusion Prevention System Feature Software" link

Q. What are the basic, advanced and default signature sets?

A. Cisco IPS Signature packages also contain a file that classifies signatures into various categories like OS vulnerability signatures or Windows vulnerability signatures. A Signature may belong to more than one category. Two of those categories are intended especially for IOS IPS use: ios_ips basic category and ios_ips advanced category. Starting with IOS 15.0(1)M Release, a new category called “IOS IPS Default” is also supported and released within IPS signature packages. IOS Advanced category contains exactly the same signatures as in the IOS Default category, allowing both category names to be used interchangeably for backward compatibility. Those categories serve as a starting Cisco recommended set of signatures to use with IOS IPS feature. Users can add or remove signatures to/from those sets after unretiring one of those IOS specific category signatures as described in detail at Getting Started with Cisco IOS IPS.

Q. How many events are stored in the Cisco Security Device Event Exchange (SDEE)?

A. Cisco SDEE is an application-level communications protocol that is used to exchange IPS messages between IPS clients and IPS servers. Cisco SDEE is always running, but it does not receive and process events from the IPS unless Cisco SDEE notification is enabled. If it is not enabled and a client sends a request, Cisco SDEE responds with a fault response message, indicating that notification is not enabled. When Cisco SDEE notification is enabled (by using the **ip ips notify sdee** command), by default, 200 events can be stored in the event buffer whose size can be increased to hold a maximum of 1000 events. When Cisco SDEE notification is disabled, all stored events are lost. A new buffer is allocated when the notifications are re-enabled.

Q. Does Cisco IOS IPS have fail-open capability?

A. Yes. By default, Cisco IOS IPS has fail-open capability. It can be turned off by using the command **ip ips fail closed**. "Fail closed" implies dropping the packet. If fail closed is not turned on, the packet passes unscanned.

Q. What happens if a signature does not load?

A. If a particular signature does not load, Cisco IOS IPS can not scan for that signature, but it continues to scan for all other loaded signatures.

Q. Should IPS be configured for incoming and outgoing directions?

A. Cisco IOS IPS can be enabled in both the incoming and outgoing directions on an interface. The direction you enable Cisco IOS IPS on depends on the needs of your individual network and the traffic you want to scan.

Q. Do I see alarms on a console?

A. When Cisco IOS IPS triggers a signature, you will be able to see alerts on the console if "logging console" has been configured. Additionally, if syslog has been turned on, you will see alerts on the syslog server. Cisco SDEE should be turned on to see alerts. They can be received on the Cisco Configuration Professional (CCP) and Cisco IPS Manager Express (IME) as well as devices such as the Cisco Security Monitoring, Analysis, and Response System (CS-MARS).

Q. How do I change an action on a signature in Cisco IOS IPS?

A. Cisco IOS IPS in Cisco IOS Software Release 12.4(11)T2 or later supports signature action configuration using the command-line interface (CLI), the Cisco Configuration Professional (CCP) or Cisco Security Manager management applications. For details on CLI use, please refer to the Cisco IOS IPS configuration guide.

Q. Can I configure IOS IPS on Cisco IOS Software prior to 12.4(11)T or any Cisco IOS Mainline Release?

A. Since no more signature updates are posted in the signature format used by Cisco IOS Software releases *prior to* 12.4(11)T and all Cisco IOS 12.4 or before Mainline releases, Cisco strongly recommends *against* configuring and using IOS IPS on routers running those IOS software releases. Customers are recommended to upgrade their router software to 12.4(15)T9 or 15.0(1)M IOS Release before turning on and configuring IOS IPS Feature as described at Getting Started with Cisco IOS IPS..

Q. Can I load and scan for all the signatures supported by IOS IPS simultaneously?

A. No. IOS IPS can only load a user-configurable subset of the signatures it supports at any given time. Increasing available memory will allow loading more signatures at the same time, but even with the maximum amount of memory supported on a particular router model, it is not possible to load all the signatures simultaneously due to the limited size of scanning tables per each signature engine. *Warning:* Attempting to load all supported IOS IPS signatures at the same time may result in high CPU and memory usage, degraded performance, and a system crash.

