

## Cisco IOS IPS Signature Deployment Guide

Starting with Cisco IOS® Software Release 12.4(11)T, Cisco IOS Intrusion Prevention System (IPS) introduces support for the Cisco IPS Software Version 5.x signature format, which is also used by other Cisco appliance-based IPS products.

The Cisco IPS version 5.x signature format is improved to support encrypted signature parameters and other features such as signature Risk Rating. The following table shows where to download correct signature packages for different Cisco IOS Releases.

**Table 1.** IOS Release and Signature Format Version

IOS Release Version	Cisco IPS Signature Format Version	Cisco.com Download URL
12.4(11)T and later	5.x	<a href="http://www.cisco.com/cgi-bin/tablebuild.pl/ios-v5sigup">http://www.cisco.com/cgi-bin/tablebuild.pl/ios-v5sigup</a>
Pre 12.4(11)T	4.x	<a href="http://www.cisco.com/cgi-bin/tablebuild.pl/ios-sigup">http://www.cisco.com/cgi-bin/tablebuild.pl/ios-sigup</a>

### Feature History

Table 2 shows the feature history of the Cisco IOS IPS.

**Table 2.** Feature History of Cisco IOS IPS

Cisco IOS Software Release	Modification
12.4(11)T	Support Cisco IPS version 5.x signature format
12.4(6)T	Session setup rate performance improvements
12.4(3a)/12.4(4)T	String engine memory optimization
12.4(4)T	<ul style="list-style-type: none"> <li>MULTI-STRING engine support for Trend Labs and Cisco Incident Control System</li> <li>Performance improvement</li> <li>Distributed Threat Mitigation (DTM) support</li> </ul>
12.4(2)T	Layer 2 transparent intrusion prevention system (IPS) support
12.3(14)T	<ul style="list-style-type: none"> <li>Support for three string engines (STRING.TCP, STRING.UDP, and STRING.ICMP)</li> <li>Support for two new local shunning event actions: denyAttackerInline and denyFlowInline</li> </ul>
12.3(8)T	<ul style="list-style-type: none"> <li>Support for Security Device Event Exchange (SDEE) protocol</li> <li>Support for ATOMIC.IP, ATOMIC.ICMP, ATOMIC.IPOPTIONS, ATOMIC.UDP, ATOMIC.TCP, SERVICE.DNS, SERVICE.RPC, SERVICE.SMTP, SERVICE.HTTP, SERVICE.FTP, and OTHER engines</li> </ul>

### Cisco IOS Software Release 12.3T New Features

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/index.htm>

### Cisco IOS Software Release 12.4T New Features

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124t/index.htm>

## Cisco IOS IPS Deployment Guide

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 Software Intrusion Prevention System (Cisco IOS IPS), with inline intrusion capabilities, is the first system in the industry to provide an inline, deep-packet-inspection-based IPS solution that helps enable Cisco® routers to effectively mitigate a wide range of network attacks. Armed with the intelligence to accurately identify, classify, and stop malicious or damaging traffic in real time, Cisco IOS IPS is a core component of the Cisco Self-Defending Network, which helps the network protect itself. This technology uses Cisco IPS Sensor Software and signatures. Because Cisco IOS IPS is inline, it can drop traffic, send an alarm, or reset a connection—facilitating immediate router response to security threats.

Cisco IOS IPS capabilities include the ability to dynamically load and enable selected IPS signatures in real time, support more than 1700 signatures supported by Cisco IPS sensor platforms, and help users modify existing signatures or create new signatures to address newly discovered threats.

### Cisco IOS IPS: Key Features and Benefits

- Uses the underlying routing infrastructure to provide an additional layer of security with investment protection
- Supports inline function on a broad range of routing platforms. Attacks can be effectively mitigated to deny malicious traffic from both inside and outside the network
- Provides superior threat protection at all entry points into the network when used in combination with [Cisco IOS Firewall](#), [VPN](#), and Network Admission Control ([NAC](#)) solutions
- Supports/shares a subset of signatures and signature format with Cisco IPS appliances and modules
- Easy and effective management tools support, reducing operational complexity and expenditure (refer to [Cisco Router and Security Device Manager](#) and [CiscoWorks VPN/Security Management Solution](#))

