

Cisco IOS IPS in Cisco IOS Software Mainline Releases and in IOS T-Train Releases Prior to 12.4(11)T

In Cisco IOS[®] Software T-Train Releases prior to 12.4(11)T Release, and in all Cisco IOS Software 12.4 Mainline Releases, IPS signature selection is done by loading an XML file onto the router. This file contains a detailed description of each "selected" signature in Cisco IPS Sensor Software 4.x signature format, and is called "signature definition file" (SDF). The latest version of SDFs that contain complete sets of IPS signatures supported in Cisco IPS Sensor Software 4.x format and SDFs that contain Cisco recommended **Basic** and **Advanced** protection signature sets (in files 128MB.sdf and 256MB.sdf, respectively) can be found at and downloaded from [Cisco IOS IPS SDFs in Cisco IPS Sensor Software 4.x signature format](#). (Requires Log In)

Note: Cisco will not provide any updates for signatures in Cisco IPS Sensor Software 4.x format after May 2008. Cisco IOS IPS users are strongly recommended to upgrade their router image to Cisco IOS Software 12.4(11)T2 or later releases at their earliest convenience.

Provisioning, loading, customization, and deployment of attack signatures for Cisco IOS IPS in Cisco IOS[®] Software T-Train Releases prior to 12.4(11)T Release and in all 12.4 Mainline Releases may be done using [Cisco Router and Security Device Manager \(SDM\) v2.3](#) for a small number of routers and [Cisco Security Manager \(CSM\) 3.01](#) for deployments with 10 or more routers. For more information, refer to the [Configuring Cisco IOS IPS Using SDM or CLI](#) or [Configuring Cisco IOS IPS Using IPSMC2.2](#) guides.

Upon detecting an attack signature, the Cisco IOS IPS feature can send a syslog message or an alarm in Secure Device Event Exchange (SDEE) format. Cisco SDM v2.3 may be used to monitor events generated by a single router and [Cisco IPS Event Monitor](#) may be used to monitor IPS events generated by up to five routers.

For monitoring events from more than five 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 may be used. Cisco Security MARS also supports automated tuning of IPS signatures on Cisco IOS routers, based on correlation of those alarms and threat mitigation rules defined for this purpose.

More information on CLI-based configuration of Cisco IOS IPS in the releases discussed in this document can be found in the [Configuration Guide for Cisco IOS IPS in 12.4\(9\)T or earlier Releases](#). For a list of signatures supported by Cisco IOS IPS in Cisco IOS Software Release 12.4(9)T or earlier T-Train releases and in all 12.4 Mainline releases, see the [Cisco IPS Sensor Software 4.x Format Signatures Supported by Cisco IOS IPS white paper](#).



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, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, 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, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, 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. (0807R)

Printed in USA

C11-407871-00 07/08