



Cisco 7600 Wireless Security Gateway Configuration Guide, Release 4.4.8

First Published: January 2017

Cisco Systems, Inc.
www.cisco.com

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.

Text Part Number:

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, 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 Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco 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. (1002R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco 7600 Wireless Security Gateway Configuration Guide, Release 4.4.8
© 2017 Cisco Systems, Inc. All rights reserved.



About this Book	1
Document Revision History	1
Organization	1
Conventions	2
Finding Related Documentation	3
Obtaining Documentation and Submitting a Service Request	4

CHAPTER 1

Learning About the WSG	1-1
WSG Overview	1-1
Cisco Service and Application Module for IP (SAMI) Overview	1-1
Supervisor Engine	1-2
WSG on a SAMI	1-2
WSG Features	1-2
Feature Exclusions	1-10
RFCs	1-10

CHAPTER 2

Setting Up the WSG	2-1
Before Getting Started with the WSG	2-1
Single-Entity Configuration	2-1
Configuration Details	2-2
Configuration Example	2-3
Understanding WSG Prerequisites	2-16
Enabling Supervisor to Collect PPC Crash Files and HA Traces	2-16
Establishing a PPC Session	2-17
Assigning a Hostname to a PPC	2-17
Setting Up VLAN Support	2-17
Setting Up the SUP	2-18
Setting Up the PPCs	2-20
Configuring the WSG	2-21
Single OAM Interface	2-22
Configuring the Single OAM Interface	2-22
Resource Monitoring	2-23

- Monitoring CPU Usage 2-23
- Monitoring Memory Usage 2-23
- Configuring WSG Global Parameters 2-24
 - Configuring IKE Retry Count 2-24
 - Configuring Remote Secret 2-24
 - Configuring a Local Address Pool 2-24
 - Adding the DNS Server to the Address Pool 2-25
 - Configuring Authentication Parameters 2-25
 - Multiple CA Trust Anchors 2-25
 - CA Certificate Chaining 2-25
 - Generating an RSA Key Pair and CSR 2-26
 - Submitting the CSR to the CA 2-27
 - Specifying Certificates and a Private Key on the WSG 2-27
- Configuring the WSG Profile 2-28
 - Configuring the WSG Parameters 2-29
- Configuring IKE 2-31
- High Availability 2-31
 - Configuring High Availability 2-32
 - Configuring Application VLAN/Alias IP Address 2-34
- Configuring High Availability on SAMI COSLI 2-35
 - Configuring the VLAN/IP Address for HA Infrastructure 2-35
 - Adding or Removing a Redundant Pair 2-41
 - Bulk Sync 2-48
- IKE SA Handling 2-50
- IPSec SA Handling 2-51
- Configuring IPSec 2-52
- Site-to-Site Scalability 2-53
 - Scalability and Throughput Improvement Description 2-54
 - Configuring Scalability and Throughput 2-54
 - Configuring Subnet Combination 2-55
- Certificate Management Protocol 2-56
 - Configuring Certificate Management Protocol 2-57
- Online Certificate Status Protocol 2-62
- DHCP Address Allocation 2-62
 - Configuring DHCP Address Allocation 2-64
- IPv6 2-67
 - Configuring IPv6 2-67
- Blacklisting 2-69
 - Configuring Blacklisting on the WSG 2-70
- RADIUS Accounting 2-70

Configuring RADIUS Accounting on the WSG	2-72
EAP Peer Authentication	2-73
Reverse Route Injection (RRI)	2-73
VRF Configuration	2-75
Configuring WSG Performance/Throughput Indicators	2-80
Traffic distribution — Hash distribution	2-83
Configuring IKE/IPSec Stats Collection and Timing Enhancements for SNMP	2-85

CHAPTER 3**Command Reference for the WSG 3-1**

Crypto Address-Pool Submode Commands	3-1
Crypto Profile Submode Commands	3-1
EXEC Commands	3-1
Global Configuration Commands	3-2
ISAKMP/IKE Commands	3-3
Interface Submode Commands	3-4
IPSec Commands	3-4
Single OAM Commands	3-4
Resource Monitoring Commands	3-4
Show Commands	3-4
SNMP Traps Commands	3-6
Debug Commands	3-6
Debug Commands	3-202

APPENDIX A**Upgrading to WSG Release 4.0 A-1****APPENDIX B****Fast Path Stats Counters B-1**



About this Book

Document Revision History

The following table lists the major changes made to this document each release, with the most recent changes listed first.

Revision	Date	Change Summary
OL-19129-19	January 2017	WSG Release 4.4.8
OL-19129-18	June 2016	WSG Release 4.4.7
OL-19129-17	January 2016	WSG Release 4.4.6
OL-19129-16	October 2015	WSG Release 4.4.5
OL-19129-15	March 2015	WSG Release 4.4.3
OL-19129-14	November 2014	WSG Release 4.4.1
OL-19129-13	October 2014	WSG Release 4.4
OL-19129-12	June 2014	WSG Release 4.3.2
OL-19129-11	April 2014	WSG Release 4.3
OL-19129-10	August 2013	WSG Release 4.2
OL-19129-09	July 2012	WSG Release 4.0
OL-19129-08	March 2012	WSG Release 3.1
OL-19129-07	26 September 2011	WSG Release 3.0
OL-19129-06	1 February 2011	WSG Release 2.2
OL-19129-05	28 September 2010	WSG Release 2.1
OL-19129-04	30 July 2010	WSG Release 2.0
OL-19129-03	8 February 2010	WSG Release 1.2
OL-19129-02	14 August 2009	WSG Release 1.0

Organization

This guide includes the following sections:

Title	Description
Chapter 1, “Learning About the WSG”	Describes the Cisco Wireless Security Gateway (WSG) and the Cisco Service and Application Module for IP (SAMI).
Chapter 2, “Setting Up the WSG”	Describes WSG software and hardware requirements and tells you what to do on the Supervisor (SUP) Engine and SAMI processors before using a WSG.
Chapter 3, “Command Reference for the WSG”	Describes how to use WSG commands.

Conventions

This guide uses the following conventions:

Convention	Indication
bold font	Commands and keywords and user-entered text appear in bold font .
<i>italic font</i>	Document titles, new or emphasized terms, and arguments for which you supply values are in <i>italic font</i> .
[]	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.
<code>courier font</code>	Terminal sessions and information the system displays appear in <code>courier font</code> .
< >	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.

Finding Related Documentation

- *Release Notes for the Cisco 7600 Wireless Security Gateway Release 4.4.8*
- *Cisco Service and Application Module for IP Memory Upgrade Installation Note*
- *Cisco Service and Application Module for IP Guide to User Documents*
- *Cisco Service and Application Module for IP User Guide*
- Cisco 7600 Series Router platform:
 - *Release Notes for Cisco IOS Release 12.2(33)SRC3 for the Cisco 7600 Series Routers*
 - *Cisco 7600 Series Router Installation Guide*
 - *Cisco 7600 Series Router Module Installation Guide*
 - *Cisco 7600 Series Router Cisco IOS Command Reference*
 - *Cisco 7600 Series Router Cisco IOS System Message Guide*
 - Application Control Engine Module Server Load-Balancing Configuration Guide, Software Version A2(1.0)
 - Configuring File Storage and the Remote Copy Protocol (RCP), see *Cisco Service and Application Module for IP User Guide*
http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/ace/v3.00_A2/configuration/slb/guide/slbgd.html
 - Configuring Load Balancing, see ACE Configuration Guide
http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/ace/v3.00_A2/configuration/slb/guide/slbgd.html
 - For information about MIBs, see
<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

The documents are located at:

- Cisco 7600 Series Router home page on Cisco.com at:
Products & Solutions > Products > Routers and Routing Systems > 7600 Series Routers
- Cisco 7600 Series Router technical documentation on Cisco.com at:
Products & Solutions > Products > Routers and Routing Systems > 7600 Series Routers >
in the Technical Documentation & Tools box on the right of the page,
Cisco 7600 Series Routers

Obtaining Documentation 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 the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.



Learning About the WSG

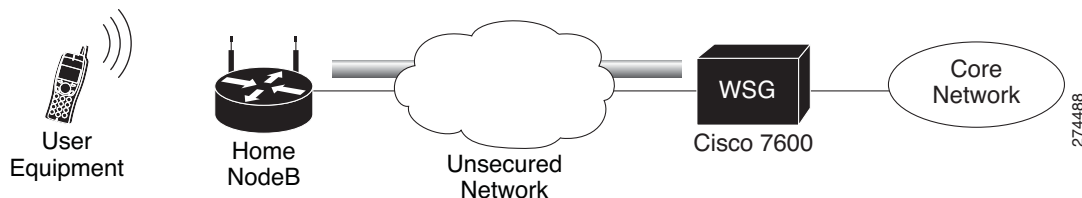
The following sections describe the WSG and Cisco Service and Application Module for IP (SAMI).

WSG Overview

The WSG is a high-density IP Security (IPSec) gateway for mobile wireless carrier networks. IPSec is an open standards set. IPSec provides confidentiality, integrity, and authentication for data between IP layer peers. The WSG uses an IPSec-protected tunnel to connect outside endpoints.

Figure 1-1 shows a WSG in a Universal Mobile Telecommunications System (UMTS) Terrestrial Radio Access Network (UTRAN).

Figure 1-1 WSG Implementation in a UTRAN



Cisco Service and Application Module for IP (SAMI) Overview

The WSG application runs on the Cisco SAMI. The SAMI offers the following features:

- Takes up one slot in a Cisco 7600 router.
- Connects to the switch fabric in the Cisco 7600 router—SAMI does not have outside ports.
- Offers parallel architecture for Cisco applications—SAMI uses an IXP2800 network processor flow-distributor running at 1.4 GHz.
- Uses six PowerPCs (PPCs)—each PPC runs the same version of a Cisco application at 1.25 GHz.

Supervisor Engine

Using the Supervisor (SUP) Engine, virtual local area networks (VLANs) direct traffic from outside ports to each instance of the WSG on PPCs. A 10 Gigabit Ethernet port on the backplane connects the SAMI and the SUP.

From the SUP, start a session to each WSG instance. This allows you to do the following with the WSG:

- Set up
- Monitor
- Troubleshoot

For more information about the SAMI, see the *Cisco Service and Application Module for IP User Guide*.

WSG on a SAMI

This process shows how the WSG installs on a SAMI:

1. SAMI's SUP downloads the WSG application.
2. The SUP sends the WSG image to each of the SAMI's six PPCs.
3. The same WSG image installs on all of the PPCs.

After installing the WSG, individually set up each PPC. Use SAMI's remote console and logging (RCAL) to log into the SUP. This acts as a single connection to access the SAMI linecard control processor (LCP) and the PPCs. Using the SUP you can:

- Debug
- View **show** command output
- View logging output

WSG Features

WSG ships loaded on SAMI PPCs with fully-functional defaults that support the following features.

The following features are supported in WSG Release 4.4.8 and above:

- A new change has been introduced in IXP Health Monitoring (HM). In Release 4.4.8, the PPC can detect the IXP HM failure within 15 seconds (default now). The behavior prior to Release 4.4.8 was to detect the failure within 10 minutes. There is a new CLI introduced as part of this release to change the behavior back to 10 minutes.
- A new feature has been introduced which allows the user to configure the High Availability (HA) timeout value in the range of 1 - 10 seconds (default 900 msec).
- A new feature is added to capture the High Availability (HA) messages between ACTIVE and STANDBY. When there is a reload due to HA failure, this feature writes HA packets captured into the `ha_trace` file in the SUP Disk0/Disk1/Bootdisk. The pcap file will have the last 2 minutes of the packets captured before the reload.
- Minor enhancement to generate SNMP trap if authentication failures are found during decryption of encrypted packets.

The following features are supported in WSG Release 4.4.6 and above:

- WSG can support maximum of 32 service interface IPs per PPC.

The following features are supported in WSG Release 4.4.5 and above:

- Service VLAN interface is a loopback interface where remote peers (eNBs) can reach for WSG services. Any VLAN interface with netmask /32 (IPv4) or with netmask /128 (IPv6) are by default treated as service interface wherein these VLANs does not require corresponding SVCLC configuration on supervisor (SUP). Each PPC can support maximum of 10 service VLAN interfaces.



Note Sharing of the same VLAN ID on different PPC's of SAMI WSG is not supported. However, sharing of service VLAN ID is allowed on different PPC's of SAMI WSG.

The following features are supported in WSG Release 4.4.3 and above:

- To generate SNMP trap on configured tunnel creation/deletion rate.

The following features are supported in WSG Release 4.4.1 and above:

- Prior to Cisco 7600 WSG Release 4.4.1, by default on WSG, the facility value was set based on the process the syslog related to. With Release 4.4.1 and above, the WSG supports to send the generated syslog's to the configured syslog server with the desired facility level, by allowing to manually configure the syslog facility.

The following features are supported in WSG Release 4.4 and above:

- To increase the overall throughput of the WSG SAMI, the IXP Traffic distribution feature provides a method to divide the Clear traffic between 2 IXPs (IXP0 and IXP1) and enables both the IXPs to handle even distribution of traffic. The IXP1 will now handle more of the post encryption traffic which was originally handled by IXP0.
- Prior to Cisco 7600 WSG Release 4.4, WSG supported only TCP as the CMPv2 Transport Protocol. With Release 4.4 and above, WSG will support both transport protocols, TCP and HTTP. The HTTP based flows will be RFC 4210/4211/6712 compliant.

The following features are supported in WSG Release 4.3.2 and above:

- On request of IPsec client, WSG allocates the DNS server IP from a DHCP server or it can be locally configured on WSG card itself. As most WSG supports 3 DNS server IPs, wherein the DNS server IPs requested from DHCP server will have more precedence than the DNS IPs which are locally configured.

The following features are supported in WSG Release 4.3 and above:

- Allocation of IPv6 addresses from a DHCPv6 server to obtain an IPv6 address for IPsec tunnel setup.



Note DHCP is supported for RAS profiles and not for site-to-site profiles.

The following features are supported in WSG Release 4.2 and above:

- WSG performance and throughput indicators added to system to provide system wide throughput capacity characteristics of WSG. It also helps to identify the traffic load so that customer can plan for any future expansion of their system. The throughput capacity data is collected separately on each of the IXP. The packet and byte count are done on each packet in the lookup engine before Nitrox/PPC processing. Fragmented ESP packets are counted after reassembly. PPC CPU utilization should be monitored for fragmented packets. The overall throughput capacity is the sum of the throughputs on each IXP. The overall throughput utilization is limited by the limit on each IXP.
- IKE/IPsec Stats Collection and Timing Enhancements for SNMP:

- Synchronized Statistics collection start times across all SAMI blades in a chassis using a NTP clock
- Real time statistics collection for CLIs similar to previous releases
- Auto adjustment of statistics collection interval based on the number of SAs
- Configurable fixed statistics collection interval length
- Persistent IKE/IPSec tunnel index for SNMP during a tunnel's lifetime
- Alignment of IKE/IPSec global and per-tunnel statistics

The following features are supported in WSG Release 4.0 and above:

- Compared to policy-based routing, the IKEv2 redirect feature provides a more flexible scheme for load balancing between multiple WSG cards. The IKEv2 redirect feature is used in conjunction with the exchange director feature on the SUP. After the tunnel is set up, the packets flow directly to each WSG card.
- The Reverse Route Injection (RRI) feature now supports IPv6 routes. The IPv6 routes are inserted into the SUP or Route Switch Processor (RSP).
- High availability (HA) active-active redundancy mode (added in addition to active-standby mode). This feature supports active-active redundancy between two WSG cards for site-to-site tunnels. Compared to an active-standby redundant pair, the active-active mode allows full utilization of packet throughput of each redundant WSG card except during switch-over scenario.
- A global PMTU value can be configured to be used on all IPv4 and IPv6 tunnels. Path MTU (PMTU) discovery is a technique using ICMP to determine MTU size on the path between two hosts. PMTU is the effective MTU along the path and indicates the largest size to avoid fragmentation of IP packets. In IPsec tunneling, PMTU is utilized when performing pre-tunnel fragmentation to avoid the more expensive post-tunnel fragmentation.
- WSG now supports SSH user authentication using RADIUS server. When the RADIUS server is unreachable, the WSG will fallback to authenticating the SSH user locally.
- IPv6 VRF Support
- IPv6 DHCP Support
- Using reverse DNS lookup, WSG now displays both IP address and hostname for IKE peers.
- S2S Blacklisting

The following features are supported in WSG Release 3.1 and above:

- Prior to WSG Release 3.1, syslog messages display the CPU ID as the name of the source host where messages originated from. The enhancement in WSG Release 3.1 adds the configured hostname along with the CPU ID to the syslog in order to make management easier.
- Up to 5 multiple access-permit statements can be configured in a remote-access crypto profile.
- Multiple external logging servers with IPv4 addresses can be configured for syslog messages. Only a single logging server with an IPv6 address can be configured at a time.

The following features are supported in WSG Release 3.0 and above:

- IPv6 support was added in WSG Release 3.0. This feature allows users to configure interfaces with IPv6 addresses. IPv6 support is present for both the IKE SAs and IPsec SAs, enabling IPv6 IKE packet handling in the control path and IPv6 ESP packet handling in the datapath. WSG also supports the use of same or different IP protocol versions for the IKE SA and the IPsec SA, so an IPv4 IKE SA can be paired with an IPv6 IPsec SA and vice versa. This allows IPv6 clear packets to be secured inside an IPv4 tunnel or IPv4 clear packets to be secured inside an IPv6 tunnel

- Virtual Routing and Forwarding (VRF) allows the creation of multiple virtual networks within a single network entity. Each VRF comprises an IP routing table and a forwarding table, allowing the use of the same or overlapping IP addresses without conflicts. In a single network entity, multiple VRFs can be used to create isolation between virtual networks. VRFs allow encrypted/decrypted traffic separation, by having the encrypted traffic in one outside VRF and the decrypted traffic in one inside VRF.

The typical case for this is an ISP that provides VPN service to multiple enterprise customers on the same box, the users and branches connect using internet for the encrypted traffic, but the decrypted traffic needs to go to the private network of each separate customer and this traffic cannot be mixed.

- Data Plane Routing

Prior to WSG Release 3.0, all return traffic between the WSG and the SUP is carried over the same VLAN. It is not desirable for customers to have all their traffic converge onto the same VLAN at any point in the packet path. This feature supports true dual-arm implementation. Traffic on the clear and protected sides traverse different VLANs.

A static routing table for IPv4/IPv6 is maintained on IXP for forwarding packets out to the correct VLAN. IPv4/IPv6 static routes are configured on the PPC. On the same PPC, two identical routes can be present in different VRFs. In case of more than one match in the routing table, the longest prefix approach is used. The maximum number of static routes per VRF per PPC is 10. The maximum number of static routes per WSG is 60. Dynamic routing is not supported in WSG Release 3.0.

- A SSH server is added in WSG Release 3.0. Open SSH is used to provide the SSH server while CLIs control and configure it. Since the main reason for SSH is to allow secure login on non-secure networks, the SSH server will respond to requests from all interfaces. Only SSHv2 and DSA are supported. DSA is similar to RSA but does not require an export license.

There is no support for groups or privileges configuration. All users have the same privilege. Admin Group or role assignments are not supported. The number of users that can be configured are limited by the size of the configuration file. There is no timeout on the SSH sessions. The user cannot kill a session from the CLI.

- Per Peer IP Tunnel Debug

WSG supports per peer debugging of tunnel setup and IKE protocol exchanges by allowing the peer IP address to be specified when turning on debugs.

- Reverse Route Injection (RRI)

Introduced in WSG Release 3.0, the RRI feature obviates the need to manually configure static routes on the SUP for clear traffic routing purposes in the reverse direction. RRI route entries are injected into the SUP when IPsec tunnels are created. These route entries are correspondingly withdrawn from the SUP when the IPsec tunnels are deleted. The BGP protocol is used to re-distribute the routes from WSG to the SUP. For WSG Release 3.0, the RRI feature supports only IPv4. Also, only site-to-site profiles are supported. The VRF feature on the WSG cannot be enabled when the RRI feature is already configured.

- WSG supports authentication of a peer through EAP-MD5, EAP-AKA and EAP-SIM protocols. These protocols are only supported with certificates for authenticating the WSG to the peer. Use of preshared keys to authenticate the WSG to the peer is not allowed by the standards, but might be required to support some legacy equipment. The EAP authentication is supported for IKEv2 only.

- RADIUS Accounting

In some Femto networks, an Access Point (AP) sets up an IPsec tunnel with the WSG and sends an Iuh Register message via the tunnel to a Femto Gateway (FGW). The Iuh Register message is an IP packet which also contains the ID of the AP registering with the FGW. The ID used by the AP is the same as the IKE ID used by the AP during IPsec tunnel setup. The FGW needs to make sure that an

authenticated AP is not presenting itself as another AP during registration. This can be achieved by the FGW by comparing the source IP address of the Iuh Register packet with the internal IP address assigned by the WSG for the same AP (ID is the lookup key). For this to work, the WSG needs to send the ID to internal IP address mapping to the FGW every time it assigns an IP to the AP. RADIUS Accounting messages are used to send the IKE ID to assigned IP address mapping from the WSG to the AAA server running in the FGW.

- Traffic-based Phase 2 rekey is introduced in WSG Release 3.0. This feature allows the user to specify security association lifetime in megabytes or seconds. Both formats of lifetime value can exist at the same time, and Phase 2 rekey is triggered by whichever occurs first.
- Blacklisting Remote Peer

The blacklisting feature is a mechanism to prevent a remote peer from setting up a tunnel to the WSG. With the blacklisting feature, when a remote peer attempts to setup a tunnel with the WSG, the IKE ID of the remote peer is searched for in a blacklist file available to the WSG. If a match is found, the IKE AUTH request is failed and the remote peer is prevented from establishing a tunnel. The blacklisting feature provides a fast and simple mechanism to block a remote peer from setting up a tunnel to the WSG.
- Multiple IKE Proposals

Remote peers can negotiate multiple proposals during IKE Phase 1. Each proposal contains one or more encryptions, integrity, prf and DH group algorithms. WSG accepts multiple proposals during IKE SA setup and rekey.
- Multiple DH groups, EAP authentication algorithms, and transform sets are supported in WSG Release 3.0.
- DHCP Address Allocation. See the [“DHCP Address Allocation” section on page 2-62](#) for more information.
- High Availability

WSG Release 2.0 and above supports inter-chassis stateful 1:1 redundancy. Redundancy works at the SAMI level. All 6 PPCs on a SAMI are in active or hot standby state. The PPC of the active WSG syncs its state to the corresponding PPC of the redundant WSG (for example, PPC3 (A) to PPC3 (S)).

The WSG redundancy feature works with all IPSec supported features including IKEv1, IKEv2, ESN, anti-replay, DPD, and NAT-traversal. WSG redundancy is applicable to both remote access and site-to-site tunnels.

If a primary card fails, traffic is switched to the newly active SAMI. The established tunnels stay up and continue to pass traffic after failover, and the IKE/IPSec internal state is synced between the active and redundant WSGs. Traffic outage is less than 1 second after the failure detection.
- Site-to-Site Scalability Improvements

In previous releases, site-to-site traffic selector lookup was done by looking up an array of TS on the IXP. This linear search limited the performance of the site-to-site traffic selector lookup algorithm. For WSG Release 2.0 and above, the traffic selector lookup algorithm improves site-to-site performance. No change occurs for remote access traffic selector lookup; it is different from the lookup algorithm for site-to-site, and is already optimized.

Up to 16666 S2S tunnels are supported per SAMI blade. S2S tunnels can only be configured on the director PPC.

IKE protocol allows a peer to negotiate multiple TS for the same tunnel. However, in WSG Release 2.0 each tunnel can negotiate only one TS.

All other features that are currently supported for site-to-site and remote access are maintained.
- Certificate Management Protocol

WSG Release 2.0 introduced support for Certificate Management Protocol (CMPv2).

The user manually requests the initial key or certificate from the CA server using the **crypto cmp initialize** command. The initial request is authenticated using the reference number and pre-shared key (PSK) from the CA server using an out-of-band mechanism. After receiving the initial certificate, the **crypto cmp enroll** command is used to enroll the certificate using the public key. Prior to the certificate expiration, the **crypto cmp update** command is used to update the certificate and private key. The WSG changes the name of the certificate and private key files during the update, so any WSG configuration commands which use the previous certificate file names must be replaced with commands using the new file names (configuration commands with **wsg-cert** or **current-wsg-cert** keywords). After the initialize, enroll, and update commands, the certificate and private key files are copied from the WSG to the SUPs in the Cisco 7600 chassis. The files must be manually copied to the SUP on other Cisco 7600 chassis.

WSG Release 3.0 introduced an automatic certificate renewal mechanism. The **crypto cmp auto-update** configuration command may be used on a WSG to automatically update the certificate and private key and send them to its SUPs. The **crypto cert renewal retrieve** configuration command is used on other WSGs to retrieve the updated certificate from the Cisco 7600 SUPs. Both commands are global configuration commands, thus the configuration is saved. In a HA configuration, both commands update the standby WSG, which then updates their SUPs. If inter-chassis redundancy is configured, the certificate and private key will be propagated to redundant chassis. A WSG may be configured to automatically update some certificates and automatically retrieve others. The maximum number of certificates that may be configured for automatic renewal (update and retrieve) is 20.

Syslog messages and two SNMP traps, **cert-expiry** and **cert-renewal**, were introduced for CMPv2 in WSG Release 3.0. The **crypto pki wsg-cert-trap expiry notification** configuration command may be used to configure a **cert-expiry** trap and syslog up to 30 days before a WSG certificate is about to expire (default is 24 hours). The **cert-renewal** trap and syslog will provide notifications for the automatic update or retrieve status, which may be configured to start 2 to 60 days before the certificate will expire. The SNMP traps are enabled using the **snmp-server enable traps ipsec** configuration command.

- Online Certificate Status Protocol

In previous releases, the WSG used CRL (Certificate Revocation List) to obtain from the CRL server, a file containing the list of certificates that were revoked.

In WSG Release 2.0 the Online Certificate Status Protocol (OCSP) feature was introduced to address some of the limitations of CRL. OCSP works to achieve the same objective as the CRL mechanism; it determines if a certificate offered by a peer has been revoked. OCSP differs from CRL in that the revocation status is obtained on a per-certificate basis rather than a trust anchor basis. Since the revocation status is obtained when the certificate is first seen by the WSG, the status is up to date.

- IKEv1 and IKEv2 and Public Key Infrastructure (PKI)—IKE is a hybrid protocol that does the following for IPsec:
 - Authenticates peers
 - Negotiates IKE and security associations (SAs)
 - Sets up encryption algorithms keys

IPsec SAs are secured links in one direction. IPsec endpoints must authenticate themselves to each other and set up Internet Security Association and Key Management Protocol (ISAKMP) shared keys.

WSG uses the IKEv1 or IKEv2 protocols to communicate with the IPSec endpoint to set up an Encapsulating Security Payload (ESP)-encapsulated tunnel. This tunnel gives protected access to a private network. The WSG encapsulates, encrypts, and authenticates packets from private networks to IPSec endpoints. In the reverse direction, the WSG decapsulates, decrypts, and authenticates.

- Site-to-site tunnels are supported. This allows WSG to establish site-to-site tunnels with a peer (which can be another WSG, or any other implementation). The site-to-site tunnels between two peers are used to encrypt clear traffic originating from their protected networks. The WSG can be configured to either auto-initiate a site-to-site tunnel with a peer, or wait for incoming IKE requests to create a tunnel. The WSG supports both IKEv1 and IKEv2 for site-to-site tunnels.
- Both remote access and site-to-site type profiles can be used in combination on a SAMI. However, only one profile of type remote access is supported while multiple site-to-site profiles can be configured.

- DPD Initiation

The DPD initiation feature allows the WSG to send DPD to peers at a regular interval. This allows WSG to detect and remove dead connections or peers. This feature is independent of existing functionality where the SAMI responds to DPD messages from its peer. The SAMI is able to both initiate DPD and respond to DPD at the same time.

- WSG Release 1.2 and above supports the extended form of traffic selectors. An additional extended syntax for the **access-permit** command is added in this release to configure the extended traffic selector used on established tunnels. The new form of traffic selectors can now include the following parameters, which are passed in the Traffic Selector payload during the IKE message exchange for establishing the tunnels:

- Source IP address range
- Source port range
- Destination IP address range
- Destination port range
- IP protocol

- Multiple Child SA

For a single IKE association with a peer, multiple child IPSec SAs can be created, each with its own traffic selector rule. We support one traffic selector per child IPSec SA.

- DNS to AP feature allows the WSG to pass the DNS server IP address to the remote peer.
- The WSG supports platform traps for PPC CPU congestion and memory exhaustion.
- OAM traffic routing feature allows the WSG to do static routes on the PPC to carry OAM traffic directly to a local network through a VLAN interface. Bearer traffic sent by IXP will go to the default gateway only. Additionally, this feature allows the WSG to create a separate VLAN interface on the PPC for carrying OAM traffic only.
- Single-entity configuration allows you to configure the SAMI from a single login interface rather than going to each of the 6 PPCs individually and configuring them. Parameters that are required to be different on each PPC (like address pool) still need to be configured multiple times (through the same session) on each PPC.
- All traps, syslog and SNMP stats are sent from a single PPC. For SNMP stats the external SNMP manager goes to the single PPC to retrieve stats for all the PPCs.

- The PPC Traffic Throttle feature throttles the number of IKE INIT messages sent to the PPC. This prioritizes the DPD traffic over new tunnel requests, and allows existing tunnels to remain intact. There is a specific bandwidth limit for each PPC which is slightly larger than the supported tunnel setup rate. Each PPC is throttled separately.
- WSG Release 1.2 and above supports debugs using the CLI.
- **Diffie-Hellman (DH)**
In WSG Release 1.2 and above, DH Groups **14, 15, 16, 17, and 18** are added to **groups 1, 2 and 5**. DH is a public-key cryptography protocol. It allows two parties to set up a shared secret key used by encryption algorithms over an insecure communications channel. DH is used within IKE to set up session keys.
- WSG Release 1.2 and above adds Extended Sequence Number (ESN) support as longer lifetimes are expected in customer deployments. Additionally, higher traffic is expected in site-to-site setups. Extended Sequence Number (64 bit sequence number) implementation is required in such cases. In this release, the sequence number length cannot be negotiated by the peer with SAMI. The peer will have to match the setting on the SAMI (default is 32-bit sequence number). The 64 bit sequence number can be configured using the CLI.

The following features were introduced prior to WSG Release 1.2 and are still applicable:

- **IPSec Security Association Lifetime**
The SA is kept by each peer until its lifetime expires. Because new SAs are negotiated before current SAs expire, they can be reused to save time. Shorter lifetimes mean more secure negotiations. Longer lifetimes mean SAs are more quickly set up.
- **IKE Encryption**
WSG supports the following IKE secret encryption schemes:
 - Data Encryption Standard (DES)
 - Triple DES (3DES), also known as Triple Data Encryption Algorithm (3TDEA)
 - Advanced Encryption Standard (AES) (128, 192, 256)
- **N + 1 Redundancy** (load balancing with ACE module)
- **IPv4 traffic**
- **ESP transforms in IPSec Tunnel Mode**
- The WSG CLI is a line-oriented user interface that gives commands for customizing IPSec environment variables. This document describes only the features related to IPSec configuration. For a complete description of the features set up at the WSG CLI, see the *Cisco Service and Application Module for IP User Guide*.
- **NAT Traversal**
The WSG supports IKE NAT traversal by encapsulating the ESP payload over UDP as in RFC 3948. The WSG listens for IKE messages on UDP ports 500 and 4500. When it receives an IKE request the WSG responds to the address and port from which the request is received. With NAT Detection Source/Destination IP notifications, if the WSG detects that the peer is behind a NAT device, it sets up an ESP tunnel to be UDP encapsulated.
- **X.509 Digital Certificate**
The digital certificate is a package containing information such as the identity of a certificate bearer: his or her name or IP address, the certificate's serial number, the certificate's expiration date, and a copy of the certificate bearer's public key. The standard digital certificate format is defined in the X.509 specification.

- 100,000 Remote Access tunnels per SAMI.
- Site-to-site tunnels are supported.
- Pre-shared Keys—WSG and another network element agree ahead of time on a shared, secret key. The two use this preshared key during security negotiation.
- SNMP Version 2 Traps and MIBs—Each PPC runs an SNMP agent and generates its own SNMP traps. WSG supports SNMP statistics using Cisco Standard IPsec and IOS infrastructure MIBs.
- IPsec Anti-Replay—IPsec Anti-Replay is a security service on the WSG. Using IPsec Anti-Replay, the WSG rejects old or duplicate packets. This protects the WSG from replay attacks, the fraudulent resending of data.
- IPsec Perfect Forward Secrecy (PFS), Groups 1, 2 and 5—IPsec PFS ensures one IPsec SA key can not be used to build another. This prevents an attacker from breaking a key associated with a session, copying data, and compromising other IPsec SAs.
- Certificate Authority (CA) Certificate Chaining—A certificate chain is a sequence of certificates with dependent trust relationships. The first certificate is self-signed by the CA. Each subsequent certificate creates an association between a certificate owners, or CAs in the chain. This process creates a trust chain from trusted peer to a CA.
- Multiple CA Trust Anchors—A trust anchor is a third party the WSG trusts and to which it has a certification path. The trust anchor certifies the WSG. This certificate has information about prefixes that a WSG is allowed to use in router advertisements. Authorization delegation discovery enables a node to adopt a WSG as its default router.
- Hash Algorithms—Hash is a one-way algorithm. Hash takes an input message of arbitrary length and turns it into a fixed-length digest. Cisco uses Secure Hash Algorithm (SHA), Message Digest 5 (MD5), and AES-XCBC.

Feature Exclusions

- VRF feature on the WSG cannot be enabled when the RRI feature is already configured.

RFCs

For additional information, refer to these RFCs:

- RFC 822, *Standard for the Format of ARPA Internet Text Messages*
- RFC 2131, *Dynamic Host Configuration Protocol*
- RFC 2132, *DHCP Options and BOOTP Vendor Extensions*
- RFC 2402, *IP Authentication Header*
- RFC 2404, *The Use of HMAC-SHA-1-96 within ESP and AH*
- RFC 2406, *IP Encapsulating Security Payload (ESP)*
- RFC 2407, *The Internet IP Security Domain of Interpretation for ISAKMP*
- RFC 2408, *Internet Security Association and Key Management Protocol (ISAKMP)*
- RFC 2409, *The Internet Key Exchange (IKE)*
- RFC 2410, *The NULL Encryption Algorithm and Its Use With IPsec*

- RFC 2412, *The OAKLEY Key Determination Protocol*
- RFC 2459, *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*
- RFC 2663, *IP Network Address Translator (NAT) Terminology and Considerations*
- RFC 2865, *Remote Authentication Dial In User Service (RADIUS)*
- RFC 2866, *RADIUS Accounting*
- RFC 2869, *RADIUS Extensions*
- RFC 3022, *Traditional IP Network Address Translator*
- RFC 3027, *Protocol Complications with the IP Network Address Translator*
- RFC 3162, *RADIUS and IPv6*
- RFC 3315, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*
- RFC 3526, *More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE), Group 2 only*
- RFC 3602, *The AES-CBC Cipher Algorithm and Its Use with IPsec, AES 128-CBC*
- RFC 3686, *Using AES Counter Mode With IPsec ESP*
- RFC 3706, *A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers*
- RFC 3947, *Negotiation of NAT-Traversal in the IKE*
- RFC 3948, *UDP Encapsulation of IPsec ESP Packets*
- RFC 4210, *Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)*
- RFC 4211, *Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)*
- RFC 4302, *IP Authentication Header*
- RFC 4303, *IP Encapsulating Security Payload (ESP)*
- RFC 4306, *Internet Key Exchange (IKEv2) Protocol*
- RFC 4307, *Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)*
- RFC 4308, *Cryptographic Suites for IPsec*
- RFC 4434, *The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)*
- RFC 4634, *US Secure Hash Algorithms (SHA and HMAC-SHA)*
- RFC 4718, *IKEv2 Clarifications and Implementation Guidelines*
- RFC 4787, *Network Address Translation (NAT) Behavioral Requirements for Unicast UDP*
- RFC 4835, *Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)*
- RFC 6712, *Internet X.509 Public Key Infrastructure: HTTP Transfer for the Certificate Management Protocol (CMP)*



Setting Up the WSG

This chapter explains how to set up the WSG. The major sections are:

- [Before Getting Started with the WSG, page 2-1](#)
- [Configuring the WSG, page 2-21](#)

Before Getting Started with the WSG

These sections explain software and hardware configuration requirements for the WSG. They also explain what to do on the Supervisor (SUP) Engine and SAMI processors before using the WSG:

- [Single-Entity Configuration, page 2-1](#)
- [Understanding WSG Prerequisites, page 2-16](#)
- [Enabling Supervisor to Collect PPC Crash Files and HA Traces, page 2-16](#)
- [Establishing a PPC Session, page 2-17](#)
- [Assigning a Hostname to a PPC, page 2-17](#)
- [Setting Up VLAN Support, page 2-17](#)
- [Setting Up the PPCs, page 2-20](#)



Note

For all of the commands you can issue on the PPC with the WSG, see the *Cisco Service and Application Module for IP User Guide*.

Single-Entity Configuration

WSG Release 1.2 and above supports a single point of configuration and a single OAM interface per service blade. These two features are intended to increase the configurability and manageability of applications using the SAMI hardware platform.

Single- entity configuration allows you to configure all CPUs using a single director CPU. Each CPU still requires its own configuration, but the single-entity configuration duplicates the configuration to all CPUs. The benefit is that a common configuration for each CPU can all be entered into a single CPU instead of having to configure each CPU separately.

You are presented with the standard single-PPC CLI mode upon opening a session (console or SUP session) to the director PPC (PPC3). From this session, you can enter the **all** mode by using the **entity all** command. By default, commands entered in **entity all** mode are executed on all PPCs. However, certain commands such as **show clock** or **show version** causes the same output on all processors and need not be repeated for each.

From the director PPC you can open a session to a specific subordinate PPC to execute commands only on that PPC. When you open the session, you will be placed in PCC-specific EXEC mode. Commands are entered as though you are connected to the PCC individually.

From PCC-specific EXEC mode, you can use the **configure terminal** command to enter **config** mode. This mode is also PPC-specific, which allows you to execute configuration commands that are applicable only to that PPC. As with the **EXEC** mode, some commands are not applicable in the PPC-specific **EXEC** mode. These commands will print an appropriate message and exit.

You can enter the **config all** mode from the **exec all** mode by entering the **configure terminal** command. Similar to the **exec all** mode, commands entered in this mode are executed on all PPCs, unless they are present in the lookup table described above.

Commands that display statistics and other counters need to be aggregated to provide you with meaningful data. Each application will have to register these commands as single-execution CLIs using the lookup table, and use IPC mechanisms to retrieve and aggregate data. For example, to display the total number of tunnels created, the callback function needs to get that information from all PPCs, and aggregate them before they are displayed.

Configuration Details

The following list provides important configuration information for the single-entity feature:

- PPC3 is designated as the director PPC.
- **Entity all** mode is available only on the director PPC. Use the **entity all** command to enter the mode; **exit**, or **entity none** will exit the **entity all** mode.
- Commands that are entered in the **entity all** mode are executed on all PPCs.
- If a command that is not applicable is entered in the **all** mode, it will only be executed only the director PPC.
- From the director PPC, you can switch to another PPC using the **processor X** command, where *X* is the specific processor number (4-8)
- All commands are supported in the **entity-all** mode. However, some commands cannot be (for example, **interface vlan**), or need not be (for example, **show version**) executed on all PPCs.

The following message is displayed when such commands are executed:

```
Info: Command executed only on the master processor. If required, execute the command on other processors
```

- If a **config** command fails on any of the subordinate PPCs, execution is aborted at that point (but not rolled back) with the following message:

```
Warning: Command failed on processor 4, aborting execution
```

- If an **exec** command fails on any of the subordinate PPCs, execution still continues on the remaining PPCs. The following message is printed:

```
Warning: Command failed on processor 4
```


Configuration Example

The following example shows the work flow that you can use to configure all processors from scratch using entity **all** mode. This example uses remote access crypto profile types. In remote-access configurations, the processors typically have common configuration parameters between them, including the names of the crypto profiles and address pools.

The following steps assume that a session is first opened from the SUP to the director PPC3 on the SAMI, using the command, **session slot slot_num processor proc_num**.

Configure Parameters That Must Be Unique To Each Processor

Step 1 Configure the hostname:

```
WSG# conf t
Enter configuration commands, one per line. End with CNTL/Z.
WSG(config)# host s3p3
```

Step 2 Configure the VLAN interface:

```
s3p3(config)# interface vlan 63
s3p3(config-if)# ip address 88.88.63.133 255.255.255.0
s3p3(config-if)# exit
```

Step 3 Configure the default gateway:

```
s3p3(config)# ip route 0.0.0.0 0.0.0.0 88.88.63.100
```

Step 4 Configure address pools:

```
s3p3(config)# crypto address-pool RAS-pool
s3p3(config-address-pool)# start-ip 10.133.0.1 end-ip 10.133.255.254 netmask 255.255.0.0
s3p3(config-address-pool)# exit
```

Step 5 Repeat the above commands on each processor, modifying the configuration appropriately. Using the **processor** command, you can switch to the other processors without logging out of the director. For example:

```
s3p3(mode-all)# processor 4
Trying 127.0.0.34...
Connected to 0x7f000022.
Escape character is '^]'.

MontaVista(R) Linux(R) Carrier Grade Edition 5.0 (custom)
Linux/ppc 2.6.21_mvlcge500-octeon-mips64-octeon_v2_be

Vegas Shell -- CGE 5.0 Version
Copyright (c) 1985-2008 by Cisco Systems, Inc.
All rights reserved.
```

Configure Parameters That are Common to all Processors or May Only Apply to the Director



Note

If a command only executes on the director processor, you will receive a warning:
INFO : Command executed only on master processor. If required, execute the command on other processors.

Step 1 Configure the single-entity OAM interface and its associated static route on the master PPC:

```
s3p3(config)# interface vlan 223
s3p3(config-if)# ip address 222.222.223.133 255.255.255.0
s3p3(config-if)# exit
s3p3(config)# oam mode single 223
s3p3(config-single-oam)# oam-ip route 44.44.44.0 255.255.255.0 222.222.223.100
s3p3(config-single-oam)# exit
s3p3(config)#
```

Step 2 Enter **entity all** mode.

```
s3p3# entity all
```

Step 3 Configure the DNS IP address:

```
s3p3(mode-all)(config)# ip name-server 44.44.44.201
s3p3(mode-all)(config)#
```

Step 4 Configure the IP address for external logging host:

```
s3p3(mode-all)(config)# logging ip 44.44.44.17
```

Step 5 Configure the SNMP host:

```
s3p3(mode-all)(config)# snmp-server host 44.44.44.16 traps version 2c public
```

Step 6 Configure the SNMP community strings:

```
s3p3(mode-all)(config)# snmp-server community public ro
s3p3(mode-all)(config)# snmp-server community private rw
```

Step 7 Configure the SNMP traps:

```
s3p3(mode-all)(config)# snmp-server enable traps snmp authentication
s3p3(mode-all)(config)# snmp-server enable traps interface
s3p3(mode-all)(config)# snmp-server enable traps syslog
s3p3(mode-all)(config)# snmp-server enable traps ipsec
```

Step 8 Configure the PKI certificates and trustpoints:

```
s3p3(mode-all)(config)# crypto pki wsg-cert Certs-SAMI.crt wsg-private-key
PrivateKeys-SAMI.prv
Copying Certs-SAMI.crt from SUP to PPC3...
done.
Copying PrivateKeys-SAMI.prv from SUP to PPC3...
done.
Copying Certs-SAMI.crt from SUP to PPC4...
done.
Copying PrivateKeys-SAMI.prv from SUP to PPC4...
done.
Copying Certs-SAMI.crt from SUP to PPC5...
done.
Copying PrivateKeys-SAMI.prv from SUP to PPC5...
done.
Copying Certs-SAMI.crt from SUP to PPC6...
done.
Copying PrivateKeys-SAMI.prv from SUP to PPC6...
done.
Copying Certs-SAMI.crt from SUP to PPC7...
done.
Copying PrivateKeys-SAMI.prv from SUP to PPC7...
done.
Copying Certs-SAMI.crt from SUP to PPC8...
done.
Copying PrivateKeys-SAMI.prv from SUP to PPC8...
done.
```

```
s3p3(mode-all)(config)# crypto pki trustpoint rootCA cacert.crt crl disable
Copying cacert.crt from SUP to PPC3...
done.
Copying cacert.crt from SUP to PPC4...
done.
Copying cacert.crt from SUP to PPC5...
done.
Copying cacert.crt from SUP to PPC6...
done.
Copying cacert.crt from SUP to PPC7...
done.
Copying cacert.crt from SUP to PPC8...
done.
```

Step 9 Configure the crypto profile:

```
s3p3(mode-all)(config)# crypto profile RAS-prof
s3p3(mode-all)(config-crypto-profile)# isakmp
s3p3(mode-all)(config-crypto-profile-isakmp)# self-identity id-type fqdn id SAMI.cisco.com
s3p3(mode-all)(config-crypto-profile-isakmp)# lifetime 86400
s3p3(mode-all)(config-crypto-profile-isakmp)# exit
s3p3(mode-all)(config-crypto-profile)# ipsec
s3p3(mode-all)(config-crypto-profile-ipsec)# access-permit ip 172.60.0.0 subnet 16
s3p3(mode-all)(config-crypto-profile-ipsec)# ip address-pool RAS-pool
s3p3(mode-all)(config-crypto-profile-ipsec)# security-association lifetime 28800
s3p3(mode-all)(config-crypto-profile-ipsec)# exit
```

Step 10 Activate the crypto profile:

```
s3p3(mode-all)(config-crypto-profile)# activate
```

Step 11 Display the Running Configuration.

```
s3p3(mode-all)# show run
```

CPU 3

```
Generating configuration.....
hostname s3p3
logging ip 44.44.44.17
snmp-server enable traps snmp authentication
snmp-server enable traps interface
snmp-server enable traps syslog
snmp-server host 44.44.44.16 traps version 2c public
snmp-server community public ro
snmp-server community private rw
ip name-server 44.44.44.201
snmp-server enable traps ipsec
crypto address-pool "RAS-pool"
    start-ip 10.133.0.1 end-ip 10.133.255.254 netmask 255.255.0.0
!
crypto pki wsg-cert Certs-SAMI.crt wsg-private-key PrivateKeys-SAMI.prv
crypto pki trustpoint rootCA cacert.crt crl disable
!
crypto profile "RAS-prof"
    isakmp
        lifetime 86400
        self-identity id-type fqdn id SAMI.cisco.com
    ipsec
        security-association lifetime 28800
        access-permit ip 172.60.0.0 subnet 16
        ip address-pool "RAS-pool"
    activate
!
interface vlan 63
```

```

ip address 88.88.63.133 255.255.255.0
interface vlan 223
ip address 222.222.223.133 255.255.255.0
ip route 0.0.0.0 0.0.0.0 88.88.63.100
oam mode single 223
oam-ip route 44.44.44.0 255.255.255.0 222.222.223.100

```

CPU 4

```

Generating configuration.....
hostname s3p4
snmp-server enable traps snmp authentication
snmp-server enable traps interface
snmp-server enable traps syslog

ip name-server 44.44.44.201
snmp-server enable traps ipsec
crypto address-pool "RAS-pool"
start-ip 10.134.0.1 end-ip 10.134.255.254 netmask 255.255.0.0
!
crypto pki wsg-cert Certs-SAMI.crt wsg-private-key PrivateKeys-SAMI.prv
crypto pki trustpoint rootCA cacert.crt crl disable
!
crypto profile "RAS-prof"
isakmp
lifetime 86400
self-identity id-type fqdn id SAMI.cisco.com
ipsec
security-association lifetime 28800
access-permit ip 172.60.0.0 subnet 16
ip address-pool "RAS-pool"
activate
!
interface vlan 64
ip address 88.88.64.134 255.255.255.0
ip route 0.0.0.0 0.0.0.0 88.88.64.100

```

CPU 5

```

Generating configuration.....
hostname s3p5
snmp-server enable traps snmp authentication
snmp-server enable traps interface
snmp-server enable traps syslog

ip name-server 44.44.44.201
snmp-server enable traps ipsec
crypto address-pool "RAS-pool"
start-ip 10.135.0.1 end-ip 10.135.255.254 netmask 255.255.0.0
!
crypto pki wsg-cert Certs-SAMI.crt wsg-private-key PrivateKeys-SAMI.prv
crypto pki trustpoint rootCA cacert.crt crl disable
!
crypto profile "RAS-prof"
isakmp
lifetime 86400
self-identity id-type fqdn id SAMI.cisco.com
ipsec
security-association lifetime 28800
access-permit ip 172.60.0.0 subnet 16
ip address-pool "RAS-pool"
activate
!
interface vlan 65

```

```
ip address 88.88.65.135 255.255.255.0
ip route 0.0.0.0 0.0.0.0 88.88.65.100
```

CPU 6

```
Generating configuration.....
hostname s3p6
snmp-server enable traps snmp authentication
snmp-server enable traps interface
snmp-server enable traps syslog

ip name-server 44.44.44.201
snmp-server enable traps ipsec
crypto address-pool "RAS-pool"
  start-ip 10.136.0.1 end-ip 10.136.255.254 netmask 255.255.0.0
!
crypto pki wsg-cert Certs-SAMI.crt wsg-private-key PrivateKeys-SAMI.prv
crypto pki trustpoint rootCA cacert.crt crl disable
!
crypto profile "RAS-prof"
  isakmp
    lifetime 86400
    self-identity id-type fqdn id SAMI.cisco.com
  ipsec
    security-association lifetime 28800
    access-permit ip 172.60.0.0 subnet 16
    ip address-pool "RAS-pool"
  activate
!
interface vlan 66
  ip address 88.88.66.136 255.255.255.0
ip route 0.0.0.0 0.0.0.0 88.88.66.100
```

CPU 7

```
Generating configuration.....
hostname s3p7
snmp-server enable traps snmp authentication
snmp-server enable traps interface
snmp-server enable traps syslog

ip name-server 44.44.44.201
snmp-server enable traps ipsec
crypto address-pool "RAS-pool"
  start-ip 10.137.0.1 end-ip 10.137.255.254 netmask 255.255.0.0
!
crypto pki wsg-cert Certs-SAMI.crt wsg-private-key PrivateKeys-SAMI.prv
crypto pki trustpoint rootCA cacert.crt crl disable
!
crypto profile "RAS-prof"
  isakmp
    lifetime 86400
    self-identity id-type fqdn id SAMI.cisco.com
  ipsec
    security-association lifetime 28800
    access-permit ip 172.60.0.0 subnet 16
    ip address-pool "RAS-pool"
  activate
!
interface vlan 67
  ip address 88.88.67.137 255.255.255.0
ip route 0.0.0.0 0.0.0.0 88.88.67.100
```

CPU 8

```

Generating configuration.....
hostname s3p8
snmp-server enable traps snmp authentication
snmp-server enable traps interface
snmp-server enable traps syslog

ip name-server 44.44.44.201
snmp-server enable traps ipsec
crypto address-pool "RAS-pool"
  start-ip 10.138.0.1 end-ip 10.138.255.254 netmask 255.255.0.0
!
crypto pki wsg-cert Certs-SAMI.crt wsg-private-key PrivateKeys-SAMI.prv
crypto pki trustpoint rootCA cacert.crt crl disable
!
crypto profile "RAS-prof"
  isakmp
    lifetime 86400
    self-identity id-type fqdn id SAMI.cisco.com
  ipsec
    security-association lifetime 28800
    access-permit ip 172.60.0.0 subnet 16
    ip address-pool "RAS-pool"
  activate
!
interface vlan 68
  ip address 88.88.68.138 255.255.255.0
ip route 0.0.0.0 0.0.0.0 88.88.68.100

```

Step 12 Save the configuration:

```

s3p3(mode-all)# copy running-config startup-config
running config of context Admin saved
Copying operation succeeded.

