# Cisco IOS Intrusion Prevention System Deployment Guide

This document only covers IOS IPS feature in 12.4(11)T and later T-Train and 15.0 IOS Mainline releases that uses IPS signature format also used by Cisco IPS software version 5.x and later releases including version 7.0.

Use of Cisco IOS IPS in IOS Mainline *prior to* IOS 15.0 Mainline Release and T-Train releases *prior to* 12.4(11)T is not recommended. No signature updates are provided in the signature format used by IOS IPS Feature in those releases. Also, support for IOS IPS feature in those older releases is very limited.

## Feature History

Table 1 shows the feature history of the Cisco IOS IPS since November, 2006.

**Table 1.** Cisco IOS IPS in the Latest IOS Releases Offers the Following Capabilities

| Feature | Advantage/Benefit |
|---|---|
| **New Default IOS IPS Category signatures (including some lightweight signatures) is updated frequently by Cisco Signature Team starting with IOS 15.0(1)M Release** | More comprehensive and effective attack coverage by default.<br>Much quicker inclusion of most relevant new threat signatures within the default set (category). |
| **Lightweight Signature Engines for HTTP, SMTP and FTP protocol signatures and Regular Expression Table chaining available also in 15.0(1)M Release** | Memory efficient traffic scanning for attack signatures consuming less memory on the router.<br>Capability to provide protection for larger number of common threats and vulnerabilities. |
| **VRF Awareness (Virtual IPS)—Available in 12.4(20)T or later IOS T-Train Releases** | Allows enterprises to apply IPS on only certain virtual network segments (VRFs) and/or with different inspection rules on each VRF, and distinguish among the IPS alarms/events generated within each virtual segment via VRF ID. |
| **Available in 12.4(15)T5 or later IOS T-Train Releases** | |
| **Supports Signatures for Vulnerabilities in Microsoft SMB and MSRPC Protocols as well as Signatures Provided by Vendors under NDA** | Efficient protection against many new Microsoft and other vulnerabilities, some even before their public release |
| **Risk Rating Value in IPS Alarms Based on Signature Severity, Fidelity, and Target Value Rating** | Allows more accurate and efficient IPS event monitoring by filtering or separating events with low/high Risk Rating |
| **Supports Signature Event Action Processor (SEAP)** | Quick and automated adjustment of signature event actions based on calculated Risk Rating of the event |
| **Automated Signature Updates from a Local TFTP or HTTP(S) Server** | Protection from latest threats with minimal user intervention |
| **IDCONF (XML) Signature Provisioning Mechanism** | Offers secure provisioning through Cisco Security Manager 3.1 and Cisco Router and Security Device Manager (SDM) 2.4 over HTTPS |
| **Individual and Category-Based Signature Provisioning through Cisco IOS CLI** | Offers granular customization and tuning of signatures through custom scripts |
| **Same Signature Format and Database as the Latest Cisco® IPS Appliances and Modules** | Offers common deployment and attack signature definitions between Cisco IPS appliances/modules and Cisco IOS® IPS |

### Cisco IOS IPS Deployment Overview

In today's business environment, network intruders and attackers can come from both outside and inside the network. They can launch denial-of-service (DoS) attacks or distributed denial-of-service (DDoS) attacks; attack Internet connections; and exploit network and host vulnerabilities. At the same time, Internet worms and viruses can spread across the world in a matter of minutes. There is often no time to wait for human intervention-the network itself must possess the intelligence to instantaneously recognize and mitigate these attacks, threats, exploits, worms, and viruses.

Cisco IOS Intrusion Prevention System (IPS) is an inline, deep-packet-inspection-based feature that enables Cisco IOS Software to effectively mitigate a wide range of network attacks. While it is common practice to defend against attacks by inspecting traffic at the data centers and corporate headquarters, it is also critical to distribute the network-level defense to stop malicious traffic close to its entry point at the branch or telecommuter offices.

Cisco IOS IPS capabilities include the ability to dynamically load and scan for IPS signatures selected from more than 3700 signatures supported by Cisco stand-alone IPS sensor platforms, as well as the ability to modify existing signatures or create new signatures to address newly discovered threats.