For IOS releases after 12.4(11)T, IOS IPS has additional capabilities that

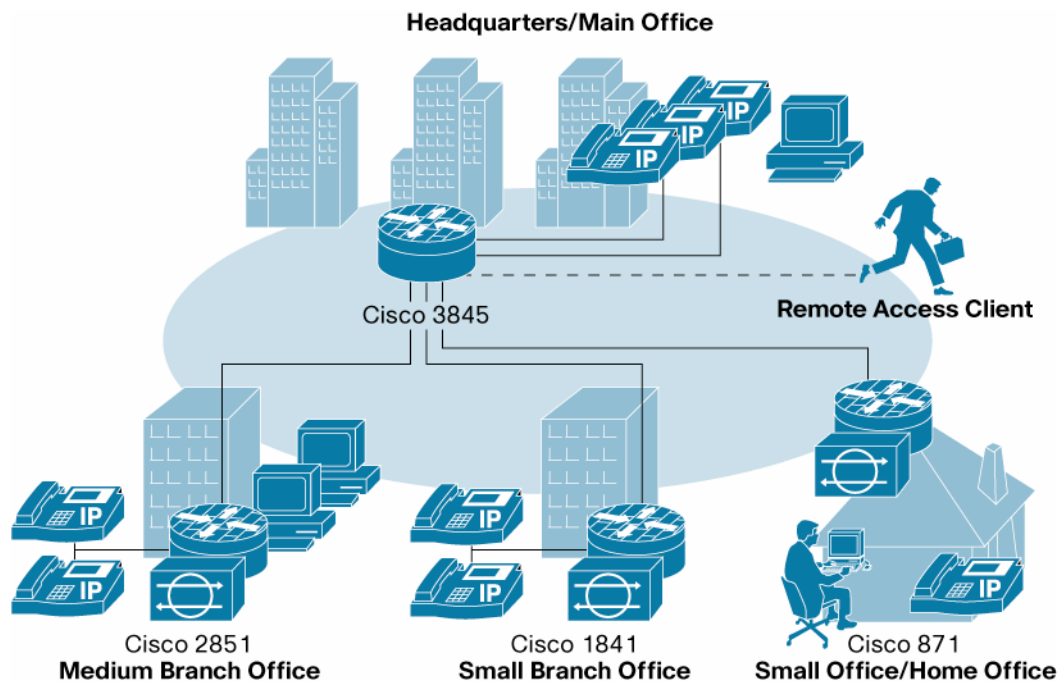
- Supports NDA (encrypted) signatures—important for supporting signatures for Microsoft vulnerabilities
- Supports Risk Rating value in IPS alarms for more accurate and efficient event correlation and monitoring
- Individual and category based signature provisioning via router CLI to provide granular customization and tuning of signature sets on routers
- Automatic signature update from a locally accessible server

## Deployment Scenarios

Cisco IOS IPS has two main deployment scenarios:

- Cisco IOS IPS protecting the Internet-facing (untrusted) interface
- Cisco IOS IPS within the internal (trusted) network

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



### Cisco IOS IPS Protecting the Internet-Facing (Untrusted) Interface

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.

### **Cisco IOS IPS within the Internal (Trusted) Network**

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.

Hub-and-spoke topologies are commonly used for networks. Figure 1 shows a typical network topology. In this topology, deploying Cisco IOS IPS on the spoke routers (Cisco 2851, 1841, and 871) will provide distributed protection for the network-attacks and exploits from one of the branch offices will not spread throughout the rest of the network. In addition, the hub router does not have to process all attacks and exploits from all branch offices, thus leaving more CPU power and memory for other tasks. 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.

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.

### **General Cisco IOS IPS Structure**

Cisco IOS IPS uses technology from Cisco Intrusion Detection System (IDS) and IPS sensor product lines, including Cisco IDS 4200 Series Sensors, Cisco Catalyst® 6500 Series IDS Services Modules, and network module hardware IDS 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 more than 1700 signatures-part of the common set of signatures that Cisco IPS sensors support-helping ensure that all Cisco products use a common resource. These signatures are available for download from Cisco.com.