```

CPU 4

```

running config of context Admin saved
Copying operation succeeded.

```

CPU 5

```

running config of context Admin saved
Copying operation succeeded.

```

CPU 6

```

running config of context Admin saved
Copying operation succeeded.

```

CPU 7

```

running config of context Admin saved
Copying operation succeeded.

```

CPU 8

```

running config of context Admin saved
Copying operation succeeded.

```

SNMP Details

WSG Release 1.2 and above supports a single interface for SNMP management. In this instance, the director PPC acts as the target for all SNMP operations. All MIBs on the SAMI are accessible through the director PPC.

Since only the director PPC accepts SNMP protocol messages from external clients, only the director needs to be configured. All subordinate PPCs forward SNMP traps to the director, and the director will send them out.

To configure the single interface for SNMP, perform the following tasks in global configuration mode:

Step 1	WSG# snmp-server ?	
	community	Sets the community string and access privileges.
	contact	Modifies the sysContact
	enable	Enables or disable traps on each PPC.
	group	Define a User Security Model group.
	host	Specify hosts to receive SNMP notifications.
	location	Modifies the sysLocation.
	user	Defines a user who can access the SNMP engine
	view	Defines an SNMPv1/v2 MIB view.
		Note All of these commands are blocked on the subordinate PPCs (PPC4 - 8) except the command to enable traps.

Table 2-1 lists the MIBs supported by the WSG:

Table 2-1 MIBs Supported by the WSG

MIB Group	Tables	Comments
MIB-II	udpTable	—
MIB-II	tcpTable	—
MIB-II	atTable	—
MIB-II	ipAddrTable	—
MIB-II	ipRouteTable	—
MIB-II	ipNetToMediaTable	—
MIB-II	tcpConnTable	—
IF-MIB	ifTable	—
IF-MIB	inetNetToMediaTable	—
IF-MIB	ifXtable	—
UDP-MIB	udpEndpointTable	—
TCP-MIB	tcptcpConnectionTable	—
TCP-MIB	tcpListenerTable	—

Table 2-1 MIBs Supported by the WSG (continued)

MIB Group	Tables	Comments
IP-MIB	ipAddressTable	—
IP-MIB	ipAddressPrefixTable	—
IP-MIB	inetNetToMediaTable	—
IP-MIB	ipv4InterfaceTable	—
IP-MIB	ipv6InterfaceTable	—
HOST-RESOURCE-MIB	hrDeviceTable	—
HOST-RESOURCE-MIB	hrProcessorTable	—
HOST-RESOURCE-MIB	hrNetworkTable	—
HOST-RESOURCE-MIB	hrFSTable	—
HOST-RESOURCE-MIB	hrSWRunTable	—
HOST-RESOURCE-MIB	hrSWRunPerfTable	—
CISCO-PROCESS-MIB	cpmProcessTable	—
CISCO-PROCESS-MIB	cpmProcessExtRevTable	—
CISCO-SYSLOG-EXT-MIB	cseSyslogServerTable	—
CISCO-SYSLOG-MIB	clogHistoryTable	—
CISCO-IF-EXTENSION-MIB	cieIfInterfaceTable	—
CISCO-IF-EXTENSION-MIB	cieIfUtilTable	—
CISCO-IF-EXTENSION-MIB	cieIfNameMappingTable	—
CISCO-CONFIG-COPY-MIB	ccCopyTable	Supported only on the Master.
CISCO-IPSEC-FLOW-MONITOR-MIB	cikeGlobalStats	<p>The following IPsec MIB variables are supported:</p> <ul style="list-style-type: none"> • cikeGlobalActiveTunnels • cikeGlobalInitTunnelFails • cikeGlobalRespTunnelFails • cikeGlobalInOctets • cikeGlobalInPkts • cikeGlobalInDropPkts • cikeGlobalOutOctets • cikeGlobalOutPkts • cikeGlobalOutDropPkts

Table 2-1 MIBs Supported by the WSG (continued)

MIB Group	Tables	Comments
CISCO-IPSEC-FLOW-MONITOR-MIB	cikeTunnelTable	<p>The following IPsec MIB variables are supported:</p> <ul style="list-style-type: none"> • cikeTunLocalAddr • cikeTunRemoteAddr • cikeTunEncryptAlgo • cikeTunHashAlgo • cikeTunAuthMethod • cikeTunActiveTime • cikeTunInOctets • cikeTunInPkts • cikeTunInDropPkts • cikeTunOutOctets • cikeTunOutPkts • cikeTunOutDropPkts

Table 2-1 MIBs Supported by the WSG (continued)

MIB Group	Tables	Comments
CISCO-ENHANCED-IPSEC-FLOW-MIB	ceipSecGlobalStats	<p>The following IPsec MIB variables are supported:</p> <ul style="list-style-type: none"> • ceipSecGlobalInDecrypts • ceipSecGlobalInOctets • ceipSecGlobalInPkts • ceipSecGlobalOutEncrypts • ceipSecGlobalOutOctets • ceipSecGlobalOutPkts • ceipSecGlobalActiveTunnels • ceipSecGlobalInAuths • ceipSecGlobalInAuthFails • ceipSecGlobalInDecryptFails • ceipSecGlobalInDrops • ceipSecGlobalInReplayDrops • ceipSecGlobalNoSaFails • ceipSecGlobalOutAuths • ceipSecGlobalOutAuthFails • ceipSecGlobalOutDrops • ceipSecGlobalOutEncryptFails • ceipSecGlobalOutCompressedPkts • ceipSecGlobalOutCompFailPkts • ceipSecGlobalOutCompSkippedPkts • ceipSecGlobalOutCompTooSmallPkts • ceipSecGlobalOutUncompOctets • ceipSecGlobalProtocolUseFails • ceipSecGlobalThroughputUtilizationInterval • ceipSecGlobalThroughputLastUpdatedTime • ceipSecGlobalLastAveragePacketSize • ceipSecGlobalLastThroughputInMbps • ceipSecGlobalLastThroughputInKpps • ceipSecGlobalLastThroughputUtilization • ceipSecGlobalPeakThroughputUtilization • ceipSecGlobalPeakThroughputDateAndTime • ceipSecGlobalPeakThroughputInMbps • ceipSecGlobalPeakAvgPacketSize

Table 2-1 MIBs Supported by the WSG (continued)

MIB Group	Tables	Comments
CISCO-ENHANCED-IPSEC-FLOW-MIB	ceipSecTunnelTable	<p>The following IPsec MIB variables are supported:</p> <ul style="list-style-type: none"> • ceipSecTunLocalAddress • ceipSecTunLocalAddressType • ceipSecTunRemoteAddress • ceipSecTunRemoteAddressType • ceipSecTunInOctets • ceipSecTunInPkts • ceipSecTunOutOctets • ceipSecTunOutPkts • ceipSecTunInAuths • ceipSecTunInAuthFails • ceipSecTunInDecompOctets • ceipSecTunInDecrypts • ceipSecTunInDecryptFails • ceipSecTunInDropPkts • ceipSecTunInReplayDropPkts • ceipSecTunOutAuths • ceipSecTunOutAuthFails • ceipSecTunOutDropPkts • ceipSecTunOutEncrypts • ceipSecTunOutEncryptFails • ceipSecTunOutCompressedPkts • ceipSecTunOutCompSkippedPkts • ceipSecTunOutCompFailPkts • ceipSecTunOutCompTooSmallPkts • ceipSecTunPmtu • ceipSecTunActiveTime
	ciscoEnhIPsecFlowActivityGroup	<p>The following IPsec MIB variables are supported:</p> <ul style="list-style-type: none"> • ceipSecGlobalPreviousTunnels • ceipSecGlobalInDecompOctets • ceipSecGlobalSysCapFails • ceipSecGlobalThroughputInMbps • ceipSecGlobalThroughputInKbps • ceipSecGlobalThroughputUtilization

Table 2-2 lists the trap table notifications on the WSG:

Table 2-2 Trap Table Notifications Supported by the WSG

Trap	Table	Comments
coldStart	SNMPv2-MIB	—
authenticationFailure	SNMPv2-MIB	Community string provided in SNMP request is wrong.
Memory congestion: • clogMessageGenerated	CISCO-SYSLOG-MIB	—
CPU congestion: • cpmCPURisingThreshold • cpmCPUFallingThreshold	CISCO-PROCESS-MIB	—
Tunnel setup: • ciscoEnhIpsecFlowTunnelStart • ciscoEnhIpsecFlowTunnelStop • ciscoEnhIpsecFlowSysFailure • ciscoEnhIpsecFlowSetupFail	CISCO-ENHANCED-IPSEC-FLOW-MIB	<ul style="list-style-type: none"> • Aggregate trap for 1000 tunnel establishment. • Aggregate trap for 1000 tunnel deletion. • Exceeds tunnel capacity threshold. • Insufficient IP addresses.
Interface state: • linkUp • linkDown	IF-MIB	<ul style="list-style-type: none"> • VLAN Interface Up. • VLAN Interface Down.
clrRedundancyStateChange	CISCO-L4L7MODULE-REDUNDANCY-MIB	No other object from the CISCO-L4L7MODULE-REDUNDANCY-MIB is supported.
Flow system failure notification: • ceipSecFailreason • ceipSecFailPktSrcAddressType • ceipSecFailPktSrcAddress • ceipSecFailPktDstAddressType • ceipSecFailPktDstAddress	CISCO-ENHANCED IPSEC-FLOW-MIB	Provides flow failure identification <ul style="list-style-type: none"> • IPsec flow fail reason • Fail packet source IP address type • Fail packet source IP address • Fail packet destination IP address type • Fail packet destination IP address
Certificate expiry notification: • ciscoEnhIpsecFlowCertExpiry	CISCO-ENHANCED IPSEC-FLOW-MIB	Provides certificate identification (Subject Name, Serial Number, Issuer Name), expiration date and time, and expiration status: <ul style="list-style-type: none"> 1—certOK 2—certGoingExpired 3—certExpired

Table 2-2 Trap Table Notifications Supported by the WSG (continued)

Trap	Table	Comments
Certificate renewal notification: • ciscoEnhIpssecFlowCertRenewal	CISCO-ENHANCED IPSEC-FLOW-MIB	Provides certificate identification (Subject Name, Serial Number, Issuer Name), expiration date and time, and renewal status: 1—renewalNotNeeded 2—renewalRequestNeeded 3—renewalRequested 4—renewalSuccess 5—renewalFailedUpdate 6—renewalFailedExpired
Performance throughput notification: • ciscoEnhIpssecFlowSysFailure	CISCO-ENHANCED IPSEC-FLOW-MIB	Provides the failure reason for IPsec flow throughput: 17—performance utilization exceeding the threshold

**Note**

Use the SNMP Object Navigator (<http://tools.cisco.com/Support/SNMP/do/BrowseOID.do?local=en>) to obtain SNMP object information. For example, enter the object name ciscoEnhIpssecFlowCertExpiry.

Syslog Details

The WSG Release 1.2 and above supports a single interface for syslog collection. As part of the Memory Usage Monitoring feature, all PPCs send the syslogs to the director, and the director PPC sends them to an external server (if configured).

The external logging server can be configured only on the director PPC. Logs from any PPC can be viewed on the director (given the correct cpuid)

Additionally, from WSG 4.4.1, we can manually configure the facility value by configuring this CLI. With this, we will be able to send the generated syslog's to the syslog server with the configured facility value.

Step 1	<pre>WSG(config)# logging ? ip lineread</pre>	<p>ip—Configures the IP address of ext logging server. Only the director needs external logging server.</p> <p>lineread—Configures the number of lines to read log. The number of lines can still be configured (for show below).</p>
---------------	---	---

Step 2	<pre>WSG# show logging ? config message</pre>	<p>config—Shows the syslog configuration.</p> <p>message—Shows syslog messages. Messages can still be viewed on each PPC (using the correct cpuid).</p>
Step 3	<pre>WSG(config)# crypto facility ? <0-23> Value 0 to 23 WSG(config)# config message</pre>	<p>config—Configures the facility level to desired value.</p> <p>message—Sends the generated syslog's to the configured syslog server with the configured facility value (Will be able to configure only on the director PPC(PPC3)).</p>

Understanding WSG Prerequisites

The WSG requires a Cisco 7600 system with these:

- SUP Engine 720, with a Multilayer Switch Feature Card (MSFC), running Cisco IOS Release 12.2(33)SRC3, and a Compact flash (min 128MB) in Disk:0 slot, or
Cisco 7600 Series SUP 32, with a MSFC, running Cisco IOS Release 12.2(33)SRC3, and a Compact flash (min 128MB) in Disk:0 slot.
For details on upgrading the Cisco IOS release running on the SUP, see the “Upgrading to a New Software Release” section in the *Release Notes for Cisco IOS Release 12.2(33)SRC3*.
- Any module with ports connected to the network.
- Cisco Service and Application Module for IP (Cisco Product Number: WS-SVC-SAMI-BB-K9) with the 2 GB memory option (Cisco Product Number: MEM-SAMI-6P-2GB[=]). Release 1.1 of the WSG application ships loaded on the SAMI.

Enabling Supervisor to Collect PPC Crash Files and HA Traces

The PPC crash files are stored on Supervisor's compact flash Disk:0/1. In case the compact flash is not available in Disk:0/1, the PPC stores the crash files on bootdisk/bootflash if the available storage on bootdisk/bootflash is more than 10 MB.

The following commands should be configured on the Supervisor:

- ip rcmd rcp-enable
- ip rcmd rsh-enable
- line vty 0 4
 - transport input telnet ssh
 - transport output telnet

Also, ensure that there are free Virtual Terminal Lines (VTYs) by issuing the “**show users**” command on the Supervisor.

Establishing a PPC Session

To set up VLAN support, establish a session with a PPC. Perform this procedure for each of the six PPCs on a SAMI with WSG.



Note

Under conditions like low processor memory, a session to the SAMI may fail. If this occurs, use the physical front-panel console connections to access the SAMI (see the “Establishing a Console Connection on the SAMI” section of the *Cisco Service and Application Module for IP User Guide*).

To set up a PPC session from the SUP Console, enter:

Step 1	Sup# show module	Returns system information, like which slot contains the SAMI with the PPC to connect to.
Step 2	Sup# session slot <i>slot_number</i> processor <i>proc_number</i>	Sets up a session to a PPC where: <ul style="list-style-type: none"> • <i>slot_number</i>—Number of the slot in which the SAMI is installed. • <i>proc_number</i>—Number of the PPC. Valid values are 3 through 8.

Assigning a Hostname to a PPC

The default session prompt when you set up a session with a PPC is “switch.” To assign a hostname to a PPC other than switch, enter:

Step 1	switch# configure	Enables global configuration mode.
Step 2	switch(config)# hostname <i>name</i>	New hostname for the PPC. Enter a case sensitive text string with 1 to 32 alphanumeric characters.

This example shows a session with PPC 3 on a SAMI in slot 6, the hostname is changed to PPC3:

```
Sup> enable
Sup# session slot 6 processor 3
Trying... Open

switch# config
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# hostname PPC3
PPC3(config)#
```

Setting Up VLAN Support

SAMI does not have outside physical interfaces to receive traffic from the network. Instead, the SAMI uses VLAN interfaces to the SUP. To set up VLAN support between the SUP and PPCs, complete tasks in these sections:

- [Setting Up the SUP, page 2-18](#)
- [Setting Up the PPCs, page 2-20](#)

Setting Up the SUP

For PPCs to receive traffic from the SUP, complete these tasks on the SUP:

- Set up a VLAN for each PPC.
- Assign the VLANs to a VLAN group.
- Assign the VLAN groups to the SAMIs.
- Set up a default gateway VLAN.

Setting Up VLANs for the PPCs

To set up the VLANs for each PPC on the SUP, enter:

	Command	Purpose
Step 1	Sup> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	Sup# configure terminal	Enters global configuration mode.
Step 3	Sup(config)# vlan <i>vlan-id</i>	Configures a VLAN where <i>vlan-id</i> is the number of the VLAN. Valid values are from 1 to 4094.
Step 4	Sup(config-vlan)# description <i>interface_description</i>	(Optional) Describes interface.
Step 5	Sup(config-vlan)# end	Exits VLAN configuration mode.

To create VLANs 71 to 76 on the SUP Console plus an OAM Vlan 100, enter:

```
Sup> enable
Sup# configure terminal
Sup(config)# vlan 71
Sup(config-vlan) exit
Sup(config)# vlan 72
Sup(config-vlan) exit
Sup(config)# vlan 73
Sup(config-vlan) exit
Sup(config)# vlan 74
Sup(config-vlan) exit
Sup(config)# vlan 75
Sup(config-vlan) exit
Sup(config)# vlan 76
Sup(config-vlan) exit
Sup(config)# vlan 100
Sup(config-vlan) exit
```

Assigning VLANs to the SAMI

SAMI PPC VLANs must be assigned to the same VLAN group. You cannot assign the same VLAN to many groups. However, you can assign a group to many SAMIs.

By default, one switched virtual interface (SVI) (required if the SUP participates in Layer-3 forwarding) can exist between an MSFC and a SAMI. Create and enable SVIs using the **svclc multiple-vlan-interfaces** command.

To assign VLANs to a SAMI, enter:

Step 1	Sup> enable	Enables privileged EXEC mode.
Step 2	Sup# configure terminal	Enters global configuration mode.
Step 3	Sup(config)# svclc vlan-group vlan_group_number vlan_range	Assigns the VLANs to a secure group. <ul style="list-style-type: none"> • <i>vlan_group_number</i>—Number of the VLAN group. • <i>vlan_range</i>—Number of the VLAN or VLANs identified as a single number (<i>n</i>), as a range of numbers (<i>n-m</i>), or as separate numbers or range of numbers, separated by commas (for example, 5,7-10,13,45-100).
Step 4	Sup(config)# svclc module slot_number vlan-group group_number_range	Assigns VLAN groups to the SAMI, where: <ul style="list-style-type: none"> • <i>slot_number</i>—Number of the slot in which the SAMI is installed. To view chassis slot numbers and modules, use the show module command in privileged EXEC mode. • <i>group_number_range</i>—VLAN group number identified as a single number (<i>n</i>), as a range of numbers (<i>n-m</i>), or as separate numbers or range of numbers, separated by commas (for example, 3,5,7-10). Only VLAN groups created using the svclc vlan-group global configuration command. <p>Note One VLAN group can be assigned to many SAMIs.</p>
Step 5	Sup(config)# svclc multiple-vlan-interfaces	Enables many SVIs to be set up for SVCLC modules.

For example:

- To create a VLAN group, group 50, with a VLAN range of 71 to 76, and 100 enter:

```
Sup> enable
Sup# configure terminal
Sup(config)# svclc vlan-group 50 71-76, 100
```

- To assign VLAN group 50 to the SAMI in slot 5, enter:

```
Sup(config)# svclc module 5 vlan-group 50
```

- To enable many SVIs to be set up for SVCLC modules (the SAMIs), enter:

```
Sup(config)# svclc multiple-vlan-interfaces
```

- To view the SAMI group configuration and associated VLANs, enter:

```
Sup(config)# exit
Sup# show svclc vlan-group
```

- To view VLAN group numbers for all modules, enter:

```
Sup# show svclc module
```

Setting Up the PPCs

To complete the configuration tasks for VLAN support do the following on each PPC:

1. Set up the default gateway.
2. Set up a VLAN interface.
3. Assign the interface to the corresponding VLAN on the SUP.



Note

Sharing of the same VLAN ID with different PPC's on SAMI WSG is not supported unless if it is for HA VLAN interface.

To set up the PPCs, enter the following commands from the SUP:

	Command	Purpose
Step 1	Sup> enable	Enables privileged EXEC mode.
Step 2	Sup# session slot <i>slot_number</i> processor <i>proc_number</i>	Sets up a session to a PPC where: <ul style="list-style-type: none"> • <i>slot_number</i>—Number of the slot in which the SAMI is installed. • <i>proc_number</i>—Number of the PPC. Valid values are 3 through 8. Note Set up one session per PPC.
Step 3	WSG# config	Enters global configuration mode.
Step 4	WSG(config)# interface vlan <i>number</i>	Creates a VLAN interface for the VLAN, and enters interface configuration mode.
Step 5	WSG(config-if)# description <i>interface_description</i>	(Optional) Describes interface.
Step 6	WSG(config-if)# ip address <i>ipv4 address</i>	Assigns an IP address to a VLAN interface for connectivity. IKE and ESP traffic from the endpoints use this IP address.
Step 7	WSG(config-if)# no shutdown	Enables a VLAN interface.
Step 8	WSG(config-if)# do show interface vlan <i>number</i>	Verifies that a VLAN is active.
Step 9	WSG(config-if)# do ping <i>ip_address</i>	Verifies network connectivity.
Step 10	WSG(config-if)# do show arp	Shows the ARP table.
Step 11	WSG(config-if)# exit	Exits interface configuration mode.
Step 12	WSG(config)# ip route 0.0.0.0 0.0.0.0 <i>ip-addr</i>	Defines a default gateway (router).
Step 13	WSG(config)# end	Exits configuration mode.
Step 14	WSG# exit	Returns to the SUP console session.

For example:

- To create a VLAN interface on PPC3 on a SAMI in slot 5, enter:

```
Sup# session 5 processor 3
WSG> config
```

```
WSG(config)# interface vlan71
WSG(config-if)# ip address 10.22.22.2 255.255.255.0
WSG(config-if)# exit
```

- To verify the interface configuration of VLAN71, enter:

```
WSG# show interface vlan71
```

- To define a default gateway, enter:

```
Sup# session 5 processor 3
switch> config
```

```
switch(config)# ip route 0.0.0.0 0.0.0.0 10.22.22.1
```

Configuring the WSG

The WSG application is preloaded on the SAMIs. Set up IPSec parameters for your network using the WSG CLI. To set up the WSG to perform these procedures:

- [Single OAM Interface, page 2-22](#)
- [Resource Monitoring, page 2-23](#)
- [Configuring WSG Global Parameters, page 2-24](#)
- [Configuring the WSG Profile, page 2-28](#)
- [Configuring IKE, page 2-31](#)
- [High Availability, page 2-31](#)
- [Configuring High Availability on SAMI COSLI, page 2-35](#)
- [IKE SA Handling, page 2-50](#)
- [IPSec SA Handling, page 2-51](#)
- [Configuring IPSec, page 2-52](#)
- [Site-to-Site Scalability, page 2-53](#)
- [Certificate Management Protocol, page 2-56](#)
- [Online Certificate Status Protocol, page 2-62](#)
- [DHCP Address Allocation, page 2-62](#)
- [IPv6, page 2-67](#)
- [Blacklisting, page 2-69](#)
- [RADIUS Accounting, page 2-70](#)
- [EAP Peer Authentication, page 2-73](#)
- [Reverse Route Injection \(RRI\), page 2-73](#)
- [VRF Configuration, page 2-75](#)
- [Configuring WSG Performance/Throughput Indicators, page 2-80](#)
- [Configuring IKE/IPSec Stats Collection and Timing Enhancements for SNMP, page 2-85](#)

To apply changes to the default configuration, save the running configuration to the configuration file using the **copy running-config startup-config** command from a PPC session.

**Note**

Individually set up each of the six PPCs.

Single OAM Interface

As described in the previous sections, the WSG uses a single interface for SNMP and syslog messages from all PPCs through the director PPC.

The single OAM interface works with the single-entity mode, allowing all management traffic (such as DNS, CRL, and HTTP) to flow through the same interface on the director PPC. It is desirable to use a single interface per blade for management traffic when only a limited number of management IP addresses are available. Rather than using a separate interface on each PPC on the management network, you can configure the single OAM interface to allow all PPCs on the WSG to use the same interface on the director PPC. Configuring the single OAM interface is a two-step process. First, identify the interface used for OAM traffic. Second, configure oam-ip routes for the management subnets. Once configured, the WSG internally routes all the traffic to the connected OAM subnet (and all management networks configured through the oam-ip route) through the director PPC.

**Note**

You should only use this feature should for protocols that generate minimal amount traffic (for example, CRL).

**Note**

SNMP and SYSLOG are only run on the director PPC. Even though SNMP and Syslog can use the single OAM interface to reach the management network, they do not need to be routed through the director PPC (there is no need to configure the OAM interface and OAM routes for SNMP and SYSLOG purposes).

Configuring the Single OAM Interface

To configure the Single OAM interface feature on the WSG, perform the following tasks:

Step 1	WSG(config)# oam mode single vlan 223	This command identifies the interface used for single mode OAM traffic. All management traffic from the director and subordinate PPC destined to vlan 223 subnet will now be directed through this interface.
Step 2	WSG(config)# oam-ip route	This command configures static routes on the director PPC and subordinate PPCs for the management subnet(s). This command is similar to ip route in functionality, with the exception that it affects the routes on the subordinate PPCs as well.

Here is an example:

```
interface vlan 223
 ip address 222.222.223.123 255.255.255.0
 oam mode single 223
 oam-ip route 44.44.44.0 255.255.255.0 222.222.223.100

R7-S2P3(mode-all)# sh ip route
```

```
127.0.0.0/24 dev eth0 src 127.0.0.23
44.44.44.0/24 via 222.222.223.100 dev eth0.223
222.222.223.0/24 dev eth0.223 src 222.222.223.123
```

```
CPU 4
127.0.0.0/24 dev eth0 src 127.0.0.24
44.44.44.0/24 via 127.0.0.23 dev eth0
222.222.223.0/24 via 127.0.0.23 dev eth0
```

Resource Monitoring

Resource monitoring notifies you (using SNMP traps) when utilization of one or more system resources such as CPU, memory, and storage of a system crosses certain predefined thresholds.

Monitoring CPU Usage

The CPU Threshold Notification feature notifies users by generating a SNMP trap message when a predefined threshold of CPU usage is crossed. Two types of CPU utilization threshold are supported: rising threshold and falling threshold. A rising CPU utilization threshold specifies the percentage of CPU resources that, when exceeded for a configured period of time, triggers the `cpmCPURisingThreshold` notification. Similarly, a falling CPU utilization threshold specifies the percentage of CPU resources that, when CPU usage falls below this level for a configured period of time, triggers `cpmCPUFallingThreshold` notification.

To configure the CPU Threshold Notification feature, perform the following tasks: use the **`process cpu threshold rising percentage interval seconds`** [**`falling percentage interval seconds`**] command.

Step 1	<code>WSG# configure</code>	Enables global configuration mode.
Step 2	<code>WSG(config)#process cpu threshold rising percentage interval seconds</code> [<code>falling percentage interval seconds</code>]	Enables the CPU Threshold Notification feature and establishes the rising and falling percentages threshold values. Threshold values: min 1% to max 100%. Threshold interval: 5 – 86400 seconds. falling threshold should always be less than, or equal to the configured rising threshold value. This parameter is optional.

The following example shows how to set a rising CPU threshold notification for total CPU utilization. When total CPU utilization exceeds 95 percent for a period of 5 seconds or longer, a rising threshold notification is sent.

```
ppc3(config)# process cpu threshold rising 95 interval 5
```

Monitoring Memory Usage

The Memory usage monitoring feature allows syslogs to be generated to indicate that free memory has fallen below a configured threshold, or the system has recovered from a low memory situation.

To configure the Memory Usage Monitoring feature, perform the following tasks:

Step 1	<code>WSG# memory free low watermark processor threshold</code>	Configures the memory threshold that, when free memory falls below, generates a syslog. The free memory threshold value can range from 1024KB to 1996000KB.
---------------	---	---

The following example specifies a threshold of 10000 KB of free processor memory before a low-memory syslog is generated:

```
ppc3(config)# memory free low-watermark processor 10000
```

Once the available free memory rises to above 5 percent of the threshold (1.05 x 10000 in the above example), another message is generated that indicates that the free memory has recovered.

Configuring WSG Global Parameters

Modifications to most of the global parameters will take effect only when the next **activate** command is issued for the profile.

Configuring IKE Retry Count

To set the number of IKE retry connection attempts, perform the following task:

Step 1	<code>WSG(config)# crypto ike-retry-count value</code>	Sets the number of IKE retry connection attempts.
---------------	--	---

Configuring Remote Secret

To set the remote shared secret, perform the following task:

Step 1	<code>WSG(config)# crypto remote-secret id_type id secret</code>	Sets the remote shared secret.
---------------	--	--------------------------------

Configuring a Local Address Pool

The WSG keeps a pool of private addresses from the protected network. When the WSG receives an endpoint SA with an internal IP address, it assigns an unused address from the address pool. The address does not expire as long as the SA is up. When the SA is removed, the address is released to the local pool.

When setting up an address pool, note:

- Set up address pools using the **start-ip** command.
- On the SUP, set up a static route to the PPC. This handles traffic sent to an address in the local address pool to be routed to the PPC.



Note

This configuration is optional for site-to-site profiles.

For example, to set up an address pool from which to assign addresses on the SAMI, enter:

```
WSG# config
Enter configuration commands, one per line. End with CNTL/Z.
WSG(config)# crypto address-pool foo
WSG(config-address-pool)# start-ip 192.168.10.1 end-ip 192.168.10.10 netmask 255.255.255.0
```

Adding the DNS Server to the Address Pool

To specify the DNS server that is passed to the access point (the remote end point) when there is a request for a DNS server during IKE negotiation, perform the following tasks:

	Command	Purpose
Step 1	<pre>WSG# conf t Enter configuration commands, one per line. End with CNTL/Z. WSG(config)# crypto address-pool foo WSG(config-address-pool)# dns-server ? <A.B.C.D> Enter IP address WSG(config-address-pool) # dns-server 172.20.10.1</pre>	<p>Specifies the DNS server IP address that is to be passed to the access point (the remote end point) when there is a request for a DNS server during IKE negotiation.</p> <p>If the DNS server IP address is not required to be sent to the remote access point, this command is not required.</p>

Configuring Authentication Parameters

For secure communication, the WSG requests and sends X.509 digital certificates to authenticate IPsec endpoints.

Multiple CA Trust Anchors

A trust anchor is a third party the WSG trusts and to which it has a certification path. The trust anchor certifies the WSG. This certificate has information about prefixes that a WSG is allowed to use in router advertisements. Authorization delegation discovery enables a node to adopt a WSG as its default router.

CA Certificate Chaining

A certificate chain is a sequence of certificates with dependent trust relationships. The first certificate is self-signed by the CA. Each subsequent certificate creates an association between a certificate owners, or CAs in the chain. This process creates a trust chain from trusted peer to a CA. The CA endorses the identity of the peer certificate by signing it.

The WSG keeps a list of trusted CA certificates in its root certificate directory. If the CA certificate is not on this list, the WSG will refuse to authenticate the peer until a CA certificate is obtained and validated. If the CA certificate is on this list, the WSG trusts the signed peer certificate and will allow a security association in that peer.



Note

This release supports manual certificate installation.

To enable digital certification, complete these tasks:

- [Generating an RSA Key Pair and CSR, page 2-26](#)
- [Submitting the CSR to the CA, page 2-27](#)

- [Specifying Certificates and a Private Key on the WSG, page 2-27](#)
- [Configuring the WSG Profile, page 2-28](#)

Generating an RSA Key Pair and CSR

RSA key pairs sign, encrypt, and decrypt. To get a Certificate Authority (CA) you first need a Certificate Signing Request (CSR).

1. The **crypto rsa-keygen** command makes a private key (`wsg.prv` file) and a CSR (`wsg-pem.csr` file) based on the CSR parameters you enter.
2. The private key file is copied to the SUP bootflash or bootdisk, depending on which is available.
3. The public key, the second key of the key pair, is embedded in the CSR.



Note

If all WSG instances in a SAMI must share a certificate, use the **crypto rsa-keygen** command only once on one PPC in the SAMI. If the WSGs must use separate certificates, use the **crypto rsa-keygen** command on each PPC in the SAMI.

To generate an RSA key pair and CSR, enter the following on a PPC in the SAMI:

	Command	Purpose
Step 1	WSG# crypto rsa-keygen id-type id-type id id	<p>Makes an RSA key pair and CSR using information to authenticate the site, where:</p> <ul style="list-style-type: none"> • id-type id-type configures the local identity type. Possible values are fqdn and ip. <p>Note Changing local identity type drops all existing tunnels.</p> <ul style="list-style-type: none"> • id sets the IP address or domain name for the key pair

To generate an RSA key pair and CSR for a remote peer, enter:

Command	Purpose
Step 1 WSG# <code>crypto rsa-keygen id-type id</code>	<p>Makes an RSA key pair and CSR for a remote peer:</p> <ul style="list-style-type: none"> • id-type—fqdn • id—test.cisco.com <p>Generating certificate request...done. Copying private key (wsg.prv) to SUP...done. Copying certificate request (wsg-pem.csr) to SUP...done.</p> <pre> -----BEGIN CERTIFICATE REQUEST----- MIIBrjCCARcCAQAwNTElMAkGA1UEBhMCVVMxDTALBgNV AsTBFNNQ1UxFzAVBgNV BAMTDnNlZ3cuY2l2Y28uY29tMIGfMA0GCSqGSIb3DQEBA QUAA4GNADCBiQKBgQCr xsJE11PDRytSqzGH7aVi4fmf8rXygmYCCOPvnIQybMoJ t5PdObtbXREJ2r4ON6Y gh4E+IXbIe3yig6friBFMEkYgQJuLe13P8wELDdHyWA6v BLzVgZuwa34Me8B0nKa LMaU7kZ47sConEOE1c27NB16mI5D4rVdBnacj4/GCQIDA QABODkNwYJKoZIHvcN AQkOMSowKDALBgNVHQ8EBAMCBaAwGQYDVR0RBBIwEIIoc 2Vndy5jaXNjby5jb20w DQYJKoZIhvcNAQEFBQADgYEASEqXB00k1VfguVdUf9LU4 Im1+31+hWErFp/M5Nh4 r+h5ukmCW9ldPPIZxOkV2n2wedLf6mUKTcdzdOLUiwgrS ozHSfLWgpXW+upxZDgn Nk/LvIW3+NpwnjzCmYJEZKFpWglxKzzwMAe99AOpH+Z6y hrw5ffcc9qZCcWXkeHw 1Iw= -----END CERTIFICATE REQUEST----- </pre>



Note

RSA key-pairs can be generated outside the PPC. If the CSR and private key are generated outside of the WSG, copy the private key file to the SUP before defining the certificates on the WSG.

Submitting the CSR to the CA

After generating the RSA key pair and CSR:

1. Submit the CSR to a CA using FTP or a cut-and-paste from the console session.
2. The CA signs the CSR using its RSA private key.
3. The CSR becomes a WSG certificate.
4. Copy the certificate to the SUP.
5. Set up the PPCs to use the private key and certificates.

Specifying Certificates and a Private Key on the WSG

When you enter the `crypto pki wsg-cert` and `crypto pki trustpoint` commands, the certificates (and optionally, the private key) are copied from the SUP to the WSG, and the WSG configuration is updated.



Note Before you can issue the **crypto pki wsg-cert** and the **crypto pki trustpoint** commands, the certificates and a private key must exist on the SUP.

To set the certificates for the WSG to use during authentication, enter:

	Command	Purpose
Step 1	WSG# config	Enters global configuration mode.
Step 2	WSG(config)# crypto pki wsg-cert <i>cert-filename.crt</i> [wsg-private-key <i>private-key-filename.prv</i>]	Configures the WSG to use the certificate for certificate based authentication. The certificate and private key are copied from the Cisco 7600 SUP to the WSG. Up to 20 certificate/private key pairs may be configured on the WSG. <i>cert-filename.crt</i> —Name of the WSG certificate file. Ensure certificate filenames end with a .crt file extension. <i>private-key-filename.prv</i> —Private key filename. To use the private key, set the name of the private key file, ending with a .prv extension. Note The WSG uses the private key from the crypto rsa-keygen command if you do not set a private key.
Step 3	WSG(config)# crypto pki trustpoint { rootCA subCA } <i>filename.crt</i> [cr1 disable]	Sets up a CA certificate.

For example:

- To set up the WSG to use a certificate with the name cert1.crt and a private key file named wsg.prv contained on the SUP, enter:

```
WSG# config
Enter configuration commands, one per line. End with CNTL/Z.
WSG(config)# crypto pki wsg-cert cert1.crt wsg-private-key wsg.prv
Copying cert1.crt from SUP...done
```

- To set up the WSG to use a CA certificate with the name cert-ca1.crt on the SUP, enter:

```
WSG# config
Enter configuration commands, one per line. End with CNTL/Z.
WSG(config)# crypto pki trustpoint rootCA cert-ca1.crt
Copying cert1-ca1.crt from SUP...done
```

Configuring the WSG Profile

As described in the earlier sections, part of the configuration for the WSG is entered globally. The rest of the configuration is entered by creating a crypto profile.

A profile is a combination of IKE and IPSec parameters that apply to all the tunnels that will get established on the WSG. A profile is created using the **crypto profile** command. The IKE and IPSec related parameters are entered in the **isakmp** and **ipsec** submodes of the **crypto profile** command mode. A profile must be activated using the **activate** command before the tunnels can be established.

The profile parameters can only be modified when the profile is in an deactivated state. The profile can be deactivated by issuing the **no activate** command under the **crypto profile** submode.

The global configuration for WSG is also effective only when the profile is active. If any global WSG configuration is modified while the crypto profile is in active state, the changes will not take effect till the profile is first deactivated, and then activated again.



The *profile name* should be unique; you cannot use the same name for two different profiles.

- [Configuring the WSG Parameters](#)
- [Configuring IKE](#)
- [Configuring IPSec](#)

Configuring the WSG Parameters

To set up an IKE identity for the WSG/PPC to use during authentication, enter:

	Command	Purpose
Step 1	WSG# config	Enters global configuration mode.
Step 2	WSG(config)# crypto profile WSG(config-crypto-profile)# profile-type ? remote-access Profile Type remote-access (default) site-to-site Profile Type site-to-site	Enters the crypto profile. A crypto profile can be either remote access type, or site-to-site type. The profile-type command is used to specify the type of each profile that you create. If the type is not specified the default is remote-access. Only one remote access profile can be active. Multiple site-to-site profiles can be active. Note You should take special care to configure the proper access-permit command that corresponds to the profile type used, as described in the access-permit command. Note The maximum number of possible site-to-site profiles supported is 25.
Step 3	WSG(config-crypto-profile)# isakmp	Enters ISAKMP submode.

	Command	Purpose
Step 4	<pre>WSG(config-crypto-profile-isakmp)# self-identity id-type type id id</pre>	<p>Defines the IKE identity of the local IPSec client, where:</p> <ul style="list-style-type: none"> self-identity must match the certificate's identity. <p> Note The supported characters while configuring the self-identity are dash, dot, underscore, a-z, A-Z and 0-9.</p> <ul style="list-style-type: none"> id-type configures the IKE identify of the local client. The IKE identity is the identity the client uses when authenticating to the gateway. Valid values are: <ul style="list-style-type: none"> ip—IP address dn—Distinguished name fqdn—Fully-qualified domain name email—E-mail address <p> Note The maximum size supported for the id-types is 256 bytes.</p> <ul style="list-style-type: none"> id sets the ID data of the remote IKE client (name, IP address, dn, FQDN, or e-mail address).
Step 5	<pre>WSG(config-crypto-profile-isakmp)# sequence-number [extended short]</pre>	<p>Specifies that a 32-bit (short) or 64-bit (extended) sequence number is used for a profile. 32-bit is the default value.</p>
Step 6	<pre>WSG(config-crypto-profile-isakmp)# exit</pre>	<p>Exits ISAKMP submode.</p>

For example, to set up an id-type of “fqdn,” id “wsg.cisco.com,” on the PPC using the crypto profile “remote-access”:

```
WSG# config
Enter configuration commands, one per line. End with CNTL/Z.
WSG (config)# crypto profile remote-access
WSG(config-crypto-profile)# isakmp
WSG(config-crypto-profile-isakmp)# self-identity id-type fqdn id wsg.cisco.com
WSG(config-crypto-profile-isakmp)# sequence-number extended
WSG(config-crypto-profile-isakmp)# exit
WSG(config-crypto-profile)# exit
```

Extended Sequence Number

WSG Release 1.2 and above adds Extended Sequence Number (ESN) support as longer lifetimes are expected in customer deployments. Additionally, more traffic is expected in site-to-site setups. Extended Sequence Number (64-bit sequence number) implementation is required in such cases. In this release,

the sequence number length cannot be negotiated by the peer with the SAMI. The peer will have to match the setting on the SAMI (default is 32-bit sequence number). The 64-bit sequence number can be configured using the above CLI.

Configuring IKE

The goal of IKE negotiation is to find a compatible key exchange on both peers:

1. Peer A sends its allowed IKE policies to Peer B.
2. Peer B compares Peer A's policies to its highest priority policy.
3. Peer B tries to find policies that have the same values for the following:
 - Encryption
 - Hash algorithm
 - Authentication
 - Diffie-Hellman parameters
 - Lifetime
4. If Peer B cannot find a match, negotiation fails and IPsec is not established. If Peer B finds a match, negotiation completes and IPsec SAs are established.

To set up IKE values, perform the following tasks:

	Command	Purpose
Step 1	<code>WSG# config</code>	Enters global configuration mode.
Step 2	<code>WSG(config)# crypto profile name</code>	Sets the crypto profile name.
Step 3	<code>WSG(config)# isakmp</code>	Enters ISAKMP submode.
Step 4	<code>WSG(config-crypto-profile-isakmp)# encryption {des 3des aes aes192 aes256}</code>	Sets the IKE secret encryption scheme.
Step 5	<code>WSG(config-crypto-profile-isakmp)# hash {sha1 sha2 md5 aes-xcbc}</code>	Sets the hash algorithm.
Step 6	<code>WSG(config-crypto-profile-isakmp)# version {1 2 both}</code>	Sets the IKE version.
Step 7	<code>WSG(config-crypto-profile-isakmp) authentication {rsa-sig pre-share}</code>	Sets IKE authentication.
Step 8	<code>WSG(config-crypto-profile-isakmp)# group {1 2 5 14 15 16 17 18}</code>	Sets a DH group ID.
Step 9	<code>WSG(config-crypto-profile-isakmp)# lifetime {seconds}</code>	Sets the SA lifetime.

