

Cisco IOS Inline Intrusion Prevention System (IPS)

This data sheet provides an overview of the Cisco IOS® Intrusion Prevention System (IPS) solution.

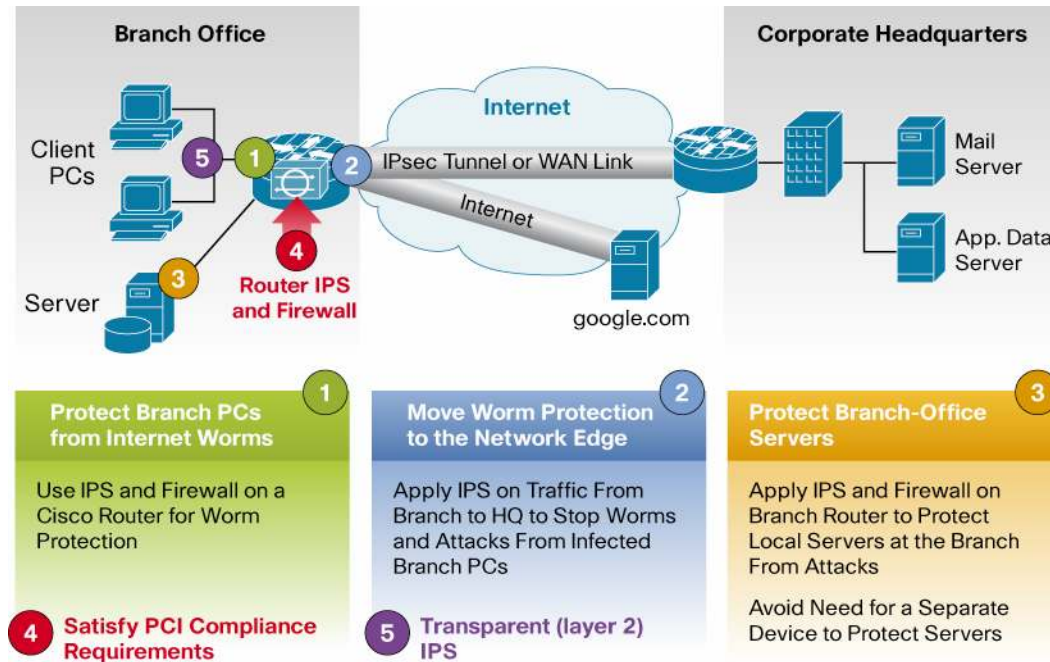
Product Overview

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 instantaneously recognize and mitigate these attacks, threats, exploits, worms and viruses.

Cisco IOS Intrusion Prevention System (IPS) is an inline, deep-packet inspection-based solution 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 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.

Cisco IOS IPS: Major Use Cases and Key Benefits

IOS IPS helps to protect your network in 5 ways:



- 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, risk rating based signature event action processor dramatically improves the ease of management of IPS policies
- 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 2400 [attack signatures](#) from the same signature database available for [Cisco Intrusion Prevention System \(IPS\) appliances](#)

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. 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. 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

Platform Support

Cisco IOS IPS is available in certain software feature sets on the 87x routers, Integrated Services Routers, SR520, 720x and 7301 routers listed in Table 2. Starting with IOS 15.0(1)M Release, IOS IPS feature is also supported on the 88x, 89x routers and next generation Integrated Services Routers with an optional license that enables use of that and other features when installed, as shown in Table 3.

Table 2. IPS Feature Availability based on IOS Image Types

Product Family	Platforms 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
SR520	SR520	Advanced Security and Advanced IP Services

Product Family	Platforms Supported	IOS Images (Feature Sets) Supported
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

Product Family	Platforms Supported	Feature License Supported
800	881, 887, 888, 891, 892	Advanced IP Services
1900	1941	Security
2900	2901, 2911,2921,2951	Security
3900	3925,3945	Security

Basic, Advanced and Default 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 by selecting one of two signature categories: Basic or Advanced. 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. Users may also add or remove individual signatures and/or can tune signature parameters via Cisco Configuration Professional (CCP) or Cisco Security Manager (CSM) management or through the command-line interface (CLI) which allows easy scripting to manage signature configuration for a large number of routers.

IOS Basic and Advanced/Default signature categories are pre-selected 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 selection and tuning of signatures outside those two categories.

Signature categories are an integral part of Cisco signature update packages posted 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.

Those signature update packages are cumulative of 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 (CCP) or Cisco Security Manager (CSM).

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 IOS IPS Feature in those releases. Also, support for IOS IPS feature in those older releases is very limited.

Signature Micro Engines

Cisco IOS IPS uses Signature Micro-Engines (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/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 more than 2400 attacks, exploits, worms and viruses. Some examples of attacks that can be detected and stopped by Cisco IOS IPS include many Microsoft Windows OS and application vulnerability exploits and viruses and worms such as ANTS, Bagle, MyDoom, Netsky, Agobot, Minmai, Klez, Sober, Zotob, Norvag, Phatbot, MyTob, GaoBot, Blaster, W2K RPC DoS, ZAFI.D, Slapper, Apache/mod_ssl, Slammer, GaoBot, Blaster, Nachi and Ping Tunnel.

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 5 actions when triggered:

1. Send an alarm via syslog message or log an alarm in SDEE (Secure Device Event Exchange) format
2. Drop 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 (CCP) version 1.1 or later can be used for configuration of IOS IPS as well as highly granular provisioning and tuning of IPS signatures on a single router running Cisco IOS 12.4(11)T2 or later releases. In addition, Cisco Security Manager (CSM) version 3.2 or later may be used for management of IPS policies and signature sets on multiple routers running Cisco IOS 12.4(11)T2 or later releases. Use of IOS IPS in IOS releases prior to 12.4(11)T or 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 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.

Cisco and Partner Services for the Branch

Services from Cisco and our certified partners can help you transform the branch experience and accelerate business innovation and growth in the Borderless Network. We have the depth and breadth of expertise to create a clear, replicable, optimized branch footprint across technologies. Planning and design services align technology with business goals and can increase the accuracy, speed, and efficiency of deployment. Technical services help improve operational efficiency, save money, and mitigate risk. Optimization services are designed to continuously improve performance and help your team succeed with new technologies.

For More Information

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

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flip Video, Flip Video (Design), Flipshare (Design), Flip Ultra, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0907R)