Prior to IOS release 12.4(11)T, Cisco IOS IPS uses Signature Definition File (SDF) to load signatures and read signature information from it, and the signatures are in Cisco IPS version 4.x signature format. A Signature Definition File (SDF) contains all or a subset of the signatures supported by Cisco IOS IPS. The IPS loads the signatures contained in the SDF and scans incoming traffic for matching signatures. If a signature matches, it enforces the policy defined in the signature action (alarm, drop, reset the TCP connection, denyAttackerInlin or denyFlowInline, for example). Cisco IOS IPS reads the SDF, parses the file, and populates its internal tables with the information necessary to detect each signature. The SDF can be saved on the router flash memory (recommended), or users can specify the location of the SDF in the Cisco IOS IPS configuration on the router.

Starting from 12.4(11)T, IOS IPS uses Cisco IPS version 5.x format signatures and a simpler signature update process. In 12.4(11)T and later releases, IOS IPS will load and save entire signature information from the signature package posted on 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.

### Cisco IOS IPS and Cisco IDS Network Module

The Cisco IDS Network Module is available on Cisco modular access router platforms. Cisco does not support the configuration when both Cisco IOS IPS and the Cisco IDS Network Module are used. To configure the Cisco IDS Network Module, visit:

[http://www.cisco.com/en/US/products/hw/vpndev/ps4077/products\\_configuration\\_guide\\_chapter09186a008045922b.html](http://www.cisco.com/en/US/products/hw/vpndev/ps4077/products_configuration_guide_chapter09186a008045922b.html)

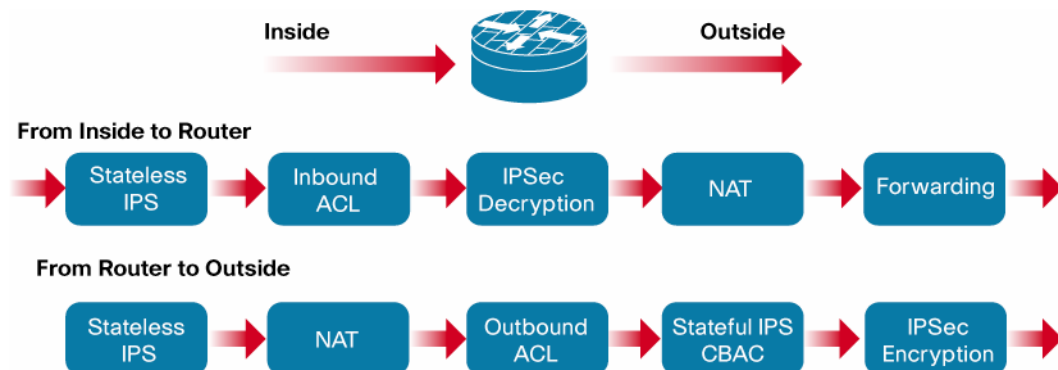
### Packet Flow

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.

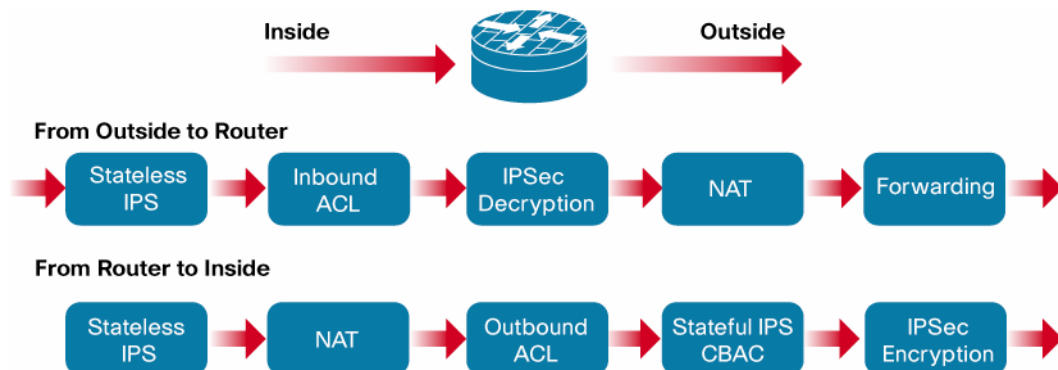
**Figure 2.** Packets Flowing from Inside to Outside the Network



### 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, rather than serially. 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.