High Availability

In WSG Release 2.0 and above, inter-chassis stateful 1:1 redundancy is supported. Two redundancy modes are supported: active-standby and active-active (introduced in WSG Release 4.0). In the active-standby mode, redundancy works at the SAMI level. Only PPC3 or all 6 PPCs on the SAMI are in either active or standby state. The PPC of the active SAMI synchronizes its state to the corresponding

PPC of the redundant, standby SAMI. In the active-active mode, redundancy works at the PPC level. Only PPC3 and PPC4 on the SAMI are used—one PPC is in active state while the other PPC is in standby state.

The WSG redundancy feature works with all IPsec supported features including IKEv1, IKEv2, ESN, anti-replay, DPD, and NAT-traversal. WSG redundancy is applicable to both remote access and site-to-site tunnels.

If a primary SAMI fails, traffic is switched to the newly active SAMI. The established tunnels stay up and continue to pass traffic after failover, and the IKE/IPsec internal state is synchronized between the active and redundant WSGs. The expected traffic loss during failover is less than one second after detection of the failure. The WSG responds to IKE packets (DPDs and SA INIT messages) and load balancer probes within one second.

There is no impact on the WSG routing for inner and outer addresses after a failover. The WSG maintains IP addresses that are assigned from the local address pool. The newly active SAMI allocates IP addresses from the local pool when a SA is created and releases IP addresses to the local pool when a SA is deleted.

**Note**

WSG does not support the single OAM feature in the active-active redundancy mode.

**Note**

WSG does not support single-entity configuration for application configuration commands.

Configuring High Availability

Follow these steps to configure high availability on redundant WSGs:

-
- Step 1** Shutdown the standby WSG (WSG B) to ensure no IP address conflicts.
 - Step 2** Configure the node-specific configuration (interface, IP address, alias IP) on the active WSG (WSG A).
 - Step 3** Configure SVCLC in your SUP for this SAMI slot.

**Note**

If SVCLC is already configured in your SUP, first remove the SVCLC configuration before performing Step 2. Then, reconfigure the SVCLC as in Step 3. These steps ensure that when you configure the alias IP, the ARP broadcast doesn't reach the SUP.

- Step 4** Verify the HA VLAN connectivity.

**Caution**

Do not ping the alias IP to trigger an ARP broadcast.

- Step 5** Save the configuration and reload WSG B. The redundant WSGs will pair up and the standby WSG will sync the remaining configuration from the active WSG.

Example of High Availability Active-Standby Redundant Pairs

The following example shows how to configure high availability active-standby redundant pairs:

On SAMI A (slot 3/PPC3):

-
- Step 1** Under entity-all mode, configure HA VLAN interface.

```
ha interface vlan start-id 51 processor-count 2 increment 1
ip address start-ip 51.51.51.3 increment 1.1.1.0 mask 255.255.255.0
```

Step 2 Configure HA redundancy mode as active-standby with preferred-role set to primary.

```
ha redundancy-mode active-standby preferred-role primary revertive
```

Step 3 Save the configuration.

```
copy running-config startup-config
```

On SAMI B (slot 4/PPC3):

Step 4 Under entity-all mode, configure HA VLAN interface.

```
ha interface vlan start-id 51 processor-count 2 increment 1
ip address start-ip 51.51.51.4 increment 1.1.1.0 mask 255.255.255.0
```

Step 5 Configure HA redundancy mode as active-standby with preferred-role set to secondary.

```
ha redundancy-mode active-standby preferred-role secondary revertive
```

Step 6 Save the configuration.

```
copy running-config startup-config
```

Step 7 Reload both SAMI A and B.

Example of High Availability Active-Active Redundant Pairs

The following example shows how to configure high availability active-active redundant pairs:

On SAMI A (slot 3/PPC3):

Step 1 Under the entity-all mode, configure the HA VLAN interface.

```
ha interface vlan start-id 51 processor-count 2 increment 1
ip address start-ip 51.51.51.3 increment 1.1.1.0 mask 255.255.255.0
```

Step 2 Configure HA redundancy mode as active-active with preferred-role set to primary.

```
ha redundancy-mode active-active preferred-role primary revertive
```

Step 3 Save the configuration.

```
copy running-config startup-config
```

On SAMI B (slot 4/PPC3):

Step 4 Under the entity-all mode, configure HA VLAN interface.

```
ha interface vlan start-id 51 processor-count 2 increment 1
ip address start-ip 51.51.51.4 increment 1.1.1.0 mask 255.255.255.0
```

Step 5 Configure HA redundancy mode as active-active with preferred-role set to secondary.

```
ha redundancy-mode active-active preferred-role secondary revertive
```

Step 6 Save the configuration.

```
copy running-config startup-config
```

Step 7 Reload both SAMI A and B. Failure to do so results in incorrect HA configuration and deployment.

Step 8 When both SAMI A and B are reset at about the same time, the result is:

Slot 3	Slot 4
PPC3 (Active)	PPC3 (Standby)
PPC4 (Standby)	PPC4 (Active)

Step 9 If the reset didn't happen at the same time, the result is:

Slot 3	Slot 4
PPC3 (Active)	PPC3 (Standby)
PPC4 (Active)	PPC4 (Standby)

Step 10 Slot 3/PPC 4 will then reset due to the revertive option, so the redundant pair will become:

Slot 3	Slot 4
PPC3 (Active)	PPC3 (Standby)
PPC4 (Standby)	PPC4 (Active)

Role Revert After Failover

Network topology ensures that the traffic is distributed across the two IPSec gateways in order to avoid a single point of failure. During a failover scenario, traffic is switched to only the secondary IPSec gateway. When the failed primary card comes back, traffic still flows to only the secondary IPSec gateway. The WSG allows you to restore traffic flow to the primary IPSec gateway so that traffic remains distributed.

The procedure to revert back after a failover is as follows:

1. After a failover, the secondary card comes up as active.
2. When the primary card comes back up as the standby, IKE/IPSec data is synced to the standby card (which is still configured as the primary).
3. The secondary card that is active is then reset.
4. The primary card becomes active again. After the reset, the secondary card becomes standby again.



Note

In an active-active redundancy configuration, the revertive option is mandatory. In the case where an active PPC configured as primary revertive fails over, upon coming back up the PPC regains the active role from the redundant PPC.

Configuring Application VLAN/Alias IP Address

For each PPC processor on the SAMI, configure a VLAN with an IP address. This IP address is used by the IKE and ESP traffic from the endpoints. In case of redundancy, this is the same VLAN number configured on both the active and standby PPCs. The alias IP address is configured for a VLAN on both the active and standby PPCs. FAP/HNB uses the alias IP address instead of the active IP address. This alias IP address must be in the same subnet as the VLAN's active IP address. When a failover occurs, the newly active node starts receiving traffic destined to this alias IP address.



Note

Sharing of the same VLAN ID with different PPC's on SAMI WSG is not supported unless if it is for HA VLAN interface.

In the following example, WSG A is configured with public IP address 88.88.23.33, WSG B is configured with public IP address 88.88.23.34, and the alias IP address is 88.88.23.35. In this case, traffic is sent to the alias IP address, 88.88.23.35. If the active WSG A fails, the standby WSG B takes over, and the newly active WSG B keeps the same tunnel state with the same alias IP address.

The following example shows how to configure the alias IP address on two WSGs:

WSG A, Slot 1/PPC3:

```
WSG (config) # interface vlan 50
WSG (config-if) # ip address 88.88.23.33 255.255.255.0
WSG (config-if) # alias 88.88.23.35 255.255.255.0
```

WSG B, Slot 3/PPC3:

```
WSG (config) # interface vlan 50
WSG (config-if) # ip address 88.88.23.34 255.255.255.0
WSG (config-if) # alias 88.88.23.35 255.255.255.0
```

Configuring High Availability on SAMI COSLI

In the SAMI COSLI HA infrastructure, a cluster contains a pair of PPCs from two SAMIs, which can be on the same (intra-chassis) or different (inter-chassis) Cisco 7600 router chassis. The PPCs with the same number on a redundant pair of SAMIs are paired together (e.g. SAMI A, Slot 1/PPC3 is paired with SAMI B, Slot 2/PPC3). To accomplish this, configure a unique subnet for these two PPCs.

In the active-standby redundancy mode, for a redundant pair of SAMIs, there are 6 different subnets configured for 6 pairs of PPCs. Even though 6 pairs of PPCs between the two SAMIs are paired independently, all 6 PPCs on the same SAMI are assigned the same role (either active or standby). Configure the same preferred role (either primary or secondary) for all 6 PPCs on each SAMI. A failure from any PPC triggers a switchover to the other SAMI.

In the active-active redundancy mode, only the PPC3 and PPC4 pairs between the SAMIs are used.

There are two kinds of CLIs on COSLI for configuring high availability: node specific CLIs (e.g. the IP address of the node) or non-node specific CLIs (e.g. SNMP). All node specific CLIs have to be entered on each PPC. Non-node specific CLIs are not available when a SAMI is in standby mode. The HA infrastructure filters these CLIs out when syncing between a pair of PPCs.

Configuring the VLAN/IP Address for HA Infrastructure

The HA VLAN and IP addresses are used internally by the HA infrastructure to communicate among the nodes in the same cluster (subnet). To configure VLAN and IP addresses, perform the following steps:

	Command	Purpose
Step 1	WSG> enable	Enables privileged EXEC mode.
Step 2	WSG# configure terminal	Enters global configuration mode.
Step 3	WSG(config)# ha interface vlan <i>vlan_ID</i>	Configures the VLAN for HA functionality.
Step 4	WSG(config)# ip address <i>ip_address</i> <i>netmask</i>	IP address and subnet netmask for this interface.

**Note**

These CLI commands must be configured on each PPC. The two PPCs that are to be paired together must be configured to have the same VLAN ID. As a result, 6 different VLAN IDs are used for 6 pairs of PPCs. If you only need to configure site-to-site (S2S) tunnels, only PPC3 needs to be configured. The other PPCs are left unconfigured.

**Note**

Starting in WSG Release 4.0, S2S is supported on PPC3 only (HA active-standby mode) or PPC3 and PPC4 (HA active-active mode).

**Note**

You must also configure these VLANs on the SUP.

The following example shows how to configure the HA VLAN ID and IP addresses for PPC3:

On Slot 1/PPC3:

```
WSG(config)# ha interface vlan 611
WSG(config-if)# ip address 11.11.1.13 255.255.255.0
```

On Slot 3/PPC3:

```
WSG(config)# ha interface vlan 611
WSG(config-if)# ip address 11.11.1.23 255.255.255.0
```

Single Point Configuration of VLAN/IP Address for HA Infrastructure

To configure the VLAN and IP address using a single point configuration, perform the following steps:

	Command	Purpose
Step 1	WSG> enable	Enables privileged EXEC mode.
Step 2	WSG# configure terminal	Enters global configuration mode.
Step 3	WSG(config)# ha interface vlan start-id vlan_ID increment increment vlan_ID	Configures the VLAN using a single point configuration.
Step 4	WSG(config)# ip address start-ip ip_address increment increment ip_address netmask	IP address and subnet netmask for this interface.

These CLI commands are available in the entity-all mode on the director PPC (PPC3).

If you execute the following CLI commands on the PPC3:

```
WSG(mode-all)(config)# ha interface vlan start-id 212 increment 2
WSG(mode-all)(config-if)# ip address start-ip 11.11.1.11 increment 0.0.1.2 mask
255.255.255.0
```

The configurations of the 6 PPCs will be:

PPC3:

```
WSG(config)# ha interface vlan 212
WSG(config-if)# ip address 11.11.1.11 255.255.255.0
```

PPC4:

```
WSG(config)# ha interface vlan 214
WSG(config-if)# ip address 11.11.2.13 255.255.255.0
```

PPC5:

```
WSG(config)# ha interface vlan 216
WSG(config-if)# ip address 11.11.3.15 255.255.255.0
```

PPC6:

```
WSG(config)# ha interface vlan 218
WSG(config-if)# ip address 11.11.4.17 255.255.255.0
```

PPC7:

```
WSG(config)# ha interface vlan 220
WSG(config-if)# ip address 11.11.5.19 255.255.255.0
```

PPC8:

```
WSG(config)# ha interface vlan 222
WSG(config-if)# ip address 11.11.6.21 255.255.255.0
```

Configuring Redundancy-mode and Preferred-role

To configure the redundancy mode of the HA feature, perform the following steps:

	Command	Purpose
Step 1	WSG> enable	Enables privileged EXEC mode.
Step 2	WSG# configure terminal	Enters global configuration mode.
Step 3	WSG(config)# ha redundancy-mode {active-active active-standby} preferred-role {primary secondary} [revertive]	The preferred-role is used to indicate which node should come up as active (primary) or standby (secondary) when both nodes are rebooted at about the same time.

The **preferred-role** is used to indicate which node should come up as active (primary) or standby (secondary) when both nodes are rebooted at about the same time.

The following example shows how to configure a redundant pair of PPCs in active-standby redundancy mode:

On Slot 3/PPC3:

```
WSG(config)# ha redundancy-mode active-standby preferred-role primary
```

On Slot 4/PPC3:

```
WSG(config)# ha redundancy-mode active-standby preferred-role secondary
```



Note

These CLI commands are available only on PPC3. If executed in the **all** mode, the command is applied to all 6 PPCs—the same role is assigned to all 6 PPCs. If the command is executed in the **single** mode, it is applied only to PPC3, and the remaining 5 PPCs will have no redundancy mode configured. The SAMI that is configured with the preferred-role of **secondary** needs to be reset before the redundant pairs can take effect.

The following example shows how to configure a redundant pair of PPCs in active-active redundancy mode:

On Slot 3/PPC3:

```
WSG(config)# ha redundancy-mode active-active preferred-role primary revertive
```

On Slot 4/PPC3:

```
WSG(config)# ha redundancy-mode active-active preferred-role secondary revertive
```



Note

In the active-active redundancy mode, only the PPC3 and PPC4 pairs are used.

Removing HA Redundancy Between a Pair of PPCs

The following example shows how to remove a redundant pair of PPCs in active-standby redundancy mode:

On Slot 3/PPC3:

```
WSG(config)# no ha interface vlan 212
WSG(config)# no ha redundancy-mode active-standby preferred-role primary
```

On Slot 4/PPC3:

```
WSG(config)# no ha interface vlan 212
WSG(config)# no ha redundancy-mode active-standby preferred-role secondary
```

The following example shows how to remove a redundant pair of PPCs in active-active redundancy mode:

On Slot 3/PPC3:

```
WSG(config)# no ha interface vlan 212
WSG(config)# no ha redundancy-mode active-active preferred-role primary revertive
```

On Slot 4/PPC3:

```
WSG(config)# no ha interface vlan 212
WSG(config)# no ha redundancy-mode active-active preferred-role secondary revertive
```



Note

You must clean up the remaining (non-HA) configuration and bring the system back to operational state. The system will not be automatically rebooted as a result of removing the HA configuration.

Verifying the HA Configuration

Use the following commands to display information about the HA state at various levels:

	Command	Purpose
Step 1	WSG> enable	Enables privileged EXEC mode.
Step 2	WSG# show ha info brief show ha info show ha info detail	Displays various levels of HA information.

The **show ha info** command shows the configuration, states, and statistics of the local node and its peer:

```
WSG# show ha info
Redundancy mode (configured) : active-standby
Redundancy state : Redundant
My Node
  Current State : Active
  Preferred Role : Primary
  IP Address    : 51.51.51.43
  Slot/PPC     : 4/3
Peer Node
  IP Address    : 51.51.51.53
  Slot/PPC     : 5/3
Bulk Sync Status : Success
Bulk Sync done  : Thu Sep 15 01:24:36 2011
HA Revertive   : Disabled
```

```
S2P4# sh ha info
Redundancy mode (configured) : Active-Active
Redundancy state : Redundant
My Node
  Current State : Active
  Preferred Role : Primary
  IP Address    : 77.77.84.24
  Slot/PPC     : 2/4
Peer Node
  IP Address    : 77.77.84.34
  Slot/PPC     : 3/4
Bulk Sync Status : Success
Bulk Sync done  : Tue Jun 19 06:54:38 2012
HA Revertive   : Enabled
```

The **show ha info brief** command shows the configuration and the state of the local node:

WSG# **show ha info brief**

Interface	IP-Address	Redundancy-State	Mode	Current-State	Preferred-Role	HA-Revertive
VLAN51	51.51.51.43	Redundant	active-standby	Active	Primary	Disabled

S2P4# **show ha info brief**

Interface	IP-Address	Redundancy-State	Mode	Current-State	Preferred-Role	Revertive
VLAN2084	77.77.84.24	Redundant	Active-Active	Active	Primary	Enabled

The **show ha info detail** command includes extra information about the cluster and node names:

WSG# **show ha info detail**

Redundancy mode (configured) : active-standby

Redundancy state : Redundant

My Node

nodename : node1

Current State : Active

Last State : Un-assigned

Preferred Role : Primary

IP Address : 51.51.51.43

Slot/PPC : 4/3

Peer Node

nodename : node2

IP Address : 51.51.51.53

Slot/PPC : 5/3

Bulk Sync Status : Success

Bulk Sync done : Thu Sep 15 01:24:36 2011

HA Revertive : Disabled

ISync Counters

Total Request Sent : 0

Total Response Rcvd : 0

Total Fail Count : 0

Total Request Rcvd : 0

Total Response Sent : 0

Cluster : cluster12

Active Mgr : node1

Standby Mgr : node2

```
S2P4# show ha info detail
Redundancy mode (configured) : Active-Active
Redundancy state : Redundant
My Node
  nodename : node1
  Current State : Active
  Last State : Un-assigned
  Preferred Role : Primary
  IP Address : 77.77.84.24
  Slot/PPC : 2/4
Peer Node
  nodename : node2
  IP Address : 77.77.84.34
  Slot/PPC : 3/4
Bulk Sync Status : Success
Bulk Sync done : Tue Jun 19 06:54:38 2012
HA Revertive : Enabled
ISync Counters
Total Request Sent : 3
Total Response Rcvd : 3
Total Fail Count : 0
Total Request Rcvd : 0
Total Response Sent : 0
Cluster : cluster12
Active Mgr : node2
Standby Mgr : node1
```

Adding or Removing a Redundant Pair

The following sections describe how to configure, add, and remove redundant nodes:

- [How to Configure Active-Standby Redundancy Before Both SAMIs are in Service](#)
- [How to Configure Active-Active Redundancy Before Both SAMIs are in Service](#)
- [How to Add Standby WSG to an Active WSG Already in Service \(Active-Standby Mode\)](#)
- [How to Remove Standby WSG from an Active WSG Already in Service \(Active-Standby Mode\)](#)

How to Configure Active-Standby Redundancy Before Both SAMIs are in Service

Perform the following steps on the secondary SAMI:

-
- Step 1** Before the secondary SAMI is inserted, please do the following on the SUP:

- Remove the startup-config files for the secondary SAMI on the bootflash or bootdisk:

```
SUP-7600# del bootflash:SLOT2SAMIC*.cfg
```

- Remove the VLAN groups that are tied to the secondary SAMI:

```
SUP-7600# no svclc module 2 vlan-group 2,30,50,70
```

- (Inter-chassis only) Ensure the time is synced between the two SUPs.

Step 2 Insert the secondary SAMI.

Step 3 Add HA VLAN interface for each PPC:

```
switch(config)# ha interface vlan 611
switch(config-if) ip address 11.11.1.2 255.255.255.252
```

Step 4 Add redundancy-mode with preferred-role for each PPC using entity-all option from PPC3:

```
switch(mode-all)(config)# ha redundancy-mode active-standby preferred-role secondary
```

Step 5 Configure all node-specific commands for each PPC:

```
switch(config)# ip route 77.77.77.0 255.255.255.0 88.88.23.1
```

Step 6 Configure alias IP addresses for the WSG for each PPC:

```
switch(config)# interface vlan 50
switch(config-if)# ip address 88.88.23.35 255.255.255.0
switch(config-if)# alias 88.88.11.35 255.255.255.0
```

Step 7 Save the configuration for each PPC:

```
switch# copy running-config startup-config
```

Perform the following steps on the primary SAMI:

Step 1 Add HA VLAN interface for each PPC:

```
switch(config)# ha interface vlan 611
switch(config-if)# ip address 11.11.1.1 255.255.255.252
```

Step 2 Add redundancy-mode with preferred-role for each PPC using entity-all option from PPC3:

```
switch(mode-all)(config)# ha redundancy-mode active-standby preferred-role primary
```

Step 3 Configure all node-specific commands for each PPC:

```
switch(config)# ip route 77.77.77.0 255.255.255.0 88.88.23.1
```

Step 4 Configure alias IP addresses and all other commands for the WSG for each PPC:

```
switch(config)# interface vlan 50
switch(config-if)# ip address 88.88.23.34 255.255.255.0
switch(config-if)# alias 88.88.23.11 255.255.255.0
switch(config)# crypto profile "prof-1"
```

Step 5 Save the configuration for each PPC:

```
switch# copy running-config startup-config
```

Step 6 Check HA status:

```
switch# show ha info
Redundancy mode (configured) : active-standby
```



```

Redundancy state : Non-Redundant
My Node
  Current State : Active
  Preferred Role : Primary
  IP Address    : 11.11.1.1
  Slot/PPC     : 4/3
  Bulk Sync Status : Not-Initiated
  HA Revertive  : Enabled

```

The primary SAMI is now ready for service. There is no need to reboot.

Perform the following steps on the secondary SAMI:

Step 1 Reload the secondary SAMI. While it is booting back up, configure its VLAN groups on the SUP:

```
SUP-7600# svc1c module 2 vlan-group 2,30,50,70
```



Note If this command is not executed before the SAMI comes back up, the SAMI cannot come up as the standby. In this case, repeat Step 1.

Step 2 After the SAMI is back up and running, check HA status:

```

switch# sh ha info
  Redundancy mode (configured) : active-standby
  Redundancy state : Redundant
  My Node
    Current State : Standby
    Preferred Role : Secondary
    IP Address    : 11.11.1.2
    Slot/PPC     : 2/3
  Peer Node
    IP Address    : 11.11.1.1
    Slot/PPC     : 4/3
  Bulk Sync Status : Success
  Bulk Sync done   : Tue May 25 00:13:31 2010
  HA Revertive    : Enabled

```

If the secondary SAMI is not in the standby state, check the following:

- Ensure VLAN groups for this SAMI are added to the SUP
- Ensure preferred roles are configured correctly on both cards
- Ensure the peer's HA IP address is reachable

Step 3 Check whether WSG CLIs are synced from the active card:

```
switch# sh running-config
```

How to Configure Active-Active Redundancy Before Both SAMIs are in Service

Perform the following steps on the secondary SAMI:

Step 1 Before the secondary SAMI is inserted, please do the following on the SUP:

- Remove the startup-config files for the secondary SAMI on the bootflash or bootdisk:

```
SUP-7600# del bootflash:SLOT2SAMIC*.cfg
```

- Remove the VLAN groups that are tied to the secondary SAMI:

```
SUP-7600# no svclc module 2 vlan-group 2,30,50,70
```

- (Inter-chassis only) Ensure the time is synced between the two SUPs.

Step 2 Insert the secondary SAMI.

Step 3 Add HA VLAN interface for each PPC:

```
switch(config)# ha interface vlan 611
switch(config-if) ip address 11.11.1.2 255.255.255.252
```

Step 4 Add redundancy-mode with preferred-role for each PPC using entity-all option from PPC3:

```
switch(mode-all)(config)# ha redundancy-mode active-active preferred-role secondary
revertive
```

Step 5 Configure all node-specific commands for each PPC:

```
switch(config)# ip route 77.77.77.0 255.255.255.0 88.88.23.1
```

Step 6 Configure alias IP addresses for the WSG for each PPC:

```
switch(config)# interface vlan 50
switch(config-if)# ip address 88.88.23.35 255.255.255.0
switch(config-if)# alias 88.88.11.35 255.255.255.0
```

Step 7 Save the configuration for each PPC:

```
switch# copy running-config startup-config
```

Perform the following steps on the primary SAMI:

Step 1 Add HA VLAN interface for each PPC:

```
switch(config)# ha interface vlan 611
switch(config-if)# ip address 11.11.1.1 255.255.255.252
```

Step 2 Add redundancy-mode with preferred-role for each PPC using entity-all option from PPC3:

```
switch(mode-all)(config)# ha redundancy-mode active-active preferred-role primary
revertive
```

Step 3 Configure all node-specific commands for each PPC:

```
switch(config)# ip route 77.77.77.0 255.255.255.0 88.88.23.1
```

Step 4 Configure alias IP addresses and all other commands for the WSG for each PPC:

```
switch(config)# interface vlan 50
switch(config-if)# ip address 88.88.23.34 255.255.255.0
switch(config-if)# alias 88.88.23.11 255.255.255.0
switch(config)# crypto profile "prof-1"
```

Step 5 Save the configuration for each PPC:

```
switch# copy running-config startup-config
```

Step 6 Check HA status:

```

S2P4# sh ha info
Redundancy mode (configured) : Active-Active
Redundancy state : Redundant
My Node
  Current State : Active
  Preferred Role : Primary
  IP Address : 11.11.1.1
  Slot/PPC : 2/4
Peer Node
  IP Address : 11.11.1.2
  Slot/PPC : 3/4
Bulk Sync Status : Success
Bulk Sync done : Tue Jun 19 06:54:38 2012
HA Revertive : Enabled

```

The primary SAMI is now ready for service. There is no need to reboot.

Perform the following steps on the secondary SAMI:

Step 1 Reload the secondary SAMI. While it is booting back up, configure its VLAN groups on the SUP:

```
SUP-7600# svc1c module 2 vlan-group 2,30,50,70
```



Note If this command is not executed before the SAMI comes back up, the SAMI cannot come up as the standby. In this case, repeat Step 1.

Step 2 After the SAMI is back up and running, check HA status:

```

S2P4# sh ha info
Redundancy mode (configured) : Active-Active
Redundancy state : Redundant
My Node
  Current State : Standby
  Preferred Role : Secondary
  IP Address : 11.11.1.2
  Slot/PPC : 3/4
Peer Node
  IP Address : 11.11.1.1
  Slot/PPC : 2/4
Bulk Sync Status : Success
Bulk Sync done : Tue Jun 19 06:54:38 2012
HA Revertive : Enabled

```

If the secondary SAMI is not in the standby state, check the following:

- Ensure VLAN groups for this SAMI are added to the SUP
- Ensure preferred roles are configured correctly on both cards
- Ensure the peer's HA IP address is reachable

Step 3 Check whether WSG CLIs are synced from the active card:

```
switch# sh running-config
```

How to Add Standby WSG to an Active WSG Already in Service (Active-Standby Mode)

Perform the following step on the active SAMI:

Step 1 Ensure the active SAMI is not paired with another SAMI:

```
switch# show ha info
Redundancy mode (configured) : active-standby
Redundancy state : Non-Redundant
My Node
  Current State : Active
  Preferred Role : Primary
  IP Address : 11.11.1.1
  Slot/PPC : 4/3
  Bulk Sync Status : Not-Initiated
  HA Revertive : Enabled
```

If it has a peer SAMI, follow the procedure in the section below to remove the standby WSG.

The preferred-role should be set to primary. If not, set it to primary using the **ha redundancy-mode** command (this will not impact service):

```
switch(mode-all)(config)# ha redundancy-mode active-standby preferred-role primary
```

Perform the following steps on the secondary SAMI:

Step 1 Before the secondary SAMI is inserted, please do the following on the SUP:

- Remove the startup-config files for the secondary SAMI on the bootflash or bootdisk:

```
SUP-7600# del bootflash:SLOT2SAMIC*.cfg
```

- Remove the VLAN groups that are tied to the secondary SAMI:

```
SUP-7600# no svcl module 2 vlan-group 2,30,50,70
```

- (Inter-chassis only) Ensure the time is synced between the two SUPs.

Step 2 Insert the secondary SAMI.**Step 3** Add HA VLAN interface for each PPC:

```
switch(config)# ha interface vlan 611
switch(config-if) ip address 11.11.1.2 255.255.255.252
```

Step 4 Add redundancy-mode with preferred-role for each PPC using entity-all option from PPC3:

```
switch(mode-all)(config)# ha redundancy-mode active-standby preferred-role secondary
```

Step 5 Configure all node-specific commands for each PPC:

```
switch(config)# ip route 77.77.77.0 255.255.255.0 88.88.23.1
```

Step 6 Configure alias IP addresses for the WSG for each PPC:

```
switch(config)# interface vlan 50
switch(config-if)# ip address 88.88.23.35 255.255.255.0
switch(config-if)# alias 88.88.11.35 255.255.255.0
```

Step 7 Save the configuration for each PPC:

```
switch(config)# copy running-config startup-config
```

Step 8 Reload the secondary SAMI. While it is booting back up, configure its VLAN groups on the SUP:

```
SUP-7600# svcl module 2 vlan-group 2,30,50,70
```



Note If this command is not executed before the SAMI comes back up, the SAMI cannot come up as the standby. In this case, repeat Step 1.

Step 9 After the SAMI is back up and running, check HA status:

```
switch# sh ha info
Redundancy mode (configured) : active-standby
Redundancy state : Redundant
My Node
  Current State : Standby
  Preferred Role : Secondary
  IP Address    : 11.11.1.2
  Slot/PPC     : 2/3
Peer Node
  IP Address    : 11.11.1.1
  Slot/PPC     : 4/3
Bulk Sync Status : Success
Bulk Sync done   : Tue May 25 00:13:31 2010
HA Revertive    : Enabled
```

If the secondary SAMI is not in the standby state, check the following:

- Ensure VLAN groups for this SAMI are added to the SUP
- Ensure preferred roles are configured correctly on both cards
- Ensure the peer's HA IP address is reachable

Step 10 Check whether WSG CLIs are synced from the active card:

```
switch# sh running-config
```

How to Remove Standby WSG from an Active WSG Already in Service (Active-Standby Mode)

Perform the following steps on the secondary SAMI:

Step 1 Ensure the secondary SAMI is in the standby state and paired with an active WSG:

```
switch# sh ha info
Redundancy mode (configured) : active-standby
Redundancy state : Redundant
My Node
  Current State : Standby
  Preferred Role : Secondary
  IP Address    : 11.11.1.2
  Slot/PPC     : 2/3
Peer Node
  IP Address    : 11.11.1.1
  Slot/PPC     : 4/3
Bulk Sync Status : Success
Bulk Sync done   : Tue May 25 00:13:31 2010
HA Revertive    : Enabled
```

Step 2 Remove the VLAN groups that are tied to this SAMI from the SUP:

```
SUP-7600# no svc1c module 2 vlan-group 2,30,50,70
```

Step 3 Remove the VLAN interfaces that have alias IP address configured for each PPC:

```
switch(config)# no interface vlan 50
```

Step 4 Remove HA VLAN interface for each PPC:

```
switch(config)# no ha interface vlan 611
```

Step 5 Remove redundancy-mode with preferred-role for each PPC using entity-all option from PPC3:

```
switch(mode-all)(config)# no ha redundancy-mode active-standby preferred-role
secondary
```

Step 6 Save the configuration for each PPC:

```
switch(config)# copy running-config startup-config
```

WSG Deployment Modes

Site-to-site or remote access tunnels can be established using active-active HA redundancy mode, but you must switch between WSG deployment modes. The two deployment modes are site-to-site and remote-access. Switch between the two modes by first deactivating all profiles and reloading the SAMIs. Once the SAMIs are back up, activate the particular profile. Depending on the profile type, only tunnels of that type can be established while being in that deployment mode. Verify the deployment mode using the **show crypto deployment-mode** CLI command.

Bulk Sync

Bulk sync procedure involves the configuration sync of the standby SAMI with the active SAMI, when a card running with the **no** redundancy scheme is configured for redundancy, and it subsequently receives a standby notification.

The configuration sync done on the standby card is a two part sync procedure; the first part involves syncing the running configuration from the active card, and the second part consists of syncing the startup configuration of the active card. These two config sync are autonomous in operation. The module that is responsible for carrying out this bulk sync procedure is the configuration controller.



Note

In the active-active HA redundancy mode, bulk sync takes place between the PPC pairs and not the SAMI pairs.

Bulk Sync Procedure

When the config-controller is assigned the active role, it performs the following actions:

- If assigned the active role, it parses the startup-config file and applies all the commands except the HA-specific CLIs (HA-specific commands are applied during bootup before the role is assigned).

If the config-controller is assigned a standby role, it will perform the following actions:

- If it is assigned the standby role, it sends a bulk-sync request to the active peer PPC.
- Upon receiving the bulk-sync request, the config-controller on the active peer strips the node-specific CLIs from the running-configuration, and transfers them to the standby card.
- The standby card applies those CLIs.
- After it completes the running-configuration, the config-controller performs the same procedure on the startup-configuration. The standby card merges it with its own node-specific commands in the startup-configuration, and saves it to the SUP.
- Notifies the HA manager that it is now Standby-Ready.

In active-active HA redundancy mode, bulk sync takes place between PPC pairs and not between SAMI pairs.

Incremental Sync

When a non-node-specific command is applied to the active card, the configuration needs to be sent to the standby peer, if it exists. A registered callback function for that command is invoked on the standby peer to apply it locally.

A message is sent to the standby peer when a **copy running-config startup-config** is applied on the active card. The startup-config file for the standby peer is saved on the SUP.

Failover

When a fatal error is detected on a node of the active card, the process is terminated due to the setting in the information model. Since the HA configuration for the system manager is set to **reset** for the restart option, it causes the SAMI to reboot. The standby card gets notification from the cluster manager to go active. The newly-active node configures the alias IP address and sends an ARP announcement for this alias IP address, if it is configured.

When a fatal error is detected on a node of the standby card, the standby card reboots.

In active-active HA redundancy mode, failover can occur between PPC pairs without affecting other PPC pairs on the SAMIs involved.

Configuring Revert Back After Failover

Reverting back after failover may not be required for all the deployment scenarios, so this functionality is configurable.

In WSG releases prior to 4.0, perform the following tasks to enable the revert-back feature:

	Command	Purpose
Step 1	WSG> enable	Enables privileged EXEC mode.
Step 2	WSG# configure terminal	Enters global configuration mode.
Step 3	WSG(config)# ha revertive	Resets the active card on secondary. This ensures that card that is configured as primary always has the state as active, and the secondary card has the standby state. This is a non-node specific command so that it is also synched across the standby.

Starting in WSG Release 4.0, the **ha revertive** functionality is replaced by a configurable option in the **ha redundancy-mode** command using the **revertive** keyword.

	Command	Purpose
Step 1	WSG> enable	Enables privileged EXEC mode.

	Command	Purpose
Step 2	WSG# configure terminal	Enters global configuration mode.
Step 3	WSG(config)# ha redundancy-mode {active-standby active-active} preferred-role {primary secondary} [revertive]	Resets the active card on the secondary to ensure that the primary card has the active state and the secondary card has the standby state. The revertive keyword is optional for the active-standby mode but required for the active-active mode.

The failover revert-back configuration is displayed in the output of **show ha info** and **show ha info brief** commands. Follow these steps to revert back after a failover:

1. Failover occurs on SAMI 1 (preferred-role = primary, state = active).
2. SAMI 2 (preferred-role = secondary, state = standby) transitions to active state.
3. SAMI 1 comes up again, and COSLI bulk sync occurs with SAMI 2.
4. WSG also bulk syncs all of its data with SAMI 2. Once the bulk sync is complete, the WSG application on SAMI 2 indicates this to the configuration controller using a new MTS message.
5. The configuration controller FSM handles this new event from the WSG in its event handler of active state.
6. In this event handler, the configuration controller first checks if the **ha revertive** command is configured. If command is not configured, no action is taken. Otherwise, step 7 is performed.
7. In case the configured **preferred-role** of the node is **secondary** and the HA state is active, SAMI 2 reloads.
8. SAMI 1 transitions to active state, and SAMI 2 comes up in standby state.

IKE SA Handling

IKE SA Create

IKE SAs are created on the standby WSG when IKE SAs are created on the active WSG.

IKE SA Update

IKE SAs are updated on the standby when IKE SAs are updated on the active for following reasons:

- IKE SA window has been updated due to initiator or responder exchange
- Remote access attributes have been set
- NAT reboot has been detected and IKE SA remote address or port has changed

IKE SA Rekey

Rekeyed IKE SA is imported, and the old IKE is deleted on the standby WSG when the IKE SA is rekeyed on the active WSG.

IKE SA Delete

IKE SAs are deleted on the standby WSG when the IKE SAs are deleted on the active WSG.

IKE Message ID

The WSG synchronizes IKE Message IDs between the active and standby WSGs, otherwise IKE SAs are unusable. If an informational exchange like DPD is performed after the SA is imported on the standby, the SA needs to be updated.

The WSG maintains the DPD initiation/response successfully after failover. Additionally, the WSG maintains IKE parameters (like encryption and hashing Algorithms), and Diffie-Hellman groups after failover.

IKE SA Life Time

The WSG maintains the Phase 1 lifetime value instead of resetting on the newly active after failover.

IKE NAT Keepalives

The WSG maintains the different NAT states after failover. NAT keepalives are still successfully initiated and responded to after failover, and on time.

IPSec SA Handling

IPSec SA Create

IPSec SAs are created on the standby WSG when IPSec SAs are created on the active WSG.

IPSec SA Update

IPSec SAs are updated on the standby when IPSec SAs are updated on the active for following reason:

- NAT reboot is detected for the parent IKE SA, and the peer address or port has changed.

IPSec SA Rekey

Rekeyed IPSec SA are imported, and old IPSec is deleted on the standby WSG when the IPSec SA is rekeyed on the active WSG.

IPSec SA Delete

IPSec SAs are deleted on the standby WSG when the IPSec SAs are deleted on the active WSG.

IPSec SA Parameters

WSG maintains IPSec parameters protocol, encryption and authentication algorithms, PFS groups, anti-replay window size, and sequence numbers both 32 bit and 64 bit (ESN). It also maintains UDP encapsulation after failover.

IPSec SA Life Time

The WSG maintains the Phase 1 lifetime value instead of resetting on the new active after failover.

IPSec Outbound SA Sequence Numbers

The Sequence number is incremented for each data packet transmitted. 32 bit Sequence number is transmitted in the ESP header of each packet. In case of ESN, only the lower 32 bit sequence number is transmitted. The high-order 32 bits are maintained as part of the sequence number counter by both transmitter and receiver, and are included in the computation of the ICV. If the receiver receives a sequence number lower than the expected number, the packets may be dropped depending on Anti-replay parameters.

The WSG on standby updates the outbound sequence number of the IPSec SA to the estimated value, otherwise the sequence number goes out sync.

IKE and IPSec SAs are imported to the standby when it comes up. During import, the policy manager calls the fast API to Program Nitrox and IXP modules for inbound and outbound SAs. Outbound sequence number is the estimated sequence number based on IMIX or 64-byte traffic.

The sequence number is updated from the active to the standby at periodic intervals. The policy manager triggers the fast API to Program Nitrox and IXP modules for each periodic update.

seqnumber = active sequence number + estimated sequence number (packets processed for 5 minutes)

IPSec SA Replay Window

The WSG on the standby updates inbound anti-replay window base and mask of IPSec SA to prevent replay attack. The base value is the highest sequence number that has been received so far. This will limit the number of packets that can be replayed after a failover.

The Anti-replay window base and mask is updated periodically from the active to the standby at regular intervals.

When the standby comes up, IKE and IPSec SAs are imported to the standby. During import, the policy manager calls fast API to Program Nitrox and IXP modules for inbound and outbound SAs.

Certificate, CRL, DNS Handling

The WSG maintains certificate status between the the active and standby (Local Certificate, private keys and trustpoint certificates should be synced between the redundant pair) by using sync message or export and import mechanism. When a new standby WSG is inserted, the static certificates are synced to the standby. WSG does not maintain the DNS and CRL cache across failover. The DNS and CRLs are cached on the new active during new tunnel establishment.

Configuring IPSec

To protect addresses to which traffic is allowed from the tunnel, perform the following tasks:

	Command	Purpose
Step 1	switch# config	Enters global configuration mode.
Step 2	switch (config)# crypto profile P1 switch(config-crypto-profile)# ipsec	Enters IPSec submodule.

	Command	Purpose
Step 3	<pre>switch(config-crypto-profile-ipsec)# remote-access: access-permit ip ip-address subnet subnet site-to-site: access-permit rule name protocol {any sctp udp tcp} [src-ip start src ip end src ip src-port start src port end src port dst-ip start dst ip end dst ip dst-port start dst port end dst port]</pre>	<p>Configures the protected IP address to which traffic is allowed from a remote access tunnel, or traffic selectors and multiple child SA features for site-to-site tunnels.</p> <p>In the 1.2 Release, the <i>rule name</i> argument is added, and applies to site-to-site type profiles only. The remote-access type profile still accepts the short access-permit syntax.</p>
Step 4	<pre>switch(config-crypto-profile-ipsec)# transform-set esp aes256 aes-xcbc</pre>	<p>Configures the Encapsulating Security Payload (ESP) encryption and hash type. ESP is a security protocol that gives data privacy services, data authentication, and anti-replay services. ESP encapsulates data to be protected.</p>
Step 5	<pre>switch(config-crypto-profile-ipsec)# pfs {group1 group2 group5 group14 group15 group16 group17 group18}</pre>	<p>Sets a Perfect Forward Secrecy (PFS) group ID to use for negotiations during a new SA exchange</p>
Step 6	<pre>ip address-pool myPool</pre>	<p>Sets the address-pool name to be used in this profile.</p> <p>Note This step is optional for site-to-site profiles.</p>

```
WSG# config
Enter configuration commands, one per line. End with CNTL/Z.
WSG (config)# crypto profile remote-access
WSG (config-crypto-profile)# ipsec
WSG (config-crypto-profile-ipsec)# access-permit ip 100.1.3.0 subnet 24
```

Here is an example of the new **access-permit** command with the **protocol** options:

```
access-permit nameA
  protocol udp src-ip 12.12.12.1 12.12.12.20 src-port 23 23 dst-ip 0.0.0.0
255.255.255.255 dst-port 0 65535
  protocol tcp src-ip 12.12.12.1 12.12.12.20 src-port 23 23 dst-ip 0.0.0.0
255.255.255.255 dst-port 0 65535

access-permit nameB
  protocol any src-ip 13.13.13.1 13.13.13.20 src-port 23 23 dst-ip 0.0.0.0
255.255.255.255 dst-port 0 65535
```

Site-to-Site Scalability

In site-to-site (S2S) scenario, tunnels are established between the WSG and the remote peer just like in a remote access scenario. The source of the traffic inside the tunnel is from multiple IP addresses on the remote peer's side. As in the remote access scenario, the addresses on the trusted network behind the WSG can be a single IP or a network.

Additionally, in a S2S scenario, the remote peer can setup multiple tunnels to the WSG.

The TS can contain the protocol, source port range and destination port range, in addition to the source and destination IP range.

In case of site-to-site type tunnels, the WSG can initiate the tunnels to the peer device.

**Note**

DHCP is supported for RAS profiles and not for site-to-site profiles.

Scalability and Throughput Improvement Description

In previous WSG releases, the S2S traffic selector lookup was done by looking up an array of TS on the IXP. This linear search limited the performance of the site-to-site traffic selector lookup algorithm. In WSG Release 2.0 and above, the traffic selector lookup algorithm speeds up the performance for site-to-site. There is no change to the remote access traffic selector lookup because it is different from the lookup algorithm for site-to-site, and is already optimized.

The new site-to-site traffic selector lookup is based on a hash lookup of the packet's source and destination IP addresses after applying a network mask.

The list of source-mask and destination-mask combinations needs to be provided by the user through the CLI. The size of this list is limited to 6 entries. For best performance, the subnet combination that carries the most traffic needs to be configured on the top of the list.

The subnet combination values need to be figured out during network design and configured initially. Graceful addition, modification, and deletion of entries is not supported once the S2S profiles are activated. To modify the subnet combination configuration, deactivate all S2S profiles, change the subnet combination configuration, and then reactivate the S2S profiles. All established tunnels are lost during this procedure.

The **access-permit** command under site-to-site profile now accepts a netmask instead of an end IP address. The access-permit network configured for a profile can be larger than what is negotiated by a remote peer. This allows multiple peers to connect to the same site-to-site profile, and negotiate a subnet of the configured network. The TS negotiated by the peers of a WSG must be unique (no overlap).

The negotiated TS for the tunnels must be subnets, and not arbitrary ranges.

When a peer negotiates the TS with WSG, it must intersect one of the configured entries in the subnet combination table. If not, the negotiation is rejected. Debug and syslog messages are generated if tunnel negotiation fails under this condition.

TS negotiations based on protocol and port are also supported, but algorithm improvements only take effect when the different child SAs have TS that have unique source and destination IP subnets. There is a performance decrease if there are child SAs that differ only by port or protocol in their TS.

Upto 16666 S2S tunnels are supported per SAMI. S2S tunnels can only be configured on the director PPC.

WSG Release 2.0 and above does not support the IKE protocol that allows a peer to negotiate multiple TSs for the same S2S tunnel. Each S2S tunnel can negotiate only one TS. All other features that are currently supported for site-to-site and remote access are maintained in this release.

Configuring Scalability and Throughput

To configure the WSG to accept the netmask for the source and destination IP address, perform the following tasks:

	Command	Purpose
Step 1	WSG# config	Enters global configuration mode.

	Command	Purpose
Step 2	WSG (config)# crypto profile P1 WSG(config-crypto-profile)# ipsec	Enters IPsec submode.
Step 3	WSG(config-crypto-profile-ipsec)# access-permit rule name protocol {any sctp udp tcp} [src-ip src ip/subnet size src-port start src port end src port dst-ip dst ip/subnet size dst-port start dst port end dst port]	Configures the protected IP address to which traffic is allowed from a remote access tunnel, or traffic selectors and multiple child SA features for site-to-site tunnels. The <i>src ip/ subnet size</i> and <i>dst ip/subnet size</i> arguments apply to only site-to-site type profiles. The remote-access type profile still accepts the short access-permit syntax.

Here is an example of the configuration:

```
WSG(config-crypto-profile-ipsec)#
access-permit nameA
    protocol udp src-ip 12.12.0.0 16 src-port 23 23 dst-ip 10.10.10.0 24 dst-port 0 65535

access-permit nameB
    protocol any src-ip 13.13.13.0 24 src-port 23 23 dst-ip 44.44.44.44 32 dst-port 0
65535
```

Configuring Subnet Combination

This command assists the IXP for site-to-site performance improvement. This configuration is made based on the design of the network.

It is mandatory to enter one or more of this command before activating any S2S profiles. S2S profile cannot be activated if this command is not configured on the WSG.

To enable this feature, perform the following tasks:

	Command	Purpose
Step 1	WSG# config	Enters global configuration mode.
Step 2	WSG (config)# crypto profile P1	Enters IPsec submode.
Step 3	WSG(config)# crypto site-to-site-lookup priority priority source-netmask src-netmask destination-netmask dst-netmask	Configures the list of source-mask and destination-mask combinations. <i>priority</i> —Priority of this lookup. The range is 1 to 6 <i>src-netmask</i> —Source IP network mask in format N. The N subnet mask format is increased from 0-32 to 0-128 for IPv6. <i>dst-netmask</i> —Destination IP network mask in format N. The N subnet mask format is increased from 0-32 to 0-128 for IPv6.

