Cisco IOS Inline Intrusion Prevention System

The Cisco IOS® Intrusion Prevention System (IPS) helps protect your network from attacks by inspecting traffic passing in both directions through any combination of router LAN and WAN interfaces.

Product Overview

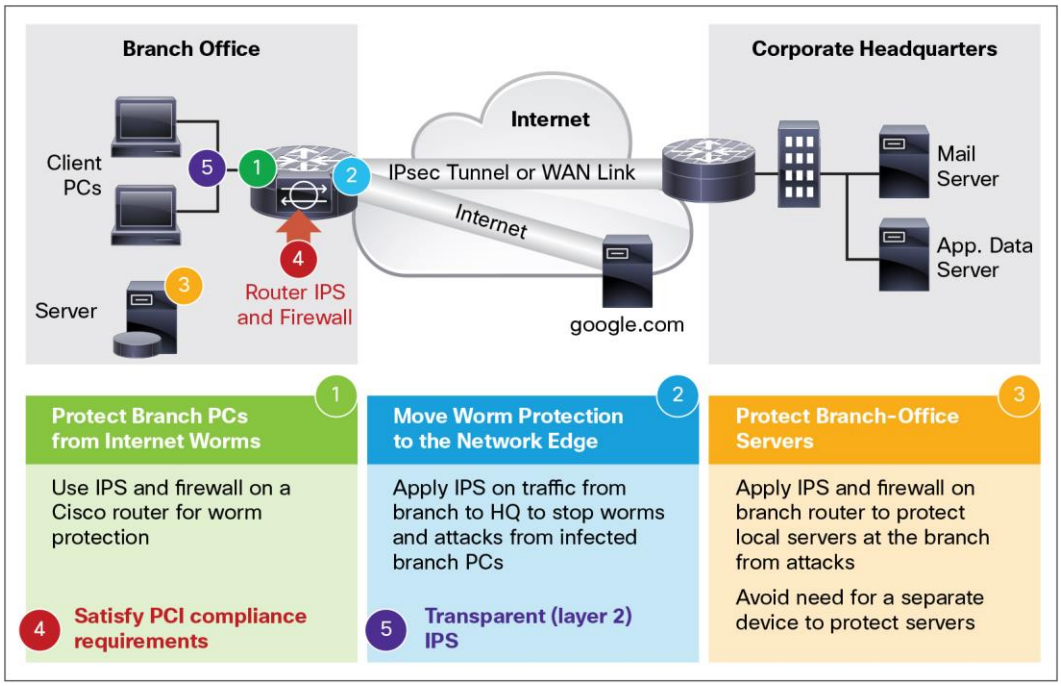
In today's business environment, network intruders and attackers can come from outside or inside the network. They can launch distributed denial-of-service attacks, they can attack Internet connections, and they can exploit network and host vulnerabilities. At the same time, Internet worms and viruses 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 recognize and mitigate these attacks, threats, exploits, worms, and viruses.

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

Major Use Cases and Benefits

Cisco IOS IPS helps to protect your network in five ways, shown in Figure 1:

Figure 1. Major Use Cases for Cisco IOS IPS



Main Benefits

- Provides networkwide, 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
- Dramatically improves the ease of management of IPS policies through a unique risk-rating-based signature-event-action processor
- 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 the 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 7000 signatures from the same signature database available for Cisco® IPS appliances

Table 1. Cisco IOS IPS Capabilities in the Latest IOS Releases

Feature	Advantage/Benefit
Capability to download IOS IPS signature packages to the router directly from cisco.com available in 15.1(1)T or later IOS T-train releases	Easier to use and deploy, eliminating the need (step) to manually download signature updates to a local server first and then to the router. Routers that have a connection to the Internet can download signature updates automatically in a periodic fashion without human intervention. For more information, see the IOS IPS Auto Update feature at http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_ios_ips/configuration/15-mt/sec-data-ios-ips-15-mt-book/ips-auto-update.html.
Frequent updates of the IOS IPS category signatures (including some lightweight signatures) by the Cisco Signature Team, starting with IOS 15.0(1)M	More comprehensive and effective attack coverage by default. Much quicker inclusion of most relevant new threat signatures.
Lightweight signature engines for HTTP, SMTP, and FTP protocol signatures and Regular Expression Table chaining available also in 15.0(1)M	Memory-efficient traffic scanning for attack signatures consuming less memory on the router. 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 to distinguish among the IPS alarms and events generated within each virtual segment using the VRF ID.
Available in 12.4(15)T5 or Later IOS T-Train Releases	
Support for 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
Support for the Signature Event Action Processor (SEAP)	Quick and automated adjustment of signature-event actions based on the calculated risk rating of the event
Automated signature updates from a local TFTP or HTTP(S) server	Protection from latest threats with little user intervention
IDCONF (XML) signature-provisioning mechanism	Highly secure provisioning through Cisco Security Manager 3.1 or later and the Cisco Router and Security Device Manager (SDM) 2.4 over HTTPS
Individual and category-based signature provisioning through Cisco IOS CLI	Precise customization and tuning of signatures through custom scripts
Same signature format and database as the latest Cisco IPS appliances and modules	Common deployment and attack signature definitions between Cisco IPS appliances or modules and Cisco IOS IPS

Platform Support

Cisco IOS IPS is available in certain software feature sets on the 87x routers; the Integrated Services Routers; the SR 520 Secure Router; and the 720x and 7301 routers listed in Table 2. Starting with IOS 15.0(1)M, the IOS IPS is also supported on the 88x and 89x routers and the next-generation ISR with an optional license that supports the use of that and other features when installed, as shown in Table 3.