In Cisco IOS Software Release 12.4(11)T, Cisco IOS IPS combined 5 ATOMIC engines into one single ATOMIC.IP engine, although flexibility in writing atomic signatures increased, the behavior for existing signatures did not change. Table 3 below show a list of SMEs supported by different IOS releases.

**Table 3.** SMEs Supported by Cisco IOS IPS

SME Prior 12.4(11)T	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

SME Prior 12.4(11)T	SME 12.4(11)T and later	Description
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 antievasive URL de-obfuscation
SERVICE.FTP	SERVICE.FTP	Provides FTP service special decode alarms
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

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

### Signature Actions

Prior IOS release 12.4(11)T, each signature can be set to send an alarm, drop the attack packets, deny the attacker, deny the attack flow, or reset the connection. Each action is enabled on a per-signature basis using Cisco SDM or the CiscoWorks Management Center for IPS Sensors—there is no CLI command to tune signature parameters. Each signature has an action assigned by default, based on the severity of the signature. “Alarm” sends a notification about the attack through syslog or SDEE. “TCP reset” is effective for TCP-based connections and sends a reset to both the source and destination addresses. For example, in case of a half-open SYN attack, Cisco IOS IPS can reset the TCP connections. “Drop” discards the packet without sending a reset. Cisco recommends using “drop and reset” in conjunction with alarm. “DenyAttackerInline” blocks the attacker’s source IP address completely. No connection can be established from the attacker to the router until the shun time expires (this time is set by the user). “DenyFlowInLine” blocks the appropriate TCP flow from the attacker. Other connections from the attacker can be established to the router.

For IOS release 12.4(11)T and later, IOS starts to support CLI configuration of these actions for signatures. 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/univercd/cc/td/doc/product/software/ios124/124newft/124t/124t11/ips\\_v5.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124t/124t11/ips_v5.htm)

### Signatures

A signature detects patterns of misuse in network traffic. Prior to IOS 12.4(11)T release, IOS IPS has 132 built-in signatures available in the Cisco IOS Software image. The built-in signatures are hard-coded into the Cisco IOS Software image for backward compatibility. Starting IOS release

12.4(11)T and later, there are no built-in (hard coded) signatures anymore within Cisco IOS Software.

Cisco IOS IPS can scan the contents of IP fragments, thereby protecting the network from fragmented attacks. The solution detects both atomic signatures in a single packet and composite signatures spread into a sequence of packets. Detection of most composite signatures requires stateful inspection of multiple packets (keeping state information across packets of a particular session between a source-destination pair). Both Cisco IOS IPS and Cisco IOS Firewall use the same session table. For example, if an HTTP request is initiated from the corporate network to the Internet, the return traffic may be compromised, so Cisco IOS IPS maintains the state of the entire session.

### **Signature Category and Signature CLI Package—12.4(11)T and Later Release**

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 IPS for 12.4(11)T and later release, a signature package in Cisco IPS version 5.x format is required to load signatures to IOS IPS. Cisco provides a version 5.x format signature package for CLI users. It can be downloaded from Cisco.com at <http://www.cisco.com/cgi-bin/tablebuild.pl/ios-v5sigup>

In IOS 12.4(11)T and later release, Cisco maintains backward compatibility with the basic and advanced signature sets. The following is an example to configure IOS IPS to use basic signature set. First, for category “all”, retired all signatures, this instructs IOS not to compile all signatures. Second, select IOS IPS category “basic” and configure retired to false, this instructs IOS to compile all signatures for “basic” category.

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

For details how to configure IOS IPS, refer to the IOS IPS configuration guide at [http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124t/124t11/ips\\_v5.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124t/124t11/ips_v5.htm)

### **Signature Definition Files—Prior 12.4(11)T Release**

Prior 12.4(11)T, the SDF is an integral part to Cisco IOS IPS; it is an Extensible Markup Language (XML) file with a definition of each signature in Cisco IPS version 4.x signature format, along with relevant configurable actions. Cisco IOS IPS reads in the SDF, parses the XML, and populates its internal tables with the information necessary to detect each signature. The SDF contains the signature definition and configuration. Actions such as alarm, drop, or reset can be selected for individual signatures within the SDF. The SDF can be modified so the router detects only specific signatures; as a result, it can contain all or a subset of the signatures supported in Cisco IOS IPS. The user specifies the location of the SDF, which can reside on the local flash file system (recommended) or on a remote server. Remote servers can be accessed with Trivial File Transfer Protocol (TFTP), FTP, HTTP, HTTPS, Secure Copy Protocol (SCP), or Remote Copy Protocol (RCP).