Here is an example of the configuration:

```
crypto site-to-site-lookup priority 5 source-netmask 112 destination-netmask 112
```

Certificate Management Protocol

WSG releases prior to Release 2.0 can generate a private key, a certificate request and support manual enrollment with CA server. WSG Release 2.0 introduced support for Certificate Management Protocol (CMPv2). CMP allows for automatic enrollment with CA server. The Keypair is generated locally and the certificate request can be sent to CA server using existing network connectivity. The certificate can be downloaded without the need for manual intervention.

Only one outstanding CMPv2 initialize, enroll, or update request is permitted at any time from a WSG. You can place a new request after the certificate is obtained for the outstanding request. Alternatively, you can clear the pending request and place a new request. The certificate and the private key will be saved on the SUP. If the SUP is redundant, the files are also copied to the redundant SUP.

In case of the WSG HA, the certificate is copied over to the SUP on the redundant chassis only when the certificate configuration command is entered. If the SUP on the secondary chassis is redundant, the certificate is also copied to the redundant SUP.

Files written to the SUP storage cannot be deleted using the WSG CLI. They need to be deleted using the SUP CLI. Revoke and recover functions are not supported in WSG Release 2.0 and above.

**Note**

A pending CMPv2 request from the WSG is not saved across reboots or WSG switchover. Do not reboot the WSG when a request is pending. If the WSG is rebooted or switched over during a pending request, the request must be reinitiated.


This feature only brings in an additional method of obtaining the certificates for WSG using new EXEC commands. The original manual enrollment process can still be used.


WSG Release 3.0 introduced support for automatic renewal of certificates, which includes automatic update and automatic retrieve. The automatic update of CMPv2 certificates is similar to the WSG CMP update command, but is performed by the system when the certificate is within a specified window before expiring (2 to 60 days). The automatic retrieval of certificates retrieves an updated certificate from the SUP when the certificate is within a specified window before expiring (2 to 60 days). Up to 20 certificates may be configured for automatic renewal.

Prior to Cisco 7600 WSG Release 4.4, WSG supported only TCP as the CMPv2 Transport Protocol. With Release 4.4 and above, WSG will support both transport protocols, TCP and HTTP. The HTTP based flows will be RFC 4210/4211/6712 compliant.

Configuring Certificate Management Protocol

To configure the WSG to generate the private key and make an initialize request to the CA server using CMPv2, perform the following tasks. The filenames for the private key and the certificate files will be automatically generated by the system.

	Command	Purpose
Step 1	<pre>WSG(config)# crypto cmp transport transport protocol</pre>	<p>Configures the Transport Protocol for CMPv2 Messages.</p> <p><i>transport protocol</i>—Transport Protocol options are <i>http</i>, and <i>tcp</i>.</p> <p><i>http</i>—HTTP will be used as transport Protocol for all CMPv2 messages.</p> <p><i>tcp</i>—TCP will be used as transport Protocol for all CMPv2 messages.</p> <p>The default is <i>tcp</i>.</p>
Step 2	<pre>WSG# crypto cmp initialize modulus modulus id-type id-type id id subject-name subject string ca-psk reference-number:key ca-root root certificate ca-url url</pre>	<p>Configures the WSG to generate the private key and make an initialize request to the CA server using CMPv2. This request for the client's initial certificate is authenticated using the reference number and corresponding PSK received from the CA.</p> <p><i>modulus</i>—Modulus of the generated certificate: 512, 1024, or 2048.</p> <p><i>id-type</i>—Type of the ID: fqdn or ip.</p> <p><i>id</i>—Word that is of id-type.</p> <p><i>subject string</i>—Subject string of the certificate in double quotes.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p> Note The supported characters while configuring the subject-name are dash, dot, underscore, a-z, A-Z and 0-9. The maximum size supported for the string is 256 bytes.</p> </div> <p><i>reference-number:key</i>—PSK provided by the CA server for CMPv2 operation.</p> <p><i>root certificate</i>—Filename of the root certificate of the CA server (file present on SUP disk).</p> <p><i>url</i>—URL where the CA server listens to requests.</p>

Command	Purpose
<p>Step 3</p> <pre>WSG# crypto cmp enroll current-wsg-cert wsg_certificate current-wsg-private-key wsg_privatekey modulus modulus id-type id-type id id subject-name subject string ca-root root certificate ca-url url</pre>	<p>Makes an enroll request to the CA server using CMPv2. The existing WSG certificate and private key are user provided as input parameters to the CLI. The filenames for the new private key and the certificate files are automatically generated by the system. This request is similar to initialize except that it is authenticated using public-key methods.</p> <p><i>wsg_certificate</i>—Current valid WSG certificate.</p> <p><i>wsg_privatekey</i>—Current valid private key corresponding to the certificate provided in the previous parameter.</p> <p><i>modulus</i>—Modulus of the generated certificate: 512, 1024, or 2048.</p> <p><i>id-type</i>—Type of the ID: fqdn or ip.</p> <p><i>id</i>—Word that is of id-type.</p> <p><i>subject string</i>—Subject string of the certificate in double quotes.</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p style="text-align: center;"> Note</p> <p>The supported characters while configuring the subject-name are dash, dot, underscore, a-z, A-Z and 0-9. The maximum size supported for the string is 256 bytes.</p> </div> <p><i>root certificate</i>—Filename of the root certificate of the CA server (file present on SUP disk).</p> <p><i>url</i>—URL where the CA server listens to requests.</p>
<p>Step 4</p> <pre>WSG# crypto cmp update current-wsg-cert wsg_certificate current-wsg-private-key wsg_privatekey ca-root root certificate ca-url url</pre>	<p>Sends an update request to the CA server using CMPv2 to update the existing WSG certificate. The existing WSG certificate and private key is provided by the user as input parameters to the CLI. The filenames for the new private key and the certificate files are automatically generated by the system.</p> <p><i>wsg_certificate</i>—Current valid WSG certificate.</p> <p><i>wsg_privatekey</i>—Current valid private key corresponding to the certificate provided in the previous parameter.</p> <p><i>root certificate</i>—Filename of the root certificate of the CA server (file present on SUP disk).</p> <p><i>url</i>—URL where the CA server listens to requests.</p>

Here is an example of the **crypto cmp transport** command:

```
crypto cmp transport http
```


Here is an example of the **crypto cmp initialize** command:

```
crypto cmp initialize modulus 1024 id-type fqdn id wsg.cisco.com subject-name
"C=US,O=Cisco,OU=Security,CN=Example" ca-psk 32438:this_is_very_secret ca-root root-ca.crt
ca-url http://212.246.144.35:8700/pkix/
```

Here is an example of the **crypto cmp enroll** command:

```
crypto cmp enroll current-wsg-cert wsg.crt current-wsg-private-key wsg.prv modulus 1024
id-type fqdn id wsg.cisco.com subject-name "C=US,O=Cisco,OU=Security,CN=Example" ca-root
root-ca.crt ca-url http://212.246.144.35:8700/pkix/
```

Here is an example of the **crypto cmp update** command:

```
crypto cmp update current-wsg-cert wsg.crt current-wsg-private-key wsg.prv ca-root
root-ca.crt ca-url http://212.246.144.35:8700/pkix/
```

The CA server may not immediately return the certificate. In this case, periodically use the **crypto cmp poll** command to check for availability. These commands are used if the request for a Privileged EXEC CMPv2 configuration command is pending.

Command	Purpose
WSG# show crypto cmp request	Displays the current status of the last CMPv2 request with an outstanding update request having priority over initialize and enroll requests. This shows the request that will be polled by the crypto cmp poll command. The output also indicates if no request is pending.
WSG# crypto cmp poll	Configure the WSG to query the CA server for the availability of the certificate requested by a previous crypto cmp initialize , enroll , or update command.
WSG# clear crypto cmp	Clears outstanding initialize, enroll, and update requests generated by this WSG. This allows you to make another initialize, enroll, or update request before the previous request is honored. No cancellation is sent to the CA server; only the state of the previous request on the WSG is cleared.

To configure the WSG to use the certificate, use the following configuration commands. The filenames for the private key and certificate files will be the same filenames generated using the Privileged EXEC CMP initialize and enroll commands.

	Command	Purpose
Step 1	WSG# config	Enters global configuration mode.
Step 2	WSG(config)# crypto pki wsg-cert <i>cert-filename.crt</i> [wsg-private-key <i>private-key-filename.prv</i>]	Configures the WSG to use the certificate for certificate based authentication. The certificate and private key are copied from the Cisco 7600 SUP to the WSG. Up to 20 certificate/private key pairs may be configured on the WSG. <i>cert-filename.crt</i> —Name of the WSG certificate file. Ensure certificate filenames end with a .crt file extension. <i>private-key-filename.prv</i> —Private key filename. To use the private key, set the name of the private key file, ending with a .prv extension. Note The WSG uses the private key from the crypto rsa-keygen command if you do not set a private key.
Step 3	WSG(config)# crypto pki wsg-cert-trap expiry notification <i>hours</i>	Configures the WSG to generate a syslog and SNMP trap a specified number of hours before the certificate expires. The range is from 1 to 720 hours. The default is 24 hours.
Step 4	WSG(config)# snmp-server enable traps ipsec trap	Configures the WSG to generate IPsec traps. If no trap option is specified with this command, all IPsec traps will be generated. If only certificate traps are needed, specify the trap options cert-expiry and cert-renewal . Note If only tunnel-rate create/delete traps are needed, enable the trap options tunnel-rate separately.

To configure CMPv2 automatic renewal, use the following configuration commands. The filenames for the private key and the certificate files will be the same filenames generated using the Privileged EXEC CMP initialize, enroll, or update commands. There is no implied command sequence in this list. Up to 20 certificate/private key pairs may be configured for automatic renewal on the WSG.

	Command	Purpose
Step 1	WSG# config	Enters global configuration mode.
Step 2	WSG(config)# crypto cert renewal retrieve current-wsg-cert <i>cert-filename.crt</i> current-wsg-private-key <i>private-key-filename.prv</i> time <i>days</i>	Configures the WSG to try to retrieve the certificate and private key files from the Cisco 7600 SUP a specified number of days prior to the certificate expiration. If the retrieved certificate has not been renewed, the WSG will continue trying to retrieve the renewed certificate until a renewed certificate is retrieved or the current certificate expires. After a renewed certificate is retrieved, it is copied to the Cisco 7600 standby SUP and standby WSG. <i>cert-filename.crt</i> —Certificate filename. <i>private-key-filename.prv</i> —Private key filename. <i>days</i> —Number of days before certificate expiration to start trying to retrieve a renewed certificate.
Step 3	WSG(config)# crypto cmp auto-update current-wsg-cert <i>cert-filename.crt</i> current-wsg-private-key <i>private-key-filename.prv</i> ca-root <i>root-filename.crt</i> ca-url <i>url</i> time <i>days</i> [key-reuse]	Configures the WSG to try to renew the certificate and optionally the private key file with the CA a specified number of days prior to the certificate expiration. Refer to the command reference chapter for a description of the retry mechanism. After the certificate is renewed, it is copied to the Cisco 7600 SUPs and standby WSG. The automatic renewal does not change the certificate or private key filename, so no additional configuration is required after automatic renewal. <i>cert-filename.crt</i> —Certificate filename. <i>private-key-filename.prv</i> —Private key filename. <i>days</i> —Number of days before certificate expiration to start trying to retrieve a renewed certificate. key-reuse —Optional parameter used to specify that the current private key should be reused. The default is to generate a new private key.

Timeline for CMPv2 certificate generation and manual certificate update:

1. CMP Initialize
2. CMP Enroll
3. Copy files to other Cisco 7600s
4. Use **crypto pki wsg-cert** command on all Cisco 7600s using the certificate
5. CMP Update
6. Copy files to other Cisco 7600s
7. Use **crypto pki wsg-cert** command on all Cisco 7600s using the certificate
8. Repeat before every expiration

Timeline for CMPv2 certificate generation and automatic certificate update:

1. CMP Initialize
2. CMP Enroll
3. Copy files to other Cisco 7600s
4. Use **crypto pki wsg-cert** command on all Cisco 7600s using the certificate
5. Use **crypto cmp auto-update** on one WSG and **crypto cert renewal retrieve** on all other WSGs using the certificate
6. No further action, unless the CA does not renew the certificate

Online Certificate Status Protocol

Currently, the WSG uses a CRL (Certificate Revocation List obtained from the CRL server), a file containing the list of certificates that have been revoked. If a peer negotiates a tunnel with a revoked certificate listed in the CRL file, the WSG will reject that negotiation. The CRL file is maintained one per trust anchor. The first negotiated tunnel for that trust anchor will retrieve the CRL file and cache it on the WSG. Subsequent negotiations will reuse the CRL file. The CRL file has an expiry data that denotes whether it is valid.

Some characteristics of the CRL mechanism make it undesirable in certain solutions. The longer the list, the longer it takes to download the CRL file. Additionally, a certificate can be revoked at any time, and the WSG will use the cached entry until the next time it retrieves the file.

The Online Certificate Status Protocol (OCSP) feature addresses some of the limitations of CRL. OCSP works to achieve the same objective as the CRL mechanism; to determine if a certificate offered by a peer has been revoked. However, OCSP differs from CRL in that the revocation status is obtained on a per-certificate basis rather than a trust anchor-basis. Since the revocation status is obtained when the certificate is first seen by the WSG, the status is up-to-date.

There is no explicit configuration. The only requirement is that CRL should be enabled for the corresponding trust anchor (we have a common knob for CRL and OCSP).

OCSP is not the best mechanism to check for certificate status in all solutions. There will be an impact to the tunnel setup rate, as each setup requires that the certificate status be verified.

DHCP Address Allocation

Previous WSG releases supported allocating IPv4 addresses from a DHCP server, or from a local IP address pool. The WSG communicates with the DHCP server as a DHCP relay agent, as configured by RFC 3046.

From Release 4.3 onwards, WSG also supports allocating IPv6 addresses from a DHCPv6 server. The WSG communicates with the DHCPv6 server as a DHCPv6 relay agent, as configured by RFC 3315. This section describes the DHCP interface from the WSG to the DHCP server, and how address pools are allocated.

Also, the WSG supports requesting DNS server IPs from the DHCP server or it can even be configured locally. As the WSG supports both DHCP configured and locally configured DNS IPs, preference will be given to IPs received from the DHCP Server. As an example, if we receive 3 DNS IPs from DHCP server and we have one DNS IP locally configured, then WSG will send only the 3 DNS IP which are

received from DHCP server, since the WSG at most supports 3 DNS IPs. In case if we receive only 2 DNS IPs from DHCP server and having one locally configured DNS IP, then all locally configured and DHCP received DNS IPs will be forwarded to remote IPsec client.

The WSG sends messages to the DHCP server under various conditions. It, the WSG, uses “RAPID COMMIT” option to assign DHCPv6 addresses. All DHCP messages are unicast to the DHCP servers by the WSG. The WSG does not send or receive broadcast messages.

Each PPC is configured with its own unique giaddr in case of IPv4 and link address in case of IPv6. Each address pool is associated with a giaddr/link address. The giaddr/link address is sent in a DHCP message and indicates to the DHCP server which address pool an IP address should be allocated from. The address pool configured on the DHCP server for each PPC can be from one or more subnets. Each subnet can be of any size. Multiple PPC of SAMI WSG can share the same address pool on the DHCP server. Based on the available pool addresses, the server will allocate addresses for the client. Server may or may not allocate the same address for different requests from the same client, depending on server configuration.

All DHCP interactions on the WSG can be debugged using the appropriate debug command. Syslogs are generated for DHCP operation status at the appropriate log level. The IP address assigned to a remote access client can be discovered using CLI commands that show details of an IPsec SA. The WSG maintains statistics for a number of DHCP messages (per type) that are sent and received. You can display these statistics using the appropriate CLI command.

During tunnel set-up time, the WSG requests a lease time for the address assigned by the DHCP server. If the lease time returned by the DHCP server is less than 2 times the IKE lifetime, the tunnel setup fails and the address is released. The DHCP statistics, debugs, and syslog events are recorded for this event. Under normal circumstances, the WSG renews the lease during each phase-1 rekey, and the lease is never allowed to expire. However, if the lease renewal fails, the assigned address is released and the tunnel is deleted. The DHCP statistics, debugs, and syslog record this event, as well.

The DHCP address allocation feature is compatible with the Single-OAM feature on the WSG. However, the DHCP server must be configured to respond to the IP address in the discover/request rather than the giaddr.

**Note**

DHCP is supported for RAS profiles and not for site-to-site profiles.

Client Identification

When the WSG contacts the DHCP server to obtain an IP address, it sends a unique ID in the DHCP messages. This client id (CID) is sent in the Client Identifier option (61) of the DHCP messages. The CID is either the entire IKE ID, or the CN field of a DN formatted IKE ID. The **type** field in the Client Identifier option is by default set to 0 unless you explicitly configure it for a different value.

Tunnel Rekey

The DHCP lease is renewed only on a phase-1 rekey. No DHCP action is taken on a phase-2 rekey (whether initiated by WSG or client).

IKE Timeout

When the WSG times out while waiting for a response to an IKE request from the HNB, the DHCP lease is released.

Load Balancing

The presence of a load balancer between an HNB and WSG(s) does not affect how the DHCP feature works in normal situations. However, if an HNB disconnects without deleting the tunnel, and then reconnects later, the load balancer might send the HNB to a different PPC. If this occurs, the DHCP server still has an active lease from the address pool for the original PPC. When the DHCP server sees the same HNB (same client identifier) from a different PPC, it needs to release the original lease and allocate a new IP address from the new PPC address pool.

High Availability

The DHCP Address Allocation feature is designed to work with a WSG is operating in a 1-1 redundant mode. The DHCP user configuration is synced from the active to standby WSG. The complete DHCP internal state is exported from the active WSG to the standby WSG. After failover the DHCP operations continue as specified for the active tunnels. But tunnels that were being setup during failover will not survive during the failover. Once the tunnel is setup, the DHCP operations must complete on either the old or new active card on failover.

Configuring DHCP Address Allocation

To configure the WSG to perform DHCP Address Allocation, perform the following tasks:

	Command	Purpose
Step 1	WSG# config	Enters global configuration mode.
Step 2	WSG (config)# crypto dhcp-server ip <i>A.B.C.D X:X:X::X port port number</i>	Configures the DHCP server IP and port number. Maximum of two DHCP servers of type either IPv4 or IPv6 can be configured by repeating the command. The no form of the command removes the DHCP server from the configuration. At least one DHCP server must be specified if DHCP address allocation is required.
Step 3	WSG(config)# crypto dhcp-client giaddr ip <i>address server-port port number</i> <i>client-port port number</i>	Specifies the giaddr, and the server and client ports used on the WSG. The server and client port number can be the same or different values. The WSG sends DHCP messages with the client port number, and receives responses from the server on the server port number. The giaddr must be unique for each PPC talking to the DHCP server. This command is required if you require DHCP address allocation.
Step 4	WSG (config)# crypto dhcp-client client-id-type extract-CN	Specifies the client id that is sent by the WSG (in option 61 of DHCP message). By default the HNB's IKE ID is used as the client ID. If the HNB IKE ID is in the DN format, and the CN part of the DN is to be sent as the client ID, then this command must be configured. The no form of the command reverts the client ID to the default setting.

	Command	Purpose
Step 5	WSG(config)# crypto dhcp-client link-addr <i>ipv6 address server-port port number</i> client-port <i>port number</i>	Specifies the global unicast IPv6 Link-Address in Relay Forward message used by the WSG. This address is more like an identifier to which address pool to be used in the server side. This command is mandatory if DHCPv6 address allocation is required.
Step 6	WSG(config)# crypto profile <i>profile-name</i> ipsec ip address-pool { dhcp <i>local-pool-name</i> }	Use this command when a profile is required to use DHCP-based address allocation. When the profile is activated, the mandatory global DHCP configuration is checked for completeness. If any profile is activated with DHCP address allocation, the global DHCP configuration commands cannot be modified or removed.

To monitor and troubleshoot the DHCP Address Allocation feature, perform the following tasks:

	Command	Purpose
Step 1	WSG# show crypto dhcp	Displays DHCP address statistics.
Step 2	WSG# debug crypto dhcp { errors events verbose }	Enables debugging for DHCP crypto parameters .

Here is a running configuration example:

```
hostname WSG
ha interface vlan 2073
  ip address 77.77.73.133 255.255.255.0
interface vlan 63
  ip address 88.88.63.133 255.255.255.0
  alias 88.88.63.3 255.255.255.0
interface vlan 223
  ip address 222.222.223.133 255.255.255.0
  alias 222.222.223.3 255.255.255.0
ip route 0.0.0.0 0.0.0.0 88.88.63.100
oam mode single 223
  oam-ip route 44.44.44.0 255.255.255.0 222.222.223.100
logging ip 44.44.44.17
snmp-server community public ro
snmp-server community private rw
snmp-server host 44.44.44.16 traps version 2c public
ip name-server 44.44.44.201
snmp-server enable traps ipsec
crypto syslog-level 1
!
crypto pki wsg-cert sami-cert.crt wsg-private-key sami-key.prv
crypto pki trustpoint rootCA cacert.crt crl disable
!
crypto dhcp-client giaddr 88.88.63.3 server-port 2133 client-port 2133
!
crypto profile "prof-1"
  isakmp
    lifetime 7200
    self-identity id-type fqdn id SAMI.cisco.com
  ipsec
    security-association lifetime 86400
    access-permit ip 172.60.0.0 subnet 16
    ip address-pool dhcp
```

```

    activate
    !

```

Here is a running configuration example of WSG with DHCPv6 server:

```

hostname s9p3
ha interface vlan 17
    ip address 192.168.17.9 255.255.255.0
interface vlan 2
    ip address 10.77.161.34 255.255.255.192
interface vlan 77
    ip address 62.21.99.95 255.255.255.0
interface vlan 8
    ip address 192.168.9.12 255.255.255.0
    alias 192.168.9.93 255.255.255.0
    ipv6 address 2003::55:55:55:110/112
interface vlan 25
    ip address 192.168.25.9 255.255.255.0
    ipv6 address 2006::77:77:77:93/112
    ipv6 alias 2006::77:77:77:103/112

router bgp 9
    neighbor 2006::77:77:77:1 remote-as 9 next-hop-alias 2006::77:77:77:93

ip route 192.168.10.12 255.255.255.255 192.168.5.1
ip route 0.0.0.0 0.0.0.0 10.77.161.1
ip route 192.168.5.0 255.255.255.0 192.168.9.1
ip route 192.168.25.32 255.255.255.255 192.168.9.1
ip route 192.178.0.0 255.255.0.0 192.168.9.1
ip route 192.179.0.0 255.255.0.0 192.168.9.1
ip route 192.177.0.0 255.255.0.0 192.168.9.1
ip route 192.168.6.33 255.255.255.255 192.168.9.1
ip route 20.20.20.1 255.255.255.255 192.168.9.1

crypto remote-secret fqdn test.cisco.com secret "test"
!
crypto pki wsg-cert sami-cert.crt wsg-private-key sami-key.prv
crypto pki trustpoint rootCA ca-cert.crt crl disable
!
crypto rri enable

crypto dhcp-server ip 2006::77:77:77:32 port 547
!
crypto dhcp-client link-addr 2006::77:77:77:93 server-port 547 client-port 546
!

crypto profile "ipv6-psk-ras"
    isakmp
        self-identity id-type email id sami@cisco.com
        local-secret "test"
        authentication pre-shared
    ipsec
        access-permit ip 2002::5:5:5:1 subnet 112
        ip address-pool dhcp
    activate
!

```


IPv6

IPv6 support in WSG Release 3.0 includes support for both IPv6 IKE and IPv6 ESP packets and related IPv6 addressing where required. WSG Release 3.0 and above supports all four of the following combinations of IPv4/IPv6 encapsulation in the tunnels:

- IPv6 Over IPv6
- IPv6 Over IPv4
- IPv4 Over IPv6
- IPv4 Over IPv4

Configuring IPv6

The PPC requires an IPv6 VLAN interface to be configured to act as an IPv6 IKE server. The other changes required are to the traffic selectors inside the profile. The traffic selector accepts IPv6 addresses.

All the profile-based configuration remains the same. Changes have been made to the CLI at the IP address option level. Every option to enter an IP address now accepts either an IPv4 or IPv6 address.

IPv6 IP addresses for self identity are supported. Access Permit, Address pools, Local IP, Peer IP and all other CLIs that accept an IP address as a parameter have been enhanced for IPv6.

The traffic selector determines the protocol of the secured traffic inside the tunnel. The local-ip and peer-ip determine the protocol used for IKE exchange and the IP addresses in the outer header of the ESP packets sent out of WSG datapath to the peer.

The following is a sample configuration of an IPv6-over-IPv6 tunnel:

```
interface vlan 39
  ipv6 address 2001:88:88:94::4/96
  ipv6 route ::/0 2001:88:88:94::1

crypto profile "s2s-IPv6-over-IPv6"
  profile-type site-to-site
  isakmp
  peer-ip 3001:99:99:94::4
  self-identity id-type email id ppcl@cisco.com
  local-secret "cisco123"
  authentication pre-shared
  ipsec
  access-permit "one"
    protocol any src-ip 4001:100:100:94::4 96 src-port 0 65535
    dst-ip 5001:200:200:94::4 96
    dst-port 0 65535
  local-ip 2001:88:88:94::4
  activate
```

The following is a sample configuration of an IPv6-over-IPv4 tunnel:

```
interface vlan 39
  ip address 39.39.39.30 255.255.255.0
  ipv6 address 2001:88:88:94::4/96
  ip route 0.0.0.0 0.0.0.0 39.39.39.3
  ipv6 route ::/0 2001:88:88:94::1
  crypto profile "s2s-IPv6-over-IPv4"
  profile-type site-to-site
```

```

isakmp
 peer-ip 59.59.59.50
 self-identity id-type email id ppc1@cisco.com
 local-secret "cisco123"
 authentication pre-shared
 ipsec
 access-permit "one"
   protocol any src-ip 4001:100:100:94::4 96 src-port 0 65535
   dst-ip 5001:200:200:94::4 96
   dst-port 0 65535
 local-ip 39.39.39.30
 activate

```

The following is a sample configuration of an IPv4-over-IPv6 tunnel:

```

interface vlan 39
 ip address 39.39.39.30 255.255.255.0
 ipv6 address 2001:88:88:94::4/96
 ip route 0.0.0.0 0.0.0.0 39.39.39.3
 ipv6 route ::/0 2001:88:88:94::1
 crypto profile "s2s-IPv4-over-IPv6"
 profile-type site-to-site
 isakmp
 peer-ip 3001:99:99:94::4
 self-identity id-type email id ppc1@cisco.com
 local-secret "cisco123"
 authentication pre-shared
 ipsec
 access-permit "one"
   protocol any src-ip 60.0.0.0 8 src-port 1 65535 dst-ip 40.0.0.0 8 dst-port 1 65535
 local-ip 2001:88:88:94::4
 activate

```

The following is a sample configuration of an IPv4-over-IPv4 tunnel:

```

interface vlan 39
 ip address 39.39.39.30 255.255.255.0
 ip route 0.0.0.0 0.0.0.0 39.39.39.3
 crypto profile "s2s-IPv4-over-IPv4"
 profile-type site-to-site
 isakmp
 peer-ip 59.59.59.50
 self-identity id-type email id ppc1@cisco.com
 local-secret "cisco123"
 authentication pre-shared
 ipsec
 access-permit "one"
   protocol any src-ip 60.0.0.0 8 src-port 1 65535 dst-ip 40.0.0.0 8 dst-port 1 65535
 local-ip 39.39.39.30
 activate

```

The subnet combination command for the site-to-site tunnels is modified to accept a full range of subnet sizes for IPv6, subnet sizes more than 32 are not used to handle IPv4 traffic in the datapath, whereas all configured subnet sizes will be used for handling IPv6 traffic.

Example:

```

crypto site-to-site-lookup priority 1 source-netmask 128 destination-netmask 128
crypto site-to-site-lookup priority 2 source-netmask 96 destination-netmask 96
crypto site-to-site-lookup priority 3 source-netmask 32 destination-netmask 32

```

Tunnel counters and show commands:

```
show crypto ipsec sa
show crypto ipsec sa remote-ip
show crypto isakmp sa
show crypto isakmp sa remote-ip
```

Blacklisting

You might want to block certain access points (APs) from connecting to the WSG. In case certificates are used to authenticate an AP, the CRL mechanism is used to revoke the certificate of the AP that needs to be blocked, which prevents it from setting up a tunnel with the WSG. However, when an AP is only required to be blocked temporarily (for instance because of an outstanding balance on the billing account), blacklisting is an easier and faster mechanism to block an AP.

The WSG blacklisting feature prevents an AP from setting up a tunnel to the WSG. When an AP attempts to setup a tunnel with WSG, the IKE ID of the AP is searched in a blacklist file available to the WSG. If a match is found, the AP is prevented from establishing a tunnel and the AUTH request fails.

You must edit the blacklist file outside of the Cisco 7600 chassis, and copy it to the SUP disk. Initially, you should configure the WSG with the filename of the blacklist file. During this configuration, the blacklist file is internally rcp-ed from the SUP disk to the WSG ram disk, and the IKE stack is informed of the location of the file. The IKE stack performs blacklisting based on the entries in the file. If you need to update the blacklist entries, follow this procedure:

- Edit the blacklist file outside the Cisco 7600 chassis.
- Copy the blacklist to the SUP disk with the same file name that you initially used.
- Execute the **crypto blacklist file resync** command on the WSG. The WSG copies the updated file from the SUP disk to its ramdisk, and informs the IKE stack about the updated file. The IKE stack now uses the new blacklist file.

You must execute the blacklist file configuration and resync operation on all PPCs of the WSG card where blacklisting is required.

The blacklist file is a text file with multiple lines. Each line is one blacklisted IKE ID. It is possible for the blacklist file to be empty (no blacklisted entries). Here is an example of a blacklist file:

```
fqdn "LS1-0.cisco.com"
fqdn "LS1-1.cisco.com"
fqdn "LS1-2.cisco.com"
fqdn "LS1-3.cisco.com"
ip "192.168.10.10"
ip "192.168.10.50"
email "user@sample.com"
dn "C=US,ST=CA,L=San Jose,O=Cisco,OU=SMBU,CN=organization.bu.org"
```

Configuring Blacklisting on the WSG

To configure and monitor the WSG's blacklisting feature, perform the following tasks:

	Command	Purpose
Step 1	wsg# config	Enters global configuration mode.
Step 2	wsg(config)# crypto blacklist file filename	Configures the blacklist filename on the WSG. The blacklist file must be present on the SUP disk before this configuration is done. If the file is not present on the SUP, the configuration fails. The default value is that the feature is off.
Step 3	wsg(config)# crypto blacklist file resync	Recopies the blacklist file from the SUP disk and inform the IKE stack about the update.
Step 4	wsg(config)# clear crypto isakmp sa remote-id remote ID	Deletes all IKE and IPsec SAs associated with a remote ID.
Step 5	wsg# show crypto blacklist file	Lists all of the currently blacklisted IDs.
Step 6	wsg# show crypto blacklist stats	Displays the following information: <ul style="list-style-type: none"> • Number of IDs in a blacklist • Number of tunnel setup attempts blocked due to blacklisting

Here is an example of the **show crypto blacklist stats** command:

```
wsg# show crypto blacklist stats
```

```
Blacklist Statistics
Number of blacklisted entries : 500
IKEv2 [R] initial exchanges      : Allowed = 53, Blocked = 101
IKEv2 [R] create child exchanges  : Allowed = 0, Blocked = 0
IKEv2 [R] IPsec SA rekeys        : Allowed = 98, Blocked = 0
IKEv2 [R] IKE SA rekeys          : Allowed = 49, Blocked = 0
IKEv2 [I] IPsec SA rekeys        : Allowed = 0, Blocked = 0
IKEv2 [I] IKE SA rekeys          : Allowed = 0, Blocked = 0
IKEv1 [R] main mode exchanges    : Allowed = 0, Blocked = 0
IKEv1 [R] aggressive mode exchanges : Allowed = 0, Blocked = 0
IKEv1 [R] quick mode exchanges   : Allowed = 0, Blocked = 0
IKEv1 [I] IPsec SA rekeys        : Allowed = 0, Blocked = 0
IKEv1 [I] DPD SA creations       : Allowed = 0, Blocked = 0
```



Note

The WSG blacklisting feature is independent of other blacklisting or security functionality that may exist as part of other Cisco products and solutions.

RADIUS Accounting

In some femto networks, an AP sets up an IPsec tunnel with the WSG, and then sends an registration message through the tunnel to a Femto Gateway (FGW). The register message is an IP packet that also contains the ID of the AP registering with the FGW. The ID used by the AP is the same as the IKE ID used by the AP during IPsec tunnel setup. The FGW must ensure that an authenticated AP is not presenting itself as another AP during registration. The FGW compares the source IP address of the

registration packet with the internal IP address assigned by the WSG for the same AP (the ID is the lookup key). Similarly, the WSG needs to send the ID to an internal IP address mapping to the FGW each time it assigns an IP to the AP.

RADIUS Accounting messages are used to send the IKE ID to the assigned IP address mapping from the WSG to the AAA server running in the FGW.

After a tunnel is successfully established, a RADIUS accounting message is sent to the AAA server to record the mapping from the AP IKE ID to the WSG assigned internal AP IP address. The RADIUS timeout and retry mechanism is used to handle cases where a RADIUS server might be down. However, failure to update the RADIUS server will not fail the tunnel setup.

Table 2-3 shows the accounting request message attributes for tunnel setup.

Table 2-3 Accounting Start Request

Attribute Type	Comment
From RFC2865...	—
User-Name	Set to IKEv2 IDi.
Framed-IP-Address (IPv6: Framed-IPv6-Prefix, from RFC3162)	Set to allocated inner IP address.
NAS-IP-Address	Set to the WSG IP address that the IKE messages were received on to setup the tunnel.
From RFC2866...	—
Acct-Status-Type	Start
Acct-Session-Id	Set to an unique value so that the start and stop records can be matched.

When the tunnel is deleted, the record is deleted from the AAA server.

Table 2-4 displays the accounting request message attributes for tunnel deletion.

Table 2-4 Accounting Stop Request

Attribute Type	Comment
From RFC2865...	—
User-Name	Set to IKEv2 IDi.
NAS-IP-Address	Set to the WSG IP address that the IKE messages were received on to setup the tunnel.
From RFC2866...	—
Acct-Status-Type	Stop
Acct-Session-Id	Set to an unique value so that the start and stop records can be matched.



Note

When upgrading to WSG Release 3.0 from a previous 2.X release, if a RADIUS server configuration exists, the crypto profile(s) will be inactive after the upgrade. To reactivate, configure the **crypto radius nas-id** or **crypto radius nas-ip** commands and then activate the profile(s).

Features of RADIUS Accounting

The RADIUS Accounting feature has the following requirements and limitations:

- The RADIUS Accounting feature supports both IKEv1 and IKEv2.
- The RADIUS Accounting feature supports both IPv4 and IPv6.
- You can enable and disable this feature at the global level, but all crypto profiles have to be in a deactivated state before enabling/disabling the feature.
- You can specify the RADIUS accounting server IP and port. If the RADIUS accounting port is not specified, then the default value of 1813 is used. There is an existing CLI (API) to use to configure for the RADIUS server. The command is modified so that specifying the auth-port/acct-port optional.
- There is an option to specify the source IP of the RADIUS packets. If the source IP is not specified, then the source IP is picked by the Linux kernel based on routing rules. There is an existing CLI to specify the source IP.
- The RADIUS Accounting update is sent whenever the WSG assigns an internal IP address during tunnel setup to the remote peer from the local address pool, or from external sources like DHCP.
- Syslogs and debugs are generated at the appropriate level for all blacklisting RADIUS accounting feature operations.
- RADIUS protocol statistics such as the different types of messages sent, timeouts, retries, etc., are maintained.

Configuring RADIUS Accounting on the WSG

To configure and monitor the RADIUS accounting feature on the WSG, perform the following tasks:

	Command	Purpose
Step 1	wsg# config	Enters global configuration mode.
Step 2	wsg(config)# crypto radius accounting {enable}	Enables the RADIUS Accounting feature. The default value is that the feature is disabled.
Step 3	wsg# show crypto radius statistics	Displays the count of different RADIUS messages sent and received. Also RADIUS timeout and retry counters are displayed.



Note

Existing CLI are used to configure the RADIUS server IP addresses, RADIUS server ports and source IP address for RADIUS messages. When multiple RADIUS servers are configured, the accounting messages are sent to the first server in the list that the WSG is successfully able to communicate with.

Here is sample output for the **show crypto radius statistics** command:

```
wsg# show crypto radius statistics
Radius Accounting Statistics
  Accounting requests sent           : 1
  Accounting-On requests sent        : 0
  Accounting-Off requests sent       : 0
  Accounting-Start requests sent     : 1
  Accounting-Stop requests sent      : 0
  Accounting Responses on received   : 0
  Accounting Invalid responses received : 0
  Accounting requests failed         : 0
```

```
Accounting requests, Invalid IKE ID : 0
Accounting requests timedout       : 1
Accounting requests retransmission : 4
Accounting requests cancelled      : 0
```

EAP Peer Authentication

WSG supports authentication of a peer through EAP-MD5, EAP-AKA and EAP-SIM protocols. These protocols are only supported with certificates for authenticating the WSG to the peer. These protocols require the IPSec stack to talk to an external RADIUS server to authenticate a peer device. Use of preshared keys to authenticate the WSG to the peer is not allowed by the standards, but might be required to support some legacy equipment. The EAP authentication is supported for IKEv2 only.

Sample configuration output:

```
crypto radius source-ip 88.88.93.3
!
crypto radius-server host 44.44.44.200 key "cisco" auth-port 1812 acct-port 1813

crypto profile "ras_eap-aka"
  isakmp
    self-identity id-type email id sami@cisco.com
    eap-type aka
  ipsec
    access-permit ip 172.0.0.0 subnet 8
    ip address-pool "myPool"
  activate

crypto profile "ras_eap-md5"
  isakmp
    self-identity id-type email id sami@cisco.com
    eap-type md5
  ipsec
    access-permit ip 172.0.0.0 subnet 8
    ip address-pool "myPool"
  activate

crypto profile "ras_eap-sim"
  isakmp
    self-identity id-type email id sami@cisco.com
    eap-type sim
  ipsec
    access-permit ip 172.0.0.0 subnet 8
    ip address-pool "myPool"
  activate
```

Reverse Route Injection (RRI)

The RRI feature is introduced in WSG Release 3.0 and obviates the need to manually configure static routes on the SUP for clear traffic routing purposes in the reverse direction. RRI route entries are injected into the SUP when IPSec tunnels are created. These route entries are correspondingly withdrawn from the SUP when the IPSec tunnels are deleted. The BGP protocol is used to re-distribute the routes from WSG to the SUP. For WSG Release 3.0, the RRI feature supports only IPv4. IPv6 is supported starting in WSG Release 4.0. Also, only site-to-site profiles are supported. The VRF feature on the WSG cannot be enabled when the RRI feature is already configured.

The BGP peer on the SUP needs to establish BGP sessions to two separate BGP neighbors on the WSG; one with the active card and one with the standby card for redundancy. The BGP AS-number is configured for an iBGP setup. Depending on the network topology, an eBGP setup is also supported between the WSG and SUP.

A sample configuration on the SUP (for IPv4):

```
router bgp 7675
  bgp router-id 10.10.14.1
  bgp log-neighbor-changes
  neighbor 33.33.33.33 remote-as 7675
  neighbor 33.33.33.34 remote-as 7675
!
address-family ipv4
  neighbor 33.33.33.33 activate
  neighbor 33.33.33.34 activate
  no auto-summary
exit-address-family
```

A sample configuration on the SUP (for IPv6):

```
ipv6 unicast-routing
mls cef error action reset
mls cef maximum-routes ipv6 32 (**)

router bgp 7675
  bgp router-id 10.12.12.1
  bgp log-neighbor-changes
  bgp graceful-restart restart-time 120
  bgp graceful-restart stalepath-time 360
  bgp graceful-restart
  no bgp default ipv4-unicast
  neighbor 2001:88:88:94::46 remote-as 7675
  neighbor 2001:88:88:94::46 ebgp-multihop 255 (*)
  neighbor 2001:88:88:94::47 remote-as 7675
  neighbor 2001:88:88:94::47 ebgp-multihop 255 (*)

address-family ipv6
  neighbor 2001:88:88:94::46 activate
  neighbor 2001:88:88:94::47 activate
exit-address-family
```

The **crypto rri enable** command is required to enable the RRI feature. The profile configuration is like before. BGP configuration on the WSG requires neighbor and next-hop-alias information so that there is a common next-hop point for the SUP to route to either the active or standby card.

A sample configuration on the WSG (for IPv4):

```
router bgp 7675
  neighbor 33.33.33.3 remote-as 7675 next-hop-alias 33.33.33.30

crypto rri enable

crypto profile "rri-site"
  profile-type site-to-site
  isakmp
    lifetime 7200
    self-identity id-type email id ppcl@cisco.com
    local-secret "cisco123"
    authentication pre-shared
  ipsec
    security-association lifetime seconds 3600
    access-permit "primary"
    protocol any src-ip 60.0.0.0 8 src-port 1 65535 dst-ip 40.0.0.0 8 dst-port 1 65535
```



```

    local-ip 33.33.33.30
  activate

```

A sample configuration on the WSG (for IPv6):

```

router bgp 7675
neighbor 2001:88:88:94::44 remote-as 7675 next-hop-alias 2001:88:88:94::43

crypto rri enable

crypto profile "rri-site-ipv6"
profile-type site-to-site
isakmp
lifetime 7200
self-identity id-type email id ppcl@cisco.com
local-secret "cisco123"
authentication pre-shared
ipsec
security-association lifetime seconds 3600
access-permit "primary"
protocol any src-ip 2001:77:77:77::1 64 src-port 0 65535 dst-ip 2001:98:98:98::1 64
dst-port 0 65535
local-ip 2001:88:88:94::43
activate

```



Note

The above IPv6 configurations require the following:

- Requires SUP software version 15.1(2)S2 or later
- Requires additional configuration on the SUP above (marked with **) to support 17K IPv6 RRI entries **mls cef maximum-routes ipv6 [maximum number RRI entries]**
- Requires additional configuration on the SUP above (marked with *) to support IPv6 in eBGP mode **neighbor [ipv6_bgp_neighbor] ebgp-multihop 255**
- When the RRI feature is used, expect an approximate 3 second delay from the time a tunnel is added to the time when the injected RRI route actually shows up on the SUP. Reverse/clear traffic will only start passing approximately 3 seconds after a tunnel is created.

VRF Configuration

Virtual Routing and Forwarding (VRF) allows the creation of multiple virtual networks within a single network entity. Each VRF comprises an IP routing table and a forwarding table, allowing the use of the same or overlapping IP addresses without conflicts.

In a single network entity, multiple VRFs can be used to create isolation between virtual networks. VRFs allow encrypted/decrypted traffic separation, by having the encrypted traffic in one VRF and the decrypted traffic in another VRF.

- Inside VRF (indoor) contains decrypted traffic
- Outside VRF (front door) contains encrypted traffic

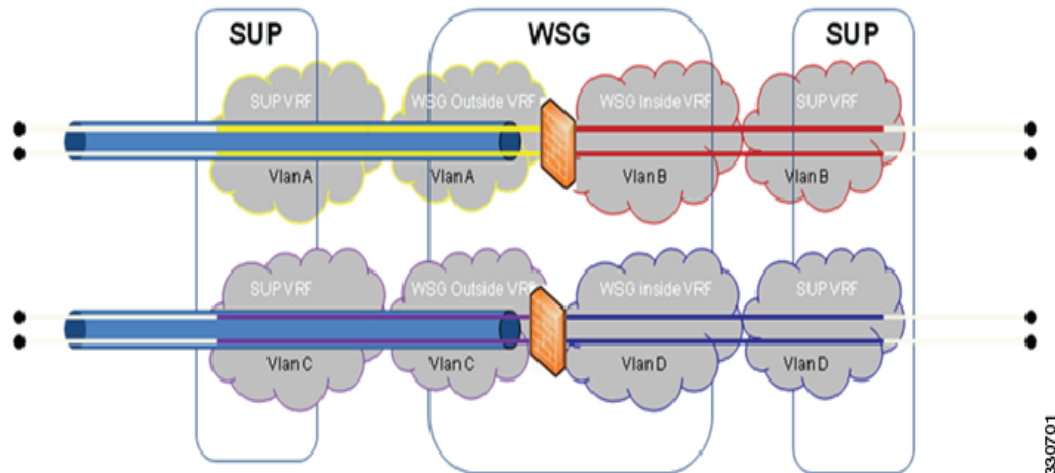
The typical case for this is an ISP that provides VPN service to multiple enterprise customers on the same box, the users and branches connect using internet for the encrypted traffic, but the decrypted traffic needs to go to the private network of each separate customer and this traffic cannot be mixed.

The sample configuration below is for two profiles. Each profile has its own inside and outside VRF configured. This ensures the encrypted and decrypted traffic for both profiles are separated onto different VRFs. The same IP address can be used on both profiles, while also remaining in separate routing tables. This configuration is flexible. The outside VRFs could be configured on the same VRF or on the global VRF if there is no potential to overlap IP addresses.

**Note**

Traffic is considered to be on the same VRF from the SUP to the WSG if the VLANs are the same.

Figure 2-1 WSG VRF Configuration.