Q. How do I see what signatures are loaded?

A. The following command on the router will display what signatures are loaded: **show ip ips signatures**. Loaded (unretired) signatures will show with a "Y' in the "Cmp" column of the command output. Additionally, the IPS Signatures GUI in Cisco Configuration Professional (CCP) or Cisco Security Manager (CSM) can show what signatures are loaded (unretired) on the router.

Q. How do I see the signature release version that are currently loaded on the router?

A. Use the following command: **show ip ips signatures** which shows the signature release version on the first line of the command output as in "Cisco SDF release version S379.0". The term SDF stands for Signature Definition File and refers to the IPS Signature Package loaded onto the router.

Q. Do Cisco IOS IPS and Cisco IOS Firewall share the same session table?

A. Yes, Cisco IOS IPS and classical Cisco IOS Firewall share the same session table. The most important session parameters are the following:

```
ip inspect max-incomplete, ip inspect one-minute, and ip inspect tcp max-incomplete
host session counters.
```

For detailed information, please refer to the Cisco IOS IPS Deployment Guide.

Q. How can signatures be tuned?

A. Starting from Cisco IOS Software Release 12.4(11)T2, you can tune signatures using Cisco IOS CLI commands, Cisco Configuration Professional (CCP) application (for a single router) or Cisco Security Manager application (for multiple routers). Cisco does not recommend use of IOS IPS Feature with IOS releases *prior to* 12.4(11)T2 or any Cisco IOS 12.4 or before Mainline Release.

Q. Can I still use Security Device Manager (SDM) application to configure IOS IPS and tune signatures on a router?

A. SDM application only supports IOS releases up to 12.4(15)T2. For later releases, Cisco Configuration Professional (CCP) application needs to be used.

Q. What is the difference between active (unretired) and enabled signatures?

A. If a signature is active (unretired), it is loaded on the router memory and packets are scanned against it. If an active (unretired) signature is enabled, when triggered by a matching packet (or packet flow), it takes the appropriate action associated with it. If an active (unretired) signature is disabled, no action is taken even if it is triggered.

Q. What does inactive mean on an engine?

A. An inactive (retired) signature is not scanned for. A disabled signature is scanned for but no action is taken even if it is triggered by a matching packet or flow.

Q. Does Cisco offer any support for IPS Signature licensing?

A. Yes. Subscriptions for signature updates require a license (contract) that you can include in the Cisco SMARTnet® services contract for an additional cost. Starting with IOS 15.0(1)M Release, existing of a valid IPS subscription license on the router will be required to load newly released IPS signatures on Cisco 88x, 89x, 19xx, 29xx and 39xx platforms. To obtain and install this license, you need to purchase the “Cisco Services for IPS” services contract SKU relevant to the router model as well as the type and level of the associated SMARTnet deliverables desired. For more information about Cisco Services for IPS, visit http://www.cisco.com/go/services/ips.

Q. How is Cisco CCP application different from Cisco Security Manager (CSM) application?

A. Cisco Configuration Professional (CCP) is a single device management tool. Using CCP, one can configure IOS IPS or any other feature on one router at a time using the GUI provided by CCP application. Cisco Security Manager (CSM) is a “network level” management application. Using CSM, you can deploy a single or multiple IPS policy/configuration across multiple Cisco IOS IPS devices. For more information, visit: How to Use CCP to Configure IOS IPS in 12.4(15)T4 and later release and How to Use CSM 3.1 to Configure IOS IPS in 12.4(11)T2.

Q. How I can load a new signature package onto my router?

A. You can download the latest signature package created for IOS IPS use via CLI from Cisco.com at http://tools.cisco.com/support/downloads/go/Model.x?mdfid=281442967&mdfLevel=Software%20Family&treeName=Security&modelName=Cisco%20IOS%20Intrusion%20Prevention%20System%20Feature%20Software&treeMdfId=268438162 into a local FTP or TFTP server which could be any FTP/TFTP server application running on your PC. You can then use the “**copy** <Signature-package-file-name> **idconf**“ CLI command on the router to load the signature package to the router.