If the Cisco IOS IPS-enabled router is configured to scan packets using the SDF, it gets signature and engine information from the SDF. All or a subset of the routers in a network can use the same SDF or a different SDF, depending on the requirements of the network. Some routers may allow for activating more signatures than routers with less memory.

Refer to reference URLs at the end of this document for a detailed description of the signatures supported by Cisco IOS IPS.

### Basic Signature Set and Advanced Signature Set Posted on Cisco.com

Prior 12.4(11)T release, Cisco IOS IPS ships with one of two preconfigured SDFs: basic (also called 128MB.sdf) and advanced (also called 256MB.sdf). These SDFs contain the latest high-fidelity (low false positives) worm, virus, instant messaging, and peer-to-peer blocking signatures for detecting security threats, allowing easier deployment and signature management for the user. Pre-built SDFs provide a good starting point for users—they do not have to start creating their own SDFs from the beginning from the wide range of signatures available in Cisco IOS Software. Signatures can be appended or modified from these SDFs. More details about how to use the SDFs appear later in this paper.

The basic signature set (in file 128MB.sdf) is the Cisco recommended signature set for routers with 128 MB or more memory, and the advanced signature set (in file 256MB.sdf) is the Cisco recommended signature set for routers with 256 MB or more memory. Cisco decommissioned the use of the file attack-drop.sdf. Although it is still possible to use this file in Cisco IOS Software releases prior to Cisco IOS Software Release 12.4(11)T, because of the very limited and old attack coverage the signatures in that file provides, Cisco does not recommend its use in production environments. These files can be downloaded from Cisco.com at <http://www.cisco.com/cgi-bin/tablebuild.pl/ios-sigup>

**Figure 4.** Location of the Three SDFs in Cisco.com

The screenshot shows a web browser window with the URL <http://www.cisco.com/cgi-bin/tablebuild.pl/ios-sigup>. The page content includes a navigation menu on the left and a main content area titled 'Cisco IOS IPS'. Under the heading 'Select a File to Download', there is a table listing available files for download.

Filename	Release	Date	Size (Bytes)
<a href="#">256MB.sdf</a> Advanced Signature Set	V7	10-DEC-2006	805532
<a href="#">128MB.sdf</a> Basic Signature Set	V7	10-DEC-2006	535439
<a href="#">Cisco_SDF_Release_v7_0_Signature_List.pdf</a> Cisco SDF V7 Release Signature List	V7	10-DEC-2006	151271
<a href="#">Cisco_SDF_Release_Note_v7_0.pdf</a> Cisco SDF V7 Release Note	V7	10-DEC-2006	63382

**Note:**

- The IOS-Sxxx.zip file contains all available signatures that Cisco IOS IPS supports, allowing the user to create a custom SDF that can be loaded on the router.
- New routers shipped from the factory contain one SDF that is recommended for their default memory. For example, Cisco 1800 Series routers ship with 128MB.sdf, and Cisco 3800 Series routers ship with 256MB.sdf.
- Additional SDFs can be downloaded from <http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-sigup> (requires Cisco.com login), and are also packaged with Cisco SDM 2.2 and later releases available on Cisco.com at <http://www.cisco.com/go/sdm>.
- For CiscoWorks Management Center for IPS Sensors, signature updates can be downloaded from: <http://www.cisco.com/pcgi-bin/tablebuild.pl/idsmc-ids4-sigup> (requires Cisco.com login).

**Memory Consideration**

With sufficient memory, Cisco IOS IPS supports more than 1700 signatures, but one major remaining concern is how many signatures various router platforms can actually support, given memory and platform constraints. The number of signatures and engines supported depends only on the memory available. The pre-built SDFs have the optimum combination of signatures for all standard memory configurations, providing a good starting point.

While adding new signatures, note that signatures in SERVICE.SMTP, STRING.TCP, and STRING.UDP engines are more memory-intensive than other signature engines. From Cisco IOS Software Release 12.4(3a) onward, these three engines have been optimized to support more signatures and use less memory than earlier releases.