## Cisco IOS IPS: Key Features and Benefits

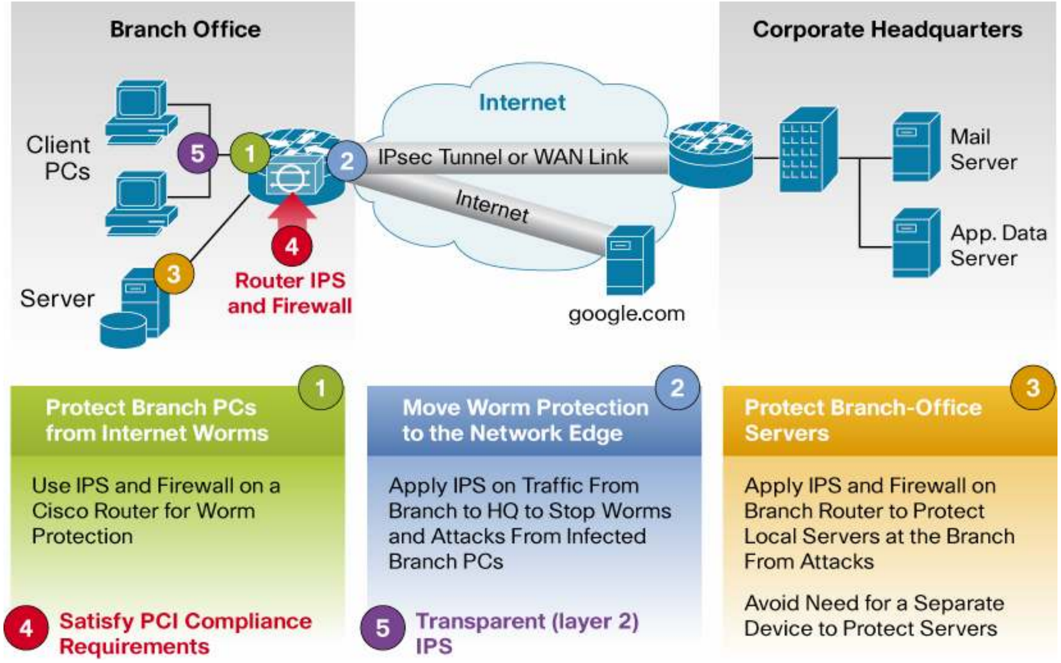
- Provides network-wide, distributed protection from many attacks, exploits, worms and viruses exploiting vulnerabilities in operating systems and applications
- Eliminates the need for a standalone IPS device at branch and telecommuter offices as well as small and medium-sized business networks
- Unique and risk rating based signature event action policy processor dramatically improves the ease of management of IPS policy.
- Offers field-customizable worm and attack signature set and event actions
- Offers inline inspection of traffic passing through any combination of router LAN and WAN interfaces in both directions
- Works with Cisco IOS® Firewall, control-plane policing, and other Cisco IOS Software security features to protect the router and networks behind the router
- Supports more than 3700 signatures from the same signature database available for Cisco Intrusion Prevention System (IPS) appliances

### Deployment Scenarios

There are 5 main deployment scenarios for Cisco IOS IPS:

- Protect branch PCs from Internet Worms
- Move worm protection to the network edge
- Protect branch office servers
- Satisfy PCI compliance requirements
- Protect one or more subnets from worms and viruses that may originate from another subnet

**Figure 1.** Cisco IOS IPS Deployment Scenarios


Branch Office
Corporate Headquarters
Internet
Client PCs
5
1
2
IPsec Tunnel or WAN Link
Internet
Mail Server
App. Data Server
4
3
Router IPS and Firewall
Server
google.com
1
Protect Branch PCs from Internet Worms
Use IPS and Firewall on a Cisco Router for Worm Protection
4
Satisfy PCI Compliance Requirements
2
Move Worm Protection to the Network Edge
Apply IPS on Traffic From Branch to HQ to Stop Worms and Attacks From Infected Branch PCs
5
Transparent (layer 2) IPS
3
Protect Branch-Office Servers
Apply IPS and Firewall on Branch Router to Protect Local Servers at the Branch From Attacks
Avoid Need for a Separate Device to Protect Servers

#### Protect Branch PCs from Internet Worms

The Internet is one of the major sources of attacks and exploits targeting today's corporate networks. Applying Cisco IOS IPS on router interfaces connected to the Internet helps defend the corporate network against such vulnerabilities. Even with a firewall enabled to restrict access from the untrusted Internet, intruders can still potentially invade the perimeter router on the telecommuter side and gain access to the corporate network. Common security attacks include IP spoofing, man-in-the-middle attacks, and unauthorized access that may have slipped through the firewall. Outgoing traffic from the telecommuter's end also poses a threat to the internal network, if the telecommuter attempts to compromise the corporate network or the Internet. Cisco IOS IPS can be applied at the incoming and outgoing interfaces of the perimeter router to monitor and discard malicious activity.