WSG VRF Configuration on a PPC

VRF Definitions

```
ip vrf OutsideYellow
ip vrf OutsidePurple
ip vrf InsideRed
ip vrf InsideBlue
```

VRF Interface Definitions

```
interface vlan 33
  vrf OutsideYellow
  ip address 33.33.33.30 255.255.255.0
interface vlan 34
  vrf OutsidePurple
  ip address 33.33.33.30 255.255.255.0
interface vlan 77
  vrf InsideRed
  ip address 77.77.77.70 255.255.255.0
interface vlan 78
  vrf InsideBlue
  ip address 77.77.77.70 255.255.255.0
```

VRF Default Route Definitions

```
ip route 0.0.0.0 0.0.0.0 33.33.33.3 vrf OutsideYellow
ip route 0.0.0.0 0.0.0.0 33.33.33.3 vrf OutsidePurple
```

```
ip route 0.0.0.0 0.0.0.0 77.77.77.7 vrf InsideRed
ip route 0.0.0.0 0.0.0.0 77.77.77.7 vrf InsideBlue
```

VRF Profile Configuration

```
crypto profile "site-to-site"
  profile-type site-to-site
  isakmp
    vrf-outside OutsideYellow
    peer-ip 50.0.0.1
    self-identity id-type email id ppcl@cisco.com
  ipsec
    vrf-inside InsideRed
    access-permit "s2s-1"
      protocol any src-ip 60.0.0.0 24 src-port 1 65535 dst-ip 40.0.0.0 24 dst-port 1
        65535
    access-permit "s2s-2"
      protocol any src-ip 60.0.0.0 24 src-port 1 65535 dst-ip 40.0.0.0 24 dst-port 1 65535
    local-ip 33.33.33.30

crypto profile "site-to-site-2"
  profile-type site-to-site
  isakmp
    vrf-outside OutsidePurple
    peer-ip 50.0.0.1
    self-identity id-type email id ppcl@cisco.com
  ipsec
    vrf-inside InsideBlue
    access-permit "s2s-1"
      protocol any src-ip 60.0.0.0 24 src-port 1 65535 dst-ip 40.0.0.0 24 dst-port 1
        65535
    access-permit "s2s-2"
      protocol any src-ip 60.0.0.0 24 src-port 1 65535 dst-ip 40.0.0.0 24 dst-port 1 65535
    local-ip 33.33.33.30
```

WSG IPv4 VRF Configuration on 7600 SUP

VRF Definitions

```
ip vrf Yellow
  rd 2:2
ip vrf Purple
  rd 3:3
ip vrf Red
  rd 4:4
ip vrf Blue
  rd 5:5
```

Physical Interface Configuration

```
interface GigabitEthernet1/1
  switchport
  switchport access vlan 30
  switchport mode access

interface GigabitEthernet1/2
  switchport
  switchport access vlan 77
  switchport mode access

interface GigabitEthernet1/3
  switchport
  switchport access vlan 31
```

```

switchport mode access

interface GigabitEthernet1/4
switchport
switchport access vlan 78
switchport mode access

```

VLAN Configuration

```

interface Vlan30
ip vrf forwarding Yellow
ip address 22.22.22.3 255.255.255.0

interface Vlan31
ip vrf forwarding Purple
ip address 22.22.22.3 255.255.255.0

interface Vlan33
ip vrf forwarding Yellow
ip address 33.33.33.3 255.255.255.0

interface Vlan34
ip vrf forwarding Purple
ip address 33.33.33.3 255.255.255.0

interface Vlan77
ip vrf forwarding Red
ip address 77.77.77.3 255.255.255.0

interface Vlan78
ip vrf forwarding Blue
ip address 77.77.77.3 255.255.255.0

```

Static Route Definitions

```

ip route vrf Yellow 50.0.0.0 255.0.0.0 22.22.22.4
ip route vrf Yellow 60.0.0.0 255.0.0.0 77.77.77.4
ip route vrf Red 44.44.0.0 255.255.0.0 77.77.77.33

ip route vrf Purple 50.0.0.0 255.0.0.0 22.22.22.4
ip route vrf Purple 60.0.0.0 255.0.0.0 77.77.77.4
ip route vrf Blue 44.44.0.0 255.255.0.0 77.77.77.33

```

WSG IPv6 VRF Configuration on 7600 SUP

VRF Definitions

```

ip vrf OutsideYellow
ip vrf OutsidePurple
ip vrf InsideRed
ip vrf InsideBlue

```

VLAN Configuration

```

interface vlan 113
vrf OutsideYellow
ip address 88.88.113.33 255.255.255.0
alias 88.88.113.93 255.255.255.0
ipv6 address 2001:88:88:113::33/64
ipv6 alias 2001:88:88:113::93/64
interface vlan 203
vrf OutsidePurple
ip address 203.203.113.33 255.255.255.0

```

```

alias 203.203.113.93 255.255.255.0
ipv6 address 2001:203:203:113::33/64
ipv6 alias 2001:203:203:113::93/64
interface vlan 77
 vrf InsideRed
 ip address 77.77.77.33 255.255.255.0
 alias 77.77.77.93 255.255.255.0
 ipv6 address 2001:77:77:77::33/64
 ipv6 alias 2001:77:77:77::93/64
interface vlan 78
 vrf InsideBlue
 ip address 78.78.78.33 255.255.255.0
 alias 78.78.78.93 255.255.255.0
 ipv6 address 2001:78:78:78::33/64
 ipv6 alias 2001:78:78:78::93/64

```

Static Route Definitions

```

ipv6 route ::/0 2001:77:77:77::7 vrf InsideRed
ipv6 route ::/0 2001:88:88:113::100 vrf OutsideYellow
ipv6 route ::/0 2001:78:78:78::8 vrf InsideBlue
ipv6 route ::/0 2001:203:203:113::100 vrf OutsidePurple

```

Crypto Profile Configuration

```

crypto profile "s2s"
 profile-type site-to-site
 isakmp
  vrf-outside OutsideYellow
  lifetime 720000
  dpd-timeout 270
  self-identity id-type email id sami@cisco.com
 ipsec
  security-association lifetime seconds 360000
  access-permit "ap-ipv4"
   protocol any src-ip 172.110.0.0 16 src-port 0 65535 dst-ip 10.33.0.0 16 dst-port 0 65535
  access-permit "ap-ipv6"
   protocol any src-ip :: 0 src-port 0 65535 dst-ip :: 0 dst-port 0 65535
  access-permit "ap-ipv4-2"
   protocol any src-ip 172.0.0.0 24 src-port 0 65535 dst-ip 10.23.0.0 16 dst-port 0 65535
  vrf-inside InsideRed
 activate

....

crypto profile "s2s-tims-tc93-ipv4-ts"
 profile-type site-to-site
 isakmp
  vrf-outside OutsidePurple
  self-identity id-type email id sami@cisco.com
 ipsec
  access-permit "ap2"
   protocol any src-ip 2001:172:110:: 64 src-port 0 65535 dst-ip 2001:10:3:3:1:2:: 96 dst-port 0 65535
  access-permit "ap1"
   protocol any src-ip :: 0 src-port 0 65535 dst-ip :: 0 dst-port 0 65535
  access-permit "ap3"
   protocol any src-ip 2001:172:110:: 64 src-port 0 65535 dst-ip 2001:10:3:3:1:3:: 96 dst-port 0 65535
  vrf-inside InsideBlue
 activate

```

Configuring WSG Performance/Throughput Indicators

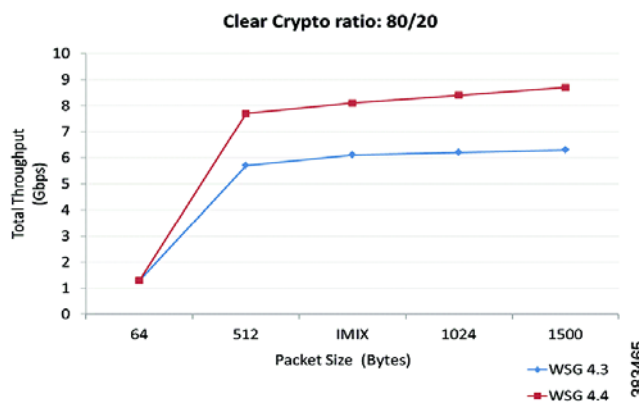
With WSG release 4.4, the IXP Traffic distribution feature is included to increase the overall throughput of the WSG SAMI. This feature provides a method to divide the Clear traffic between 2 IXPs (IXP0 and IXP1) and enables even distribution of traffic among 2 IXPs. The IXP1 now handles more of the post encryption data which was originally handled by IXP0.

Table 2-5 shows the throughput comparison between Release 4.3 and 4.4 when Clear-ESP traffic ratio is 80/20. Figure 2-2 illustrates the same through a line chart.

Table 2-5 Max Throughput comparison between release 4.3 and 4.4 for 80/20 traffic



Packet Size (Bytes)	WSG 4.3 throughput (Gbps)	WSG 4.4 throughput (Gbps)
64	1.3	1.3
512	5.7	7.7
IMIX	6.1	8.1
1024	6.2	8.4
1500	6.3	8.7


Figure 2-2 Line chart for max throughput comparison between release 4.3 and 4.4 for 80/20 traffic



To generate SNMP trap when WSG throughput utilization goes above the configured value, perform the following tasks:

	Command	Purpose
Step 1	<code>switch# config</code>	Enters global configuration mode.
Step 2	<code>switch (config)# snmp-server enable traps ipsec throughput-threshold</code>	Enables the SNMP trap when WSG throughput utilization goes above the configured or default value for a sustained number of intervals.

	Command	Purpose
Step 3	switch (config)# crypto throughput threshold <i>threshold interval interval</i>	Sets the throughput utilization threshold in percentage and number of sustained intervals. By default threshold is 50% and interval is 2. Note Each interval is of 5 mins.
Step 4	wsg# show crypto throughput	Displays the throughput data for the last calculated interval on WSG.
Step 5	wsg# show crypto throughput ixp <1/2>	Displays the throughput data for packets to/from Nitrox and the average throughput utilization for the last calculated interval on WSG for each IXP. IXP0 display also shows the packet data punted to IXP1. <ul style="list-style-type: none">• <i>ixp</i> — Selects IXP number<ul style="list-style-type: none">- 1 — IXP0- 2 — IXP1  Note This command is added with Release 4.4.
Step 6	wsg# show crypto throughput history interval <i>interval type</i>	Displays the history of throughput in Mbp/s and Packets/s. <ul style="list-style-type: none">• <i>interval</i> — Set refresh interval for history stats collection:<ul style="list-style-type: none">- 1 - 5 minutes- 2 - 1 hour- 3 - 3 hours• <i>type</i> — Sets type of unit of throughput:<ul style="list-style-type: none">MbpsKpps (Kilo-Packets-per-second)
Step 7	wsg# show crypto throughput history interval interval type ixp <1/2>	Displays the history of throughput in Mbp/s and Packets/s separately for each IXP. <ul style="list-style-type: none">• <i>ixp</i> — Selects IXP number<ul style="list-style-type: none">- 1 — IXP0- 2 — IXP1  Note This command is added with Release 4.4.
Step 8	wsg# show crypto throughput distribution history	Displays the number of intervals the throughput fell in a certain bucket range. Each interval is 5 minutes.

	Command	Purpose
Step 9	<code>wsg# show crypto throughput distribution history ixp <1/2></code>	<p>Displays the number of intervals the throughput fell in a certain bucket range for each IXP. Each interval is 5 minutes.</p> <ul style="list-style-type: none"> • <i>ixp</i> — Selects IXP number <ul style="list-style-type: none"> - 1 — IXP0 - 2 — IXP1 <p> Note This command is added with Release 4.4.</p>
Step 10	<code>wsg# clear crypto throughput counters</code>	This optional command clears throughput counters.

```
WSG# config
Enter configuration commands, one per line. End with CNTL/Z.
WSG (config)# snmp-server enable traps ipsec throughput-threshold
WSG (config)# crypto throughput threshold 80 interval 5
```

Here are examples of the **show crypto throughput** commands:

```
wsg# show crypto throughput
Throughput (Mbp/s) : 4992
Throughput (Kpp/s) : 626
Average Packet Size (bytes) : 996
Throughput Utilization (%) : 58
Peak Throughput Utilization (%) : 100 Sat Sep 06 15:39:50.012 UTC
Peak Throughput (Mbp/s) : 18400
Peak Packet Size (bytes) : 509

wsg# show crypto throughput ixp 1
Throughput - First Path (Mbp/s) : 3941
Throughput - First Path (Kpp/s) : 501
Average Packet Size - First Path (bytes) : 983
Throughput - Return Path (Mbp/s) : 1051
Throughput - Return Path (Kpp/s) : 125
Average Packet Size - Return Path (bytes) : 1051
Throughput Utilization (%) : 58
Peak Throughput Utilization (%) : 100 Sat Sep 06 15:39:50.012 UTC
Peak Throughput - First Path (Mbp/s) : 9200
Peak Packet Size - First Path (bytes) : 876
Peak Throughput - Return Path (Mbp/s) : 9200
Peak Packet Size - Return Path (bytes) : 1021
Punted to IXP2 (Mbp/s) : 2956
Punted to IXP2 (Kpp/s) : 376
```

Here is an example of the **show crypto throughput history** command:

```
wsg# show crypto throughput history interval 5minutes Kpps ixp 1
3200
3000
2800
2600
2400
2200
2000
1800
1600
```



```

1400
1200 #
1000
800
600
400 #####
200
.... 1....1....2....2....3....3....4....4....5....5....6....6....7..
0 5 0 5 0 5 0 5 0 5 0 5 0 5 0
Kpps per five min (last 6 hrs)

```

Here is an example of the **show crypto throughput distribution history** command:

```

wsg# show crypto throughput distribution history ixp 2
% Throughput Utilization bucket                               Number of Intervals

 1 - 25                                                         0
26 - 50                                                         0
51 - 60                                                         4
61 - 65                                                         0
66 - 70                                                         0
71 - 75                                                         0
76 - 80                                                         0
81 - 82                                                         0
83 - 84                                                         0
85 - 86                                                         0
87 - 88                                                         0
89 - 90                                                         0
91 - 92                                                         0
93 - 94                                                         0
95 - 96                                                         0
97 - 98                                                         0
99 - 100                                                        1

```

Traffic distribution — Hash distribution

To distribute the post encryption traffic among 2 IXPs, a hash table is programmed. The PPC can program this hash table in 2 ways:

- Scheme 1 – Sequential Distribution of hash entries
- Scheme 2 – Random Distribution of hash entries (recommended)

Based on traffic type and distribution of user source/destination ip addresses, an administrator can use either of the scheme to get the best throughput utilization results between both the IXPs. Overall or per IXP utilization can be displayed by the crypto throughput CLIs in PPC as explained above.

Command	Purpose
<pre>switch (config)# crypto clear-traffic load <50%-100%></pre>	<p>Sets the number of punt entries to be programmed into traffic distribution hash table in IXP0 based on the current Clear traffic load %.</p> <ul style="list-style-type: none"> • load — Percentage of clear traffic load <ul style="list-style-type: none"> – 50% — IXP0 is handling 50% of total incoming traffic. No punt entries will be programmed. • • • 100% — IXP0 is handling 100% of total incoming traffic.
<pre>switch (config)# crypto clear-traffic switch-distribution-sch eme <1/2></pre>	<p>Sets the traffic distribution hash table in IXP0 either with sequential punt entries or random punt entries.</p> <ul style="list-style-type: none"> • switch-distribution-scheme — Selects the scheme number <ul style="list-style-type: none"> – 1 — Sequential hashing – 2 — Random hashing (default)

Given below is the IXP show command executed only from IXP0 (proc 1):

Command	Purpose
<pre>ucdump -t puntbl</pre>	<p>Displays the entries programmed in the traffic distribution hash table in IXP0 when the CLI commands are executed from the PPC to enable the traffic distribution.</p>

Here is an example of the **ucdump -t puntbl** command:

```
# ucdump -t puntbl
Punt table entry base is 0x907d0e10 End is 0x907d1210
=====
Word Offset   Hash Addr    Count Addr   Access Count
-----
0             0x1800e10    0x1802210    596587
1             0x1800e14    0x1802214    602678
2             0x1800e18    0x1802218    602680
3             0x1800e1c    0x180221c    602683
4             0x1800e20    0x1802220    602687
:
:
:
250          0x18011f8    0x18025f8    603275
252          0x1801200    0x1802600    603278
254          0x1801208    0x1802608    603282
Test Summary
Total Punt Entries: 192
Punt Entries Accessed: 192
Total Packets: 154715912
Total Packets Punted: 116112365
Achieved Punt %: 75.05
```

Configuring IKE/IPSec Stats Collection and Timing Enhancements for SNMP

To configure the statistics refresh interval for SNMP in manual mode, or be set automatically (auto mode) based on number of IPSec tunnels, perform the following tasks:

	Command	Purpose
Step 1	switch# config	Enters global configuration mode.
Step 2	switch (config)# crypto snmp stats-refresh-interval {auto manual interval}	<p>Configure the statistics refresh interval for SNMP. It can be a fixed interval (manual mode), or be set automatically (auto mode) based on number of IPSec tunnels.</p> <ul style="list-style-type: none"> • auto — Sets referesh interval automatically based on number of tunnels, on average about 1.5 sec for 1000 tunnels. • <i>interval</i> — Set refresh interval manually in range from 1 to 300 sec.

```
WSG# config
```

Enter configuration commands, one per line. End with CNTL/Z.

```
WSG (config)# crypto snmp stats-refresh-interval auto
```




Command Reference for the WSG

The following sections provide details about WSG commands.

Commands appear in the submodes under which you enter them.

Crypto Address-Pool Submode Commands

- [start-ip](#), page 3-7
- [dns-server](#), page 3-9

Crypto Profile Submode Commands

- [activate](#), page 3-11
- [ipsec](#), page 3-12
- [isakmp](#), page 3-13
- [profile-type](#), page 3-14
- [vrf-inside](#), page 3-15
- [vrf-outside](#), page 3-16

EXEC Commands

- [clear crypto cmp](#), page 3-17
- [clear crypto ipsec sa](#), page 3-18
- [clear crypto isakmp sa remote-id](#), page 3-19
- [clear crypto rri](#), page 3-20
- [clear crypto throughput counters](#), page 3-21
- [copy-sup](#), page 3-22
- [copy tftp](#), page 3-26
- [crypto blacklist file resync](#), page 3-27
- [crypto cmp enroll](#), page 3-28
- [crypto cmp initialize](#), page 3-30

- [crypto cmp poll](#), page 3-32
- [crypto cmp update](#), page 3-33
- [crypto rsa-keygen](#), page 3-34
- [username](#), page 3-36

Global Configuration Commands

- [crypto address-pool](#), page 3-38
- [crypto blacklist file](#), page 3-40
- [crypto cert renewal retrieve](#), page 3-41
- [crypto clear-traffic load](#), page 3-42
- [crypto clear-traffic switch-distribution-scheme](#), page 3-43
- [crypto cmp auto-update](#), page 3-44
- [crypto cmp transport](#), page 3-46
- [crypto datapath icmp rate-limit](#), page 3-47
- [crypto dfp agent max-tunnels](#), page 3-48
- [crypto dfp agent max-weight](#), page 3-49
- [crypto dhcp-client](#), page 3-50
- [crypto dhcp-client client-id-type extract-cn](#), page 3-51
- [crypto dhcp-client link-address](#), page 3-52
- [crypto dhcp-server](#), page 3-53
- [crypto dhcp-dns server](#), page 3-54
- [crypto facility](#), page 3-55
- [crypto ike-retry-timeout](#), page 3-56
- [crypto ike-retry-count](#), page 3-57
- [crypto ike-nat-keepalive](#), page 3-58
- [crypto ike-export-buf-size](#), page 3-59
- [crypto ipsec-fragmentation](#), page 3-60
- [crypto ipsec security-association replay](#), page 3-62
- [crypto nameresolver](#), page 3-63
- [crypto pki trustpoint](#), page 3-64
- [crypto pki wsg-cert](#), page 3-65
- [crypto pki wsg-cert-trap expiry notification](#), page 3-67
- [crypto profile](#), page 3-68
- [crypto radius accounting enable](#), page 3-69
- [crypto radius nas-id](#), page 3-70
- [crypto radius nas-ip](#), page 3-71
- [crypto radius-server host](#), page 3-72

- [crypto radius source-ip](#), page 3-73
- [crypto redirect ip](#), page 3-74
- [crypto remote-secret](#), page 3-76
- [crypto responder-redirect enable](#), page 3-77
- [crypto rri enable](#), page 3-78
- [crypto snmp stats-refresh-interval](#), page 3-79
- [crypto site-to-site-lookup](#), page 3-80
- [crypto syslog-level](#), page 3-81
- [crypto throughput threshold](#), page 3-82
- [crypto decrypt auth-failure rate](#), page 3-83
- [ha interface vlan](#), page 3-84
- [ha interface vlan start-id](#), page 3-85
- [ha redundancy-mode](#), page 3-87
- [ha timeout](#), page 3-89
- [interface](#), page 3-90
- [service interface](#), page 3-92
- [hm interval-10sec](#), page 3-94
- [ip name-server](#), page 3-98
- [ip route](#), page 3-99
- [ip ssh auth-type](#), page 3-100
- [ip ssh enable](#), page 3-101
- [ip ssh key dsa](#), page 3-102
- [ip ssh port](#), page 3-103
- [ip ssh radius-server](#), page 3-104
- [ipv6](#), page 3-105
- [ip vrf](#), page 3-106
- [logging](#), page 3-107
- [router bgp](#), page 3-108
- [neighbor](#), page 3-109

ISAKMP/IKE Commands

- [auto-initiate](#), page 3-110
- [dpd-timeout](#), page 3-111
- [sequence-number](#), page 3-113
- [eap-type](#), page 3-114
- [encryption](#), page 3-115
- [group](#), page 3-116

- [hash](#), page 3-117
- [self-identity](#), page 3-119
- [lifetime](#), page 3-121
- [local-secret](#), page 3-122
- [peer-ip](#), page 3-123
- [ike-version](#), page 3-124
- [ike-start-with-natt](#), page 3-125
- [authentication](#), page 3-126

Interface Submode Commands

- [alias](#), page 3-37
- [ip address](#), page 3-95
- [ip address start-ip](#), page 3-96
- [ipv6](#), page 3-127

IPSec Commands

- [ip address-pool](#), page 3-129
- [local-ip](#), page 3-131
- [pfs](#), page 3-132
- [security-association lifetime](#), page 3-133
- [security-association replay](#), page 3-134
- [access-permit](#), page 3-135
- [transform-set](#), page 3-138

Single OAM Commands

- [oam mode single](#), page 3-139
- [oam-ip route](#), page 3-140

Resource Monitoring Commands

- [process cpu threshold](#), page 3-141
- [memory free low watermark processor](#), page 3-142

Show Commands

- [show crypto blacklist file](#), page 3-143

- [show crypto blacklist stats](#), page 3-144
- [show crypto cmp request](#), page 3-145
- [show crypto dhcp](#), page 3-146
- [show crypto ipsec info](#), page 3-147
- [show crypto ipsec summary](#), page 3-148
- [show crypto ipsec sa](#), page 3-153
- [show crypto ipsec sa](#), page 3-153
- [show crypto ipsec sa spi-in](#), page 3-157
- [show crypto isakmp info](#), page 3-159
- [show crypto isakmp sa](#), page 3-161
- [show crypto isakmp summary](#), page 3-164
- [show crypto pki certificate](#), page 3-166
- [show crypto radius statistics](#), page 3-168
- [show crypto throughput](#), page 3-169
- [show crypto throughput ixp](#), page 3-170
- [show crypto throughput distribution history](#), page 3-172
- [show crypto throughput distribution history ixp](#), page 3-173
- [show crypto throughput history](#), page 3-175
- [show crypto throughput history ixp](#), page 3-177
- [show debug crypto](#), page 3-180
- [show ha info](#), page 3-181
- [show hosts](#), page 3-183
- [show icmp6 statistics](#), page 3-184
- [show interface](#), page 3-186
- [show interface internal iftable](#), page 3-188
- [show ip bgp](#), page 3-189
- [show ip interface brief](#), page 3-190
- [show ip route](#), page 3-191
- [show ip route np](#), page 3-192
- [show ip ssh](#), page 3-193
- [show ipv6 neighbors](#), page 3-194
- [show ipv6 route](#), page 3-195
- [show ipv6 route np](#), page 3-196
- [show ip vrf](#), page 3-197
- [show logging](#), page 3-199

SNMP Traps Commands

- [snmp-server enable traps ipsec](#), page 3-200
- [snmp-server host](#), page 3-202

Debug Commands

- [debug crypto](#), page 3-204
- [debug crypto ike remote-ip](#), page 3-205

start-ip

To set up a local IPSec address pool from which to assign addresses to an endpoint during the SA establishment, use the **start-ip** command. To remove the address pool range configuration, use the **no** form of the command.

start-ip *start-ip-address* **end-ip** *end-ip-address* **netmask** *netmask* **ipv6-prefix** *prefix*

no start-ip *start-ip-address* **end-ip** *end-ip-address* **netmask** *netmask* **ipv6-prefix** *prefix*



Note

To modify the pool range, you need to delete an address range and add a new one.

Syntax Description

<i>start-ip-address</i>	First IP address in the address pool range. The format is either A.B.C.D or X:X:X::X.
<i>end-ip-address</i>	Last IP address in the address pool range. The format is either A.B.C.D or X:X:X::X.
netmask <i>netmask</i>	Netmask.
ipv6-prefix <i>prefix</i>	IPv6 prefix. An integer value. The range is 0 to 128.

Defaults

None.

Command Modes

Crypto address-pool submode

Command History

Release	Modification
WSG Release 1.0	This command was introduced as the ipsec address-pool command .
WSG Release 1.1	This command was changed.
WSG Release 3.0	IPv6 support was added, and the ipv6-prefix keyword was added.

Usage Guidelines

Use the **start-ip** command to set up a local address pool from which to assign addresses to an endpoint. The WSG keeps a pool of private addresses from the protected network. When the WSG receives an endpoint SA with an internal IP address request, it assigns an unused address from the address pool. The address does not expire as long as the SA is up. When the SA is removed, the address is released to the local pool.

Examples

This example shows how to set up an address pool name:

```
switch(config-address-pool)# crypto address-pool "dummy"

switch(config-address-pool)# start-ip 2001:0DB8:1:0::0 end-ip 2001:0DB8:1:FC00::0 ?
  ipv6-prefix Enter IPV6 prefix
```

```
netmask      Enter IPV4 netmask
switch(config-address-pool)# start-ip 2001:0DB8:1:0::0 end-ip 2001:0DB8:1:FC00::0
ipv6-prefix ?
  <0-128>  Enter IPV6 prefix
switch(config-address-pool)# start-ip 2001:0DB8:1:0::0 end-ip 2001:0DB8:1:FC00::0
ipv6-prefix 64
```

dns-server

To specify the DNS server that is passed to the access point (the remote end point) when there is a request for a DNS server during IKE negotiation, use the **dns-server** command in crypto-profile submode. Use the **no** form of the command to disable this feature.

dns-server *ip_address*

no dns-server

Syntax Description

<i>ip_address</i>	The <i>ip_address</i> is the DNS server IP address that is given to the endpoint by the WSG when requested. The <i>ip_address</i> format is either <i>A.B.C.D</i> or <i>X:X:X::X</i> .
-------------------	--

Defaults

The default is that the **dns-server** is unconfigured.

Command Modes

Crypto address-pool submode.

Command History

Release	Modification
WSG Release 1.2	This command was introduced.
WSG Release 3.0	IPv6 support was added.

Usage Guidelines

If the DNS server name is not required to be sent to the remote access point, this command is not required.

In WSG Release 3.0, the **dns-server** command is modified to accept both IPv4 and IPv6 addresses for the server configuration.

Examples

This example shows how to enable the **dns-server** command:

```
WSG# conf t
Enter configuration commands, one per line. End with CNTL/Z.
WSG(config)# crypto address-pool foo
WSG(config-address-pool)# dns-server ?
  <A.B.C.D> Enter IP address
WSG(config-address-pool)# dns-server 172.20.10.1
IPv6 example:
Crypto address-pool <name>
  dns-server ?
    <A.B.C.D>|<X:X:X::X> Enter IP address
Crypto address-pool foo
  dns-server 2001:10:22::10
```


activate

To activate a profile, use the **activate** command. To deactivate a profile, use the **no** form of the command.

activate

no activate



Note

- The profile must be active to establish tunnels/SA.
- If the profile is deactivated, all tunnels/SA will be destroyed.

Defaults

None.

Command Modes

Crypto profile submode

Command History

Release	Modification
WSG Release 1.1	This command was introduced.

Usage Guidelines

Use the **activate** command to activate a profile.

Examples

This example shows how to activate a profile using the **activate** command:

```
WSG(config-crypto-profile)# activate
```

ipsec

To enter the IPsec submode use the **ipsec** command in crypto profile submode. Use the **no** form of the command, or **exit** to exit the IPsec submode.

ipsec

no ipsec

Defaults

There are no default values.

Command Modes

Crypto profile submode

Command History

Release	Modification
WSG Release 1.1	This command was introduced.

Examples

This example shows how to enter the **ipsec** submode:

```
WSG(config-crypto-profile)# ipsec
```


isakmp

To enter the ISAKMP submode, use the **isakmp** command under the crypto profile submode. Use the **no** form of the command or **exit** to exit the ISAKMP submode.

isakmp

no isakmp

Defaults

None.

Command Modes

Crypto profile submode

Command History

Release	Modification
WSG Release 1.1	This command was introduced.

Examples

This example shows how to enter the ISAKMP submode:

```
WSG(config-crypto-profile)# isakmp  
WSG(config-crypto-profile-isakmp)#
```

profile-type

To specify the type of each profile created by the user, use the **profile-type** command in crypto profile submode. Use the **no** form of the command to disable this feature.

profile-type {remote-access | site-to-site}

no profile-type {remote-access | site-to-site}

Syntax Description

remote-access	Type remote-access (default).
site-to-site	Type site-to-site.

Defaults

Remote access.

Command Modes

Crypto profile submode.

Command History

Release	Modification
WSG Release 1.2	This command was introduced.

Usage Guidelines

A crypto profile can be either remote access type, or site-to-site type. The **profile-type** command is used to specify the type of each profile that you create. If the type is not specified the default is remote-access.

Only one remote access profile can be active.

Multiple Site-to-site profiles can be active.

You should take special care to configure the proper access-permit command that corresponds to the profile type used, as described in the **access-permit** command.

Examples

This example illustrates the default setting:

```
WSG(config)# crypto profile One
WSG(config-crypto-profile)# profile-type ?
  remote-access Profile Type remote-access (default)
  site-to-site   Profile Type site-to-site
```

vrf-inside

To add an inside VRF, use the **vrf-inside** command to the IPsec submode of a profile. To remove a VRF, use the **no** form of the command, including the specific *vrf_name*.

```
vrf-inside vrf_name
```

```
no vrf-inside vrf_name
```

Syntax Description

<i>vrf_name</i>	Specifies the name of the VRF.
-----------------	--------------------------------

Defaults

The default inside *vrf_name* is global.

Command Modes

IPsec submode

Command History

Release	Modification
WSG Release 3.0	This command was introduced.

Usage Guidelines

By default, the inner IP addresses of a profile belong to a VRF, which is VRF_GLOBAL (VRF_NAME = global). In order to associate the inner IP addresses with a specific VRF, use the **vrf-inside** *vrf_name* command. To remove an inside VRF, use the **no vrf-inside** *vrf_name* command.

Examples

This example shows how to add an inside VRF using the **vrf-inside** command:

```
wsg(config-crypto-profile-ipsec)# vrf-inside insideGreen
```

vrf-outside

To add an outside VRF, use the **vrf-outside** command in the ISAKMP submode of a profile. To remove a VRF, use the **no** form of the command, including the specific *vrf_name*.

vrf-outside *vrf_name*

no vrf-outside *vrf_name*

Syntax Description

<i>vrf_name</i>	Specifies the name of the VRF.
-----------------	--------------------------------

Defaults

The default outside *vrf_name* is global.

Command Modes

ISAKMP submode

Command History

Release	Modification
WSG Release 3.0	This command was introduced.

Usage Guidelines

By default, the outer IP addresses of a profile belong to a VRF, which is VRF_GLOBAL (VRF_NAME = global). In order to associate the outer IP addresses with a specific VRF, use the **vrf-outside** *vrf_name* command.

Examples

This example shows how to add an outside VRF using the **vrf-outside** command:

```
wsg(config-crypto-profile-isakmp)# vrf-outside outsideGreen
```

clear crypto cmp

To clear a pending CA request generated by this WSG, use the **clear crypto cmp** command in privileged EXEC mode.

clear crypto cmp

Syntax Description There are no keywords or arguments for this command.

Command Default None.

Command Modes Privileged EXEC

Command History	Release	Modification
	WSG Release 2.0	This command was introduced.

Usage Guidelines The **clear crypto cmp** command clears a pending CA request generated by this WSG. This allows you to make another CA request before the previous CA request is honored. No cancellation is sent to the CA server; only the state of the pending request on the WSG is cleared.



Note The **clear crypto cmp** command will not clear auto-update requests.

Examples Here is an example of the **clear crypto cmp** command:
WSG# **clear crypto cmp**


clear crypto ipsec sa

To clear all tunnels and security associations, use the **clear crypto ipsec sa** command in privileged EXEC mode.

```
clear crypto ipsec sa [ A.B.C.D | X:X:X::X ] [ vrf vrf_name ]
```

```
clear crypto ipsec sa [ profile_name ]
```

Syntax Description

none	 <p>Caution This is very destructive. Destroys all tunnels and SAs.</p> <ul style="list-style-type: none"> This would restore the tunnels on the site-to-site profiles if the auto-initiate is turned on at the local or remote peer node.
A.B.C.D X:X:X::X	Peer IPv4 or IPv6 address—removes one tunnel based on the peer IP address specified.
vrf_name	Specifies the VRF.
profile_name	Destroy all tunnels and SAs associated with a particular profile. <ol style="list-style-type: none"> This command is supported for site-to-site profile types only. This would restore the tunnels on the site-to-site profiles if the auto-initiate is turned on at local or remote peer node.

Command Default

None.

Command Modes

Privileged EXEC

Command History

Release	Modification
WSG Release 1.1	This command was introduced.
WSG Release 3.0	IPv6 support was added.

Examples

Here is an example of the **clear crypto ipsec sa** command:

```
WSG# clear crypto ipsec sa ?
  <A.B.C.D> Enter Peer IPv4 address
  <X:X:X::X/n> Enter an IPv6 prefix
  <WORD> Specify profile to clear Sa's (Max Size - 50)
  <cr> Carriage return
WSG# clear crypto ipsec sa
or
WSG# clear crypto ipsec sa 50.0.0.1
or
WSG# clear crypto ipsec sa 2001:88:88:94::1
or
WSG# clear crypto ipsec sa site-to-site
```

clear crypto isakmp sa remote-id

To delete all IKE and IPsec security associations with a remote ID, use the **clear crypto isakmp sa remote-id** command in privileged EXEC mode.

```
clear crypto isakmp sa remote-id {dn | email | fqdn | ip}
```

Syntax Description

dn	Remote ID type Distinguished Name
email	Remote ID type e-mail
fqdn	Remote ID type FQDN
ip	Remote ID type IP

Command Default

This command is disabled by default.

Command Modes

Privileged EXEC

Command History

Release	Modification
WSG Release 3.0	This command was introduced.

Examples

Here is an example of the **clear crypto isakmp sa remote-id** command:

```
wsg# clear crypto isakmp sa remote-id ?
dn      Remote ID type Distinguished Name
email   Remote ID type email
fqdn    Remote ID type fqdn
ip      Remote ID type IP
```

clear crypto rri

To delete the crypto RRI IP address, use the **clear crypto rri** command in privileged EXEC mode.

clear crypto rri *IP_address*

Syntax Description	<i>IP_address</i>	The IPv4 or IPv6 address. The format is either A.B.C.D or X:X:X::X.
Command Default	None.	
Command Modes	Privileged EXEC	
Command History	Release	Modification
	WSG Release 4.0	This command was introduced.

Examples

Here is an example of the **clear crypto rri** command:

```
wsg# clear crypto rri ?
<A.B.C.D>|<X:X:X::X> Enter Peer IPv4 or IPv6 address
```


clear crypto throughput counters

To delete the crypto throughput counters, use the **clear crypto throughput counters** command in privileged EXEC mode.

clear crypto throughput counters

Syntax Description There are no keywords or arguments for this command.

Command Default None.

Command Modes Privileged EXEC

Command History	Release	Modification
	WSG Release 4.2	This command was introduced.

Examples Here is an example of the **clear crypto throughput counter** command:

```
wsg# clear crypto throughput counter
```

copy-sup

To copy files and running configurations to and from the SUP, use the **copy-sup** command in privileged EXEC mode.

```
copy-sup src_file dst_file
```

Syntax Description

<i>src_file</i>	Specifies the source file.
<i>dst_file</i>	Specifies the destination file.

Command Default

This command is disabled by default.

Command Modes

Privileged EXEC

Command History

Release	Modification
WSG Release 3.0	This command was introduced.

Usage Guidelines

You can run the **copy-sup** command in single-entity mode.

If the source file is the running-config or a file from one of the following PPC filesystems:

log:
core:
disk0:

Then the destination file is a file at one of the following SUP filesystems:

bootdisk-sup:
bootflash-sup:
disk0-sup:

If the source file is a file from one of the following SUP filesystems:

bootdisk-sup:
bootflash-sup:
disk0-sup:

Then the destination file can be the running-config or a file at one of the following PPC filesystems:

log:
core:
disk0:

This command will attach the *slot#ppc#* tag for either entity **all** or entity **none** modes (i.e. SLOT3SAMIC3_) to the front of the file name saved at the SUPs. The command will also attach the “.cfg” tag to the end of the file name when you save the running configuration file to the SUPs.

You do not need to type in the tags when you specify the source or destination file names for **copy-sup**. The tags are automatically generated by the command.

The directory names used by this command that refer to the SUP filesystems are:

```
disk0-sup:
bootdisk-sup:
bootflash-sup:
```

Examples

Here are examples of the **copy-sup** command:

```
copy-sup ?
 bootdisk-sup:  Select source file system at the SUP
 bootflash-sup: Select source file system at the SUP
 core:         Select source file system
 disk0-sup:    Select source file system at the SUP
 disk0:       Select source file system
 log:         Select source file system
 running-config Copy running configuration to destination
switch# copy-sup running-config ?
 bootdisk-sup:  Select destination file system at the SUP
 bootflash-sup: Select destination file system at the SUP
 disk0-sup:    Select destination file system at the SUP
switch# copy-sup running-config disk0-sup: ?
 <cr> Carriage return.
switch# copy-sup running-config disk0-sup:
```

Copy File to the Sup

A file at the PPC can be copied to the SUP's disk0, bootflash (or bootdisk) directory:

```
switch# copy-sup src_file sup-disk0:filename | sup-bootflash:filename |
sup-bootdisk:filename
```

If the remote filename is not specified, this command will prompt you for the remote file name to be used on the SUP.

Example 1 (entity none mode):

```
switch# copy-sup log:messages sup-disk0:myLogMessages
Copying operation succeeded.
switch#
```

Example 2 (entity node mode):

```
switch# copy-sup log:messages sup-bootflash:
Enter the destination filename[]?myLogMessages
Copying operation succeeded.
switch#
```

The following file on the SUP will be created as the result of above command:

```
bootflash:myLogMessages
```

Example 3 (entity all mode):

```
Switch(mode-all)#copy-sup log:messages sup-bootflash:myLogMessages
```

The following example files are created on the SUP:

```
SLOT3SAMIC3_myLogMessages
SLOT3SAMIC4_myLogMessages
```

```
SLOT3SAMIC5_myLogMessages
SLOT3SAMIC6_myLogMessages
SLOT3SAMIC7_myLogMessages
SLOT3SAMIC8_myLogMessages
```

Copy Running Config File to the Sup

Here are examples of the **copy-sup** command used to copy running configurations to the SUP:

```
switch# copy-sup running-config sup-disk0:filename | sup-bootflash:filename |
sup-bootdisk:filename
```

If the remote filename is not specified, this command prompts you for the remote file name to be used on the SUP. The configuration files at the SUP have the “.cfg.” attached.

Example 1 (entity none mode):

```
switch# copy-sup running-config sup-bootflash:myconfig
Copying operation succeeded.
switch#
```

The following file is created on the SUP as the result of the previous command (for example, the command is entered from slot#3/ppc#5):

```
bootflash:SLOT3SAMIC5_myconfig.cfg
```

Example 2 (entity all mode):

```
switch# copy-sup running-config sup-bootflash:myconfig
Copying operation succeeded.
switch#
```

The following files are created on the SUP as the result of the previous command:

```
bootflash:SLOT3SAMIC3_myconfig.cfg
bootflash:SLOT3SAMIC4_myconfig.cfg
bootflash:SLOT3SAMIC5_myconfig.cfg
bootflash:SLOT3SAMIC6_myconfig.cfg
bootflash:SLOT3SAMIC7_myconfig.cfg
bootflash:SLOT3SAMIC8_myconfig.cfg
```

Copy File from the Sup

Here are examples of the **copy-sup** command used to copy files from the SUP:

If the remote or local file names are not specified, this command prompts you for the local and remote file names to be copied.

Example 1 (entity none mode),

```
switch# copy-sup sup-bootflash:myFileAtSup disk0:myFile
Copying operation succeeded.
```

The following file from the SUP is copied as the result of the previous command:

```
bootflash:myFileAtSup
```

Example 2 (entity all mode),

```
switch# copy-sup sup-bootflash:myFileAtSup disk0:myFile
Copying operation succeeded.
```

The following file from the SUP will be copied as the result of above command:

```
bootflash:myFileAtSup
```

Each PPC will have the file disk0:myFile.

Copy Running Config file from the Sup

Here are examples of the **copy-sup** command used to copy running configuration files from the SUP:

```
switch# copy-sup sup-disk0:filename | sup-bootflash:filename | sup-bootdisk:filename  
running-config
```

If the remote file name is not specified, this command will prompt the user for the remote config file name to be copied.

Example 1 (entity none mode),

```
switch# copy-sup sup-bootflash:myConfig running-config  
Copying operation succeeded.
```

As the result of issuing the previous command, the following file from the SUP is copied (for example, the command is entered from slot#3/ppc#5), and the current running configuration is replaced with it:

```
bootflash:SLOT3SAMIC5_myConfig.cfg
```

Example 2 (entity all mode),

```
switch# copy-sup sup-bootflash:myConfig running-config  
Copying operation succeeded.
```

The following files from the SUP will be copied as the result of above command:

```
bootflash:SLOT3SAMIC3_myConfig.cfg  
bootflash:SLOT3SAMIC4_myConfig.cfg  
bootflash:SLOT3SAMIC5_myConfig.cfg  
bootflash:SLOT3SAMIC6_myConfig.cfg  
bootflash:SLOT3SAMIC7_myConfig.cfg  
bootflash:SLOT3SAMIC8_myConfig.cfg
```

The running configuration of each of the PPCs is replaced by the corresponding file.

copy tftp

To allow an IPv6 address to be specified as the source or destination IP address in a copy configuration, use the **copy tftp** command in privileged EXEC mode.

copy tftp

Syntax Description

There are no keywords or arguments for this command.

Command Modes

Privileged EXEC

Command History

Release	Modification
WSG Release 3.0	This command was introduced.

Examples

Here is an example of the **copy tftp** command:

```
switch# copy tftp://2001:88:88:94::1/auto/tftpboot-users/user-eng/ppc4.out disk0:ppc4.out
```

crypto blacklist file resync

To recopy the blacklist file from the SUP disk and inform the WSG IKE stack about the update, use the **crypto blacklist file resync** command in privileged EXEC mode.

crypto blacklist file resync

Syntax Description There are no keywords or arguments for this command.

Defaults By default the feature is disabled.

Command Modes Privileged EXEC

Command History	Release	Modification
	WSG Release 3.0	This command was introduced.

Usage Guidelines If you need to update the blacklist entries, follow this procedure:

- Edit the blacklist file outside the Cisco 7600 chassis.
- Copy the blacklist to the SUP disk with the same file name that you initially used.

Execute the **crypto blacklist file resync** command on the WSG. The WSG copies the updated file from the SUP disk to its ramdisk, and informs the IKE stack about the updated file. The IKE stack now uses the new blacklist file.

Examples The following example shows how to resync the blacklist file:


```
WSG# crypto blacklist file resync
```

crypto cmp enroll

To generate an enroll certificate request to the CA server using the public key, use the **crypto cmp enroll** command in privileged EXEC mode.

```
crypto cmp enroll current-wsg-cert wsg_certificate current-wsg-private-key wsg_privatekey
modulus modulus id-type id-type id id subject-name subject_string ca-root root_certificate
ca-url url [pop]
```

Syntax Description

<i>wsg_certificate</i>	Current valid WSG certificate.
<i>wsg_privatekey</i>	Current valid private key corresponding to the certificate provided in the previous parameter.
<i>modulus</i>	Modulus of the generated certificate: 512, 1024, or 2048.
<i>id-type</i>	Type of ID: fqdn or ip.
<i>id</i>	ID can be a domain name. If ID type is ip, it can be an IPv4 or IPv6 address.
<i>“subject_string”</i>	Subject string of the certificate in double quotes.
 Note	
The supported characters while configuring the subject-name are dash, dot, underscore, a-z, A-Z and 0-9. The maximum size supported for the string is 256 bytes.	
<i>root_certificate</i>	Filename of the CA root certificate (should be in DER format) present on the SUP bootflash disk.
<i>url</i>	URL (must start with “http://” or “tcp://”) where the CA server listens to get requests.
pop	Enables indirect encryption method of proof-of-possession.

Command Default

None.

Command Modes

Privileged EXEC

Command History

Release	Modification
WSG Release 2.1	This command was introduced.
WSG Release 3.0	IPv6 support and pop keyword were added.

Usage Guidelines

You provide the existing WSG certificate and private key as input parameters to the CLI. The filenames for the new private key and the certificate files are automatically generated by the system. This request is similar to initialize except that it is authenticated using public-key methods.

**Note**

In WSG Release 4.0 and below, the *subject_string* cannot include spaces.

Examples

Here is an example of the **crypto cmp enroll** command:


```
WSG# crypto cmp enroll current-wsg-cert wsg.crt current-wsg-private-key wsg.prv  
modulus 1024 id-type fqdn id wsg.cisco.com subject-name  
"C=US,O=Cisco,OU=Security,CN=Example" ca-root root-ca.crt ca-url  
http://212.246.144.35:8700/pkix/
```

crypto cmp initialize

To configure the WSG to generate a private key and make an initialize request to the CA server using CMPv2, use the **crypto cmp initialize** command in privileged EXEC mode.

```
crypto cmp initialize modulus modulus id-type id-type id id subject-name subject_string ca-psk
reference-number:key ca-root root_certificate ca-url url
```

Syntax Description

<i>modulus</i>	Modulus of the generated certificate: 512, 1024, or 2048.
<i>id-type</i>	Type of ID: fqdn or ip.
<i>id</i>	ID can be a domain name. If ID type is ip, it can be an IPv4 or IPv6 address.
<i>subject_string</i>	Subject string of the certificate in double quotes (we can include the subject alternate name subsequent to a colon).
	
Note	
The supported characters while configuring the subject-name are dash, dot, underscore, a-z, A-Z and 0-9. The maximum size supported for the string is 256 bytes.	
<i>reference-number:key</i>	CA issued reference number and corresponding key value for CMPv2 operation.
<i>root_certificate</i>	Filename of the CA root certificate (should be in DER format) present on the SUP bootflash disk.
<i>url</i>	URL (must start with “http://” or “tcp://”) where the CA server listens to get requests.

Command Default

None.

Command Modes

Privileged EXEC

Command History

Release	Modification
WSG Release 2.0	This command was introduced.
WSG Release 3.0	Data storage capabilities and IPv6 support were added.

Usage Guidelines

The request is authenticated using the reference number and corresponding PSK received from the CA. The data you input will be stored in a database that is synchronized between the active and standby SUPs. The *initialize_config.txt* file that has the init parameters is stored on the PPC */app/segw/initialize_config.txt*.



Note In WSG Release 4.0 and below, the *subject_string* cannot include spaces.

Examples

Here is an example of the **crypto cmp initialize** command:

```
Router# crypto cmp initialize modulus 1024 id-type fqdn id wsg.cisco.com subject-name  
"C=US,O=Cisco,OU=Security,CN=Example" ca-psk 32438:this_is_very_secret ca-root  
root-ca.crt ca-url http://212.246.144.35:8700/pkix/
```

crypto cmp poll

To configure the WSG to poll the CA server for the availability of the pending certificate request (update, enroll, or initialize), use the **crypto cmp poll** command in privileged EXEC mode.

crypto cmp poll

Syntax Description There are no keywords or arguments for this command.