**Alarming and Logging**

Cisco IOS IPS supports alarming and logging of events through syslog and SDEE. Cisco SDM 2.2 and later release as well as Cisco Security Monitoring, Analysis, and Response System (CS-MARS) can be used to view signature alarms, events, and logs.

In addition, the Cisco IPS Event Viewer (IEV) offers a free monitoring solution for small-scale IPS deployments. Monitoring individual IPS devices, the IPS Event Viewer is easy to set up and use, and provides the user with:

- Support for IOS IPS through SDEE compatibility
- Customizable reporting
- Tunable notification actions such as e-mail and paging
- Visibility into applied response actions, learned DST OS, and threat rating

Cisco IPS Event View can be downloaded from Cisco.com at <http://www.cisco.com/cgi-bin/tablebuild.pl/ids-ev>

**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 attempted 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.

### Out-of-Order Packets

Starting with 12.4(11)T release, IOS IPS will perform TCP reassembly for out-of-order packets by default. The following discussion regarding out-of-order packets only applies to IOS releases prior to 12.4(9)T2.

Cisco IOS IPS performs deep packet inspection for certain signatures. To perform deep packet inspection correctly, IPS needs the packets in a sequential order. If TCP traffic is going through an IPS-enabled router and signatures that require deep inspection are provisioned, IPS enforces the stipulation that the traffic stream must be in a sequential order by dropping out-of-order packets. Typically networks have low levels of out-of-order TCP segments and although such packets get dropped by Cisco IOS IPS, they are retransmitted by the end hosts and the end-to-end connection is not significantly affected. However, if the network has excessive amounts of out-of-order packets, these are dropped by Cisco IOS IPS, causing frequent retransmissions and hence detrimental effect on the performance of the end-to-end connection. In such cases, the network deployment should be carefully studied to correct the root cause of high levels of out-of-order packets; caution is advised when deploying Cisco IOS IPS in such networks.

If out-of-order packets are inevitable or are caused by reasons out of your legitimate control, a possible workaround to prevent out-of-order packets is to use access lists to prevent inspection of the traffic by Cisco IOS IPS. For example, if the out-of-order packet occurs between host A (10.10.10.66) and host B (192.168.16.15), you can configure Cisco IOS IPS as follows:

```
Router #configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 150 deny ip host 10.10.10.66 host 192.168.16.15
Router(config)#access-list 150 permit ip any any
Router(config)#ip ips name myips list 150
Router(config)#exit
```

After applying the IPS rule myips to the interface, Cisco IOS IPS will not inspect the traffic denied by access-list 150 associated with it. The sample ACL addresses two specific hosts. You can use ACLs to filter networks or even specific applications using port numbers, depending on the class of traffic that has the out-of-order problem.

## Deploying to Multiple Routers

Table 4 summarizes the options for managing Cisco IOS IPS on multiple routers.

**Table 4.** Managing Cisco IOS IPS on Multiple Routers Running 12.4(9)T or Earlier IOS Releases

Software or Hardware	Number of Devices	Reference
Cisco SDM	1-10	<a href="http://www.cisco.com/go/sdm">http://www.cisco.com/go/sdm</a>
Command Scheduler Job	10-100	<a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hnm_c/ch30/hg_kron.htm">http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hnm_c/ch30/hg_kron.htm</a>
Cisco Management Center for IPS Sensors	50-500	<a href="http://www.cisco.com/en/US/products/ps6680/index.html">http://www.cisco.com/en/US/products/ps6680/index.html</a>
Cisco Configuration Engine	500-5000	<a href="http://www.cisco.com/en/US/partner/products/sw/netmgtsw/ps4617/tsd_products_support_series_home.html">http://www.cisco.com/en/US/partner/products/sw/netmgtsw/ps4617/tsd_products_support_series_home.html</a> (requires Cisco.com login)

SDM is best used for managing 1 to 10 devices. For up to 100 routers, KRON jobs can be used to download SDFs from a server where predefined or updated SDFs are stored. A KRON policy list can be created, and scheduled occurrences can be set up to retrieve the SDF at regular intervals. For more information about KRON job configuration and command reference, refer to the [Command Scheduler](#) document.