In the network topology shown in Figure 1, the branch offices are the best places to enable Cisco IOS IPS on both directions of the Internet-facing interface. A common scenario is when split tunneling is enabled while running VPN tunnels to the corporate network. Cisco recommends enabling Cisco IOS IPS on the Internet traffic to protect the network from attacks and exploits that might come into the branch office or telecommuter personal computers, which could in turn affect the corporate network.

### Move Worm Protection to the Network Edge

In today's corporate network environment, network attacks and exploits come from not only the Internet, but often from within the corporate network itself. These attacks or exploits could be deliberate or inadvertent (for example, an infected laptop brought into the office and connected to the corporate LAN). Deploying Cisco IOS IPS within the corporate network helps mitigate attacks, and helps prevent exploits from spreading within the network.

In the network topology shown in Figure 1, the branch offices have client PCs and might provide guest access to customers. Applying IOS IPS on the inside interface on the branch router will protect attacks, worms from spreading from branch office to the head-quarter office and the rest of the network. Move worm protection to the network edge by deploying Cisco IOS IPS as close to the entry point into the network as possible will mitigate the attacks and exploits from their early stages into the network.

### Protect Branch-Office Servers

In the network topology shown in Figure 1, the branch offices not only have client PCs but also hosting servers on the inside network. Deploying IOS IPS on the branch router will protect inside network and server from being attacked without adding additional device to perform this function.

By enabling Cisco IOS IPS together with IP Security (IPsec) VPN, NAC, and Cisco IOS Firewall, a Cisco router can perform encryption, firewalling, and traffic inspection at the first point of entry into the network-an industry first. This setup reduces the additional devices needed to support the system, reduces operating and capital expenditures, and enhances security.

### Satisfy PCI Compliance Requirements

IOS IPS is a key security feature that is required for one of the twelve Payment Card Industry (PCI) compliance requirements  (requirement # 11), combined with IOS VPN, Firewall and other security features available on the Integrated Services Routers, as well as complementary threat policy management and monitoring applications/appliances such as Cisco Security Manager (CSM) and Cisco Security MARS. As PCI compliance has become mandatory for retail offices and shops, use of IOS security features including IPS has been an increasingly popular common use case among our customers.

### Transparent (Layer 2) IPS

IOS IPS can also be configured to protect one or more subnets from worms and viruses that may originate from another subnet. This is especially useful and common to protect subnets assigned to employee PCs from partner and guest PCs usually connected to an unprotected subnet(s) for wireless access point(s).

## General Cisco IOS IPS Structure

Cisco IOS IPS leverages technology from Cisco Intrusion Prevention (IPS) sensor product lines, including Cisco IDS 4200 Series stand-alone Sensors and IPS modules for Cisco ISR routers and ASA appliances.  Cisco IOS IPS relies on signature micro-engines (SMEs) to support IPS signatures. Each engine categorizes a group of signatures, and each signature detects patterns of misuse in network traffic. For example, all HTTP signatures are grouped under the HTTP engine. Currently, Cisco IOS IPS supports approximately 3700 signatures—all part of the common set of Cisco IPS Signatures. Those signatures packages are available for download from Cisco.com.

Since IOS IPS can not load all the signatures, the IOS IPS configuration governs which signatures are loaded by IOS IPS. In addition, the signature update process can be configured to automatically download signature package from a locally accessible storage location, such as a local TFTP server. So the major task of using IOS IPS in this release is to configure IOS IPS to run a desired set of signatures. For detailed information of how to use IOS IPS in 5.x signature format, please refer the step by step guide Getting Started with Cisco IOS IPS with 5.x Format Signatures**.**

### Cisco IOS IPS and Cisco IPS AIM (Advanced Integration Module) and IPS Network Module

Those stand-alone IPS modules for Integrated Services Routers have dedicated CPU, DRAM and Flash and run Cisco IPS software that also runs on Cisco 4200 series IPS sensors and AIP modules for Cisco ASA platform*. Note that Cisco IOS IPS and any of those hardware IPS modules can not be used* at the same time. For details on dedicated IPS modules on the routers, visit: http://www.cisco.com/en/US/prod/collateral/routers/ps5853/ps5875/product_data_sheet0900aecd806c4e2a_ps2641_Products_Data_Sheet.html

