About this Guide

Note Control and User Plane Separation (CUPS) represents a significant architectural change in the way StarOS-based products are deployed in the 3G, 4G, and 5G networks. Unless otherwise specified, it should not be assumed that any constructs (including, but not limited to, commands, statistics, attributes, MIB objects, alarms, logs, services) referenced in this document imply functional parity between legacy/non-CUPS and CUPS products. Please contact your Cisco Account or Support representative for any questions about parity between these products

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Note The HA, HSGW, PDSN, and SecGW products have reached end of life and are not supported in this release. Any references to these products (specific or implied) their components or functions including CLI commands and parameters in this document are coincidental and are not supported. Full details on the end of life for these products are available at https://www.cisco.com/c/en/us/products/collateral/wireless/asr-5000-series/eos-eol-notice-c51-740422.html.

This preface describes the *IPSec Reference*, how it is organized and its document conventions.

This guide describes configuration requirements for IP Security services. IPSec provides security for transmission of sensitive information over unprotected networks such as the Internet. IPSec is a standards-based robust solution that provides data authentication and anti-replay services in addition to data confidentiality services.

Important IPSec is a suite of standard and licensed Cisco features. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *System Administration Guide*.

Important This guide documents IPSec features that appear in the StarOS command line interface (CLI). IPSec features are not universally supported across all StarOS products. Support for IPSec features varies per platform, service type and StarOS release. Refer to the gateway administration guides and StarOS *Release Notes* for additional information.

- Conventions Used, on page ii
- Related Documentation, on page iii
- Contacting Customer Support, on page iv

Conventions Used

The following tables describe the conventions used throughout this documentation.

Notice Type	Description
Information Note	Provides information about important features or instructions.
Caution	Alerts you of potential damage to a program, device, or system.
Warning	Alerts you of potential personal injury or fatality. May also alert you of potential electrical hazards.

Typeface Conventions	Description
Text represented as a `screen display`	This typeface represents displays that appear on your terminal screen, for example: `Login:`
Text represented as **commands**	This typeface represents commands that you enter, for example: **show ip access-list** This document always gives the full form of a command in lowercase letters. Commands are not case sensitive.
Text represented as a **command** *variable*	This typeface represents a variable that is part of a command, for example: **show card** *slot_number* *slot_number* is a variable representing the desired chassis slot number.
Text represented as menu or sub-menu names	This typeface represents menus and sub-menus that you access within a software application, for example: Click the **File** menu, then click **New**

Command Syntax Conventions	Description
{ keyword or *variable* **}**	Required keyword options and variables are those components that are required to be entered as part of the command syntax. Required keyword options and variables are surrounded by grouped braces { }. For example: **sctp-max-data-chunks { limit** *max_chunks* **| mtu-limit }** If a keyword or variable is not enclosed in braces or brackets, it is mandatory. For example: **snmp trap link-status**
[keyword or *variable* **]**	Optional keywords or variables, or those that a user may or may not choose to use, are surrounded by brackets.
|	Some commands support multiple options. These are documented within braces or brackets by separating each option with a vertical bar. These options can be used in conjunction with required or optional keywords or variables. For example: **action activate-flow-detection { intitiation | termination }** or **ip address [count** *number_of_packets* **| size** *number_of_bytes* **]**

Related Documentation

The most up-to-date information for this product is available in the product *Release Notes* provided with each software release.

The following related product documents are also available:

- *AAA Interface Administration and Reference*
- *ASR 5500 Installation Guide*
- *Command Line Interface Reference*
- *GTPP Interface Administration and Reference*
- Platform-specific System Administration Guides
- Product-specific Administration Guides
- *Release Change Reference*

- *SNMP MIB Reference*
- *Statistics and Counters Reference*
- *Statistics and Counters Reference - Bulk Statistics Descriptions*
- *Thresholding Configuration Guide*

Contacting Customer Support

Use the information in this section to contact customer support.

Refer to the support area of http://www.cisco.com for up-to-date product documentation or to submit a service request. A valid username and password are required to access this site. Please contact your Cisco sales or service representative for additional information.