[Cisco Management Center for IPS Sensors](#) should be used when managing from 50 to 500 Cisco IOS IPS routers or Cisco IPS sensors. For large-scale deployment of up to 5000 devices, [Cisco Configuration Engine](#) (requires Cisco.com login) should be used.

At this point, CLI is the only option to provision and tune IOS IPS signatures in 12.4(11)T release.

## Performance Considerations

To ascertain the expected performance of Cisco IOS IPS, Cisco used the Spirent Avalanche and Reflector test system. The avalanche was programmed to rapidly establish multiple HTTP sessions to the reflector, with the router running Cisco IOS IPS between them.

The avalanche opens the TCP session to the reflector, and requests a single 64-KB file from the reflector. The reflector sends the file, and then the avalanche receives the file and closes the TCP/HTTP session. The avalanche is programmed to keep increasing the number of such

transfers, increasing the total throughput load offered to the router. The load is increased until sessions start failing because of router performance limitations.

Table 5 lists the maximum throughput obtained for various router platforms with Cisco IOS IPS enabled, using the test methodology just described.

**Note:** These numbers are derived from tests performed in isolated or ideal conditions. Your results may vary depending on your network architecture, traffic patterns, and services running on the router.

**Table 5.** Maximum Throughput on Cisco Routers

Platform Tested	Throughput
Cisco 871	50 Mbps
Cisco 1811	55 Mbps
Cisco 1841	60 Mbps
Cisco 2801	65 Mbps
Cisco 2811	70 Mbps
Cisco 2821	200 Mbps
Cisco 2851	250 Mbps
Cisco 3825	325 Mbps
Cisco 3845	425 Mbps

## Advanced Topics

There are total 13 engines in 12.4(11)T and later release.

### ATOMIC-IP Engine

Atomic engine do not store persistent data across packets; instead, it can fire an alarm from the analysis of a single packet. Therefore, the basic features of the engine do not require attachment to a nonglobal StorageKey—they use the StorageKey xxxx. Because atomic engine has no storage, atomic engine signatures are essentially 1:1 signatures.

Starting 12.4(11)T release, the previous ATOMIC.L3.IP, ATOMIC.ICMP, ATOMIC.UDP, ATOMIC.IPOPTIONS and ATOMIC.TCP engines are merged into one single engine – ATOMIC-IP.

### MULTI-STRING Engine

The MULTI-STRING engine inspects Layer 4 protocol packets in a flexible manner. This engine also supports Trend Labs network virus signatures normally deployed to Cisco IOS IPS through the Cisco Incident Control System (ICS).

### String Engines

String engines include STRING-ICMP, STRING-TCP and STRING-UDP engines. String engine is a generic-based pattern-matching inspection engine for ICMP, TCP, and UDP, it uses 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-RPC and SERVICE-DNS 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 Layer 5+ 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 of the data to make the signature determinations but do not decode more 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 BadPort. 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 MySDN:** <http://tools.cisco.com/MySDN/Intelligence/home.x>
- **Cisco Incident Control System (ICS):**  
<http://www.cisco.com/en/US/products/ps6542/index.html>
- **Cisco IOS IPS Configuration Guide:**  
[http://www.cisco.com/en/US/products/ps6441/products\\_feature\\_guide09186a0080747eb0.html](http://www.cisco.com/en/US/products/ps6441/products_feature_guide09186a0080747eb0.html)
- **Cisco IDS Event Viewer:** <http://www.cisco.com/cgi-bin/tablebuild.pl/ids-ev>



Americas Headquarters  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
[www.cisco.com](http://www.cisco.com)  
Tel: 408 526-4000  
800 553-NETS (6367)  
Fax: 408 527-0883

Asia Pacific Headquarters  
Cisco Systems, Inc.  
168 Robinson Road  
#28-01 Capital Tower  
Singapore 068912  
[www.cisco.com](http://www.cisco.com)  
Tel: +65 6317 7777  
Fax: +65 6317 7799

Europe Headquarters  
Cisco Systems International BV  
Haarlerbergpark  
Haarlerbergweg 13-18  
1101 GH Amsterdam  
The Netherlands  
[www.europe.cisco.com](http://www.europe.cisco.com)  
Tel: +31 0 800 020 0701  
Fax: +31 0 20 367 1100

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](http://www.cisco.com/go/offices).