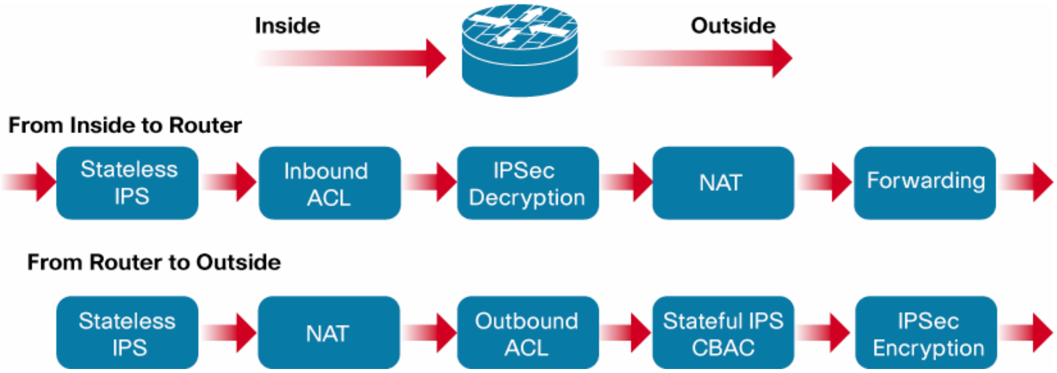
### Packet Flow

Packets traverse routers in a particular order. When multiple features are configured on a router, understanding the traffic flow helps in the understanding of how the router works and how each feature plays a role in inspecting the traffic passing through the router.

### Packets Flowing from Inside the Network to Outside the Network

In Figure 2, at the inside interface, the packet is scanned against any inbound IPS policy at the inside interface. Next, the inbound access control list (ACL) is checked for, if applied. The Network Address Translation (NAT) and routing process follows. Finally, inbound Cisco IOS Firewall policy inspects the packet. If the stateless IPS input policy drops a packet, the other feature will not see the packet. As the packet is on its way out of the router, at the outside interface the packet is checked against atomic signatures per outbound IPS policy and then checked against any outbound ACLs (if applied), followed by NAT, and then it goes through stateful inspection based on outbound Cisco IOS Firewall and IPS policy. Finally, the packet is encrypted by the IPsec rule as it leaves the router.

**Figure 2.** Packets Flowing from Inside to Outside the Network

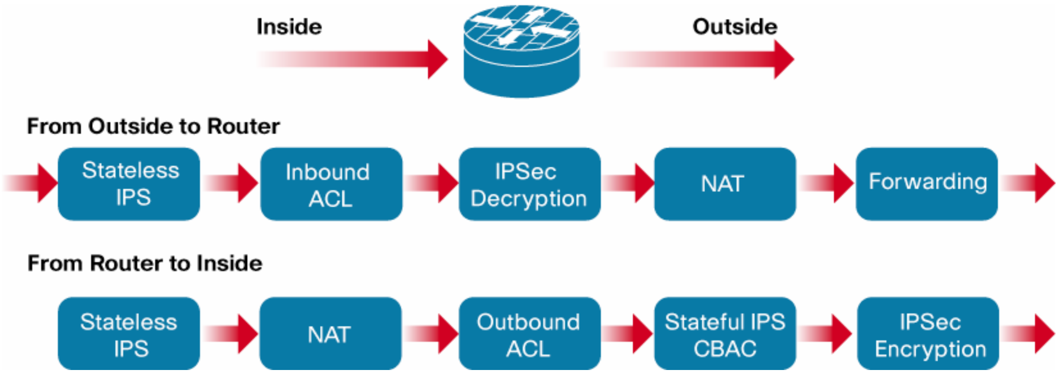


### Packets Flowing from Outside the Network to Inside the Network

In Figure 3, as the packet enters from the outside interface, the IPsec policy decrypts the packet (if needed). Next, the inbound IPS policy scans the packet for atomic signatures, followed by inbound ACL checks. The NAT and routing process follows. If the inbound IPS policy drops a packet, the other features will not see the packet.

At the inside interface, the packet is checked against atomic signatures per outbound IPS policy, followed by outbound ACL checking, NAT process, and finally stateful inspection based on outbound Cisco IOS Firewall and IPS policy, before it makes its way into the private network.