Q. What is the best way to configure Cisco IOS IPS with a firewall?

A. When configuring Cisco IOS IPS with Cisco IOS Firewall, tune the inspection threshold values to best suit your network use. These inspection threshold values are used by both the Cisco IOS IPS and Cisco IOS Firewall features. Refer to the Cisco IOS IPS Deployment Guide for information about how to understand and tune these threshold values.

Q. What is the effect on performance?

A. Signatures in IOS Basic and Advanced categories are tested for performance impact and those increasing CPU utilization significantly are not included in those sets. However, when additional signatures are loaded, one or more of those added signatures may cause CPU spikes and thus significantly drop packet throughput with IPS feature. Adding few signatures at a time and checking CPU utilization after each time should help identifying those bad-performing signatures which should not be loaded There is no linear correlation between the number of signatures loaded and their relative performance impact although as more signatures are loaded, the probability of loading one or more bad-performance signatures increases.

Q. How much memory is consumed when enabling Cisco IOS IPS?

A. As soon as Cisco IOS IPS is enabled on the interface, the signatures are compiled. The compilation process is highly CPU-intensive while the signatures are being compiled. Compilation can last up to 2 minutes, depending on the number of signatures being compiled. The number of signatures that can be loaded on a router is dependent on available (free) memory.

Q. What happens if the connections start dropping with no signature (firing) during a TCP SYN Flood protection?

A. Signature 3050 prevents half-open TCP SYN attacks. If 3050 is disabled, Cisco IOS Firewall takes over and sends TCP resets. Signature 3050 uses the Cisco IOS Firewall engine, so messages from signature 3050 and Cisco IOS Firewall are the same.

Q. How does fragmentation work with Cisco IOS IPS?

A. Signatures with IDs 1201 to 1208 are set to detect fragmentation. They drop fragments for the IP address. Virtual Fragment Reassembly (VFR) and Cisco IOS IPS overlap in this capability.

Q. Is Cisco IOS IPS supported on older platforms such as the Cisco 1700 and 2600 Series Routers?

A. IOS IPS in Cisco IOS Software 12.4(11)T2 and later IOS T-Train releases requires *at least* 128MB memory installed on the router. Cisco does not recommend using IOS IPS on those older platforms even with 128MB memory due to limited signature coverage and CPU constraints.

Q. What are signature micro-engines and signature categories?

A. A signature micro-engine (SME) is a component of Cisco IOS IPS that supports signatures in a certain category. Each engine is customized for the protocol and fields it is designed to inspect, and defines a set of legal parameters that have allowable ranges or sets of values. The SMEs look for malicious activity in a specific protocol. Signatures can be defined for any of the supported SMEs using the parameters offered by that micro-engine. Packets are scanned by the micro-engines that understand the respective protocols contained in the packet.

Q. Does each signature category have the same effect on performance? If not, can you explain?

A. No. Each signature category defines a different set of signatures, and they are designed to search and examine different portions of the packets. The deeper a signature has to look into a packet, the more processing it needs. Generally, STRING.TCP engine signatures need more processing time than the other engines.

Q. Does each signature, signature category or engine consume the same or similar amount of memory?

A. No. Different signatures and engines consume different amounts of memory. Memory consumed only depends on the particular set (combination) of signatures loaded on the router at a given time. There is no linear or other type of mathematical relation between the number of signatures loaded and the amount of memory consumed by them. A set of 100 signatures may consume more memory than another set of 150 signatures that contain simpler signatures. There is no way to guess or know the exact memory consumption by a particular set of selected (unretired) signatures before actually loading (compiling) them on the router. Typically, STRING.TCP engine signatures are more memory-intensive than the other engine signatures.