Table 2. IPS Feature Availability Based on IOS Image Types

Router Series	Models Supported	IOS Images (Feature Sets) Supported
800	871, 876, 877, 878	Advanced IP Services
1800	1801,1802,1803,1811,1812,1841, 1861	Advanced Security, Advanced Enterprise, and Advanced IP Services
2800	2801, 2811,2821,2851	Advanced Security, Advanced Enterprise, and Advanced IP Services
3800	3825,3845	Advanced Security, Advanced Enterprise, and Advanced IP Services
SR 520	SR 520	Advanced Security and Advanced IP Services
7200	7204VXR, 7206VXR	Advanced Security, Advanced Enterprise, and Advanced IP Services
7301	7301	Advanced Security, Advanced Enterprise, and Advanced IP Services

Table 3. IPS Feature Availability Based on Optional Feature Licenses

Router Series	Models Supported	Feature License Supported
800	819, 860VAE, 880VA, 881, 881W, 887V, 888E, 888EA, 888, 888W, 891, 891F, 891W, 892, 892F, 892FW, 892W, C892FSP-K9, C-881	Advanced IP Services
1900	1905, 1921, 1941, 1941W	Security
2900	2901, 2911, 2921, 2951	Security
3900	3925, 3945	Security

Basic and Advanced Signature Categories for IOS IPS

In Cisco IOS Software Release 12.4(11)T and later T-train releases, IOS IPS signature provisioning is accomplished through the selection of one of two signature categories: Basic or Advanced. Users may also add or remove individual signatures and can tune signature parameters using Cisco Configuration Professional or Cisco Security Manager or the command-line interface (CLI), which allows easy scripting to manage signature configuration for a large number of routers.

IOS Basic and Advanced signature categories are preselected signature sets intended to serve as a good starting set for most users of IOS IPS. They contain the latest high-fidelity (low false positives) worm, virus, IM, or peer-to-peer blocking signatures for detecting security threats, allowing easier deployment and signature management. Cisco IOS IPS also allows the selection and tuning of signatures outside those two categories.

Signature categories are an integral part of Cisco signature update packages posted at http://software.cisco.com/download/release.html?mdfid=281442967&flowid=4836&softwareid=280775022&release=S807&relind=AVAILABLE&rellifecycle=&reltype=latest.

Users can also access this link from the Cisco Software Download page by clicking Security > Network Security > Integrated Threat Control > Cisco IOS Intrusion Prevention System Feature Software.

Those signature update packages incorporate all previous Cisco IPS signature updates and can be downloaded to the router from a local PC or server using the router CLI, Cisco Configuration Professional, or Cisco Security Manager.

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

Cisco Services for IPS

Entitlement to download and use signature update packages for the Cisco IOS IPS feature requires purchase of the appropriate Cisco Services for IPS contract, which includes Cisco Smart Net Total Care™ support in a single comprehensive offering. Supported by the Cisco Global Security Intelligence organization, Cisco Services for IPS delivers continuously updated, comprehensive, and accurate detection technology to identify and block fast-moving and emerging threats before they damage your network assets.

Starting with IOS 15.0(1)M1, a valid IOS IPS Signature Subscription license is required to be installed on 88x, 89x, 19xx, 29xx, and 39xx routers to load signature packages. To obtain and install this license, you need to purchase the Cisco Services for IPS contract relevant to the router model as well as the type and level of the desired Cisco Smart Net Total Care deliverables.

For more information about Cisco Services for IPS, visit: http://www.cisco.com/web/services/portfolio/product-technical-support/intrusion-prevention-ips/index.html.

Signature Microengines

Cisco IOS IPS uses signature microengines (SMEs) to load (into the router's memory) and scan for a set of attack signatures. Each engine is customized for inspecting a Layer 4 or 7 protocol and its fields and arguments. Within each packet carrying data for that protocol, it looks for a set of legal parameters that have allowable ranges or sets of values. It also scans for malicious activity specific to that protocol using a parallel signature-scanning technique to scan for multiple patterns within an SME at any given time.

Attack Mitigation

Cisco IOS IPS can protect your network from more than 3700 different attacks, exploits, worms, and viruses. Attacks that can be detected and stopped by Cisco IOS IPS include many Microsoft Windows OS and application vulnerability exploits, viruses, and worms.

Actions for Detected Signatures

Each individual signature or category of signatures selected to scan traffic for matching attacks can be configured to take any combination of the following five actions when triggered:

1. Send an alarm by syslog message or log an alarm in Secure Device Event Exchange (SDEE) format
2. Drop a malicious packet
3. Send TCP-reset packets to both ends of the connection to terminate the session
4. Deny all packets from the attacker (source address) temporarily
5. Deny further packets belonging to the same TCP session (connection) from the attacker (source address)

Configuration and Signature Provisioning

The router CLI or Cisco Configuration Professional version 1.1 or later can be used for the configuration of IOS IPS as well as the precise provisioning and tuning of IPS signatures on a single router running Cisco IOS Release 12.4(11)T2 or later. In addition, Cisco Security Manager version 3.2 or later may be used to manage IPS policies and signature sets on multiple routers running Cisco IOS Software Release 12.4(11)T2 or later. Use of IOS IPS in IOS releases prior to 12.4(11)T or in IOS Mainline releases is not recommended.

Event Monitoring

Upon detecting an attack signature, Cisco IOS IPS can send a syslog message or log an alarm in the Secure Device Event Exchange (SDEE) format. Cisco Configuration Professional 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 10 routers.

Cisco Capital

Financing to Help You Achieve Your Objectives

Cisco Capital can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital is available in more than 100 countries. Learn more.

For More Information

For more information about Cisco IOS IPS, visit http://www.cisco.com/c/en/us/products/security/ios-intrusion-prevention-system-ips/index.html or contact your local Cisco account representative.

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 C78-381294-09 11/15