Command Default None.

Command Modes Privileged EXEC

Command History

Release	Modification
WSG Release 2.0	This command was introduced.

Usage Guidelines Use the **show crypto cmp request** command to see the pending request that will be polled.

Examples

Here is an example of the **crypto cmp poll** command:

```
Router# crypto cmp poll
```

crypto cmp update

To send an update request to the CA server using CMPv2 to update the existing WSG certificate, use the **crypto cmp update** command in privileged EXEC mode.

```
crypto cmp update current-wsg-cert wsg_certificate current-wsg-private-key wsg_privatekey
ca-root root_certificate ca-url url
```

Syntax Description		
<i>wsg_certificate</i>		Current valid WSG certificate.
<i>wsg_privatekey</i>		Current valid private key corresponding to the certificate provided in the previous parameter.
<i>root_certificate</i>		Filename of the root certificate of the CA server (file present on SUP disk).
<i>url</i>		URL (must start with “http://” or “tcp://”) where the CA server listens to get requests.

Command Default None.

Command Modes Privileged EXEC

Command History	Release	Modification
	WSG Release 2.1	This command was introduced.

Usage Guidelines You provide the existing WSG certificate and private key as input parameters to the CLI. The filenames for the new private key and the certificate files are automatically generated by the system.



Note If you issue this command to update a certificate that has been configured for auto-update or retrieval, a notice is displayed. This is not an error, just a notification. A manual update will change the certificate’s certificate and private key filenames. If you perform auto-update or retrieval using the new certificate and private key files, the auto-update and renewal must be reconfigured on all the active PPCs.


Examples Here is an example of the **crypto cmp update** command:

```
WSG# crypto cmp update current-wsg-cert wsg.crt current-wsg-private-key wsg.prv ca-root
root-ca.crt ca-url http://212.246.144.35:8700/pkix/
```

crypto rsa-keygen

To generate an RSA key pair and Certificate Signing Request (CSR), use the **crypto rsa-keygen** command in privileged EXEC mode.

crypto rsa-keygen modulus *modulus_value* **id-type** *id-type* **id** *id* **subject-name** *subject-name*

Syntax Description	
<i>modulus_value</i>	Enter the modulus value. The integer value is 1, 512, 1024, 2048, or 4096.
<i>id-type</i>	<p>IKE identify of the client. The IKE identity is the identity the remote client uses when authenticating to the gateway. Valid values are:</p> <ul style="list-style-type: none"> • fqdn—Fully-qualified domain name • IP—IP address
<i>subject-name</i>	<p>Distinguished name (DN) that defines the entity associated with this certificate.</p> <p>List of attributes, separated by commas and enclosed in double quotes (“,”), that identify the entity associated with this certificate. These attributes are commonly used in subject-names:</p> <ul style="list-style-type: none"> • CN—Common name of the user in the directory • OU—Organizational unity in the directory • O—Organization in the directory • L—Locality in the directory • ST—State in the directory • C—Country in the directory
	<p> Note The supported characters while configuring the subject-name are dash, dot, underscore, a-z, A-Z and 0-9. The maximum size supported for the string is 256 bytes.</p>

Defaults None.

Command Modes Privileged EXEC

Command History	Release	Modification
	WSG Release 1.0	This command was introduced as the ipsec rsa-keygen command.
	WSG Release 1.1	This command was changed.

Usage Guidelines

RSA key pairs sign, encrypt, and decrypt. To get a CA, you first need a CSR.

1. The **crypto rsa-keygen** command makes a private key (segwSLOTxSAMIx.prv) and a CSR (segw-pem.csr) based on the CSR parameters you enter.
2. The private key file is copied to the SUP engine bootflash or bootdisk, depending on which is available. The default filename for the the private key is segwSLOTxSAMIx.prv where x is a slot and processor number that may vary. An example would be asegwSLOT3SAMI6.prv.
3. The public key, the second key of the key pair, is embedded in the CSR. The default filename for the the certificate request is segw-pem.csr.

**Note**

If all WSGs on a SAMI must share the same certificate, use the **crypto rsa-keygen** command one time on one WSG. If the WSGs must use separate certificates, use the **crypto rsa-keygen** command on each WSG on the SAMI.

Examples

This example shows how to generate an RSA key pair and CSR for a client:

```
WSG# config
Enter configuration commands, one per line. End with CNTL/Z.
WSG(config)# crypto rsa-keygen modulus 1024 id-type fqdn id test.cisco.com subject-name
"C=US,OU=DEV,CN=Test"
Generating certificate request...done.
Copying private key (wsg.prv) to SUP...done.
Copying certificate request (wsg-pem.csr) to SUP...done.

-----BEGIN CERTIFICATE REQUEST-----
MIIBrjCCARcCAQAwNTELMkGA1UEBhMCVVMxDTALBgNVBAsTBWFNNQ1UxZzAVBgNV
BAMTDnNlZ3cuY2lzy28uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCx
sJE11PDrytSqzGH7aVi4fmf8rXygmYCCoPvnIQybMojt5PdObtbXREJ2r4ON6Y
gh4E+IXbIe3yig6friBFMEkYgQJuLe13P8wELDdHyWA6vBLzVgZuwa34Me8B0nKa
LMaU7kz47sConEOElc27NB16mI5D4rVdBnacj4/GCQIDAQABoDkwNwYJKoZIhvcN
AQkOMsowKDALBgNVHQ8EBAMCBaAwGQYDVR0RBBIwEIIOc2Vndy5jaXNjby5jb20w
DQYJKoZIhvcNAQEFBQADgYEASEqXB00k1VfguVdUf9LU4Im1+31+hWErFp/M5Nh4
r+h5ukmCW9ldPPIZxOkV2n2wedLf6mUKTcdzdOLUiwgrSozHSfLWgpXW+upxZDgn
Nk/LvIw3+NpwnjzCmYJEZKFPwglxKzzwMAe99AOPH+Z6yhrw5ffcc9qZCCcWXkeHw
1Iw=
-----END CERTIFICATE REQUEST-----
```

username

To configure the SSH username, use the **username** configuration command. Use the **no** form of the command to unconfigure a user.

username *name of user* **password** *0 unencrypted password*

username *name of user* **password** *5 encrypted password*

no username *name of user*

Syntax Description

<i>name of user</i>	The name of the user.
<i>unencrypted password</i>	The unencrypted password.
<i>encrypted password</i>	The encrypted password.

Command Modes

Global configuration

Command History

Release	Modification
WSG Release 3.0	This command was introduced.

Usage Guidelines

The first variant of the command takes an unencrypted password and subsequently encrypts it. When it is next displayed using the **show running-configuration** command, it will display the encrypted version.

The second variant requires an encrypted password, and is used mainly to transfer a login/password to a different card. Unencrypted passwords will never be displayed.

The **no** variant does not require the password.

The maximum length for the *username* is 32 characters. The maximum length for the unencrypted password is also 32 characters. The maximum permissible length for the encrypted password is 64 characters. Permitted characters for all of the above fields are standard alphanumeric characters with the exception of “]”, “?”, “\$”, TAB, and spaces.

Examples

Here is an example of the **username** command:

```
switch(config)# username test1 password 5 f2500a1a1dJID.4KVT0YvcPR.E98F/
```


alias

To configure the alias IP address for a VLAN on both the active and standby, use the **alias** command in interface configuration submode. Use the **no** form of the command to remove the alias.

```
alias ip_address netmask
```

```
no alias
```

Syntax Description	<i>ip_address netmask</i>	Specifies the alias IP address and its subnet netmask for a VLAN.
--------------------	---------------------------	---

Defaults	None.
----------	-------

Command Modes	Interface configuration submode
---------------	---------------------------------

Command History	Release	Modification
	WSG Release 2.0	This command was introduced.

Usage Guidelines	The alias IP address is configured for a VLAN on both the active and standby. FAP/HNB uses the alias IP address instead of the active IP address. When a switchover or failover occurs, the newly-active node starts receiving traffic destined to this alias IP address.
------------------	--

Examples	The following examples show how to configure the alias IP address on 2 PPCs:
----------	--

On Slot#1/PPC#3:

```
WSG (config) # interface vlan 50
WSG (config-if) # ip address 88.88.23.33 255.255.255.0
WSG (config-if) # alias 88.88.23.35 255.255.255.0
```

On Slot#3/PPC#3:

```
WSG (config) # interface vlan 50
WSG (config-if) # ip address 88.88.23.34 255.255.255.0
WSG (config-if) # alias 88.88.23.35 255.255.255.0
```

crypto address-pool

To set up a local IPsec address pool from which to assign addresses to an endpoint during the SA creation, or to add an address pool, use the **crypto address-pool** command. To remove the address pool, use the **no** form of the command.

```
crypto address-pool pool_name [start-ip start-ip end-ip end-ip < netmask | ipv6-prefix >
netmask | dns-server ip_address | do | end | exit | no ]
```

```
no crypto address-pool pool_name
```



Note

address pool configuration changes will only take effect after a **no activate -> activate** command sequence.

Syntax Description

<i>pool_name</i>	Name of the IPsec address pool.
start-ip	The starting IP address.
<i>end-ip</i>	The ending IP address.
netmask	The IPv4 netmask or IPv6 prefix.
<i>ip_address</i>	The IPv4 or IPv6 DNS server address. The format is either A.B.C.D or X:X:X::X.
do	EXEC command.
end	Exits from configuration mode.
exit	Exits from this submenu.
no	Negate a command or set its defaults.

Defaults

None.

Command Modes

Global configuration

Command History

Release	Modification
WSG Release 1.0	This command was introduced as the ipsec address-pool command .
WSG Release 1.1	This command was replaced.
WSG Release 3.0	The command was modified to include IPv4 and IPv6 IP addresses and subnets.

Usage Guidelines

Use the **crypto address-pool** command to change an address pool.

In WSG Release 3.0, the command is modified to accept both IPv4 (A.B.C.D) and IPv6 (X:X:X::X) addresses with the subnet in netmask and prefix format.

Additionally, the **dns-server** *ip_address* was modified to accept IPv6 addresses.

Examples

This example shows how to add an IPv6 address pool named *foo*:

```
WSG# config
WSG(config)# crypto address-pool foo
start-ip 2001:0DB8:1:0::0 end-ip 2001:0DB8:1:FC00::0 ipv6-prefix 64
```

crypto blacklist file

To configure the blacklist filename on the WSG, use the **crypto blacklist file** global configuration command. Use the **no** form of the command to disable the blacklisting feature.

crypto blacklist file *filename*

no crypto blacklist file *filename*

Syntax Description	<i>filename</i>	The IKE ID that is to be blacklisted. The blacklist file must be present on the SUP disk before this configuration is done. If the file is not present on the SUP, the configuration fails.
---------------------------	-----------------	---

Defaults	By default the feature is disabled.
-----------------	-------------------------------------

Command Modes	Global configuration.
----------------------	-----------------------

Command History	Release	Modification
	WSG Release 3.0	This command was introduced.

Usage Guidelines	<p>You must edit the blacklist file outside of the Cisco 7600 chassis, and copy it to the SUP bootflash or SUP bootdisk. Initially, you should configure the WSG with the filename of the blacklist file. During this configuration, the blacklist file is internally rep-ed from the SUP disk to the WSG ram disk, and the IKE stack is informed of the location of the file. The IKE stack performs blacklisting based on the entries in the file. If you need to update the blacklist entries, follow this procedure:</p> <ul style="list-style-type: none"> • Edit the blacklist file outside the Cisco 7600 chassis. • Copy the blacklist to the SUP disk with the same file name that you initially used. <p>Execute the crypto blacklist file resync command on the WSG. The WSG copies the updated file from the SUP disk to its ramdisk, and informs the IKE stack about the updated file. The IKE stack now uses the new blacklist file.</p>
-------------------------	---

Examples	The following examples show how to configure the blacklisting feature on the WSG:
-----------------	---

```
WSG(config)# crypto blacklist file
```

crypto cert renewal retrieve

To specify the parameters for copying renewed certificate files from the SUP, use the **crypto cert renewal** global configuration command. To disable this feature, use the **no** form of the command to remove all certificate entries configured for renewal retrieve.

```
crypto cert renewal retrieve current-wsg-cert cert_file current-wsg-private-key pvk_file
time time
```

```
no crypto cert renewal retrieve current-wsg-cert cert_file current-wsg-private-key pvk_file
```

Syntax Description	Parameter	Description
	cert_file	Name of the CMP certificate file to update, ending with .crt.
	pvk_file	Name of the Private Key file, ending with .prv.
	time	Time in days to start automatic renewal before certificate expires. The range is 2 to 60 days. We suggest a minimum value of 8 days.

Command Default None.

Command Modes Global configuration

Command History	Release	Modification
	WSG Release 3.0	This command was introduced.

Usage Guidelines This feature is enabled as long as there is at least one certificate configured for renewal retrieve. To disable this feature, use the **no** form of the command to remove all certificate entries configured for renewal retrieve.



Note If a manual update of the certificate and private key file is performed using the **crypto cmp update EXEC** mode command, use the **crypto cert renewal retrieve** command to remove the old certificate filename and add the updated certificate filename.

Examples Here is an example of the **crypto cert renewal retrieve** command:

```
WSG(config)# crypto cert renewal retrieve current-wsg-cert wsg.crt
current-wsg-private-key wsg.prv time 30
```

crypto clear-traffic load

This command is used to set the number of punt entries to be programmed into traffic distribution hash table in IXP0 based on the current % of total traffic that is Clear. Use the **no** form of the command to remove the clear-traffic load distribution. This will set the default load % as 50%.

crypto clear-traffic load <50%-100%>

no crypto clear-traffic load

Syntax Description

load	Percentage of clear traffic load on IXP0. 50% — IXP0 is handling 50% of total incoming traffic. No punt entries will be programmed. . . . 100% — IXP0 is handling 100% of total incoming traffic.
no	Negate a command or set it's defaults.

Command Default None.

Command Modes Global configuration.

Command History	Release	Modification
	WSG Release 4.4	This command was introduced.

Examples

Here is an example of the **crypto clear-traffic load** command:

(If Clear traffic is 60% and ESP traffic is 40%, then command to be used is):

```
WSG(config)# crypto clear-traffic load 60
```

crypto clear-traffic switch-distribution-scheme

To set the traffic distribution hash table in IXPO either with sequential punt entries or random punt entries, use the **crypto clear-traffic switch-distribution-scheme** command. Use the **no** form of the command to switch to the default distribution scheme.

crypto clear-traffic switch-distribution-scheme <1/2>

no crypto clear-traffic switch-distribution-scheme

Syntax Description

switch-distribution-scheme	Selects the scheme number.
1	Sequential hashing.
2	Random hashing (default).
no	Negate a command or set it's defaults.

Command Default

Default is 2.

Command Modes

Global configuration.

Command History

Release	Modification
WSG Release 4.4	This command was introduced.

Examples

Here is an example of the **crypto clear-traffic switch-distribution-scheme** command:

```
WSG(config)# crypto clear-traffic switch-distribution-scheme 2
```

crypto cmp auto-update

To provide the information necessary to automatically renew an enrolled CMP certificate, and to copy the updated certificate files to the SUP, use the **crypto cmp auto-update** global configuration command. Use the **no** form of the command to disable this feature.

```
crypto cmp auto-update current-wsg-cert cert_file current-wsg-private-key pvk_file ca-root
  ca_file ca-url url time time [key-reuse]
```

```
no crypto cmp auto-update current-wsg-cert cert_file current-wsg-private-key pvk_file ca-root
  ca_file ca-url url time time
```

Syntax Description

cert_file	Name of the CMP certificate file to update, ending with .crt.
pvk_file	Name of the Private Key file, ending with .prv.
ca_file	CA Server Root Certificate File.
url	CA Server URL must start with “http://” or “tcp://”
time	Time in days to start automatic renewal before certificate expires. The range is 2 to 60 days. We suggest a minimum value of 8 days.
key-reuse	Reuse private key. Default is to generate a new private key file.

Command Default

None.

Command Modes

Global configuration

Command History

Release	Modification
WSG Release 3.0	This command was introduced.

Usage Guidelines

This feature is enabled as long as there is at least one certificate configured for auto-update. To disable this feature, use the **no** form of the command to remove all certificate entries configured for auto-update.



Note

If the CA is unreachable, the WSG will try 3 times with an hour wait between each attempt. The renewal notification trap is sent when the renewal is initiated and when it succeeds or fails. If it fails, the operator will need to correct the problem and manually update the certificate. If the CA acknowledges receiving the request but does not issue the renewed certificate, the WSG will poll for the certificate 10 times with an hour (or the CA provided time) between each poll. The renewal notification trap is sent with the status, and if the status is failed, the operator will need to manually renew the certificate.

**Note**

If a manual update of the certificate and private key file is performed using the **crypto cmp update EXEC** mode command, use the **crypto cmp auto-update** command to remove the old certificate filename and add the updated certificate filename

Examples

Here is an example of the **crypto cmp auto-update** command:

```
WSG(config)# crypto cmp auto-update ?
  current-wsg-cert  Name of the CMP certificate file for update

WSG(config)# crypto cmp auto-update current-wsg-cert ?
  <WORD>  Enter certificate filename ending with .crt (Max Size - 128)

WSG(config)# crypto cmp auto-update current-wsg-cert wsg.crt current-wsg-private-key
wsg.prv ca-root root-ca.crt ca-url http://212.246.144.35:8700/pkix time 3
```

crypto cmp transport

To configure the Transport Protocol for CMPv2 messages, use the **crypto cmp transport** global configuration command. Use the **no** form of the command to set the CMPv2 default protocol.

crypto cmp transport *transport protocol*

no crypto cmp transport *transport protocol*

Syntax Description

<i>transport protocol</i>	Transport Protocol options are <i>http</i> , and <i>tcp</i> .
<i>http</i>	HTTP will be used as transport Protocol for all CMPv2 messages.
<i>tcp</i>	TCP will be used as transport Protocol for all CMPv2 messages.
<i>no</i>	Negate a command or set it's defaults.

Command Default

By default, *tcp* Transport Protocol is used.

Command Modes

Global configuration

Command History

Release	Modification
WSG Release 4.4	This command was introduced.

Usage Guidelines

Use the **crypto cmp transport** to configure the transport protocol for CMPv2 messages.

Examples

Here is an example of the **crypto cmp transport** command:

```
WSG(config)# crypto cmp transport http
```

crypto datapath icmp rate-limit

To control the rate at which the Segw datapath generates ICMP error packets, use the **crypto datapath icmp rate-limit** global configuration command. Use the **no** form of the command to remove the rate-limit.

crypto datapath icmp rate-limit *interval*

no crypto datapath icmp rate-limit *interval*

Syntax Description	<i>interval</i>	Specifies the time interval in milliseconds before another ICMP error packet can be sent by the datapath. The value range is 1 to 10,000 ms.
---------------------------	-----------------	--

Defaults	None.
-----------------	-------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	WSG Release 4.0	This command was introduced.

Usage Guidelines	None.
-------------------------	-------

Examples	<p>This example shows how to use the crypto datapath icmp rate-limit command to configure a 1000 ms time interval between sent ICMP error packets:</p> <pre>WSG(config)# crypto datapath icmp rate-limit 1000</pre>
-----------------	---

crypto dfp agent max-tunnels

To specify the maximum number of active tunnels supported on the WSG when the redirect feature is enabled, use the **crypto dfp agent max-tunnels** global configuration command. Use the **no** form of the command to remove the maximum number of tunnels.

crypto dfp agent max-tunnels *number*

no crypto dfp agent max-tunnels *number*

Syntax Description

<i>number</i>	Specifies the maximum number of active tunnels supported.
---------------	---

Defaults

By default 16,666 active tunnels are supported.

Command Modes

Global configuration

Command History

Release	Modification
WSG Release 4.0	This command was introduced.

Usage Guidelines

This command is configured in conjunction with **crypto redirect ip** and SLB commands on the SUP.

Examples

This example shows how to configure WSG to support 1000 maximum active tunnels when the redirect feature is enabled:

```
WSG(config)# crypto dfp agent max-tunnels 1000
```

crypto dfp agent max-weight

To specify the maximum weight associated with the real server that will be reported to the Dynamic Feedback Protocol (DFP) manager on the SUP, use the **crypto dfp agent max-weight** global configuration command. Use the **no** form of the command to remove the maximum associated weight.

crypto dfp agent max-weight *number*

no crypto dfp agent max-weight *number*

Syntax Description	<i>number</i>	Specifies the maximum weight or metric of the real server.
---------------------------	---------------	--

Defaults	By default the maximum weight is 20.
-----------------	--------------------------------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	WSG Release 4.0	This command was introduced.

Usage Guidelines	This command is configured in conjunction with crypto redirect ip commands on the WSG and SLB commands on the SUP.
-------------------------	---

Examples	This example shows how to configure a maximum weight of 10:
-----------------	---

```
WSG(config)# crypto dfp agent max-weight 10
```

crypto dhcp-client

To specify the relay agent IP address, and the server and client ports used on the WSG, use the **crypto dhcp-client** global configuration command. Use the **no** form of the command to remove the specified server and client ports.

```
crypto dhcp-client giaddr ip_address server-port port number client port port number
```

```
no crypto dhcp-client giaddr ip_address server-port port number client port port number
```

Syntax Description

<i>ip_address</i>	Specifies the relay agent IP address.
server-port <i>port number</i>	Specifies the server port used on the WSG.
client-port <i>port number</i>	Specifies the client port used on the WSG.

Defaults

None.

Command Modes

Global configuration.

Command History

Release	Modification
WSG Release 2.2	This command was introduced.

Usage Guidelines

The server and client port number can be the same or different values.

The WSG sends DHCP messages with the client port number, and receives responses from the server on the server port number.

The giaddr must be unique for each PPC talking to the DHCP server.

This command is required if you require DHCP address allocation.

Examples

The following example shows how to configure the **crypto dhcp-client** command:

```
WSG(config)# crypto dhcp-client giaddr 88.88.63.3 server-port 2133 client-port 2133
```

crypto dhcp-client client-id-type extract-cn

To specify the client ID that is sent by the WSG (in option 61 of a DHCP message), use the **crypto dhcp-client client-id-type extract-cn** global configuration command. Use the **no** form of the command to revert the client ID to the default setting.

```
crypto dhcp-client client-id-type extract-cn
```

```
no crypto dhcp-client client-id-type extract-cn
```

Syntax Description

There are no keywords or arguments for this command.

Defaults

By default the HNB's IKE ID is used as the client ID.

Command Modes

Global configuration.

Command History

Release	Modification
WSG Release 2.2	This command was introduced.

Usage Guidelines

By default the HNB's IKE ID is used as the client ID. If the HNB IKE ID is in the DN format, and the CN part of the DN is to be sent as the client ID, then this command must be configured.

Examples

The following example shows how to configure the **crypto dhcp-client client-id-type extract-cn** command:

```
WSG(config)# crypto dhcp-client client-id-type extract-cn
```

crypto dhcp-client link-address

To specify the global unicast IPv6 Link-Address in Relay Forward message used by the WSG, use the **crypto dhcp-client link-address** global configuration command.

crypto dhcp-client link-address *X:X:X::X* **server-port** *port number* **client port** *port number*

Syntax Description		
	<i>X:X:X::X</i>	Specifies the DHCP-client link IPv6 address.
	server-port <i>port number</i>	Specifies the server port used on the WSG.
	client-port <i>port number</i>	Specifies the client port used on the WSG.

Defaults None.

Command Modes Global configuration

Command History	Release	Modification
	WSG Release 4.3	This command was introduced.

Usage Guidelines This command is mandatory if DHCPv6 address allocation is required.

Examples The following example shows how to configure the **crypto dhcp-client link-address** command:

```
WSG(config)# crypto dhcp-client link-addr 2006::77:77:77:93 server-port 547 client-port 546
```


crypto dhcp-server

To configure the DHCP server IP address and port number, use the **crypto dhcp-server** global configuration command. Use the **no** form of the command to remove a specific DHCP server from the configuration.

```
crypto dhcp-server ip A.B.C.D | X:X:X::X port port_number
```

```
no crypto dhcp-server ip A.B.C.D | X:X:X::X port port_number
```

Syntax Description

<i>A.B.C.D</i>	Specifies the IPv4 dhcp-server address.
<i>X:X:X::X</i>	Specifies the IPv6 dhcp-server address.
<i>port_number</i>	Specifies the DHCP port number. The range is from 1 to 65535.

Defaults

The default value of *port_number* for IPv4 is 67.
The default value of *port_number* for IPv6 is 547.

Command Modes

Global configuration

Command History

Release	Modification
WSG Release 2.2	This command was introduced.
WSG Release 4.3	This command was modified to accept IPv6 addresses.

Usage Guidelines

You must specify at least one DHCP server if you require DHCP address allocation.
You can configure multiple DHCP servers by repeating the command.

Examples

The following example shows how to configure the DHCP server IP address and port number:

```
WSG(config)# crypto dhcp-server ip 44.44.44.143 port 67
```

crypto dhcp-dns server

To configure the DNS server IP address locally, use the **crypto dhcp-dns server** global configuration command.

Use the no form of the command to remove a specific DNS server IP from the configuration.

crypto dhcp-dns server ip < <A.B.C.D>|<X:X:X::X> Enter a valid IPv4 or IPv6 Address>

no crypto dhcp-dns server ip < <A.B.C.D>|<X:X:X::X> Enter a valid IPv4 or IPv6 Address>

Syntax Description

A.B.C.D	Specifies the IPv4 DNS server address.
X:X:X::X	Specifies the IPv6 DNS server address.

Defaults

None.

Command Modes

Global configuration.

Command History

Release	Modification
WSG Release 4.3.2	This command was introduced.

Usage Guidelines

This command is optional and is required only if locally configured DNS server IP is needed. You can configure both IPv4 and IPv6 DNS servers IP.

Examples

The following example shows how to configure the DNS server IPv4 address:

```
WSG(config)# crypto dhcp-dns server ip 9.9.9.9
```

The following example shows how to configure the DNS server IPv6 address:

```
WSG(config)# crypto dhcp-dns server ip 2006::77:77:77:93
```

crypto facility

To configure the syslog facility value, use the **crypto facility** global configuration mode. Use the **no** form of the command to disable this feature.

crypto facility *value*

Syntax Description

facility	Configures syslog facility.
values	The values supported on WSG are 0 to 23.

Defaults

By default, the facility value will be independent of the process.

Example: By default, the facility value for the syslog's generated from IPSEC process will be four (4).

Command Modes

Global configuration.

Command History

Release	Modification
WSG Release 4.4.1	This command was introduced.

Usage Guidelines

Use the **crypto facility** command to control the WSG syslog facility value.

Examples

The following example shows how to configure the facility value:

```
WSG(config)# crypto facility 7
```

crypto ike-retry-timeout

crypto ike-retry-timeout [**initial** *initial-value* | **max** *maximum-value*]

Syntax Description	initial	(Optional) Configures the initial retry timeouts.
	initial-value	Configures the initial timer value in msec. The range is 1000-4294967295. The default value is 5000.
	max	(Optional) Configures the max retry timeouts.
	maximum-value	Configures the max timer value in msec. The range is 2000-4294967295. The default value is 10000.

Command Default The default value of *initial-value* is 5000.
The default value of the *maximum-value* is 10000.

Command Modes Global configuration.

Command History	Release	Modification
	WSG Release 1.1	This command was introduced.

Examples Here is an example of the **crypto ike-retry-timeout** command:

```
switch(config)# crypto ike-retry-timeout initial 1000 max 2000
```

crypto ike-retry-count

To set the number of IKE retry connection attempts, use the **crypto ike-retry-count** command. To remove the IKE retry connection attempts, use the **no** form of the command.

crypto ike-retry-count *value*

no crypto ike-retry-count *value*

Syntax Description	<i>value</i>	Specifies the maximum number of connection retry attempts, 1 to 10.
---------------------------	--------------	---

Defaults	The default value is 1.
-----------------	-------------------------

Command Modes	Global configuration.
----------------------	-----------------------

Command History	Release	Modification
	WSG Release 1.1	This command was introduced.

Usage Guidelines	Use the crypto ike-retry-count command to set IKE retry connection attempts.
-------------------------	---

Examples	This example shows how to set IKE retry connection attempts:
-----------------	--

```
WSG# config
Enter configuration commands, one per line. End with CNTL/Z.
WSG(config)# crypto ike-retry-count 4
WSG(config)#
```

crypto ike-nat-keepalive

To set the time interval for the nat keepalives from the WSG use the **crypto ike-nat-keepalive** command. To remove the configuration, use the **no** version of the command.

crypto ike-nat-keepalive *interval*

no crypto ike-nat-keepalive *interval*

Syntax Description	<i>interval</i>	Configures the NAT keepalive packets interval in seconds. The range is 20-3600.
---------------------------	-----------------	---

Command Default	The default value is 0 (disabled).
------------------------	------------------------------------

Command Modes	Global configuration.
----------------------	-----------------------

Command History	Release	Modification
	WSG Release 1.1	This command was introduced.

Usage Guidelines	Use ike-nat-keepalive command to set the NAT keepalive interval.
-------------------------	---



Note

This command cannot be entered if the profile is in active state.
--

Examples	<pre>Router(config)# crypto ike-nat-keepalive ? <20-3600> Enter the packet interval in seconds (default: 0 (Disabled)) Router(config)# crypto ike-nat-keepalive 3000</pre>
-----------------	--

crypto ike-export-buf-size

To set the IKE export buffer size, use the **crypto ike-export-buf-size** command. To remove the configuration, use the **no** version of the command.

crypto ike-export-buf-size *size*

no crypto ike-export-buf-size *size*

Syntax Description

crypto ike-export-buf-size <i>size</i>	Configures the IKE export buffer size. The range is 3700-6000.
--	--

Command Default

The default value is 3700.

Command Modes

Global configuration.

Command History

Release	Modification
WSG Release 4.4.7	This command was introduced.

Usage Guidelines

Use **crypto ike-export-buf-size** command to increase the IKE buffer size, if below conditions are observed:

1. Count of IPsec tunnels differ between Active and standby WSGs.
2. Error message "**Could not export IKE SA**" found in syslogs/show eventlog.
3. IKE export error counters increment in "**show crypto ha stats**".



Note

Configuring this command is allowed only after deactivating all the profiles.

Examples

```
WSG(config)# crypto ike-export-buf-size ?
<3700-6000> Enter the ike export buf size (default/min: 3700, Max: 6000)
WSG(config)# crypto ike-export-buf-size 5000
```

crypto ipsec-fragmentation

To control the fragmentation point in hardware crypto engine for outbound traffic, use the **crypto ipsec-fragmentation** global configuration command. Use the **no** form of this command to remove the feature and reset the PMTU to the default value of 1400.

crypto ipsec-fragmentation [**none** | **before-encryption** {**ipv6**} **mtu** *MTU*]

no crypto ipsec-fragmentation [**none** | **before-encryption** {**ipv6**} **mtu** *MTU*]

Syntax Description

none	The hardware crypto engine fragmentation for outbound traffic is disabled.
MTU	The hardware crypto engine fragmentation for outbound traffic is done before encryption. In this case, the MTU should be set properly so that the length of the packet after expansion (caused by outbound IPsec processing) will still be within the MTU of the outgoing network. Acceptable IPv4 values are between 1100 and 3800. Acceptable IPv6 values are between 1280 and 3800.

Defaults

IPv4: **crypto ipsec-fragmentation before-encryption mtu 1400**

IPv6: **crypto ipsec-fragmentation before-encryption ipv6 mtu 1400**

Command Modes

Global configuration

Command History

Release	Modification
WSG Release 1.2	This command was introduced.
WSG Release 4.0	Allow configuration of a global PMTU value for IPv4 and IPv6.

Usage Guidelines

Use **crypto ipsec-fragmentation** command control the fragmentation point in hardware crypto engine for outbound traffic.

When the MTU size is modified after a tunnel is already established, the new MTU size will be reflected in the output of the **show crypto ipsec sa remote-ip** command for that tunnel, the new MTU size will not be used by the data traffic flowing through the tunnel until that tunnel is re-keyed. Tunnels that are established after the MTU size is modified will use the new MTU size right away.

Examples

Here are two examples of the **crypto ipsec-fragmentation** command including its verification:

```
WSG(config)# crypto ipsec-fragmentation before-encryption mtu 1200
segw_cli_fragmentation: Case enable the flag
segw_ipsec_frag_mtu_cmd: pre frag = 0, mtu = 1200
segw_cli_fragmentation: exiting ...
```



```
WSG# show run

Generating configuration.....

ip host localhost.localdomain 127.0.0.1

interface vlan 33
 ip address 33.33.33.30 255.255.255.0
interface vlan 77
 ip address 77.77.77.33 255.255.255.0
ip route 0.0.0.0 0.0.0.0 33.33.33.3

crypto syslog-level 1
crypto ipsec-fragmentation before-encryption mtu 1200

WSG(config)# crypto ipsec-fragmentation before-encryption ipv6 mtu 1280
segw_ipsec_frag_mtu_cmd: pre frag = 0, mtu = 1280
received msg:, retry_count =1

0x0 0x0 0x0 0x50 0x0 0x0 0x0 0x0
received msg:, retry_count =1

0x0 0x0 0x0 0x50 0x0 0x0 0x0 0x0

WSG# show run

Generating configuration.....

ha interface vlan 2143
ip address 77.77.143.43 255.255.255.0
interface vlan 143
ip address 88.88.143.43 255.255.255.0
interface vlan 149
ip address 10.10.149.43 255.255.255.0
ip route 0.0.0.0 0.0.0.0 88.88.143.100

crypto ipsec-fragmentation before-encryption mtu 1280
crypto ipsec-fragmentation before-encryption ipv6 mtu 1280
```

crypto ipsec security-association replay

To set the anti-replay window size, use the **crypto ipsec security association replay** global configuration command. Use the no form of the command to disable this feature.

crypto ipsec security-association replay [*window-size*] *window-size*

no crypto ipsec security-association replay [*window-size*] *window-size*

Syntax Description

window-size	32 64 128 256 384 512
--------------------	---------------------------------

Command Default

Default window size is 32 bits for short sequence number and 64 bit for extended sequence number. Supported window sizes are: 32, 64, 128, 256, 384 and 512.



Note

If **sequence number extended** is configured, the window size default will be 64 instead of 32.

Command Modes

Global configuration.

Command History

Release	Modification
WSG Release 2.1	This command was introduced.

Usage Guidelines

This example shows how to set the anti-replay window size:

```
WSG# config
Enter configuration commands, one per line. End with CNTL/Z.
WSG(config)# crypto ipsec security association replay window-size 128
```

crypto namerresolver

To enable the reverse DNS lookup feature, use the **crypto namerresolver** global configuration command. Use the **no** form of the command to disable this feature.

crypto namerresolver

no crypto namerresolver

Defaults

The reverse DNS lookup feature is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
WSG Release 4.0	This command was introduced.

Examples

This example shows how to enable the reverse DNS lookup feature:

```
WSG# config
Enter configuration commands, one per line. End with CNTL/Z.
WSG(config)# crypto namerresolver ?
enable Enable the name resolver(default: disable)
WSG(config)# crypto namerresolver enable
```

This example shows how to disable the reverse DNS lookup feature:

```
WSG(config)# no crypto namerresolver
```

crypto pki trustpoint

To set up a CA certificate to use for certificate-based authentication, use the **crypto pki trustpoint** command. To remove a CA certificate, use the **no** form of the command.

```
crypto pki trustpoint {rootCA | subCA} filename.crt crl disable
```

```
no crypto pki trustpoint {rootCA | subCA} filename.crt crl disable
```

Syntax Description

rootCA	Use this if a certificate comes from a root CA.
subCA	Use this for additional certificates from non-root CAs or RAs.
filename	Name of the CA certificate. Certificate filenames must end with a .crt file extension.
crl disable	Use this to disable the CRL. This option is only available for rootCA.

Defaults

None.

Command Modes

Global configuration

Command History

Release	Modification
WSG Release 1.0	This command was introduced as the ipsec ca-cert command.
WSG Release 1.1	This command was changed.

Usage Guidelines

The CA certificate must exist on the SUP before issuing this command.

Use the **crypto pki trustpoint** command multiple times to set up a certificate chain.

Up to 20 root certificates can be configured on the WSG.



Note

crypto pki trustpoint configuration changes will only take effect after a **no activate -> activate** command sequence.

Examples

This example shows how to set up the WSG to use a CA certificate on the SUP named cert-ca1.crt:

```
WSG# config
Enter configuration commands, one per line. End with CNTL/Z.
WSG(config)# crypto pki trustpoint rootCA cert-ca1.crt
Copying cert-ca1.crt from SUP...done
```

For rootCA, there is an option to disable the CRL (Certificate Revocation List).

```
WSG(config)# crypto pki trustpoint rootCA root_ca.crt crl disable
```

crypto pki wsg-cert

To set up the WSG certificate and (optionally) the private key file for a WSG to use for certificate-based authentication, use the **crypto pki wsg-cert** global configuration command. Use the **no** form of this command to remove the WSG certificate.

```
crypto pki wsg-cert cert_filename.crt [wsg-private-key private-key-filename.prv]
```

```
no crypto pki wsg-cert cert_filename.crt [wsg-private-key private-key-filename.prv]
```

Syntax Description

<i>cert_filename</i>	Name of the WSG certificate on the SUP. Ensure certificate filenames end with a .crt file extension.
<i>private-key-filename</i>	(Optional) Keyword option and variable to set up the filename of the private key. The private key filename must end with a .prv extension. Up to 20 certificate/key pairs can be configured. If a private key filename is not specified, it is assumed that the user is trying to use a locally generated private key (using the crypto rsa-keygen command).

Defaults

None.

Command Modes

Global configuration

Command History

Release	Modification
WSG Release 1.0	This command was introduced as the ipsec segw-cert command.
WSG Release 1.1	This commands was changed.

Usage Guidelines

The WSG certificate must be in the SUP bootflash or SUP bootdisk file system before issuing this command. The WSG uses both file systems to locate the files.

If a private key filename is not specified, it is assumed the user is trying to use a locally generated private key (using the **crypto rsa-keygen** command).



Note In releases prior to WSG Release 4.0, **wsg-cert** configuration changes will only take effect after a **no activate -> activate** command sequence.



Note If a manual update of the certificate and private key file is performed using the **crypto cmp update EXEC** mode command, use the **crypto pki wsg-cert** command to remove the old certificate filename and add the updated certificate filename. This is not required after an automatic renewal.

Examples

To set up the WSG certificate with the name wsg.crt and a private key named wsg.prv, enter:

```
WSG# config
Enter configuration commands, one per line. End with CNTL/Z.
WSG(config)# crypto pki wsg-cert wsg.crt wsg-private-key wsg.prv
Copying cert1.crt from SUP...done
```

crypto pki wsg-cert-trap expiry notification

To specify the trap notification time before the trap expires, use the **crypto pki wsg-cert-trap expiry notification** global configuration command. The **no** form of this command sets the time before the trap is not valid back to the default 24 hours.

crypto pki wsg-cert-trap expiry notification *time*

no crypto pki wsg-cert-trap expiry notification *time*

Syntax Description	<i>time</i>	Time in hours to send the expiry trap before the certificate is not valid. The range is 1 to 720 hours (30 days). The default value is 24 hours.
---------------------------	-------------	--

Defaults	Default is 24 hours.
-----------------	----------------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	WSG Release 3.0	This command was introduced.

Examples Here is an example of the **crypto pki wsg-cert-trap expiry notification** command set for 72 hours (3 days):

```
WSG# config
```

```
Enter configuration commands, one per line. End with CNTL/Z
```

```
WSG(config)# crypto pki wsg-cert-trap expiry notification 72
```

crypto profile

To create a profile and to enter the crypto profile submode, use the **crypto profile** global configuration command. Use the **no** form of this command to remove a profile.

crypto profile *profile-name*

no crypto profile *profile-name*

Syntax Description

<i>profile-name</i>	Specifies the name of each profile created by the user.
---------------------	---

Defaults

None.

Command Modes

Global configuration

Command History

Release	Modification
WSG Release 1.0	This command was introduced.

Usage Guidelines

A crypto profile can be either remote-access type or site-to-site type. The **type** command is used to specify the type of each profile that you create. If the type is not specified, the default is remote-access.

Examples

This example illustrates the **crypto profile** command:

```
WSG(config)# crypto profile Example_Name
```


crypto radius accounting enable

To enable the RADIUS accounting feature on the WSG, use the **crypto radius accounting enable** global configuration command. Use the **no** form of the command to disable the feature.

crypto radius accounting enable

no crypto radius accounting enable

Syntax Description There are no keywords or arguments for this command.

Defaults RADIUS accounting is not enabled.

Command Modes Global configuration

Command History	Release	Modification
	WSG Release 3.0	This command was introduced.

Usage Guidelines Use the **crypto radius accounting enable** command to enable the RADIUS accounting feature.



Note All profiles must be deactivated before enabling RADIUS accounting.

Examples Here is an example configuration of the **crypto radius accounting enable** command:

```
WSG# config
Enter configuration commands, one per line. End with CNTL/Z.
WSG(config)# crypto radius accounting enable
```

crypto radius nas-id

Identification of the WSG as NAS to the RADIUS server is required. To configure the NAS Identifier on the WSG, use the **crypto radius nas-id** global configuration command. Use the **no** form of the command to disable the feature.

crypto radius nas-id *identifier-string*

no crypto radius nas-id *identifier-string*



Note

This CLI command is applicable to both RADIUS Authentication and Accounting features. It is mandatory to configure one or both of the **crypto radius nas-id** and **crypto radius nas-ip** commands before configuring the **crypto radius-server host** command.

Syntax Description

<i>identifier-string</i>	This RADIUS attribute contains a string to identify the NAS originating the access request.
--------------------------	---

Defaults

None.

Command Modes

Global configuration

Command History

Release	Modification
WSG Release 3.0	This command was introduced.

Usage Guidelines

Use the **crypto radius nas-id** command to configure the NAS Identifier on the WSG.



Note

When upgrading to WSG Release 3.0 from a previous 2.X release, if a RADIUS server configuration exists, the crypto profile(s) will be inactive after the upgrade. To reactivate, configure the **crypto radius nas-id** or **crypto radius nas-ip** commands and then activate the profile(s).

Examples

Here is an example configuration of the **crypto radius nas-id** command:

```
WSG# config
Enter configuration commands, one per line. End with CNTL/Z.
WSG(config)# crypto radius nas-id example.cisco.com
```

crypto radius nas-ip

Identification of the WSG as NAS to the RADIUS server is required. To configure the NAS IP address on the WSG, use the **crypto radius nas-ip** global configuration command. Use the **no** form of the command to disable the feature.

crypto radius nas-ip *ip*

no crypto radius nas-ip *ip*

Syntax Description

ip IPv4 or IPv6 address of the NAS. Format is A.B.C.D or X:X:X::X.

Defaults

None.

Command Modes

Global configuration

Command History

Release	Modification
WSG Release 3.0	This command was introduced.

Usage Guidelines

Use the **crypto radius nas-ip** command to configure the NAS IP address on the WSG.



Note

This CLI command is applicable to both RADIUS Authentication and Accounting features. It is mandatory to configure one or both of the **crypto radius nas-id** and **crypto radius nas-ip** commands before configuring the **crypto radius-server host** command.



Note

When upgrading to WSG Release 3.0 from a previous 2.X release, if a RADIUS server configuration exists, the crypto profile(s) will be inactive after the upgrade. To reactivate, configure the **crypto radius nas-id** or **crypto radius nas-ip** commands and then activate the profile(s).

Examples

Here is an example configuration of the **crypto radius nas-ip** command:

```
WSG# config
Enter configuration commands, one per line. End with CNTL/Z.
WSG(config)# crypto radius nas-ip 10.10.10.10
```

crypto radius-server host

To authenticate remote end points with a RADIUS server, use the **crypto radius-server host** global configuration command. Use the **no** form of the command to disable this feature.

crypto radius-server host *ip* **key** *keyword* [**auth-port** *auth_port_#*] [**acct-port** *acct_port_#*]

no crypto radius-server host *ip* **key** *keyword* [**auth-port** *auth_port_#*] [**acct-port** *acct_port_#*]

Syntax Description

<i>ip</i>	The IPv4 or IPv6 address of the RADIUS server. The format is either A.B.C.D or X:X:X::X.
<i>keyword</i>	The secret key that is used with the RADIUS server.
<i>auth_port_#</i>	The authentication port that the RADIUS server uses. The integer value is in the 0 to 65535 range. The default value is 1812.
<i>acct_port_#</i>	The accounting port that the RADIUS server uses. The integer value is in the 0 to 65535 range. The default value is 1813.

Defaults

The default port number for *auth_port* is 1812 and for *acct_port* is 1813.

Command Modes

Global configuration

Command History

Release	Modification
WSG Release 1.2	This command was introduced.
WSG Release 3.0	This command was modified to accept IPv6 addresses and added optional auth-port and acct-port parameters.

Usage Guidelines

This command must be configured if you use the RADIUS authentication feature.
RADIUS authentication can be used with remote-access type profiles only.

Examples

Here is an example of the **crypto radius-server host** command:

```
WSG# config
Enter configuration commands, one per line. End with CNTL/Z.
WSG(config)# crypto radius-server host 5.5.5.5 key cisco123 auth-port 8120 acct-port 8112
```

crypto radius source-ip

To specify the source IP address of the RADIUS packets that are sent to the RADIUS server, use the **crypto radius source-ip** global configuration command. Use the **no** form of the command to disable this feature.

crypto radius source-ip *src-ip-address*

no crypto radius source-ip *src-ip-address*

Syntax Description

src-ip-address The source IPv4 or IPv6 address of the RADIUS packets that are sent to the RADIUS server. The format is either A.B.C.D or X:X:X::X.

Defaults

None.

Command Modes

Global configuration

Command History

Release	Modification
WSG Release 1.2	This command was introduced.
WSG Release 3.0	This command was modified to also accept IPv6 addresses.

Usage Guidelines

This is an optional command configured when the RADIUS authentication feature is used. If not specified, the IKE stack will get the source IP address to use for RADIUS packets from the kernel (which is based on the route to reach the RADIUS server). RADIUS authentication can be used with remote-access type profiles only.

Examples

Here is an example of the **crypto radius source-ip** command:

```
WSG# config
Enter configuration commands, one per line. End with CNTL/Z.
WSG(config)# crypto radius source-ip 2.2.2.2
```

crypto redirect ip

To specify the real and redirect IP addresses for the IKEv2 redirect feature, use the **crypto redirect ip** command in global configuration mode. Use the **no** form of the command to remove the IP addresses.

```
crypto redirect ip real_IP redirect to redirect_IP [vrf vrf_name]
```

```
no crypto redirect ip real_IP redirect to redirect_IP [vrf vrf_name]
```

Syntax Description

<code>real_IP</code>	Real IP address.
<code>redirect_IP</code>	Redirect IP address.
<code>vrf_name</code>	Name of VRF.

Defaults

None.

Command Modes

Global configuration

Command History

Release	Modification
WSG Release 4.0	This command was introduced.