**Figure 3.** Packets Flowing from Outside to Inside the Network



## Signature Micro-Engines and Signatures

### Signature Micro-engines

An SME is a component of Cisco IOS IPS that supports signatures in a certain category. Customized for the protocol and fields it is designed to inspect, each engine 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 those micro-engines. Packets are scanned by the micro-engines that understand the protocols contained in the packet.

A regular expression is a systematic way to specify a search for a pattern in a series of bytes. When a signature engine is built (building refers to loading an SME on the router when Cisco IOS IPS is enabled on the interface), it may compile one or more regular expressions. Compiling a regular expression requires more memory than the final storage of the regular expression-important information to know when considering loading and merging new signatures.

Cisco IOS IPS also introduces the concept of parallel scanning. All the signatures in a given micro-engine are scanned in parallel, in a single pass of the packet bytes, rather than serially (one signature at a time). Each SME extracts values from the packet and passes portions of the packet to the regular expression engine. The regular expression engine can search for multiple patterns at the same time (in parallel). Parallel scanning increases efficiency, resulting in higher throughput.

For more details about SMEs and signature parameters, refer to the “Advanced Topics” section at the end of this document.

### Signature Actions

IOS IPS supports signature action configuration on a per-signature basis. Each signature can be set to any combination of the following actions:

| | |
|---|---|
| produce-alert: | send a alarm when a signature fires |
| deny-packet-inline: | drop the packet when a signature fires, this action will not send TCP reset |
| reset-tcp-connection: | send TCP reset to both the attacker and victim when a signature fires |
| deny-attacker-inline: | deny the attacker ip address by using a dynamic access list |
| deny-connection-inline: | deny the attacker session by using a dynamic access list |

Customers can use Cisco Configuration Professional (CPP) version 1.1or later (version 1.4 recommended) or Cisco Security Manager (CSM) version 3.1 or later (version 3.3 recommended) to manage IOS IPS, or they can use IOS CLI to tune signature parameters. The event action configuration can be performed either based on signature category groups or on a per signature basis. For detailed CLI configuration, refer to IOS IPS configuration guide at http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_ips5_sig_fs_ue_ps6350_TSD_Products_Configuration_Guide_Chapter.html

### Signature Category and Signature CLI Package

Signature category is a group of relevant signatures represented by a meaningful name. For example, p2p category contains all peer-to-peer application signatures such as Bittorrent, eDonkey and Kazaa. The signature category information is an integral part for each signature update in version 5.x signature format.

To configure IOS, customers need to download a signature package (preferably the latest) and load it to the IOS IPS router. IOS IPS signature packages for CLI users can be downloaded 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.

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” will be also supported and released within IPS signature packages. At that time, IOS Advanced category will be changed to contain exactly the same signatures as in the IOS Default category, allowing both category names to be used interchangeably for backward compatibility.

The following is an example to configure IOS IPS to use ios_ips advanced signature set. First, for category “all”, retire all signatures, this instructs IOS not to compile any signatures. Second, select IOS IPS category “advanced” and configure the *retired* parameter to false; this instructs IOS to compile all the signatures included in the “advanced” category (set) for IOS IPS.

```
ip ips signature-category
 category all
 retired true
 category ios_ips advanced
 retired false
```

Customers should either use basic or advanced category (or default category starting with with IOS 15.0(1)M Release) intended mainly for use by IOS IPS . 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 (loading) one of those category signatures by using management applications such as CSM and CPP or by using proper CLI commands as described in detail at Getting Started with Cisco IOS IPS.

### Memory Consideration

The number of signatures that can be unretired and loaded on the router at the same time depends on the free (remaining) memory available. However, 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.

### Alarming, Event Logging and Monitoring

Upon detecting an attack signature, Cisco IOS IPS can send a syslog message or log an alarm in Secure Device Event Exchange (SDEE) format. CCP may be used to monitor events generated by a single router and Cisco IPS Manager Express (IME) may be used to monitor IPS events generated by up to 5 routers. For monitoring events from more than 5 routers, Cisco highly recommends the Cisco Security Monitoring, Analysis, and Response System (MARS) appliance for network wide monitoring and correlation of IPS alarms, although any compatible monitoring application or device supporting syslog and/or SDEE may be used.

