

Why Should I Care About Cisco IOS IPS?

In today's environment, Internet worms and viruses spread across the world in mere minutes. Without the luxury of time to react, the network itself must possess the intelligence to instantaneously recognize and mitigate these threats.

Cisco IOS Intrusion Prevention System (IPS) is an in-line, deep-packet inspection-based feature that offers *network wide protection* from worms, viruses and attacks against various vulnerabilities. Working in conjunction with other threat defense features such as IOS firewall available, it can:

- Protect core networks by stopping worm/attack at branch office before it enters WAN link/IPSec tunnel to corporate headquarters
- Protect branch office PCs and servers from external worms & attacks that can come through branch's direct connections to the Internet

What Problems Need to be Solved?

Since worms, viruses and other forms of attacks can spread around and cause damage in short amount of time, it is critical to stop malicious traffic as close to its entry point as possible. That requires deep inspection of traffic not only at a corporate headquarters but also at branch office and telecommuter gateway/access routers.

IOS IPS feature running on Cisco ISR (Integrated Services Routers) targeted specifically for branch and SOHO or telecommuter offices is an ideal solution to detect and stop all types of network attacks before they get a chance to spread over and damage hosts and servers at other branches or the head or regional offices.

What is New in Cisco IOS IPS in 12.4(11)T Release?

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.

What are the Key Features and Benefits of Cisco IOS IPS in 12.4(11)T Release?

- Supports/shares a subset of signatures and signature format with Cisco IPS appliances and modules
- 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

Customers

Cisco IOS IPS, Cisco IOS Firewall, and the Cisco IOS security feature set are ideal for:

- Customers that want to protect their Internet-facing connection using integrated threat defense security features
- Customers that want to apply worm and threat detection/prevention on their edge networks using threat defense security services of Cisco integrated services routers
- Customers that want to provide security services for their customers as managed security services

Software Options

Cisco IOS IPS is available on the following Cisco IOS Software feature sets:

- adventerprisek9
- advsecurityk9
- advservicesk9

Why Cisco?

Cisco IOS IPS feature provides network wide threat protection with a highly customizable attack signature set and it is very well integrated with all other routing/QoS, security, voice and wireless features available on the industry-leading Cisco Integrated Services Routers operating as WAN/Internet gateway devices at telecommuter/SOHO, branch and regional offices.

Figure 1. Cisco IOS IPS Protecting Malicious Attacks

