Preface

Published: January 15, 2014, OL-30788-01

Revised: April 23, 2014

Contents

This document describes how to configure the sensor using the Cisco IPS 7.3 CLI. It contains the following sections:

- Audience, page xxiii
- Organization, page xxiii
- Conventions, page xxv
- Related Documentation, page xxvi
- Obtaining Documentation, Using Cisco Bug Search Tool, and Submitting a Service Request, page xxvi

Audience

This guide is intended for administrators who need to do the following:

- Configure the sensor for intrusion prevention using the CLI.
- Secure their network with IPS sensors.
- Prevent intrusion on their networks and monitor subsequent alerts.

Organization

This guide includes the following sections:

Section	Title	Description
1	"Introducing the CLI Configuration Guide"	Describes the purpose of the CLI Configuration Guide.
2	"Logging In to the Sensor"	Describes how to log in to the various sensors.

Section	Title	Description
3	"Initializing the Sensor"	Describes how to use the **setup** command to initialize sensors.
4	"Setting Up the Sensor"	Describes how to use the CLI to configure initial settings on the sensor.
5	"Configuring Interfaces"	Describes how to configure promiscuous, inline, inline VLAN pair, and VLAN group interfaces.
6	"Configuring Virtual Sensors"	Describes how to configure virtual sensors.
7	"Configuring Event Action Rules"	Describes how to configure event action rules policies on the sensor.
8	"Defining Signatures"	Describes how to add, clone, and edit signatures.
9	"Configuring Anomaly Detection"	Describes how to configure anomaly detection policies on the sensor.
10	"Configuring Global Correlation"	Describes how to configure global correlation features on the sensor.
11	"Configuring External Product Interfaces"	Describes how to configure external product interfaces for CSA MC.
12	"Configuring IP Logging"	Describes how to configure IP logging on the sensor.
13	"Displaying and Capturing Live Traffic on an Interface"	Describes how to display and capture live traffic on sensor interfaces.
14	"Configuring Attack Response Controller for Blocking and Rate Limiting"	Describes how to configure blocking and rate limiting on Cisco routers, and switches, and how to configure a master blocking sensor.
15	"Configuring SNMP"	Describes how to configure SNMP on the sensor.
16	"Working With Configuration Files"	Describes how to use configuration files on the sensor.
17	"Administrative Tasks for the Sensor"	Describes various administrative procedures to help you keep your sensor working and up to date.
18	"Configuring the ASA 5500-X IPS SSP"	Describes how to configure the ASA 5500-X IPS SSP.
19	"Configuring the ASA 5585-X IPS SSP"	Describes how to configure the ASA 5585-X IPS SSP.
20	"Obtaining Software"	Describes where to go to get the latest IPS software and describes the naming conventions.
21	"Upgrading, Downgrading, and Installing System Images"	Describes how to upgrade sensors and reimage the various sensors.
A	"System Architecture"	Describes the IPS system architecture.
B	"Signature Engines"	Describes the IPS signature engines and their parameters.
C	"Troubleshooting"	Contains troubleshooting tips for IPS hardware and software.

Section	Title	Description
D	"CLI Error Messages"	Lists the CLI error messages.
	"Glossary"	Contains IPS acronyms and terms.

Conventions

This document uses the following conventions:

Convention	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x	y	z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x	y	z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
courier font	Terminal sessions and information the system displays appear in courier font.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means *reader take note*.

Tip Means *the following information will help you solve a problem*.

Caution Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Warning **Means *reader be warned*. In this situation, you might perform an action that could result in bodily injury.**

Related Documentation

For information on Cisco IPS 7.3 documentation and how to find it, refer to the documentation roadmap found at this URL:

http://www.cisco.com/c/en/us/td/docs/security/ips/7-3/roadmap/roadmap7_3.html

For all IPS documentation, refer to this URL:

http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/tsd_products_support_series_home.html

For a complete list of the Cisco ASA 5500 series documentation and where to find it, refer to the documentation roadmap found at this URL:

http://www.cisco.com/en/US/docs/security/asa/roadmap/asaroadmap.html

Obtaining Documentation, Using Cisco Bug Search Tool, and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.