Q. What are the various ways or tools to update signature files on routers?

A. IPS signature packages can be updated using Cisco Configuration Professional (CCP) 1.x or Cisco Security Manager (CSM) Version 3.1 or later, or using the router CLI.

Q. Are Cisco IOS IPS signature updates always synchronized with the signature updates for Cisco IPS appliances or modules?

A. Signature updates on Cisco IOS Software routers are not always synchronized with the updates for Cisco IPS sensors or modules. However, IOS signature update packages are usually posted within a few days following the posting of updates for IPS sensors and modules.

Q. How do I know if a new signature is supported on the routers?

A. The easiest way to find out if a new signature is supported on the routers is to load a signature package released at the same time or after that signature was first released by Cisco IPS Signature Team. To find out the Release Date for a Cisco signature, you can go to http://tools.cisco.com/security/center/search.x, choose the Signatures radio button, enter the Signature ID in the Keyword(s) box and click the Search button below. Once the loading of the package containing the signature completes on the router, you can type the CLI command "**show ip ips signature sigid** <signature-ID> **subid** <signature-subid>" command on the router. If any detailed information is displayed about that signature by that command, then the signature is supported by IOS IPS. Otherwise, the router will display "Unable to locate Sig<signature-ID>:<signature-subid>" Note that that signature must be unretired (most show a 'Y' in the "Cmp" column of the output) and enabled (must show a 'Y' in the "En" column of the output) to scan for matching traffic and take an action when triggered. Note that only a subset of those signatures can be loaded and scanned for at the same time depending on available memory. Cisco recommends IPS customers to subscribe to IPS Active Update Bulletins to receive notifications on the new Cisco IPS signature releases.

Q. What is the difference between the Cisco IPS Advanced Integration Module (IPS AIM), Cisco IPS Network Module (NM) and Cisco IOS IPS?

A. The Cisco IPS AIM for the Cisco 1841 and Cisco 2800 and 3800 Series Integrated Services Routers is an internal security service module which provides dedicated CPU and memory to offload inline and promiscuous intrusion prevention processing. The Cisco IPS Network Module for the Cisco 2811, 2821, 2851 and 38x5 Integrated Services Routers and Cisco 2911, 2921, 2951 and 39x5 Next Generation Integrated Services Routers is an external Network Module that serves the same purpose with higher performance. Both modules run the latest Cisco IPS 7.x (dedicated) sensor software to provide feature parity with Cisco IPS 4200 Series Sensors and Cisco ASA 5500 Series Adaptive Security Appliances. The main differences between Cisco IOS IPS and the Cisco IPS AIM/NM follow:

- The Cisco IPS AIM/NM offloads IPS processing from the main router CPU and memory. Hence, they can support all Cisco IPS signatures unretired by default simultaneously. Cisco IOS IPS runs on the router's own CPU and memory, and can load only a user configurable subset of supported signatures at a given time.
- The Cisco IPS AIM/NM also provides advanced IPS features such as Day-0 attack protection and Meta Event signatures (across multiple sessions) that are not available in Cisco IOS IPS.

More information on the Cisco IPS AIM and Cisco IPS NM can be found at http://www.cisco.com/en/US/products/ps8395/index.html

Q. Can Cisco IOS IPS and the Cisco IPS AIM/NM be used together?

A. No. Cisco IOS IPS and the Cisco IPS AIM/NM can not be used together. Cisco IOS IPS must be disabled when the AIM-IPS or NME-IPS is installed

Q. What platforms support Cisco IOS IPS?

A. The Cisco 87x, 88x, 89x, 18xx, 28xx, 38x5, 72xx, 7301 and SR 520 platforms support Cisco IOS IPS. Starting with IOS 15.0(1)M Release, the next generation Integrated Services Routers, namely 1921, 1941, 1941W, 29xx and 39x5 routers, also support IOS IPS when enabled with a Security Feature license.

Q. Does IOS IPS support multicast traffic?

A. No.

For More Information

For more information about Cisco IOS IPS, visit http://www.cisco.com/go/iosips.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C67-440235-05 05/10