Usage Guidelines

Unlike IPv4 real addresses, IPv6 real addresses do not report the weight to the SUP. IPv6 real addresses report the weight through IPv4 real addresses. Therefore, verify that the correct IPv4 and IPv6 real addresses are associated with each other on the SUP. Also, verify that a DFP agent with a IPv4 real address is defined on the SUP.

```
ip slb serverfarm SEGW76-14-IPV4
nat server
failaction purge
!
real 10.10.149.3
inservice
!
ip slb serverfarm SEGW76-14-IPV6
nat server
!
real 10.10.149.3 ipv6 2001:10:10:149::3
inservice
!
ip slb dfp
agent 10.10.149.3 4700 10 0 5
```



Note

The DFP agent source port should always be 4700.

Examples

This example shows how to configure real and redirect IP addresses for the IKEv2 redirect feature:

```
WSG# config  
Enter configuration commands, one per line. End with CNTL/Z.  
WSG(config)# crypto redirect ip 11.11.1.11 redirect to 12.12.2.22
```

crypto remote-secret

To set the remote shared secret, use the **crypto remote-secret** command. To remove the remote shared secret, use the **no** form of the command.

```
crypto remote-secret id_type id secret
```

```
no crypto remote-secret id_type id secret
```

Syntax Description

<i>id_type</i>	<ul style="list-style-type: none"> dn—Distinguished name ip—IP address fqdn—Fully-qualified domain name. email—Email address
<i>id</i>	Value of <i>id_type</i> .
<i>secret</i>	Name of the shared, secret key.

Defaults

Remote secret is not set.

Command Modes

Global configuration

Command History

Release	Modification
WSG Release 1.1	This command was introduced.
WSG Release 3.0	IPv6 support was added.

Usage Guidelines

Remote secrets help set pre-shared keys for IKE authentication for remote clients. Use the **crypto remote-secret** command to set the remote secret shared. The **crypto remote-secret** command is used for authentication and can be configured as an IP address. In WSG Release 3.0, the command accepts either an IPv4 or an IPv6 address.

```
wsg(config)# crypto remote-secret ip A.B.C.D | X:X:X::X
```



Note

The maximum number of supported remote-secret entries is 1000.

Examples

This example shows how to set pre-shared keys information for IKE authentication for remote clients.

```
WSG# config
Enter configuration commands, one per line. End with CNTL/Z.
WSG(config)# crypto remote-secret ip 10.95.20.110 secret_key
```


crypto responder-redirect enable

To enable the IKEv2 redirect feature, use the **crypto responder-redirect enable** command in global configuration mode. Use the **no** form of the command to disable the feature.

crypto responder-redirect enable

no crypto responder-redirect enable

Syntax Description There are no keywords or arguments for this command.

Defaults None.

Command Modes Global configuration

Command History	Release	Modification
	WSG Release 4.0	This command was introduced.

Usage Guidelines Reviewers: Any text for this section?

Examples This example shows how to enable the IKEv2 redirect feature:

```
WSG# config
Enter configuration commands, one per line. End with CNTL/Z.
WSG(config)# crypto responder-redirect enable
```

crypto rri enable

To enable the RRI feature, use the **crypto rri enable** command. To disable the RRI feature, use the **no** form of the command.

crypto rri enable

no crypto rri enable

Defaults

The RRI feature is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
WSG Release 3.0	This command was introduced.

Usage Guidelines

For WSG Release 3.0, the RRI feature only supports IPv4.

Only site-to-site profiles are supported.

The VRF feature on the WSG cannot not be enabled when the RRI feature is already configured.

Examples

This example shows how to enable

```
WSG# config
Enter configuration commands, one per line. End with CNTL/Z.
WSG(config)# crypto rri ?
enable Enable RRI feature (default:disable)
WSG(config)# crypto rri enable
WSG(config)#
```

crypto snmp stats-refresh-interval

To configure statistics refresh interval to either auto mode or manual mode. In auto mode, the refresh interval is adjusted automatically based on number of tunnels.

no crypto snmp stats-refresh-interval auto will change to the default setting (manual mode with 300 seconds interval) and **no crypto snmp stats-refresh-interval manual interval** will change to auto mode.

```
crypto snmp stats-refresh-interval {auto | manual interval}
```

```
no crypto snmp stats-refresh-interval {auto | manual}
```

Syntax Description

auto	Set referesh interval automatically based on number of tunnels, on average about 1.5 sec for 1000 tunnels.
interval	Set refresh interval manually in range from 1 to 300 sec.

Defaults

By default this command is set to manual mode 300 seconds interval.

Command Modes

Global configuration

Command History

Release	Modification
WSG Release 4.2	This command was introduced as the crypto snmp stats-refresh-interval command.

Usage Guidelines

Use the **crypto snmp stats-refresh-interval** command to configure the statistics refresh interval.

Examples

This example shows how to set up the WSG to configure the auto length for IKE/IPSec tunnel:

```
switch(config)# crypto snmp stats-refresh-interval auto
```

This example sets the default setting manual mode with 300 seconds interval:

```
switch(config)# no crypto snmp stats-refresh-interval auto
```

crypto site-to-site-lookup

To configure the list of source-mask and destination-mask combinations, use the **crypto site-to-site-lookup** global configuration command. Use the **no** form of the command to disable this feature.

```
crypto site-to-site-lookup [priority priority | source-netmask src-netmask | destination-netmask dst-netmask]
```

```
no crypto site-to-site-lookup [priority priority | source-netmask src-netmask | destination-netmask dst-netmask]
```

Syntax Description

<i>priority</i>	Priority of this lookup. The range is 1 to 6.
<i>src-netmask</i>	Source IP network mask in format N. The N subnet mask format is increased from 0-32 to 0-128 for IPv6.
<i>dst-netmask</i>	Destination IP network mask in format N. The N subnet mask format is increased from 0-32 to 0-128 for IPv6.

Defaults

None.

Command Modes

Global configuration

Command History

Release	Modification
WSG Release 2.0	This command was introduced.
WSG Release 3.0	The N subnet mask format is increased from 0-32 to 0-128 for IPv6.

Usage Guidelines

You must enter this command one or more times before activating any S2S profiles. S2S profile cannot be activated if this command is not configured on the WSG.

Examples

This example shows how to configure the **crypto site-to-site-lookup** command:

```
WSG# config
Enter configuration commands, one per line. End with CNTL/Z.
WSG(config)# crypto site-to-site-lookup priority 1 source-netmask 24
destination-netmask 24
WSG(config)# crypto site-to-site-lookup priority 1 source-netmask 64
destination-netmask 64
WSG(config)# crypto site-to-site-lookup priority 5 source-netmask 112
destination-netmask 112
```

crypto syslog-level

To configure the syslog level, use the **crypto syslog-level** global configuration mode.

crypto syslog-level *number*

Syntax Description	<i>number</i>	Message levels from the WSG. Valid values are: <ul style="list-style-type: none"> • 1—Informational messages • 2—Notification messages • 3—Warning messages • 4—Error messages • 5—Critical messages
---------------------------	---------------	---

Defaults By default the *number* value is 3.

Command Modes Global configuration

Command History	Release	Modification
	WSG Release 1.0	This command was introduced as the crypto syslog-level command.
	WSG Release 1.1	This command was changed.

Usage Guidelines Use the **crypto syslog-level** command to control WSG message types. Syslog level 1 logs the largest amount of information. A limited amount of the logs are saved on the WSG. You can send the syslog to a remote syslog server using the **ip logging** command.

Examples This example shows how to set up the WSG to generate messages at and above level 1:

```
switch(config)# crypto syslog-level 1
```

crypto throughput threshold

To configure the system to generate an SNMP trap when WSG throughput utilization goes above the configured value for a sustained number of intervals, use the **crypto throughput threshold** global configuration mode.

no crypto throughput threshold will change values back to the default setting; i.e. threshold with 50% and interval value 2.

crypto throughput threshold *threshold interval interval*

no crypto throughput threshold *threshold interval interval*

Syntax Description

<i>threshold</i>	WSG throughput utilization in percentage
<i>interval</i>	Number of sustained intervals where each interval is of 5 mins.

Defaults

By default the *threshold* value is 50.

By default the *interval* value is 2.

Command Modes

Global configuration

Command History

Release	Modification
WSG Release 4.2	This command was introduced as the crypto throughput threshold command.

Usage Guidelines

Use the **crypto throughput threshold** command to generate an SNMP trap when WSG throughput utilization goes above the configured value for a sustained number of intervals.

Examples

This example shows how to set up the WSG to generate an SNMP trap when WSG throughput utilization goes above the configured value for a sustained number of intervals:

```
switch(config)# crypto throughput threshold 80 interval 5
```

crypto decrypt auth-failure rate

This CLI allows to configure the authentication decryption failure rate and above which SNMP trap should be sent. The CLI allows the configurable rate value from 1 to 10000. Use the **no** form of this command to remove the OID in traps.

```
crypto decrypt auth-failure rate <1-10000>
```

```
no crypto decrypt auth-failure rate <1-10000>
```

Defaults

By default, the rate is 30 per 5 minutes interval.

Command Modes

Global configuration

Command History

Release	Modification
WSG Release 4.4.8	This command was introduced.

Examples

The following example shows the rate being set to 3:

```
WSG(config)# crypto decrypt auth-failure rate 3
```

ha interface vlan

To configure the HA VLAN that is used to communicate among the nodes in the same cluster (subnet), use the **ha interface vlan** global configuration command. Use the **no** form to disable this functionality.

```
ha interface vlan vlan_ID
```

```
no ha interface vlan vlan_ID
```

Syntax Description	<i>vlan_ID</i> The number of the VLAN you are configuring.
---------------------------	--

Defaults	None.
-----------------	-------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	WSG Release 2.0	This command was introduced.

Usage Guidelines	These CLIs must to be configured on each PPC. The 2 PPCs that are to be paired together should have the same VLAN ID. 6 different VLAN IDs will be used for 6 pairs of PPCs.
-------------------------	--

Examples	The following examples show how to configure the HA VLAN/IP address for the PPC#3 on Slot#1 and the PPC#3 on Slot#3:
-----------------	--

On Slot#1/PPC#3:

```
WSG(config)# ha interface vlan 611
WSG(config-if)# ip address 11.11.1.13 255.255.255.0
```

On Slot#3/PPC#3:

```
WSG(config)# ha interface vlan 611
WSG(config-if)# ip address 11.11.1.23 255.255.255.0
```


ha interface vlan start-id

To configure the VLAN and IP address using a single point configuration, use the **ha interface vlan start-id** command in global configuration mode. Use the **no** form of the command to disable this functionality.

```
ha interface vlan start-id vlan_ID [processor-count count] increment increment_vlan_ID
```

```
no ha interface vlan start-id vlan_ID
```

Syntax Description

<i>vlan_ID</i>	The number of the VLAN you are configuring.
count	Specifies how many PPCs the HA VLAN interface should be applied to. Without this optional keyword, the HA VLAN interface is applied to all 6 PPCs.
increment	The increment number to use in the next VLAN configuration
<i>increment_vlan_ID</i>	The incremented VLAN ID number.

Defaults

None.

Command Modes

Global configuration

Command History

Release	Modification
WSG Release 2.0	This command was introduced.
WSG Release 4.0	The optional keyword processor-count was added.

Usage Guidelines

This command is available in the entity-all mode on the director PPC (PPC3). You can use the **ip address start-ip** submode command to configure the start IP address for the director PPC (PPC3) and the increment value for the IP addresses of the slave PPCs (PPC4 to PPC8).

Examples

If you execute the following CLI commands on the director PPC (PPC3):

```
WSG(mode-all)(config)# ha interface vlan start-id 212 increment 2
WSG(mode-all)(config-if)# ip address start-ip 11.11.1.11 increment 0.0.1.2 mask
255.255.255.0
```

The resulting configurations of the 6 PPCs appear as follows:

PPC3:

```
WSG(config)# ha interface vlan 212
WSG(config-if)# ip address 11.11.1.11 255.255.255.0
```

PPC4:

```
WSG(config)# ha interface vlan 214
WSG(config-if)# ip address 11.11.2.13 255.255.255.0
```

PPC5:

```
WSG(config)# ha interface vlan 216
WSG(config-if)# ip address 11.11.3.15 255.255.255.0
```

PPC6:

```
WSG(config)# ha interface vlan 218
WSG(config-if)# ip address 11.11.4.17 255.255.255.0
```

PPC7:

```
WSG(config)# ha interface vlan 220
WSG(config-if)# ip address 11.11.5.19 255.255.255.0
```

PPC8:

```
WSG(config)# ha interface vlan 222
WSG(config-if)# ip address 11.11.6.21 255.255.255.0
```

If you execute the following CLI commands on the director PPC (PPC3):

```
WSG(mode-all)(config)# ha interface vlan start-id 215 processor-count 2 increment 2
WSG(mode-all)(config-if)# ip address start-ip 11.11.8.22 increment 0.0.1.2 mask
255.255.255.0
```

Then PPC3 and PPC4 are configured as follows:

PPC3:

```
WSG(config)# ha interface vlan 215
WSG(config-if)# ip address 11.11.8.22 255.255.255.0
```

PPC4:

```
WSG(config)# ha interface vlan 217
WSG(config-if)# ip address 11.11.9.24 255.255.255.0
```

ha redundancy-mode

To configure the redundancy mode of the HA feature, use the **ha redundancy-mode** command in global configuration mode. Use the **no** form of the command to remove a redundancy mode.

```
ha redundancy-mode {active-active | active-standby} preferred-role {primary | secondary}
[revertive]
```

```
no ha redundancy-mode {active-active | active-standby} preferred-role {primary | secondary}
[revertive]
```

Syntax Description	redundancy-mode	Indicate which redundancy mode.
	active-active	Configure redundancy between PPC3 and PPC4.
	active-standby	Configure redundancy roles on all 6 PPCs.
	preferred-role	Indicate which node should come up as active (primary) or standby (secondary) when both nodes are rebooted at about the same time.
	<i>primary</i>	Set the preferred-role of the node to active.
	<i>secondary</i>	Set the preferred-role of the node to standby.
	<i>revertive</i>	Resets the active card on the secondary to ensure that the primary card has the active state and the secondary card has the standby state. This keyword is optional for the active-standby mode but required for the active-active mode.

Defaults None.

Command Modes Global configuration

Command History	Release	Modification
	WSG Release 2.0	This command was introduced.
	WSG Release 4.0	Modified to support active-active and active-standby node redundancy.

Usage Guidelines The **ha redundancy-mode active-active** CLI command can only be executed on the director PPC (PPC3) under entity-all mode. The command would then be applied to PPC3 and PPC4 only. The roles on PPC3 and PPC4 would be either primary/secondary or secondary/primary, depending on the **preferred-role** setting. If **preferred-role** is configured to be primary, PPC3 is primary and PPC4 is secondary. If **preferred-role** is configured to be secondary, PPC3 is secondary and PPC4 is primary.

In active-active mode, a failure in a PPC triggers a failover to its redundant peer PPC. The rest of the PPCs on the SAMI are not affected. However, if the failure occurs on the card level (such as IXP), the entire SAMI reloads.

**Note**

Since PPC3 and PPC4 have different roles in active-active mode, the entity-all mode should not be used to configure the HA setup.

**Note**

In active-active mode, the **revertive** keyword is a mandatory option. You must enter the **revertive** keyword for this CLI to be executed.

The **ha redundancy-mode active-standby** CLI command can only be executed on the director PPC (PPC3). It can be applied to just the PPC3 or, if under entity-all mode, applied to all of the PPCs. If under entity-all mode, the same preferred-role (primary or secondary) would be applied to all of the PPCs.

In active-standby mode, a failover causes the SAMI to reload, regardless of whether the failure occurred on an individual PPC or on the card level.

When the command is configured, the redundancy mode remains the same. The redundancy mode is applied and takes effect only after the SAMI reloads. You must save the configuration and reload the SAMI in order to activate these commands.

If the command is executed in the **all** mode, the command is applied to all PPCs so that the same role is assigned to them all. If the command is executed in the **single** mode, the role is assigned to only that particular PPC. The SAMI that is configured with the preferred-role of **secondary** needs to be reset before the redundant pairs can take effect.

Examples

The following command configures PPC3 as primary and PPC4 as secondary:

On Slot#1/PPC#3:

```
WSG(config)# ha redundancy-mode active-active preferred-role primary revertive
```

The following command configures PPC3 as secondary and PPC4 as primary:

On Slot#2/PPC#3:

```
WSG(config)# ha redundancy-mode active-active preferred-role secondary revertive
```

**Note**

You are responsible to clean up the remaining (non-HA) configuration and bring the system back to operational state. Also, the system will not reboot automatically as a result of removing the HA configuration.

ha timeout

To configure an HA timeout in the range of 1 through 10 seconds. Use the **no** form of the command to remove the limit.

ha timeout *integer*

no ha timeout *integer*

Syntax Description	<i>integer</i>	It is the maximum HA timeout that can be configured. Valid values are 1 to 10.
--------------------	----------------	--

Defaults	Default timeout is 900 milliseconds.
----------	--------------------------------------

Command Modes	Global configuration
---------------	----------------------

Command History	Release	Modification
	WSG Release 4.4.8	This command was introduced.

Usage Guidelines	<p>Following are the usage guidelines of this command:</p> <ul style="list-style-type: none"> • This command is allowed only when all the profiles are in deactivated state. • This command will not be synced from ACTIVE to STANDBY. • This command is allowed to configure on all the subordinate PPC's. • After configuring the command, it is mandatory to save the config and reload the SAMI card for the command to take effect.
------------------	--

Examples	The following command configures the HA timeout to 2 seconds:
----------	---

```
WSG(config)# ha timeout 2
```

interface

To create a VLAN interface, use the **interface** command. The CLI prompt changes to (config-if). Use the **no** form of this command to remove the interface.

interface *vlan number*

no interface *vlan number*

Syntax Description	<i>number</i>	Assigns the VLAN to the context and accesses interface configuration mode commands for the VLAN. The <i>number</i> argument is the number for a VLAN assigned to the PPC. Valid value is a number between 2 and 4094.
---------------------------	---------------	---

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	COSLI 1.0	This command was introduced.
	WSG Release 3.0	The ipv6 address and alias keywords were added.

Usage Guidelines

Use the **interface vlan** command to configure a VLAN interface on a PPC.

WSG Release 3.0 and above allows you to configure an IPv6 address and alias on the interface. Each interface is allowed to have one or both IPv4 address/alias and IPv6 address/alias.

While in interface configuration mode, you can use the following commands:

- **alias**—Alias IPv4 address for the interface
- **do**—Issue EXEC mode command from within configuration mode
- **end**—Exit configuration mode
- **description**—Description for the interface
- **ip address**—IPv4 address for the interface
- **ipv6 address**—IPv6 address for the interface
- **ipv6 alias**—Alias IPv6 address for the interface
- **mtu**—Maximum Transmission Unit (MTU) for the interface
- **no**—Negate an interface configuration command or return it to its default value
- **shutdown**—Shut down the interface
- **vrf**—Specify the VRF for the interface



Note

This CLI is a node-specific command, and cannot be executed under entity-all mode.

Examples

To create VLAN interface 100, enter the following command:

```
switch(config)# interface vlan 100
```

To configure the interface under a VRF inside, enter the following command:

```
switch(config-if)# vrf inside
```

To configure an IPv4 address and an alias IPv4 address under VLAN 100, enter the following commands:

```
switch(config-if)# ip address 10.10.10.43 255.255.255.0
switch(config-if)# alias 10.10.10.11 255.255.255.0
```

To configure an IPv6 address and an alias IPv6 address under VLAN 100, enter the following commands:

```
switch(config-if)# ipv6 address 2001:88:88:94::43/96
switch(config-if)# ipv6 alias 2001:88:88:94::11/96
```

To configure an IPv6 address using eui-64 interface identifier, enter the following command:

```
switch(config-if)# ipv6 address 2001:88:88:94::/96 eui-64
```

The following is the result of the above configuration:

```
interface vlan 100
  vrf inside
  ip address 10.10.10.43 255.255.255.0
  alias 10.10.10.11 255.255.255.0
  ipv6 address 2001:88:88:94::/96 eui-64
  ipv6 alias 2001:88:88:94::11/96
```

service interface

To create a service VLAN interface, use the **service interface** command. Use the **no** form of this command to remove the service interface.

service interface *vlan number*

no service interface *vlan number*

Syntax Description	<i>number</i>	Assigns the VLAN to the context and accesses interface configuration mode commands for the VLAN. Valid value is a number between 2 and 4094. This service VLAN number does not require SVCLC configuration on supervisor.
---------------------------	---------------	---

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	WSG Release 4.4.5	This command was introduced supporting up to 10 service IPs per PPC.
	WSG Release 4.4.6	Support was increased to maximum of 32 service IPs per PPC.

Usage Guidelines

Use the **service interface** *vlan* command to configure a service VLAN interface.

This command is allowed to have IPv4 address with netmask /32 and IPv6 with netmask /128, which acts as a sort of loopback interface.

While in service interface configuration mode, you can use the following commands:

- **do**—Issue EXEC mode command from within configuration mode
- **end**—Exit configuration mode
- **description**—Description for the interface
- **ip address**—IPv4 address for the interface
- **ipv6 address**—IPv6 address for the interface
- **mtu**—Maximum Transmission Unit (MTU) for the interface
- **no**—Negate an interface configuration command or return it to its default value
- **shutdown**—Shut down the interface
- **vrf**—Specify the VRF for the interface



Note

- This CLI is a node-specific command, and cannot be executed under entity-all mode.
- While upgrading from 3.x to 4.2.x, a loopback interface (with netmask /32 or /128) will be treated as service interface.
- While downgrading to releases older than WSG 4.2, the **service interface** configuration is lost.

Examples

To create service VLAN interface 1000, enter the following command:

```
switch(config)# service interface vlan 1000
```

To configure the interface under a VRF inside, enter the following command:

```
switch(config-if)# vrf inside
```

To configure an IPv4 address under VLAN 1000, enter the following commands:

```
switch(config-if)# ip address 10.10.10.43 255.255.255.255
```

To configure an IPv6 address under VLAN 1000, enter the following commands:

```
switch(config-if)# ipv6 address 2001:88:88:94::43/128
```

The following is the result of the above configuration:

```
service interface vlan 1000
vrf inside
ip address 10.10.10.43 255.255.255.255
ipv6 address 2001:88:88:94::43/128
```

hm interval-10sec

To configure Health Monitoring (HM) timeout as per day-one design between PPC and IXP. Use the **no** form of this command to remove command.

hm interval-10sec

no hm interval-10sec

Syntax Description There are no keywords or arguments for this command.

Command Modes Global configuration

Command History	Release	Modification
	WSG Release 4.4.8	This command was introduced.

Usage Guidelines Following are the usage guidelines:

- As per 4.4.8, new changes have been introduced in HM infra where IXP failure can be detected within 15 seconds. Above CLI should be avoided until directed by BU/Support teams as plan of contingency.
- This CLI needs to be enabled only in Maintenance window with no profiles and traffic.
- This CLI will not be synced from ACTIVE to STANDBY.
- After configuring the CLI, reloading the SAMI card is mandatory for the CLI to take effect.



Note

This CLI needs to be used with caution considering which of six PPCs would require this CLI, because it depends on the type of configuration like site-to-site or other modes.

Examples To configure HM interval and reload:

```
switch(config)# hm interval-10sec
```

ip address

To configure the IP address used by the HA infrastructure to communicate among the nodes in the same cluster (subnet), use the **ip address** command in interface configuration submode. Use the **no** form of the command to remove the IP address.

```
ip address ip_address netmask
```

```
no ip address ip_address netmask
```

Syntax Description

ip_address netmask IP address and its subnet netmask for this interface.

Defaults

None.

Command Modes

Interface configuration submode

Command History

Release	Modification
WSG Release 2.0	This command was introduced.

Usage Guidelines

These CLIs must to be configured on each PPC. The 2 PPCs that are to be paired together should have the same VLAN ID. 6 different VLAN IDs will be used for 6 pairs of PPCs.

Examples

The following examples show how to configure the HA VLAN/IP addresses for the PPC#3 on Slot#1 and the PPC#3 on Slot#3:

On Slot#1/PPC#3:

```
WSG(config)# ha interface vlan 611
WSG(config-if)# ip address 11.11.1.13 255.255.255.0
```

On Slot#3/PPC#3:

```
WSG(config)# ha interface vlan 611
WSG(config-if)# ip address 11.11.1.23 255.255.255.0
```

ip address start-ip

To configure the start IP address of the HA VLANs that you are configuring for incremental sync, use the **ip address start-ip** command in interface configuration submode. Use the **no** form of the command to disable this functionality.

ip address start-ip *ip_address* **increment** *increment* **mask** *ip_address_netmask*

no ip address start-ip

Syntax Description

<i>ip_address</i>	The starting IP address.
increment	The number of the incremental change of the IP address.
<i>ip_address_netmask</i>	IP address and IP subnet for this interface.

Defaults

None.

Command Modes

Interface configuration submode

Command History

Release	Modification
WSG Release 2.0	This command was introduced.

Usage Guidelines

This command is available in the entity-all mode at director PPC (PPC3).

Examples

If you execute the following CLI on the director PPC (PPC3):

```
WSG(mode-all)(config)# ha interface vlan start-id 212 increment 2
WSG(mode-all)(config-if)# ip address start-ip 11.11.1.11 increment 0.0.1.2 mask
255.255.255.0
```

The resulting configurations on the 6 PPCs appear as follows:

PPC3:

```
WSG(config)# ha interface vlan 212
WSG(config-if)# ip address 11.11.1.11 255.255.255.0
```

PPC4:

```
WSG(config)# ha interface vlan 214
WSG(config-if)# ip address 11.11.2.13 255.255.255.0
```

PPC5:

```
WSG(config)# ha interface vlan 216
WSG(config-if)# ip address 11.11.3.15 255.255.255.0
```

PPC6:

```
WSG(config)# ha interface vlan 218
WSG(config-if)# ip address 11.11.4.17 255.255.255.0
```

PPC7:

```
WSG(config)# ha interface vlan 220
WSG(config-if)# ip address 11.11.5.19 255.255.255.0
```

PPC8:

```
WSG(config)# ha interface vlan 222
WSG(config-if)# ip address 11.11.6.21 255.255.255.0
```

ip name-server

To specify the name-server address, use the **ip name-server** global configuration command. Use the **no** form of the command to disable this feature.

```
ip name-server A.B.C.D | X:X:X::X
```

```
no ip name-server
```

Syntax Description

<i>A.B.C.D</i>	Specifies the IPv4 name-server address.
<i>X:X:X::X</i>	Specifies the IPv6 name-server address.

Defaults

None.

Command Modes

Global configuration

Command History

Release	Modification
WSG Release 2.0	This command was introduced.
WSG Release 3.0	Added support for IPv6.

Usage Guidelines

If multiple DNS servers are configured, verify that all DNS servers are redundant with each other and identically configured.

Examples

This example shows how to enable the **ip name-server** command for IPv6:

```
wsg(config)# ip name-server ?
                <A.B.C.D>|<X:X:X::X>  Enter an IP address
wsg(config)# ip name-server 2001:88:88:94::1
```

ip route

To add a route to a VRF, use the **ip route** global configuration command. Use the **no** form of the command to disable a route.

ip route *ip_address subnet_mask gateway [vrf vrf_name]*

no ip route *ip_address subnet_mask gateway [vrf vrf_name]*

Syntax Description

<i>ip_address</i>	Specifies the IP address of the route you are adding.
<i>subnet_mask</i>	Specifies the subnet mask of the route.
<i>gateway</i>	Specifies the gateway of the route.
<i>vrf_name</i>	Specifies the VRF.

Defaults

None.

Command Modes

Global configuration

Command History

Release	Modification
WSG Release 3.0	This command was introduced.

Usage Guidelines

Up to 10 IPv4/IPv6 routes can be configured for each VRF on each PPC. A total of 60 routes can be configured for a SAMI.

Examples

This example shows how to add a route to a VRF with the **ip route** command:

```
wsg(config)# ip route 192.200.10.0 255.255.255.0 192.100.10.1 vrf green_vrf
```

ip ssh auth-type

To start the SSH server or RADIUS client, use the **ip ssh auth-type** global configuration command. Use the **no** form of the command to stop this feature.

ip ssh auth-type {radius | local}

no ip ssh auth-type {radius | local}

Syntax Description There are no keywords or arguments for this command.

Command Default By default the auth-type is local.

Command Modes Global configuration

Command History	Release	Modification
	WSG Release 4.0	This command was introduced.

Usage Guidelines The following authentication types are possible:

```
switch(config)# ip ssh auth-type local
switch(config)# ip ssh auth-type radius
switch(config)# ip ssh auth-type local radius
switch(config)# ip ssh auth-type radius local
```

If more than one auth-type is specified, they are tried in order. The authentication attempt fails only if both attempts fail.

Examples Here is an example of the **ip ssh auth-type** command:

```
switch(config)# ip ssh auth-type radius local
```


ip ssh enable

To start the SSH service, use the **ip ssh enable** global configuration command. Use the **no** form of the command to stop the SSH service.

ip ssh enable

no ip ssh enable

Syntax Description There are no keywords or arguments for this command.

Command Default The SSH service is stopped by default.

Command Modes Global configuration

Command History	Release	Modification
	WSG Release 3.0	This command was introduced.

Examples Here is an example of the **ip ssh enable** command:

```
switch(config)# ip ssh enable
switch(config)# do sh run
```

Generating configuration.....

```
hostname switch
ip ssh key dsa
MIIBuwIBAAKBgQDA4F79tssxgc4TkMI/xUJz2vCWJD70OS/4sNxP42oRTuBHgp0ZJwltWGv50MtNpr/qAnlANsxTZC
bdREC2t6yVQFopF0sg7Owi/Xk6XN9iglNy1qo0TU9UvZcv/lRgU8FpocBRdKgQjhUZy7pVnSVzrw3H4Dx8LJJ4dEvP
2hJOhwIVAPe7Tr40TuwGoQPyQRIDxjQLTbuTAoGAXoc60iM521FDGOZLgQm9JNWU/vV18YkeS8iCLpj2Y8zzJd0SCM
v42vtRDajFyf8I+0ahKzei8HNgmxlariYsHv6HrW0DtD+vwMsbFFtOqNczv4Qakgl6Qasd87y8FSIyNsIdd32tc2zj
MwX+Nvow5Efq6yUGJpBQVm3Gpgwu3ggCgYEAmGVuTfPL0pkTYoTN1iCbPWIGB+ATuwsxuxiUp39cInzBORTL5R0hPt
xiS0NeY8PrQfHVUBt4jIQ1TqnfyKFMqOHSanTX+fbfUk1CQ44GNNUF4ivkBMJxGCtm/j8zaTT+09oWJ1WK20CDvIBA
KrSVOyBYBeTpbDEq79uph2/bx48CFFTZMItzfWQa6sSPN9NNqxnk3X8g
ip ssh enable
ip ssh auth-type local radius
ip ssh radius-server host 22.22.110.100 key cisco123 port 5000
ip ssh radius-server host 44.44.44.212 key cisco
ip ssh radius-server host 22.22.110.101 key cisco123 port 1812 timeout 30
ip ssh radius-server host 22.22.110.102 key cisco123 port 1812 timeout 30
username test3 password 5 c9608fbcDqzJgUvInwJ2i83zb46/0/
```

ip ssh key dsa

To create a dsa key for the ssh service, use the **ip ssh key dsa** global configuration command. Use the **no** form of the command to disable this feature.

ip ssh key dsa *key*

no ip ssh key dsa

Syntax Description	<i>key</i>	The dsa key that the ssh service uses.
Command Default	None.	
Command Modes	Global configuration	
Command History	Release	Modification
	WSG Release 3.0	This command was introduced.

Usage Guidelines

Since generating a dsa key is not easy, we recommend that you allow the service to automatically generate a key. If one is not configured when the ssh service is enabled using **ip ssh enable**, then one will be automatically generated. This command is mainly used to transfer the key between blades.

The **no** variant does not require that the user enter the entire key. Instead it stops short with:

```
no ip ssh key dsa
```

This is avoid having to cut and paste the whole key. Issuing a **no ip ssh key dsa** command while the ssh service is running will cause it to automatically generate a new key. If you wish to avoid this, first disable the ssh service.

Examples

Here is an example of the **ip ssh key dsa** command:

```
router(config)# ip ssh key dsa
MIIBuwIBAAKBgQCecmWQsoFY8VYOCs0zEmI8Vn1OMMSNxr7RuLzhsHzTL3jhSW5bEpi9vprjC6JR774Dvr2rebP5m
tv8GhDebVEyqDFy0D1jiJw6AxBd6Begu5PZy3zrHjlmxnOcGiCqM4GOW6qP1drj7aPYBxZzY9IXjFis7QXxmVCAovE
O95XtQIVAMIZuoiYMoYyLMEvvZJ91DVfz1pBAoGBAIJep7IWolxhXByAc/iiUX0erJz0Qb64n+g5Hm3Y1Jg7mdn0BA
EBoOsZrdRHvowHp5gyufjDFztMYcWm1r07vEX0K5atuAhjacTwyH9zGuvK0HREu88Uza+M92o6JARYar5ip3luhmow
tZGnMcrLn49CZ8z0oIGzJtWclvfpOjZAoGAY1D4CBRerptiTBHyCUPnNXfu3m7NVzSYIyxNflpWfp+3Tp7DcqwASA
fncuvV9vXK3WuCGTle+jAFC2qdTvYJmI4At+sa8JmN9mR9Lc5Ryb2qJ/iriWZiimZhleVLCc0wzFSMOWqFd77cm5TB
FRkNY19gI01KNMdwI6Kk2Ce32v0CFck5nas4jBwZ2KlHnn1ur+Kf7VKE
```

ip ssh port

To change the port used by SSH, use the **ip ssh port** global configuration command. Use the **no** form of the command to remove this assignment.

```
ip ssh port port_number
```

```
no ip ssh port
```

Syntax Description

<i>port_number</i>	The port number to be used by SSH.
--------------------	------------------------------------

Command Default

By default the port number is 22.

Command Modes

Global configuration

Command History

Release	Modification
WSG Release 3.0	This command was introduced.

Usage Guidelines

This command has no variant to revert back to the default port value of 22.

Examples

Here is an example of the **ip ssh port** command:

```
switch(config)# ip ssh ?
  enable  Enable SSH server
  key     SSH server key
  port    SSH server port
switch(config)# ip ssh port ?
  <0-65535> Portnum
switch(config)# ip ssh port 65535
switch(config)# do sh run

Generating configuration.....
hostname S2P8
ip ssh port 65535

switch(config)# no ip ssh port 65535
switch(config)#
```

ip ssh radius-server

To configure one or more RADIUS servers, use the **ip ssh radius-server** global configuration command. Use the **no** form of the command to remove specified RADIUS servers.

ip ssh radius-server host *host_IP* **key** *key_str* [**port** *port_number* **timeout** *timeout_number*]

no ip ssh radius-server host *host_IP* **key** *key_str* [**port** *port_number* **timeout** *timeout_number*]

Syntax Description

<i>host_IP</i>	IP address of the RADIUS server.
<i>key_str</i>	Shared key to authenticate with the RADIUS server.
<i>port_number</i>	Port number to be used with the RADIUS server. Default is port 1812.
<i>timeout_number</i>	Number of seconds to wait before deciding that the server has failed to respond. Default is 3 seconds.

Command Default

The default value for *port_number* is port 1812. The default value for *timeout_number* is 3 seconds.

Command Modes

Global configuration

Command History

Release	Modification
WSG Release 4.0	This command was introduced.

Usage Guidelines

If multiple RADIUS servers are configured, they are tried in order. The first server to return a success or failure determines the RADIUS authentication status. A server that fails to respond is skipped, and the next server is used.

Examples

This example shows how to add a RADIUS server to the WSG:

```
wsg(config)# ip ssh radius-server host 172.29.98.37 key secretkey port 1822 timeout 10
```

ipv6

To add an IPv6 host or route, use the **ipv6** global configuration command. Use the **no** form of the command to remove an IPv6 host or route.

```
ipv6 {host ipv6_address | route ipv6_prefix ipv6_gateway}
```

```
no ipv6 {host ipv6_address | route ipv6_prefix ipv6_gateway}
```

Syntax Description

host	Maps the host name to the IPv6 address.
ipv6_address	Specifies the IPv6 address.
route	Configures static IPv6 routing.
<i>ipv6_prefix</i>	Specifies the IPv6 prefix.
<i>ipv6_gateway</i>	Specifies the IPv6 gateway.

Defaults

None.

Command Modes

Global configuration

Command History

Release	Modification
WSG Release 3.0	This command was introduced.

Usage Guidelines

Up to 10 IPv4/IPv6 routes can be configured for each VRF on each PPC. A total of 60 routes can be configured for a SAMI.

This CLI is node-specific and cannot be executed under entity-all mode.

Examples

This example shows how to enter an IPv6 host and route:

```
wsg(config)# ipv6 host ?
<X:X:X::X> Enter an IPv6 address
wsg(config)# ipv6 host 2001:88:88:94::1
wsg(config)# ipv6 route ?
<X:X:X::X/n> Configure destination prefix
wsg(config)# ipv6 route 2001:88:88:94::4/96 ?
<X:X:X::X> Configure gateway
wsg(config)# ipv6 route 2001:88:88:94::4/96 2001:88:88:94::1
```

ip vrf

To add a VRF, use the **ip vrf** global configuration command. To remove a VRF, use the **no** form of the command, including the specific *vrf_name*.

```
ip vrf vrf_name
```

```
no ip vrf vrf_name
```

Syntax Description

<i>vrf_name</i>	Specifies name of the VRF.
-----------------	----------------------------

Defaults

The **ip vrf** command is unconfigured by default.

Command Modes

Global configuration.

Command History

Release	Modification
WSG Release 3.0	This command was introduced.

Usage Guidelines

By default, a network interface belongs to exactly one VRF, which is VRF_GLOBAL (VRF_NAME = global). In order to associate a VLAN interface with a specific VRF, use the **vrf vrf_name** command after the interface is created (but before the IP address is assigned):

```
switch(config)# interface vlan 11
switch(config-if)# vrf green_vrf
switch(config-if)# ip address 11.11.11.11 255.255.255.
```

After associating a VLAN device to a VRF, IP addresses can be added to the VLAN interface. These addresses and any automatic routes created as a result of address addition belong to the same VRF as the VLAN interface. Use the **show interface vlan** command to display the VRF membership of an interface.



Note

VRFs can be set on an interface that already has an IP address assigned. After adding the interface to the new VRF, the IPv4/IPv6 addresses on the interface are deleted. Any routes associated with the interface within the old VRF are also removed.

To remove a vrf-interface association, use the **no vrf** command. Upon removal, interfaces that are part of the deleted VRF are migrated back to the VRF global. The IPv4/IPv6 addresses and routes associated with the migrated interfaces are cleared.

Up to 1,000 VRFs can be configured for each PPC.

Examples

This example shows how to enable the **ip vrf** command:

```
wsg(config)# ip vrf green_vrf
```

logging

To configure the IP address of the external logging server, use the **logging** global configuration command. Use the **no** form of the command to disable this feature.

```
logging {ip A.B.C.D | ipv6 X:X:X::X | lineread}
```

```
no logging {ip A.B.C.D | ipv6 X:X:X::X | lineread}
```

Syntax Description

<i>A.B.C.D</i>	Specifies the IPv4 address of the external logging server.
<i>X:X:X::X</i>	Specifies the IPv6 address of the external logging server.
lineread	Configures the number of lines to read from the log.

Defaults

By default, this command is not configured.

Command Modes

Global configuration

Command History

Release	Modification
WSG Release 3.0	This command was introduced.
WSG Release 3.1	Allow multiple external logging servers with IPv4 addresses.

Usage Guidelines

In WSG Release 3.1 and above, the **logging** command allows you to configure multiple external logging servers with IPv4 addresses. However, only a single logging server with an IPv6 address can be configured at a time.

Examples

This example shows how to enable the **logging** command for IPv6:

```
wsg(config)# logging ?
    ip          Configure ip address of ext logging server
    ipv6        Configure IPv6 address of ext logging server
    lineread    Configure number of lines to read log
wsg(config)# logging ipv6 ?
    <X:X:X::X>  Enter IPv6 address
wsg(config)# logging ipv6 2001:88:88:94::1
```

router bgp

To enable Border Gateway Protocol (BGP) routing and place you in the BGP configuration mode, use the **router bgp** global configuration command. Use the **no** form of the command to disable BGP routing.

```
router bgp local-asn
```

```
no router bgp local-asn
```

Syntax Description	<i>local-asn</i>	The autonomous system (AS) number is a required parameter that specifies the local BGP. The range is from 1 to 65535.
---------------------------	------------------	---

Defaults	None.
-----------------	-------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	WSG Release 3.0	This command was introduced.

Usage Guidelines	In WSG Release 3.0, the BGP neighboring address only supports IPv4 addresses.
-------------------------	---

Examples Here is an example of the **router bgp** command:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# router bgp ?
  <1-65535> Autonomous system number
switch(config)# router bgp 65535
switch(config)#
```


neighbor

To configure a BGP peer, use the **neighbor** command in BGP configuration submode. To remove a BGP peer, use the **no** form of the command.

```
neighbor ip_address remote-as remote_asn next-hop-alias next_ip_address
```

```
no neighbor ip_address remote-as remote_asn
```

Syntax Description

<i>ip_address</i>	Specifies the IPv4 or IPv6 address of a neighboring BGP peer. Each address should be a unique identifier of a neighboring BGP peer.
<i>remote_asn</i>	Specifies the remote Autonomous System (AS) number of the BGP peer. The range is from 1 to 65535.
<i>next_ip_address</i>	Specifies the IPv4 or IPv6 address of the next hop alias.

Defaults

None.

Command Modes

Router BGP configuration submode

Command History

Release	Modification
WSG Release 3.0	This command was introduced.
WSG Release 4.0	Support for IPv6 addresses was added.

Usage Guidelines

Support for IPv6 addresses in *ip_address* and *next_ip_address* was added in WSG Release 4.0.

Examples

Here is an example of the **neighbor** command:

```
switch(config)# router bgp 65535
switch(config-router)# neighbor ?
<A.B.C.D>|<X:X:X::X> Neighbor address (IPv4 or IPv6)
switch(config-router)# neighbor 33.33.33.3 remote-as 65535 next-hop-alias 33.33.33.30
switch(config-router)# no neighbor 33.33.33.3 remote-as 65535
switch(config-router)# neighbor 2001:88:88:114::100 remote-as 76 next-hop-alias
2001:88:88:114::94
switch(config-router)# no neighbor 2001:88:88:114::100 remote-as 76 next-hop-alias
2001:88:88:114::94
```

auto-initiate

To configure the WSG to initiate a tunnel with a peer when a site-to-site type profile is activated, use the **auto-initiate** command in ISAKMP submode. Use the **no** form of the command to disable this feature.

auto-initiate

no auto-initiate

Syntax Description There are no keywords or arguments for this command.

Defaults The default setting is to not initiate tunnels.

Command Modes ISAKMP submode

Command History	Release	Modification
	WSG Release 1.2	This command was introduced.

Usage Guidelines When **auto-initiate** is configured, the peer's IP address must be specified in the profile.

- Try to initiate a tunnel as soon as the profile is activated.
- Keep re-trying, if it fails.
- Retry even after clearing the tunnel.

Examples This example shows how to initiate a tunnel:

```
crypto profile <name>
  isakmp
    auto-initiate
```

dpd-timeout

To define the interval in which the DPD packets are initiated from the WSG, use the **dpd-timeout** command in ISAKMP submode. Use the **no** form of the command to disable DPD initiation on the profile tunnels.

dpd-timeout *timeout*

no dpd-timeout

Syntax Description	<i>timeout</i>	Value of the dpd-timeout in seconds. Default value is 0. Range is 0 to 5040. Enter timeout value as 0, 90, 180, 270, etc. (by multiples of 90) up to 5040.
---------------------------	----------------	--

Defaults	The default is 0 (off).
-----------------	-------------------------

Command Modes	ISAKMP submode
----------------------	----------------

Command History	Release	Modification
	WSG Release 1.2	This command was introduced.
WSG Release 3.0	The <i>timeout</i> argument is enhanced to count in multiples of 90.	

Usage Guidelines The **no dpd-timeout** *timeout* form of the command disables DPD initiation on the profile tunnels.



Note When upgrading the WSG, a previously configured DPD value will be rounded to a WSG Release 3.0 value.



Note For solutions requiring more than 5,000 tunnels per PPC, Cisco recommends configuring a dpd-timeout greater than 180 seconds.

Examples This example shows how to enter a DPD value of 270 seconds:

```
switch(config-crypto-profile-isakmp)# dpd-timeout 260
Incorrect DPD timeout value. Please configure value in multiple of 90 secs.

switch(config-crypto-profile-isakmp)# dpd-timeout ?
<0-5040> Enter timeout as 0,90,180,270...up to 5040 sec(default:0 turn-off)
switch(config-crypto-profile-isakmp)# dpd-timeout 270
switch(config-crypto-profile-isakmp)# end
switch# show running-config
...
crypto profile "remote-access"
  isakmp
```

■ dpd-timeout

```
dpd-timeout 270
```

sequence-number

To specify that a 32-bit (short) or 64-bit (extended) sequence number is used for a profile, use the **sequence-number** command in ISAKMP submode. Use the **no** form of the command to disable the sequence number.

```
sequence-number { extended | short }
```

```
no sequence-number { extended | short }
```

Syntax Description

extended	64-bit sequence number.
short	32-bit sequence number (default).

Defaults

The default setting is the **short** (32-bit) value.

Command Modes

ISAKMP submode

Command History

Release	Modification
WSG Release 1.2	This command was introduced.

Examples

This example shows the extended sequence number:

```
crypto profile name
  isakmp
    sequence-number extended
```

eap-type

To set the EAP method, use the **eap-type** command in ISAKMP submode.
To remove an EAP method, use the **no** form of the command.

eap-type {aka | md5 | sim}

no eap-type {aka | md5 | sim}

Syntax Description

aka	128-bit AKA authentication method.
md5	128-bit MD5 authentication method
sim	128-bit SIM authentication method.

Defaults

Disabled by default.

Command Modes

ISAKMP submode

Command History

Release	Modification
WSG Release 3.0	This command was introduced.

Usage Guidelines

Extensible Authentication Protocol (EAP) is an authentication framework that defines message formats. WSG supports the following EAP authentication methods:

- UMTS Authentication and Key Agreement (EAP-AKA)
- Message Digest algorithm 5 (EAP-MD5)
- GSM Subscriber Identity Module (EAP-SIM)

Use the **eap-type** command to set the EAP method. When all user-entered configurations for this parameter are removed, then the feature again becomes disabled by default.

Multiple eap-type authentication methods can be configured in a profile. This is not supported in S2S profiles.

Examples

This example shows how to set an EAP method using 128-bit SIM:

```
WSG# config
Enter configuration commands, one per line. End with CNTL/Z.
WSG (config)# crypto profile name
WSG(config-crypto-profile)# isakmp
WSG(config-crypto-profile-isakmp)# eap-type sim
```

encryption

WSG supports the following IKE secret encryption schemes:

- Data Encryption Standard (DES)
- Triple DES (3DES), also known as Triple Data Encryption Algorithm (3TDEA)
- Advanced Encryption Standard (AES)

To set the IKE secret encryption scheme, use the **encryption** command in ISAKMP submode. To remove an IKE secret encryption scheme, use the **no** form of the command.

