DATA SHEET

CISCO IOS IPS

OVERVIEW

In today's technology environment, Internet worms and viruses can spread across the world in a matter of minutes. Without the luxury of time to react, the network itself must possess the intelligence to instantaneously recognize and mitigate these threats. A networking architecture paradigm shift is required to defend from these fast moving attacks. It is no longer possible to contain these intrusions at a few points in the network. Intrusion Prevention is required throughout the entire network to detect and stop an attack at every ingress and egress point in the network. The only scalable and cost effective way to accomplish this is by integrating Intrusion Prevention into the access points of the network.

An industry first, Cisco has integrated an Intrusion Prevention System (IPS) into Cisco IOS Software® based Routers. IOS IPS is now inline, deep-packet, inspection technology—which helps to effectively mitigate a wide range of network attacks without compromising performance and is available at every network access point. The intelligence and capability to accurately identify, classify, and stop malicious or damaging traffic in real time makes Cisco IOS IPS a core component of the Cisco Self-Defending Network.

CISCO IOS IPS BENEFITS

While it is common practice to deploy an IPS system to inspect traffic for attacks at the head-end, protecting branch offices is also important to ensure that malicious traffic is stopped as close to the entry point into the network as possible. By using Cisco IOS Inline IPS at the branch, the branch connected routers can drop traffic, send an alarm, or reset the connection as needed to stop attacking traffic at the point of origination and remove unwanted traffic from the network as quickly as possible. Although IT professionals agree to this defense approach, it has always been cost prohibitive to deploy an IPS system at every access point. Now, with an IPS solution integrated into the existing access router the cost is only an incremental to implement this best practice throughout the network.

Benefits:

- **Investment protection**—No new hardware deployments are required when Cisco Access routers are already in place.
- **Inline support**—Effectively mitigating both internal and external attacks to successfully deny malicious traffic.
- **Integrated Security**—Complements Cisco IOS Firewall and VPN solutions for superior threat protection at all entry points into the network.
- **Integrated Management**—Easy and effective management tools, like Cisco Router and Device Manager (SDM), reducing operational complexity and expenditure.
- **Consistency**—The same signature database as the Cisco IPS Appliances creating interoperability, consistency and familiarity for IT staff.
- **Flexibility against new attacks**—Customizable signatures created and deployed while the router is in service.

Whether threats are targeted at endpoints, servers, or the network infrastructure, pervasive Cisco IPS solutions integrate smoothly into your network infrastructure and proactively protect your vital resources.

THREAT DEFENSE: CISCO IOS INTRUSION PREVENTION

IPS

Cisco leads the industry with the first router-based IPS capabilities, a core component of the Cisco Self-Defending Network initiative. Cisco IOS IPS is an inline, deep-packet, inspection-based solution that helps enable Cisco IOS Software to effectively mitigate network attacks. Used for intrusion prevention and event notification, Cisco IOS IPS uses technology from Cisco intrusion detection system (IDS) products, including Cisco IDS 4200

Series appliances, Cisco Catalyst® 6500 Series IDS services modules, and IDS Network Module. Because Cisco IOS IPS is inline, it can drop traffic, send an alarm, or reset the connection, which enables the router to respond immediately to security threats and protect the network.

While the hub is a common location to deploy an IPS solution and inspect traffic for attacks, it is not the only location to consider when deploying security—attacks can also originate at the branch. Through collaboration with other integrated security capabilities: IP Security (IPSec) VPN, generic routing encapsulation (GRE), and Cisco IOS Firewall, Cisco IOS allows for traffic encryption and decryption, tunnel termination, firewalling, and traffic inspection at the first point of entry into the network (branch or hub)—an industry first. Cisco IOS IPS helps stop attacking traffic as close to the source as possible.

Cisco IOS IPS offers several new capabilities:

- The ability to load and enable selected IPS signatures in the same manner as Cisco IDS sensor appliances
- More than 700 of the same signatures also supported by Cisco IDS Sensor platforms
- The ability for a user to modify an existing signature or create a new custom signature on the fly to address newly discovered threats (each signature can be enabled to send an alarm, drop the packet, or reset the connection)

An additional capability allows users who want maximum intrusion protection to select an easy-to-use signature file that recognizes “most-common” worms and attacks. Traffic matching these high-confidence-rated worm and attack signatures drops malicious traffic. Cisco Router and Security Device Manager (SDM) provides an intuitive user interface to provision these signatures, including the ability to download new signatures from Cisco.com without requiring a new Cisco IOS version and without interrupting routing services.