### Using Cisco IOS IPS with Cisco IOS Firewall

One of the main advantages of running Cisco IOS Firewall and Cisco IOS IPS together is the additional layer of security this setup provides. Cisco IOS Firewall helps ensure that traffic policies are enforced. For example, if inspection rules are configured to allow TCP packets only from a certain source address, the firewall inspects that traffic stream. Cisco IOS IPS works together with Cisco IOS Firewall and verifies this TCP traffic against its signature database. If a hacker manages to spoof the source IP address and attempts to send an attack, the firewall inspects the source address and allows the traffic. However, Cisco IOS IPS finds a match against the signature database and drops the malicious traffic or denies (shuns) all or only bad traffic from the spoofed IP address.

⚠ **IMPORTANT WARNING**

You should understand and set proper DOS protection threshold values for your network. Refer the section below for details.

#### Understanding the Inspection Threshold Values

Cisco IOS IPS uses the same set of threshold values as Cisco IOS Firewall. These threshold values are used to mitigate DoS attacks. Cisco IOS Firewall maintains counters of the number of “half-open” or “embryonic” TCP connections, as well as the total connection rate through the firewall and IPS software. These embryonic connections are TCP connections that have not completed the SYN-SYN/ACK-ACK handshake that is always used by TCP peers to negotiate the parameters of their mutual connection. Some malicious individuals write worms or viruses that infect multiple hosts on the Internet, and then attempt to overwhelm specific Internet servers with a SYN attack, in which large numbers of SYN connections are sent to a server by multiple hosts on the public Internet or within an organization’s private network. SYN attacks represent a hazard to Internet servers, because a server connection table can be loaded with “bogus” SYN connection attempts that arrive faster than the server can deal with the new connections. This type of attack is called a denial-of-service (DoS) attack, because the large number of connections in the victim’s server TCP connection list prevents legitimate users from gaining access to the victim’s Internet servers.

Cisco IOS Firewall provides protection from DoS attacks as a default when an inspection rule is applied. The DoS protection is enabled on the interface, in the direction in which the firewall is applied, for the protocols that the firewall policy is configured to inspect. DoS protection is enabled on network traffic only if the traffic enters or leaves an interface with inspection applied in the same direction as the initial movement of the traffic. Cisco IOS Firewall inspection provides several adjustable values to protect against DoS attacks. These settings have default values that may interfere with proper network operation if they are not configured for the appropriate level of network activity:

- ip inspect max-incomplete high <number-of-connections> (default 500)
- ip inspect max-incomplete low <number-of-connections> (default 400)
- ip inspect one-minute high <number-of-connections> (default 500)
- ip inspect one-minute low <number-of-connections> (default 400)
- ip inspect tcp max-incomplete host <half-open-sessions> (default 50) [block-time <block-time-in-minutes> (default 0)]

These parameters allow you to configure the points at which your firewall router DoS protection begins to take effect. When your router DoS counters exceed the default or configured values, the router resets one old embryonic connection for every new connection that exceeds the configured max-incomplete or one-minute high values, until the number of embryonic sessions drops below the max-incomplete low values. The router sends a syslog message if logging is enabled, and if IPS is configured on the router, the router sends a DoS signature message through SDEE. If the DoS parameters are not adjusted to the normal behavior or your network, normal network activity may trigger the DoS protection mechanism, causing application failures, poor network performance, and high CPU use on the Cisco IOS Firewall router.

These threshold values are important in protecting your network from DoS and DDoS attacks. You should set the threshold values to the correct values to ensure smooth operation of the network. If the values are set too high, DoS and DDoS attacks might not be blocked at the early stage of the attack. On the other hand, if the values are set too low, legitimate traffic might get dropped because of the lower limit imposed by the thresholds.

The following example shows the default threshold configuration values:

```
Router#show ip inspect all
Session audit trail is disabled
Session alert is enabled
one-minute (sampling period) thresholds are [400:500] connections
(low threshold 400, high threshold 500)
max-incomplete sessions thresholds are [400:500]
(low threshold 400, high threshold 500)
max-incomplete tcp connections per host is 50. Block-time 0 minute.
tcp synwait-time is 30 sec -- tcp finwait-time is 5 sec
tcp idle-time is 3600 sec -- udp idle-time is 30 sec
dns-timeout is 5 sec
```

### Tuning the Inspection Threshold Values

Although you cannot “disable” the DoS protection of your firewall, you can adjust the DoS protection so that it does not take effect unless a very large number of embryonic connections are present in your firewall router Stateful Inspection session table.

Follow this procedure to tune your firewall DoS protection to the activity of your network:

Step 1. Be sure your network is not infected with viruses or worms that could lead to erroneously large embryonic connection values. If your network is not “clean”, there is no way to properly adjust your firewall DoS protection.

Step 2. Set the max-incomplete high values to very high values:

```
ip inspect max-incomplete high 20000000
ip inspect one-minute high 100000000
ip inspect tcp max-incomplete host 100000 block-time 0
```

These settings will prevent the router from providing DoS protection during the time you observe your network connection patterns. If you wish to leave DoS protection disabled, stop following this procedure now.

Step 3. Clear the IOS Firewall statistics, using the following command:

```
show ip inspect statistics reset
```

Step 4. Leave the router configured in this state for some time, perhaps as long as 24 to 48 hours, so you can observe the network pattern over at least a full day’s activity cycle. *While the values are adjusted to very high levels, your network will not benefit from Cisco IOS Firewall or IPS DoS protection.*

Step 5. When your observation period is over, check the DoS counters with the following command (the parameters you must observe to tune your DoS protection are highlighted in **BOLD**:

```
router#show ip inspect statistics
Packet inspection statistics [process switch:fast switch]
tcp packets: [528:22519]
udp packets: [318:0]
Interfaces configured for inspection 1
Session creations since subsystem startup or last reset 766
Current session counts (estab/half-open/terminating) [1:0:0]
Maxever session counts (estab/half-open/terminating) [48:12:5]
Last session created 00:12:21
Last statistic reset never
Last session creation rate 0
Last half-open session total 0
```

Step 6. Configure ip inspect max-incomplete high to a value 25-percent higher than the indicated maxever session count half-open value on your router.
For example:

```
Maxever session counts (estab/half-open/terminating) [920:460:331]
460 * 1.25 = 575, thus, configure:
router(config)#ip inspect max-incomplete high 575
```

Step 7. Configure ip inspect max-incomplete low to the value your router displayed for its maxever session count half-open value.
For example:

```
Maxever session counts (estab/half-open/terminating) [920:460:331]
Thus, configure:
router(config)#ip inspect max-incomplete low 460
```

Step 8. The counters for ip inspect one-minute high and one-minute low maintain a sum of all TCP, UDP and ICMP connection attempts during the preceding minute of the router’s operation, whether the connections have been successful or not. A rising connection rate could be indicative of a worm infection on a private network, or an attempglted DoS against a server. Cisco IOS IPS does not maintain a value of the maxever one-minute connection rate, so you must calculate the value you will apply based on observed maxever values. To calculate the ip inspect one-minute low value, multiply the “established” value by 3.

For example:

```
Maxever session counts (estab/half-open/terminating) [920:460:331]
920 * 3 = 2760, thus, configure:
ip inspect one-minute low 2760
```

Step 9. Calculate and configure ip inspect max-incomplete high. The ip inspect one-minute high value should be 25-percent greater than the calculated one-minute low value.

For example:

```
ip inspect one-minute low (2760) * 1.25 = 3450, thus, configure:
ip inspect one-minute high 3450
```

Step 10. You need to determine a value for ip inspect tcp max-incomplete host according to your understanding of the capability of your server.

Step 11. Monitor your network DoS protection activity. Ideally, you should use a syslog server and record occurrences of DoS attack detection. If detection happens frequently, you may need to monitor and adjust your DoS protection parameters.

No predefined threshold values suit every network. The best practice is to fine-tune your network based on real network usage patterns. When the network is operational with a first set of threshold values, look out for the inspection logs and network usage pattern changes. If legitimate traffic is getting dropped at the firewall, increase these threshold values. If you are experiencing a DoS or DDoS attack, decrease the threshold values such that the firewall can detect and mitigate the attack at an earlier time.

### Understanding the Inspect Hash Table Size

The ip inspect hashtable-size command is available to fine-tune the system hash-table size for session counters. How is this command related to session threshold values? To understand this relationship, one must understand what this parameter is used for and how the mechanism works: A firewall inspects packets and keeps track of sessions by using a hash table. When it inspects packets, it must find out which session the packet belongs to; thus the firewall implements a hash table to search for the session of the packet. Collisions in a hash table result in poor hash function distribution because many entries are hashed into the same bucket for certain patterns of addresses. As the number of sessions increases, the collisions increase, thereby increasing the length of the linked lists and deteriorating the throughput performance.

As a general rule, to configure inspect hash-table size, the ip inspect hashtable-size command can be used to dynamically change the hash-table size to ensure optimum performance. The hash-table size should be increased when the total number of sessions running through the firewall router is approximately twice the current hash size, and should be decreased when the total number of sessions is reduced to approximately half the current hash size. Essentially, try to maintain a 1:1 ratio between the number of sessions and the size of the hash table.