THE ORIGIN OF CISCO IOS IPS

Cisco IOS Intrusion Prevention System (IPS) restructures the existing Cisco IOS Intrusion Detection System (IDS). Cisco IOS IPS inherited the original signatures from Cisco IOS (IDS) Technology and, with the introduction of inline IPS, this solution can add new signatures by downloading a Signature Definition File (SDF) to the router’s flash.

This enhancement allows customers to choose between loading the default, built-in signatures or loading a Signature Definition File (SDF) called “attack-drop.sdf,” or merging both onto their router. Cisco IOS IPS feature was introduced in 12.3(8)T and “attack-drop.sdf” file is available in flash on all Cisco access routers that are shipped with Cisco IOS Release 12.3(8)T or later. The file contains high fidelity (or “high probability”) IPS signatures, providing customers with the latest available detection of security threats. In addition, customers can customize this file by adding or deleting signatures based on their network’s requirement.

SIGNATURE DEFINITION FILE

The signature definition file (SDF) contains signature details and configuration and can reside on the router or on a file server. The Cisco IOS IPS-enabled router uses this SDF to update the existing IPS configuration in real time, without any interruption to the normal functioning of the router. This means that the number of running signatures, and the way that they are configured to react to a signature match, for example: alarm, drop, or reset, can all be changed without a Cisco IOS image update or router reload.

Once the SDF is created, it can be replicated to all routers on the network for expedient IPS signature updates to the entire network of Cisco IOS IPS-enabled routers. New signatures that are created by Cisco will be posted to Cisco.com at: http://www.cisco.com/cgi-bin/tablebuild.pl/ios-sigup

The latest signatures can be downloaded and applied to Cisco IOS IPS-enabled routers. This can be done with Cisco management tools like Cisco SDM 2.0 and CiscoWorks VPN/Security Management (VMS) 2.3

SIGNATURE MICRO ENGINES

Cisco IOS IPS uses signature micro-engines (SMEs) to load the SDF and scan signatures. Currently, Cisco IOS IPS supports these 10 SMEs:

- ATOMIC.L3.IP
- ATOMIC.IPOPTIONS
- ATOMIC.ICMP
- ATOMIC.UDP
- ATOMIC.TCP
- SERVICE.HTTP
- SERVICE.DNS
- SERVICE.RPC
- SERVICE.SMTP
- SERVIC.FTP

Signatures contained within the SDF are handled by a variety of SMEs. The SDF typically contains signature definitions for multiple engines. The SME typically corresponds to the protocol in which the signature occurs and looks for malicious activity in that protocol. A packet is processed by several SMEs. Each SME scans for various conditions that can lead to a signature pattern match. When an SME scans the packets, it extracts certain values, searching for patterns within the packet via the regular expression engine.

PARALLEL SIGNATURE SCANNING

Cisco IOS IPS uses a Parallel Signature Scanning Engine to scan for multiple patterns within a signature micro-engine (SME) at any given time. IPS signatures are no longer scanned on a serial basis so there will be minimum impact on the performance of the router when increasing the number of signatures to inspect.

ATTACK MITIGATION

Cisco IOS IPS is typically used in a distributed IPS mitigation fashion where routers are deployed throughout the network, including all entry points from external networks. This includes remote VPN branch offices, partner connected links, and telecommuters' remote-access connections. Cisco IOS IPS lets customers detect attempts from outside hackers that are trying to use one of these remote locations as a back door into the protected network. In addition, Cisco IOS IPS can detect such attacks before they penetrate deeper into the network by providing early detection at the distributed remote connections.

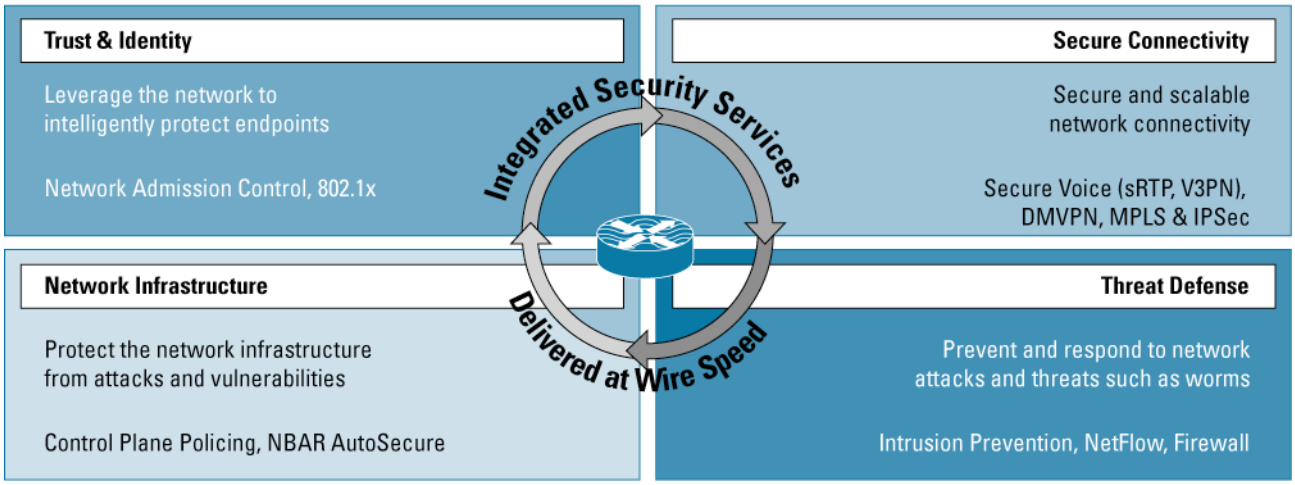
CISCO SELF-DEFENDING NETWORK

A core component of the Cisco Self-Defending Network, Cisco IOS IPS is one of several threat defense solutions that work together to prevent and respond to network attacks and threats through the use of network services. Using the network to protect the network, integrated security solutions combine proven Cisco IOS functionality and industry-leading LAN/WAN connectivity with world-class security features to give customers the following benefits:

- **Use what you have**—Use the existing network infrastructure, enabling new security features on the router through Cisco IOS without deploying additional hardware
- **Deploy security where you need it most**—Provide the flexibility to apply security capabilities like IPS, firewall, and VPN anywhere in the network to maximize security benefit
- **Protect your gateways**—Allow best-in-breed security to be deployed at all entry points into the network, including remote branch offices

- **Save time and money**—Reduce the number of devices, lowering training and manageability costs
- **Protect your infrastructure**—Protect the router, defending against attacks targeted directly at the network infrastructure, like distributed denial of service (DDoS) attack

Figure 1. Complete. Preventive. Scalable Security Solutions.



The Cisco Self-Defending Network has four categories of protection that apply to the router:

- **Secure connectivity**—Provides secure and scalable network connectivity, incorporating multiple types of traffic. Examples include VPN, Dynamic Multipoint VPN (DMVPN), Multi-VPN routing/forwarding instance (VRF) and Multiprotocol Label Switching (MPLS) secure contexts, voice- and video-enabled VPN (V3PN), and secure voice.
- **Threat defense**—Prevents and responds to network attacks and threats using network services. Examples include Cisco IPS and Cisco IOS Firewall.
- **Trust and identity**—Allows the network to intelligently protect endpoints using technologies such as Network Admission Control (NAC), identity services, and authentication, authorization, and accounting (AAA).
- **Network infrastructure protection**—Protects the network infrastructure from attacks and vulnerabilities, especially at the network level. Examples include control-plane policing, Network-Based Application Recognition (NBAR), and Cisco AutoSecure.

AVAILABILITY

Cisco IOS IPS is available in Cisco IOS Software Release 12.3(8)T and higher, and is supported on Cisco 800, 1700, 1800, 2600, 2800, 3700, 3800, 7200 and 7301 series routers.

FOR MORE INFORMATION

For more information about Cisco IOS IPS, contact your local Cisco account representative or visit: http://www.cisco.com/go/iosips

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

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

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 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.**