## Advanced Topics

Currently, Cisco IOS IPS has implemented 15 diffrerent Signature Micro Engines (SMEs) to be able to compile and load selected (unretired) signatures into respective Regular Expression tables. All signatures supported in IOS IPS belong to one of those engines. When IPS is enabled on one or more router interfaces, IOS attempts to compile one engine at a time in a fixed order even if no signatures have been selected to compile for one or more particular engines. If one or more signatures belonging to an SME fails to compile due to insufficient memory or Regular Expression size limit per engine, remaining selected signatures for that engine will still be attempted to be compiled, but loading will not continue after 3 consecutive failed attempts to load different signatures.

The following gives further details on those 15 engines used to compile/load selected (unretired) signature on the router.

### ATOMIC-IP Engine

ATOMIC engine does not store persistent protocol based state data across packets; instead, it can trigger a signature from the analysis of the header (layers 3 and 4) of a single packet.

### MULTI-STRING Engine

The MULTI-STRING engine inspects Layer 4 protocol packets in a flexible manner.

### STRING Engines

Those engines include STRING-ICMP, STRING-TCP and STRING-UDP engines. STRING engines are generic pattern-matching inspection engines for ICMP, TCP, and UDP protocol; packets. They use a regular expression engine that can combine multiple patterns into a single pattern-matching table, allowing for a single search through the data.

### Service Engines

Service engines include SERVICE-HTTP, SERVICE-FTP, SERVICE-SMTP, SERVICE-RPC, SERVICE-DNS, SERVICE-MSRPC and SERVICE-SMB-ADVANCED engines. Service engines analyze Layer 5+ traffic between two hosts. These signatures are 1:1 signatures that track persistent data on the stream (AaBb) for TCP or QUAD (AaBb) for User Datagram Protocol (UDP). The engines decode and interpret the IP Layers 5-7 payload in a manner similar to that for the live service. A full-service-like decode may not be necessary if the partial decode provides adequate information to inspect the signatures. The engines decode enough bytes of the packet to make the signature determinations but do not decode more bytes than is needed, minimizing CPU and memory load.

Service engines have common characteristics, such as using the output from the stream processor, but each engine has specific knowledge of the service that it is inspecting. Service engines supplement the capabilities of the generic string engine, specializing in algorithms where using the string engine is inadequate or undesirable.

The purpose of the service decode is to mimic the interpretation of the live server of the Layer 5+ payload. These interpretations are used primarily in the determination of signatures, as the decoded fields are compared to the signature parameters.

As the engine is decoding, errors with bad payloads can occur. These error conditions are linked to different kinds of signatures, known as protocol violations or error traps, which occur when the engine is decoding the payload and an error occurs because of a malformation in the payload that violates the rules of the service protocol. An error trap handles this malfunction in the analysis code. Specifying the trap conditions that map to signatures is done by using the normal parameters, such as the SERVICE-FTP with Bad Port. In some cases, these trap conditions can be combined to form a signature that results when multiple trap conditions are encountered. However, in most cases, the trap conditions have a 1:1 mapping to the trap signatures.

### STATE Engine

The State engine provides state-based regular expression-based pattern inspection of TCP streams. A state engine is a device that stores the state of something and at a given time can operate on input to transition from one state to another and/or cause an action or output to take place. State machines are used to describe a specific event that causes an output or alarm.

### NORMALIZER Engine

The Normalizer engine deals with IP fragment reassembly. Intentional or unintentional fragmentation of IP datagrams can hide exploits making them difficult or impossible to detect. Fragmentation can also be used to circumvent access control policies. And different operating systems use different methods to queue and dispatch fragmented datagrams. If the sensor has to check for all possible ways that the end host can reassemble the datagrams, the sensor becomes vulnerable to DoS attacks. Reassembling all fragmented datagrams inline and only forwarding completed datagrams, refragmenting the datagram if necessary, prevents this.

## References

- **Cisco IPS Signatures Database:** http://tools.cisco.com/security/center/search.x?search=Signature
- **Cisco IPS Active Update Bulletins:** http://tools.cisco.com/security/center/bulletin.x?i=57
- **Cisco Security IntelliShield Alert Manager Service:** http://www.cisco.com/en/US/products/ps6834/serv_group_home.html

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 C11-404273-02 03/10