```
encryption {des | 3des | aes | aes192 | aes256}
```

```
no encryption {des | 3des | aes | aes192 | aes256}
```

Syntax Description

des	56-bit DES encryption algorithm. This is faster than 3des .
3des	168-bit Triple DES encryption algorithm. 3des is more secure but one third as fast as des .
aes	128-bit AES encryption algorithm. AES is more efficient than Triple DES and requires less memory.
aes192	192-bit AES encryption algorithm. This is stronger than 128-bit AES.
aes256	256-bit AES encryption algorithm. This is stronger than 192-bit AES.

Defaults

The default value is **aes**.

Command Modes

ISAKMP submode

Command History

Release	Modification
WSG Release 1.1	This command was introduced.
WSG Release 3.0	This command was enhanced to configure multiple encryptions.

Usage Guidelines

Use the **encryption** command to set the IKE secret encryption scheme. Multiple algorithms can be configured together. The default values are not displayed. When you enter a scheme, the default is overwritten. When all user-entered configurations for this parameter are removed, then the default again becomes the **aes** value.

Examples

This example shows how to set an IKE encryption scheme using the 128-bit AES encryption algorithm:

```
WSG# config
Enter configuration commands, one per line. End with CNTL/Z.
WSG (config)# crypto profile name
WSG(config-crypto-profile)# isakmp
WSG(config-crypto-profile-isakmp)# encryption des
```

group

IKE uses Diffie-Hellman to establish session keys. Diffie-Hellman is a public-key cryptography protocol that allows two parties to share a secret over an unsecured channel. IKE Groups set the allowed Diffie-Hellman groups for IKE SAs.

To set a group ID, use the **group** command in ISAKMP submode. To remove the group ID, use the **no** form of the command.

```
group {1 | 2 | 5 | 14 | 15 | 16 | 17 | 18}
```

```
no group {1 | 2 | 5 | 14 | 15 | 16 | 17 | 18}
```

Syntax Description

1	Group 1 (768 bits).
2	Group 2 (1024 bits).
5	Group 5 (1536 bits).
14	Group 14 (2048 bits).
15	Group 15 (3072 bits).
16	Group 16 (4096 bits).
17	Group 17 (6144 bits).
18	Group 18 (8192 bits).

Defaults

The default value is Group 2.

Command Modes

ISAKMP submode

Command History

Release	Modification
WSG Release 1.1	This command was introduced.
WSG Release 2.0	Groups 14 , 15 , 16 , 17 , and 18 were added.
WSG Release 2.2	Added support for multiple DH groups.

Usage Guidelines

Use the **group** command to set the group ID.

Multiple Diffie-Hellman groups can be specified.

Examples

This example shows how to set the group ID to 5:

```
WSG# config
Enter configuration commands, one per line. End with CNTL/Z.
WSG (config)# crypto profile name
WSG(config-crypto-profile)# isakmp
WSG(config-crypto-profile-isakmp)# group 5
```


hash

Hash algorithms are used to authenticate packet data. WSG Release 1.2 and above supports three types of ISAKMP hash protocols: Message Digest Algorithm 5 (MD5), Secure Hash Algorithm (SHA) and AES Cipher Block Chaining Algorithm (aes-xcbc).

To set a hash algorithm, use the **hash** command in ISAKMP submode. To remove the hash algorithm, use the **no** form of the command.

```
hash {aes-xcbc | md5 | sha1 | sha2}
```

```
no hash {aes-xcbc | md5 | sha1 | sha2}
```

Syntax Description

aes-xcbc	aes-xcbc is a hash algorithm which uses AES block cipher with its increased size of 128 bits and increased key length (128 bits). aes-xcbc-mac-96 is used as an authentication mechanism within the context of IPSec encapsulation and authentication header protocols. Note Supported in IKEv2 only.
md5	MD5 (HMAC variant)— md5 (Message Digest 5) is a hash algorithm. It is one-way algorithm that makes a 128-bit digest. It is less secure but faster than SHA.
sha1	SHA1 (HMAC variant)—SHA (Secure Hash Algorithm) is a hash algorithm. It is one-way algorithm that makes a 160-bit digest. It is more secure but slower than MD5.
sha2	SHA2 is a cryptographic hash algorithm used for securing information and messages. It consist of SHA-224, SHA-256, SHA-384, and SHA-512 - collectively known as SHA2. It is a one-way algorithm which is more secure but slower than MD5.

Defaults

The default value is sha1.

Command Modes

ISAKMP submode

Command History

Release	Modification
WSG Release 1.1	This command was introduced.
WSG Release 2.2	Added support for multiple hash algorithms.

Usage Guidelines

Use the **hash** command to set a hash algorithm. In WSG Release 2.2 and above, multiple hash algorithms can be combined. The default values are not displayed. When you enter an algorithm, the default is overwritten. When all user entered configurations for this parameter are removed, then the default again becomes the **sha1** value.

Examples

This example shows how to set the hash algorithm to **md5**:

```
WSG# config  
Enter configuration commands, one per line. End with CNTL/Z.  
WSG (config)# crypto profile remote-access  
WSG(config-crypto-profile)# isakmp  
WSG(config-crypto-profile-isakmp)# hash md5
```


self-identity

To set up an ID type for the local client to use during IKE negotiation, use the **self-identity** command in the ISAKMP submode. To remove the configuration, use the **no** form of the command.

```
self-identity id-type id-type id id
```

```
no self-identity id-type id-type id id
```

Syntax Description

<i>id-type</i>	IKE identify. The IKE identity is the identity sent to the remote client during IKE negotiation. Valid values are: <ul style="list-style-type: none"> ip—IP address can be either IPv4 or IPv6 [A.B.C.D X:X:X::X] fqdn—Fully-qualified domain name. email—Email address dn—Distinguished name.
	 Note The maximum size supported for the id-types is 256 bytes.
<i>id</i>	Data for the ID type—IP address, DN, FQDN, or email address as in RFC 822. WSG Release 3.0 adds IPv6 address support for this argument.

Defaults

None.

Command Modes

ISAKMP submode

Command History

Release	Modification
WSG Release 1.0	This command was introduced as the ipsec local-identity command.
WSG Release 1.1	This command was changed.
WSG Release 3.0	Added DN and IPv6 support.

Usage Guidelines

Use the **self-identity** command to set up an identity for the local client.



Note

- local-identity must match the certificate's identity when using certificates for authentication.
- The supported characters while configuring the self-identity are dash, dot, underscore, a-z, A-Z and 0-9.

Examples

This example shows how to define the local client IKE identity as an IP address:

```
WSG(config-crypto-profile-isakmp)# self-identity id-type ip id ?  
<A.B.C.D>|<X:X:X::X> Enter IP address
```

lifetime

The IKE SA is kept by each peer until it's lifetime expires. Because new SAs are negotiated before current SAs expire, they can be reused to save time. Shorter lifetimes mean more secure negotiations. Longer lifetimes mean SAs are more quickly set up.

To set the IKE lifetime of an SA, use the **lifetime** command. To reset the SA lifetime to the default value, use the **no** form of the command.

lifetime {seconds}

no lifetime {seconds}

Syntax Description	seconds	7200 to 2147483647 seconds.
---------------------------	----------------	-----------------------------

Defaults	28800 seconds
-----------------	---------------

Command Modes	ISAKMP submode
----------------------	----------------

Command History	Release	Modification
	WSG Release 1.1	This command was introduced.

Usage Guidelines

Use the **lifetime** command to set how long an IKE SA lives before expiring.

Depending on the application, the IKE SA lifetime may also be configured on the peer. We recommend that you do not configure a peer IKE SA lifetime that is shorter than the minimum supported by the WSG.

Examples

This example shows how to set an SA lifetime to 7200 seconds (120 minutes):

```
WSG# config
Enter configuration commands, one per line. End with CNTL/Z.
WSG (config)# crypto profile remote-access
WSG(config-crypto-profile)# isakmp
WSG(config-isakmp)# lifetime 7200
```

local-secret

To set a shared key, use the **local-secret** command. To remove the key, use the **no** form of the command.

local-secret *secret*

no local-secret *secret*

Syntax Description	secret	String of the shared, secret key.
--------------------	--------	-----------------------------------

Defaults	local-secret is disabled.
----------	---------------------------

Command Modes	ISAKMP submode
---------------	----------------

Command History	Release	Modification
	WSG Release 1.1	This command was introduced.

Usage Guidelines	Use the local-secret command to set a shared key.
------------------	--

Examples	<p>This example shows how to set the shared key name to <i>foo</i>:</p> <pre>WSG# config Enter configuration commands, one per line. End with CNTL/Z. WSG (config)# crypto profile name WSG(config-crypto-profile)# isakmp WSG(config-crypto-profile-isakmp)# local-secret foo</pre>
----------	--

peer-ip

To set the peer for the IKE and IPsec negotiations, use the **peer-ip** command. To remove the configuration use the **no** form of the command.

peer-ip *ip-address*

no peer-ip *ip-address*



Note

Only for site-to-site configuration. Not applicable to Remote access profile.

Command Default

Peer IP is not configured.

Command Modes

ISAKMP submode

Command History

Release	Modification
WSG Release 1.1	This command was introduced.
WSG Release 1.2	This command was moved to ISAKMP submode.
WSG Release 3.0	Support for IPv6 was added.

Usage Guidelines

Use the **peer-ip** command to set peer-ip for the tunnel profile.



Note

You should not configure this command for remote access type profiles.

Examples

This example shows how to set peer-ip for the tunnel profile.

```
WSG# config
Enter configuration commands, one per line. End with CNTL/Z.
WSG (config)# crypto profile name
WSG(config-crypto-profile)# isakmp
WSG(config-crypto-profile-isakmp)# peer-ip ?
  <A.B.C.D>|<X:X:X::X>  Enter IP address
```

ike-version

To set the IKE version, use the **ike-version** command. To remove the IKE version, use the **no** form of the command.

ike-version {1 | 2 | both}

no ike-version {1 | 2 | both}

Syntax Description	1 2 both	<p>1—IKE version 1</p> <p>2—IKE version 2</p> <p>both—IKE version 1 and IKE version 2, use this if you are not sure which IKE version the client is using.</p>
---------------------------	--------------	---

Defaults	2
-----------------	---

Command Modes	ISAKMP submodule
----------------------	------------------

Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>WSG Release 1.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	WSG Release 1.1	This command was introduced.
Release	Modification				
WSG Release 1.1	This command was introduced.				

Usage Guidelines	Use the ike-version {1 2 both} command to set the IKE version.
-------------------------	---



Note

ike-version both is not supported with auto-initiate in site-to-site profiles.

Examples	This example shows how to set the IKE version to 1:
-----------------	---

```
WSG# config
Enter configuration commands, one per line. End with CNTL/Z.
WSG (config)# crypto profile name
WSG(config-crypto-profile)# isakmp
WSG(config-crypto-profile-isakmp)# ike-version 1
```


ike-start-with-natt

WSG can be configured to disable the usage of NAT ports when an IKE message is initiated from WSG like in case of a rekey.

This would make sure that the IKE messages on a rekey are sent out on port 500 instead of 4500. This command is only required for IKEV1. The NAT ports will be enabled by default; to disable it and make the WSG use the port 500 on IKE negotiations, use this command.

To disable the IKE initiations on the NAT ports, use **ike-start-with-natt** command. To undo the configuration use the **no** command.

ike-start-with-natt disable

no ike-start-with-natt disable

Syntax Description	disable	Disable the ike initiation with natt
--------------------	---------	--------------------------------------

Defaults NAT initiation is disabled.

Command Modes ISAKMP Submode.

Command History	Release	Modification
	WSG Release 1.1	This command was introduced.

Usage Guidelines Use **ike-start-with-natt** command to disable IKE initiation with NATT for IKEV1.

Examples

```
Router(config-crypto-profile-isakmp)# ike-start-with-natt ?
      disable  Disable the ike initiation with natt
Router(config-crypto-profile-isakmp)# ike-start-with-natt disable
```

authentication

To set the IKE authentication method, use the **authentication** command. To remove the IKE authentication method, use the **no** form of the command.

authentication { **rsa-sig** | **pre-shared** }

no authentication { **rsa-sig** | **pre-shared** }

Syntax Description

rsa-sig | pre-shared

- **rsa-sig**—Peer routers to get certificates from a CA.
- **pre-shared**—Preshared keys are separately configured.

Defaults

RSA signatures are used.

Command Modes

ISAKMP submodule

Command History

Release	Modification
WSG Release 1.1	This command was introduced.

Usage Guidelines

Use the authentication command to set IKE authentication method.

Examples

This example shows how to set IKE authentication method:

```
WSG# config
Enter configuration commands, one per line. End with CNTL/Z.
WSG (config)# crypto profile name
WSG(config-crypto-profile)# isakmp
WSG(config-crypto-profile-isakmp)# authentication rsa-sig
```

ipv6

To enter the IPv6 address or alias, use the **ipv6** command in interface configuration submode. Use the **no** form of the command to disable this feature.

```
ipv6 {address | alias}
```

```
no ipv6 {address | alias}
```

Syntax Description

address	The IPv6 address of the interface.
alias	The IPv6 alias of the interface.

Defaults

The default is that the **ipv6** command is unconfigured.

Command Modes

Interface configuration submode

Command History

Release	Modification
WSG Release 3.0	This command was introduced.

Usage Guidelines

Each interface is allowed to have one or both IPv4 address/alias and IPv6 address/alias.

Examples

This example shows how to enable various instances of the **ipv6** command:

```
wsg(config)# interface vlan 10
wsg(config-if)# ipv6 ?
    address    IPv6 address of interface
    alias      IPv6 alias address of interface

wsg(config-if)# ipv6 address ?
    <X:X:X::X/n> Enter an IPv6 prefix

wsg(config-if)# ipv6 address 2001:88:88:94::/96 ?
    eui-64 Use eui-64 interface identifier
    <cr> Carriage return

wsg(config-if)# ipv6 alias ?
    <X:X:X::X/n> Enter an IPv6 prefix
```

Each interface is allowed to have one or both IPv4 address/alias and IPv6 address/alias. For example,

```
interface vlan 10
  ip address 10.10.10.3 255.255.255.0
  alias 10.10.10.1 255.255.255.0
  ipv6 address 2001:88:88:94::4/96
  ipv6 alias 2001:88:88:94::1/9
```

**Note**

This CLI is a node-specific command and cannot be executed under entity-all mode.

ip address-pool

To specify when a profile is required to use DHCP-based address allocation, or to specify the name of the address pool to be used for a profile, set the **ip address-pool** command. Use the **no** form of the command to remove the address-pool name configuration.

```
ip address-pool {dhcp | address-pool-name}
```

```
no ip address-pool {dhcp | address-pool-name}
```

Syntax Description

dhcp	Specifies when a profile is required to use DHCP-based address allocation.
<i>address-pool-name</i>	The name of the address pool used for a profile.

Command Default

Address pool is not configured.

Command Modes

IPSec submode

Command History

Release	Modification
WSG Release 1.1	This command was introduced.
WSG Release 2.2	The dhcp keyword was added.

Usage Guidelines

Use the **ip address-pool** command to set the address pool to be used for the profile.



Note

This command is not applicable for a site-to-site profile.

Use the **dhcp** keyword in the command when a profile is required to use DHCP-based address allocation. When the profile is activated, the mandatory global DHCP configuration is checked for completeness. If any profile is activated with DHCP address allocation, the global DHCP configuration commands cannot be modified or removed.

Examples

This example shows how to set the address pool for a profile named *foo*.

```
WSG# config
Enter configuration commands, one per line. End with CNTL/Z.
WSG (config)# crypto profile name
WSG (config-crypto-profile)# ipsec
WSG (config-crypto-profile-ipsec)# ip address-pool foo
```

This example activates the profile for DHCP-based address allocation:

```
crypto profile "prof-1"
  isakmp
  lifetime 7200
  self-identity id-type fqdn id SAMI.cisco.com
```

```
ipsec
  security-association lifetime 86400
  access-permit ip 172.60.0.0 subnet 16
  ip address-pool dhcp
activate
```

local-ip

To set up the local IP address to use during SA negotiation, use the **local-ip** command. To return to the default value, use the **no** form of the command.

local-ip *ip-address*

no local-ip *ip-address*

Syntax Description	<i>ip-address</i>	IP address of the local client. This can be an IPv4 or IPv6 address.
---------------------------	-------------------	--

Defaults	IP address not configured.
-----------------	----------------------------

Command Modes	IPSec submode
----------------------	---------------

Command History	Release	Modification
	WSG Release 1.0	This command was introduced as the ipsec local-ip command.
WSG Release 1.1	This command name was changed.	
WSG Release 3.0	IPv6 support was added.	

Usage Guidelines	Use the local-ip command to set up a local IP address that is used during SA negotiation.
-------------------------	--

Examples	This example shows how to define 10.95.10.110 as the IP address of the WSG to use during SA negotiation:
-----------------	--

```
WSG# config
Enter configuration commands, one per line. End with CNTL/Z.
WSG (config)# crypto profile name
WSG(config-crypto-profile)# ipsec
WSG(config-crypto-profile-ipsec)# local-ip 10.95.10.110
```

pfs

To set a Perfect Forward Secrecy (PFS) group ID to use for negotiations during a new SA exchange, use the **pfs** command. Use the **no** form of the command to remove the key.

```
pfs {group1 | group2 | group5 | group14 | group15 | group16 | group17 | group18}
```

```
no pfs {group1 | group2 | group5 | group14 | group15 | group16 | group17 | group18}
```

Syntax Description

group1	768-bit, lowest security, fastest processing time.
group2	1024-bit.
group5	1536-bit.
group14	2048-bit.
group15	3072-bit.
group16	4096-bit.
group17	6144-bit.
group18	8192-bit, highest security, slowest processing time.

Defaults

PFS is disabled.

Command Modes

IPSec submode

Command History

Release	Modification
WSG Release 1.1	This command was introduced.
WSG Release 3.0	Added group14, group15, group16, group17, and group18 keywords.

Usage Guidelines

Use the **pfs** command to set a group type for use in negotiations during a child SA exchange.

In WSG Release 3.0 support for multiple groups was added.

Examples

This example shows how to set **group2** as the group ID:

```
WSG# config
Enter configuration commands, one per line. End with CNTL/Z.
WSG (config)# crypto profile name
WSG(config-crypto-profile)# ipsec
WSG(config-crypto-profile-ipsec)# pfs group2
```


security-association lifetime

To set the SA timed lifetime, use the **security-association lifetime** command in IPsec submode. To remove the SA timed lifetime, use the **no** form of this command.

security-association lifetime { *megabytes megabytes* | *seconds seconds* }

no security-association lifetime { *megabytes megabytes* | *seconds seconds* }

Syntax Description	megabytes	seconds
	Specifies the lifetime in megabytes. The minimum value is 4500MB. The default value is 36000MB.	Specifies the lifetime in seconds. The range is 3600 to 2147483647. The default value is 25200 seconds.

Defaults The default values are 36000MB and 25200 seconds.

Command Modes IPsec submode

Command History	Release	Modification
	WSG Release 1.1	This command was introduced.
	WSG Release 3.0	This command was modified.

Usage Guidelines Use the **security-association lifetime** command to set the SA timed lifetime in megabytes or seconds. Depending on the application, the IPsec SA lifetime may also be configured on the peer. We recommend that you do not configure peer IPsec SA lifetimes that are shorter than the minimum values supported by the WSG.

Examples This example shows how to set the IPsec SA lifetime in seconds or megabytes:

```
WSG# config
Enter configuration commands, one per line. End with CNTL/Z.
WSG (config)# crypto profile name
WSG (config-crypto-profile)# ipsec
WSG (config-crypto-profile-ipsec)# security-association lifetime seconds ?
<1-2147483647> Enter lifetime in seconds (default:25200s)
WSG (config-crypto-profile-ipsec)# security-association lifetime seconds 10800
or
WSG (config-crypto-profile-ipsec)# security-association lifetime megabytes ?
<4500-2097151> Enter lifetime in MB (default:36000MB, min 4500MB)
WSG (config-crypto-profile-ipsec)# security-association lifetime megabytes 20000
```

security-association replay

To disable IPSec security association replay, use the **security-association replay** command. To enable IPSec security association replay, use the **no** form of the command.

security-association replay disable

no security-association replay disable

Defaults

Security association replay is enabled with window size 32 bits.

Command Modes

IPSec submode

Command History

Release	Modification
WSG Release 1.1	This command was introduced.

Usage Guidelines

Use the **security-association replay** command to disable IPSec security association replay.

Examples

This example shows how to disable IPSec security association replay:

```
WSG# config
Enter configuration commands, one per line. End with CNTL/Z.
WSG (config)# crypto profile name
WSG(config-crypto-profile)# ipsec
WSG(config-crypto-profile-ipsec)# security-association replay disable
```

access-permit

To configure the protected IP address to which traffic is allowed from a remote access tunnel, or traffic selectors and multiple child SA features for site-to-site tunnels, use the **access-permit** command. Use the **no** form of the command to remove the access-permit configuration.

remote-access:

```
access-permit ip ip-address subnet subnet
```

```
no access-permit ip ip-address subnet subnet
```

site-to-site:

```
access-permit rule-name protocol {any | sctp | udp | tcp}
[src-ip src_ip src_prefix | src-port start_src_port end_src_port |
dst-ip dst_ip dst_prefix | dst-port start_dst_port end_dst_port]
```

```
no access-permit rule-name
```

Syntax Description

<i>ip-address</i>	Applies only to remote-access profile type. IP address to which traffic is allowed from the tunnel. IPv4 or IPv6 format: A.B.C.D or X:X:X::X.
<i>subnet</i>	Applies only to remote-access profile type. Mask for the associated IP subnet in number of bits from 1 to 32. For IPv6 the range can be 1 to 128.
<i>rule-name</i>	Applies only to site-to-site. Configures the rule name. Note IKEv1 requires port and full port range.
protocol	Applies only to site-to-site. Configures the type of IP protocol.
any	Applies only to site-to-site. Any protocol. The protocol must be any when using IKEv1.
sctp	Applies only to site-to-site. SCTP protocol.
udp	Applies only to site-to-site. UDP protocol.
tcp	Applies only to site-to-site. TCP protocol.
<i>src_ip src_prefix</i>	Applies only to site-to-site. The source IP address and its prefix that defines the range of permitted source IP addresses. This command is modified to take a prefix and accepts both A.B.C.D and X:X:X::X formats.
<i>start_src_port end_src_port</i>	Applies only to site-to-site. The start and end source port numbers. The range is 0 to 65535.
<i>dst_ip dst_prefix</i>	Applies only to site-to-site. The destination IP address and its prefix that defines the range of permitted destination IP addresses. This command is modified to take a prefix and accepts both A.B.C.D and X:X:X::X formats.
<i>start_dst_port end_dst_port</i>	Applies only to site-to-site. The start and end destination port numbers. The range is 0 to 65535.

Defaults

A specific access-permit must be specified based on the network configuration.

Command Modes IPsec submode

Command History	Release	Modification
	WSG Release 1.0	This command was introduced.
	WSG Release 1.1	No changes were made to this command.
	WSG Release 1.2	The following keywords and arguments were introduced. <ul style="list-style-type: none"> • <code>rule-name</code> • protocol <i>protocol</i> • src-ip <i>start src ip end src ip</i> • src-port <i>start src port end src port</i> • dst-ip <i>start dst ip end dst ip</i> • dst-port <i>start dst port end dst port</i>
	WSG Release 2.0	The following keywords and arguments were changed for site-to-site scalability improvements: <ul style="list-style-type: none"> • src-ip <i>src ip/subnet mask</i> • dst-ip <i>dst ip/subnet mask</i>
	WSG Release 3.0	Added support for IPv6.
	WSG Release 3.1	Allow up to 5 multiple access-permit statements in a remote-access crypto profile.

Usage Guidelines Use the **access-permit** command to set the IP address and subnet from which traffic is allowed from the remote-access tunnel.

In WSG Release 4.2 and above when a customer is configuring a site to site access permit, a check has been added to determine, if the user has configured overlapping traffic selectors. If misconfigured a warning will be triggered to the user and will be logged into the syslog.

In WSG Release 3.1 and above, you can configure multiple access-permit statements in a remote-access crypto profile. Up to 5 access-permit statements can be added.

For site-to-site tunnels, the extended access-permit configuration defines the parameters of the traffic permitted on the tunnel.

There is no default, and at least one access-permit needs to be specified for each profile. If multiple child SAs are required, multiple access-permit configurations need to be entered.

In WSG Release 1.2, the *rule-name* argument is added, and applies to site-to-site type profiles only. The WSG Release 1.1 syntax for access-permit only applies to the remote-access type profile. The *profile name* should be unique; you cannot use the same name for two different profiles.

Examples This example shows how to allow traffic from all remote-access clients to the 100.1.3.0/24 and 88.88.0.0/16 subnets:

```
WSG# config
Enter configuration commands, one per line. End with CNTL/Z.
WSG (config)# crypto profile name
WSG(config-crypto-profile)# ipsec
```

```
WSG(config-crypto-profile-ipsec)# access-permit ip 100.1.3.0 subnet 24  
WSG(config-crypto-profile-ipsec)# access-permit ip 88.88.0.0 subnet 16
```

The following is an example of the extended **access-permit** command with the protocol options and IPv6 addresses:

```
WSG# config  
Enter configuration commands, one per line. End with CNTL/Z.  
WSG (config)# crypto profile name  
WSG(config-crypto-profile)# ipsec  
WSG(config-crypto-profile-ipsec)#  
access-permit A  
protocol udp src-ip 12.12.0.0 255.255.0.0 src-port 23 23 dst-ip 10.10.10.0  
255.255.255.0 dst-port 0 65535  
WSG(config-crypto-profile-ipsec)#  
access-permit B  
protocol any src-ip 2001:0DB8:1:1::0 96 src-port 23 23 dst-ip 2001:0DB8:1:2::0 96  
dst-port 0 65535
```

The following is an example that includes the **ras** type access permit:

```
WSG(config)# crypto profile ras  
WSG(config-crypto-profile)# ipsec  
WSG(config-crypto-profile-ipsec)# access-permit ip 2001:F8D0:1::0 subnet ?  
<0-128> Enter subnet mask  
WSG(config-crypto-profile-ipsec)# access-permit ip 2001:F8D0:1::0 subnet 64
```

transform-set

To set an Encapsulating Security Payload (ESP) encryption and hash type, use the **transform-set** command in IPsec submode.

```
transform-set esp {3des | aes | aes192 | aes256 | des | null} {aes-xcbc | md5 | sha1}
```

Syntax Description	3des aes aes192 aes256 des null	See encryption, page 3-115
	aes-xcbc md5 sha1	See hash, page 3-117
	Note SHA2 is not supported as a phase-2 hash algorithm.	

Defaults	esp aes sha1
-----------------	--------------

Command Modes	IPsec submode
----------------------	---------------

Command History	Release	Modification
		WSG Release 1.1
	WSG Release 3.0	Added support for multiple transform sets.

Usage Guidelines	ESP is a security protocol that gives data privacy services, data authentication, and anti-replay services. ESP encapsulates data to be protected. Use the transform-set command to set ESP encryption and hash type. In WSG Release 2.2 and above, multiple transform sets can be configured together.
-------------------------	--

Examples	This example shows how to set ESP encryption and hash type:
-----------------	---

```
WSG# config
Enter configuration commands, one per line. End with CNTL/Z.
WSG (config)# crypto profile name
WSG(config-crypto-profile)# ipsec
WSG(config-crypto-profile-ipsec)# transform-set esp aes256 aes-xcbc
```

oam mode single

To identify the interface used for single mode OAM traffic, use the **oam mode single** command. Use the **no** form of the command to disable this feature.

oam mode single *vlan_number*

no oam mode single *vlan_number*

Syntax Description	<i>vlan_number</i>	Specifies the VLAN number.
--------------------	--------------------	----------------------------

Defaults	None.
----------	-------

Command Modes	Global configuration
---------------	----------------------

Command History	Release	Modification
	WSG Release 1.2	This command was introduced.

Usage Guidelines	IPv6 is not supported under single mode OAM.
------------------	--

Examples	This example shows a sample configure with the oam mode single command. All management traffic from the director and subordinate PPCs destined to the VLAN 223 subnet will now be directed through this interface:
----------	---

```
interface vlan 223
  ip address 222.222.223.123 255.255.255.0
oam mode single 223
oam-ip route 44.44.44.0 255.255.255.0 222.222.223.100
```

oam-ip route

To configure the static routes on the director and subordinate PPCs for subnet management, use the **oam-ip route** command. Use the **no** form of the command to disable these routes.

```
oam-ip route ip_address subnet_mask gateway
```

```
no oam-ip route ip_address subnet_mask gateway
```

Syntax Description		
	<i>ip_address</i>	Specifies the IP address of the route you are adding.
	<i>subnet_mask</i>	Specifies the subnet mask of the route.
	<i>gateway</i>	Specifies the gateway of the route.

Defaults None.

Command Modes Global configuration

Command History	Release	Modification
	WSG Release 1.2	This command was introduced.

Usage Guidelines This command is similar to **ip route** in functionality, with the exception that it affects the routes on the subordinate PPCs as well. It does not support IPv6.

Examples This example shows how to configure the **oam-ip route** command:

```
interface vlan 223
  ip address 222.222.223.123 255.255.255.0
oam mode single 223
  oam-ip route 44.44.44.0 255.255.255.0 222.222.223.100
```

```
WSG(mode-all)# sh ip route
127.0.0.0/24 dev eth0 src 127.0.0.23
44.44.44.0/24 via 222.222.223.100 dev eth0.223
222.222.223.0/24 dev eth0.223 src 222.222.223.123
```

```
CPU 4
127.0.0.0/24 dev eth0 src 127.0.0.24
44.44.44.0/24 via 127.0.0.23 dev eth0
222.222.223.0/24 via 127.0.0.23 dev eth0
```


process cpu threshold

To enable the CPU Threshold Notification feature and establish the rising and falling percentage threshold values, use the **process cpu threshold** Global configuration command. Use the no form to disable this feature.

process cpu threshold rising *percentage interval seconds* [**falling** *percentage interval seconds*]

no process cpu threshold [**rising** *percentage interval seconds* | **falling** *percentage interval seconds*]

Syntax Description

rising <i>percentage interval seconds</i>	Establishes the rising percentage threshold values. Threshold values: minimum 1% to maximum 100%. Threshold interval: 5 – 86400 seconds.
falling <i>percentage interval seconds</i>	Establishes the falling percentage threshold values. Threshold values: minimum 1% to maximum 100%. Threshold interval: 5 – 86400 seconds.
	falling threshold should always be less than, or equal to the configured rising threshold value. This parameter is optional.

Defaults

None.

Command Modes

Global configuration

Command History

Release	Modification
WSG Release 1.2	This command was introduced.

Usage Guidelines

The CPU Threshold Notification feature notifies users by generating a SNMP trap message when a predefined threshold of CPU usage is crossed. Two types of CPU utilization threshold are supported: rising threshold and falling threshold. A rising CPU utilization threshold specifies the percentage of CPU resources that, when exceeded for a configured period of time, triggers the cpmCPURisingThreshold notification. Similarly, a falling CPU utilization threshold specifies the percentage of CPU resources that, when CPU usage falls below this level for a configured period of time, triggers cpmCPUFallingThreshold notification.

Examples

The following example shows how to set a rising CPU threshold notification for total CPU utilization. When total CPU utilization exceeds 95 percent for a period of 5 seconds or longer, a rising threshold notification is sent.

```
ppc3(config)# process cpu threshold rising 95 interval 5
```

memory free low watermark processor

To configure the memory threshold that generates a syslog when free memory falls below the configured value, use the **memory free low watermark processor** command. Use the no form to disable this function.

memory free low watermark processor *threshold*

no memory free low watermark processor *threshold*

Syntax Description	<i>threshold</i>	Specifies the memory threshold. When free memory falls below the configured value a syslog is generated. The free memory threshold value can range from 1024KB to 1996000KB.
---------------------------	------------------	--

Defaults	There are no default values.
-----------------	------------------------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	WSG Release 1.2	This command was introduced.

Examples	The following example specifies a threshold of 10000 KB of free processor memory before a low-memory syslog is generated:
-----------------	---

```
ppc3(config)# memory free low-watermark processor 10000
```

Once the available free memory rises to above 5 percent of the threshold (1.05 x 10000 in the above example), another message is generated that indicates that the free memory has recovered.

show crypto blacklist file

To list all of the current blacklisted IKE IDs, use the **show crypto blacklist file** command in EXEC mode.

show crypto blacklist file

Syntax Description There are no keywords or arguments for this command.

Defaults None.

Command Modes EXEC

Command History	Release	Modification
	WSG Release 3.0	This command was introduced.

Usage Guidelines Use the **show crypto blacklist file** command to view the current blacklisted IDs.

Examples Here is example show output for the **show crypto blacklist file** command:

```
WSG# show crypto blacklist file
```

```
Blacklisted Entries:  
fqdn      "LS1-995.cisco.com"  
email     "peer1@example.com"
```

show crypto blacklist stats

To display the number of IDs in a blacklist, and the number of tunnel setup attempts blocked due to blacklisting, use the **show crypto blacklist stats** command in EXEC mode.

show crypto blacklist stats

Syntax Description There are no keywords or arguments for this command.

Defaults None.

Command Modes EXEC

Command History	Release	Modification
	WSG Release 3.0	This command was introduced.

Usage Guidelines Use the **show crypto blacklist stats** command to display the number of IDs in a blacklist, and the number of tunnel setup attempts blocked due to blacklisting.

Examples Here is example show output for the **show crypto blacklist stats** command:

```
wsg# show crypto blacklist stats

Blacklist Statistics
Number of blacklisted entries : 500
IKEv2 [R] initial exchanges      : Allowed = 53, Blocked = 101
IKEv2 [R] create child exchanges  : Allowed = 0, Blocked = 0
IKEv2 [R] IPsec SA rekeys        : Allowed = 98, Blocked = 0
IKEv2 [R] IKE SA rekeys          : Allowed = 49, Blocked = 0
IKEv2 [I] IPsec SA rekeys        : Allowed = 0, Blocked = 0
IKEv2 [I] IKE SA rekeys          : Allowed = 0, Blocked = 0
IKEv1 [R] main mode exchanges     : Allowed = 0, Blocked = 0
IKEv1 [R] aggressive mode exchanges : Allowed = 0, Blocked = 0
IKEv1 [R] quick mode exchanges   : Allowed = 0, Blocked = 0
IKEv1 [I] IPsec SA rekeys        : Allowed = 0, Blocked = 0
IKEv1 [I] DPD SA creations       : Allowed = 0, Blocked = 0
```

show crypto cmp request

To display the current status of pending CMPv2 request, use the **show crypto cmp request** command in EXEC mode. The output also indicates if no request is pending.

show crypto cmp request

Syntax Description There are no keywords or arguments for this command.

Defaults None.

Command Modes EXEC

Command History	Release	Modification
	WSG Release 2.0	This command was introduced.

Usage Guidelines Use the **show crypto cmp request** command to display the current status of pending CMPv2 request. This is the pending request that will be polled by the **crypto cmp poll** command. If an update and an initialize or enroll request is pending, only the pending update request is displayed.

Examples Here is example output for the **show crypto cmp request** command:

```
7606-4-S3P3# show crypto cmp request
CMP enroll request pending with transaction id : 1371987489
```

show crypto dhcp

To display DHCP address allocation statistics, use the **show crypto dhcp** command in EXEC mode.

show crypto dhcp

Syntax Description There are no keywords or arguments for this command.

Defaults None.

Command Modes EXEC

Command History	Release	Modification
	WSG Release 2.2	This command was introduced.

Usage Guidelines Use the **show crypto dhcp** command to view DHCP address allocation statistics.

Examples Here is an example of crypto DHCP statistics after tunnel set-up and tear-down:

```
WSG# show crypto dhcp
DHCP Detailed Statistics
Total packets transmitted : 1
Total packets received : 1
Total packets dropped : 0
Total discover messages sent : 0
Total offer messages received : 0
Total request messages sent : 0
Total ack messages received : 0
Total nak messages received : 0
Total decline messages sent : 0
Total release messages sent : 0
Total DHCPv6 relay forward messages sent : 1
Total DHCPv6 relay reply messages received : 1
Total DHCPv6 solicit messages sent : 1
Total DHCPv6 reply messages received : 1
Total DHCPv6 decline messages sent : 0
Total DHCPv6 renew messages sent : 0
Total DHCPv6 release messages sent : 0
```

show crypto ipsec info

To display IPsec parameters for all configured profiles, use the **show crypto ipsec info** command in EXEC mode.

```
show crypto ipsec info [profile_name]
```

Syntax Description	profile_name	Displays IPsec parameters for the specified profile.
Defaults	None.	
Command Modes	EXEC	
Command History	Release	Modification
	WSG Release 1.1	This command was introduced.

Usage Guidelines Use the **show crypto ipsec info** command to view IPsec parameters configured for all the profiles.

Examples This example shows how to view configured IPsec parameters:

```
WSG# show crypto ipsec info ?
  <WORD> Specify the Profile for which IPSEC info is req (Max Size - 50)
  <cr>   Carriage return.
WSG# show crypto ipsec info
Displayed Information for Profile: site-to-site
Transform:                esp-aes128-shal
Pfs Group:                Disabled
Sa lifetime:              25200 seconds
Sa anti-replay:          enable, Window 32

Displayed Information for Profile: remote-access
Transform:                esp-aes128-shal
Pfs Group:                Disabled
Sa lifetime:              25200 seconds
Sa anti-replay:          enable, Window 32

WSG# show crypto ipsec info remote-access

Displayed Information for Profile: remote-access
Transform:                esp-aes128-shal
Pfs Group:                Disabled
Sa lifetime:              25200 seconds
Sa anti-replay:          enable, Window 32
```

show crypto ipsec summary

To display all global IPsec statistics, use the **show crypto ipsec summary** command in EXEC mode.

```
show crypto ipsec summary {fast-path | slow-path}
```

Syntax Description	fast-path	For global fast path statistics. Applicable to the entire card.
	slow-path	For global slow path statistics.

Defaults None.

Command Modes EXEC

Command History	Release	Modification
	WSG Release 1.1	This command was introduced.

Usage Guidelines Use the **show crypto ipsec summary** command to view all global IPsec statistics.

[Table 3-1](#) lists the Field description for IPsec fast-path Stats:

Table 3-1 Field Descriptions for IPsec fast-path Stats

Counters	Field Descriptions
Fast Path	
Total SAS	
Decrypted	Current active decrypt SAs in Crypto chip = Number of decrypt SA creation - Number of decrypt SA deletions.
Encrypted	Current active encrypt SAs in Crypto chip = Number of encrypt SA creation - Number of encrypt SA deletions
Decrypted Create	Number of decrypt SA creations in Crypto chip.
Encrypted Create	Number of encrypt SA creations in Crypto chip.
Decrypted Delete	Number of decrypt SA deletions in Crypto chip.
Encrypted Delete	Number of encrypt SA deletions in Crypto chip.
Total packets	
Decrypted	The total number of packets decrypted by Crypto chip for all current and previous IPsec Phase-2 Tunnels.
Encrypted	The total number of packets encrypted by Crypto chip for all current and previous IPsec Phase-2 Tunnels.
Packets dropped	

Counters	Field Descriptions
Decrypted	The total number of packets dropped during receive processing by all current and previous IPsec Phase-2 Tunnels. This count does NOT include packets dropped due to Anti-Replay processing.
Encrypted	The total number of packets dropped during send processing by all current and previous IPsec Phase-2 Tunnels.
Authorizations	
Decrypted	The total number of inbound authentications performed by all current and previous IPsec Phase-2 Tunnels.
Encrypted	The total number of outbound authentications performed by all current and previous IPsec Phase-2 Tunnels.
Total Bytes	
Decrypted	The total number of bytes decrypted by the Crypto chip for all current and previous IPsec Phase-2 Tunnels.
Encrypted	The total number of bytes encrypted by the Crypto chip for all current and previous IPsec Phase-2 Tunnels.
Total Errors	
Decrypted	Total decrypt errors reported by the Crypto chip for all current and previous IPsec Phase-2 Tunnels.
Encrypted	Total encrypt errors reported by the Crypto chip for all current and previous IPsec Phase-2 Tunnels.
Wrong SAs	
Decrypted	Missing or invalid SA for a packet to be decrypted (When SA bit is invalid or SPI/Dest checks fails).
Encrypted	Missing SA for a packet to be encrypted (When SA bit is invalid or SPI/Dest checks fails)
Policy Bad SAs	
Decrypted	Total number of times the operation request to the Crypto chip was decrypted but the SA was for encrypted.
Encrypted	Total number of times the operation request to the Crypto chip was encrypted but the SA was for decrypted.
Replay Failures	The total number of packets dropped during receive processing due to Anti-Replay processing by all current and previous IPsec Phase-2 Tunnels.
Authentication Failures	
Decrypted	The total number of decrypt packet authentications which ended in failure by all current and previous IPsec Phase-2 Tunnels.
Encrypted	The total number of encrypt packet authentications which ended in failure by all current and previous IPsec Phase-2 Tunnels.
IP Fragmentation Failures	Number of times the fragmentation is required but DF (Don't Fragment) bit is set.
Decrypt Failures	Number of times ESP nextHeader or ESP pad bytes mismatch with expected value.
IP Version Failures	
Decrypted	The total number of packets with mismatched IP version (inner or outer) during decryption for all current and previous IPsec Phase-2 tunnels.

Counters	Field Descriptions
Encrypted	The total number of packets with mismatched IP version (inner or outer) during encryption for all current and previous IPsec Phase-2 tunnels.
Total Decaps NATT	
Decrypted	Total decrypted NAT-T packet decapsulations.
Encrypted	Total encrypted NAT-T packet encapsulations.
Total Decaps NATT Errors	Total decrypted NAT-T packet decapsulation errors (Packets has UDP encapsulation and SA does not expect this).
Sequence Number Overflows	Number of times that Encrypt Sequence Number Overflows.
SA Creation Requests	
No Memory	
Decrypted	Number of failed memory allocations while programming the Crypto chip to create a decrypt SA.
Encrypted	Number of failed memory allocations while programming the Crypto chip to create an encrypt SA.
Communication Error	
Decrypted	Number of write/read failures while programming the Crypto chip to create/delete a decrypt SA.
Encrypted	Number of write/read failures while programming the Crypto chip to create/delete a encrypt SA.
SA Read Requests	
Total Requests	Number of successful SA stats reads from the Crypto chip.
Total Failures	Number of failed reads from the Crypto chip while programming the Crypto chip or retrieving SA stats.
Invalid SA	Number of invalid SA requests while retrieving SA stats from the Crypto chip or when updating SA sequence number from IKE stack.
Request Errors	
Invalid PPC message	Number of invalid PPC messages while updating SA sequence number from IKE stack.
Sequence Num write fail	Number of failures to write SA to the Crypto chip while updating SA with sequence number from IKE stack.
No Memory for SA Chain	Number of failed memory allocations while updating SA with sequence number from IKE stack.
Total Global Read Requests	Number of successful global stats reads from the Crypto chip.

Examples

This example shows how to view all global IPsec statistics:

```
ppc1# show crypto ipsec summary fast-path
```

```
SeGW Global Statistics
```

```
Started at: Wed Sep 14 2011 18:15:54
```

```
Uptime: 03:13:05
```

```
Fast Path
```

```

Total SAS
  Decrypted          : 16668
  Encrypted          : 16668
  Decrypted Create   : 37199
  Encrypted Create   : 20531
  Decrypted Delete   : 37199
  Encrypted Delete   : 20531
Total packets
  Decrypted          : 2098436
  Encrypted          : 2096338
Packets dropped
  Decrypted          : 0
  Encrypted          : 0
Authorizations
  Decrypted          : 2098436
  Encrypted          : 2096338
Total Bytes
  Decrypted          : 1011446152
  Encrypted          : 1010434916
Total Errors
  Decrypted          : 0
  Encrypted          : 0
Wrong SAs
  Decrypted          : 0
  Encrypted          : 0
Policy Bad SAs
  Decrypted          : 0
  Encrypted          : 0
Replay Failures    : 0
Authentication Failures
  Decrypted          : 0
  Encrypted          : 0
IP Fragmentation Failures : 0
Result Failures     : 0
IP Version Failures
  Decrypted          : 0
  Encrypted          : 0
Total Decaps NATT
  Decrypted          : 0
  Encrypted          : 0
Total Decaps NATT Errors : 0
Sequence Number Overflows : 0
SA Creation Requests
  No Memory
    Decrypted          : 0
    Encrypted          : 0
  Communication Error
    Decrypted          : 0
    Encrypted          : 0
SA Read Requests
  Total Requests     : 46326
  Total Failures     : 0
  Invalid SA         : 0
Request Errors
  Invalid PPC message : 0
  Sequence Num write fail : 0
  No Memory for SA Chain : 0
Total Global Read Requests : 11

```

```
ppc1# show crypto ipsec summary slow-path
```

```
SeGW Global Statistics
```

```
Started at: Wed Jan 27 2010 13:52:13
```

show crypto ipsec summary

```

Uptime:      00:09:40

Slow Path
Packets
  In          : 12
  Out         : 0
  Forwarded   : 0
Bytes
  In          : 720
  Out         : 0
  Forwarded   : 0
Crypto Transforms
  Active      : 0
  Free        : 1000
  Total       : 0
  ARP         : 12
  Other       : 0
ESP
  In          : 0
  Out         : 0
Dropped Packets
  Corrupt     : 0
  IP Option   : 0
  Resource    : 0
  No Route    : 0
  Rule Drop   : 0
  Rule Reject : 0
  ESP MAC     : 0
  AH MC       : 0
  Replay      : 0
  Internal    : 0
  Reassembly  : 0
  HW Accel    : 0
  No Rule Lookup : 0
  No Rule     : 0
  Out of Transforms : 0
  Protocol Monitor Drops : 0
  Dropped Packets : 0
Resource Drops
  Out of Packet Contexts : 0
  Out of Transform Contexts : 0

```

show crypto ipsec sa

To show a list of all SAs on the WSG, use the **show crypto ipsec sa** command in EXEC mode.

```
show crypto ipsec sa [remote-ip remote_ipv4_address mask remote_ipv4_mask]
[remote-ip remote_ipv6_address ipv6-prefix ipv6_prefix_length] [remote-host remote_host]
[vrf-local vrf_name]
```

Syntax Description		
remote_ipv4_address	Remote IPv4 address to be used with the mask to filter the set of IPsec SAs displayed.	
remote_ipv4_mask	Mask to be used with the IPv4 address to filter the set of IPsec SAs displayed.	
remote_ipv6_address	Remote IPv6 address to be used with the prefix length to filter the set of IPsec SAs displayed.	
ipv6_prefix_length	Prefix length to be used with the IPv6 address to filter the set of IPsec SAs displayed.	
remote_host	Remote hostname.	
vrf_name	Filters the set of IPsec SAs to display within a specific VRF.	

Defaults None.

Command Modes EXEC

Command History	Release	Modification
	WSG Release 1.1	This command was introduced.
	WSG Release 3.0	Command modified to display any IPv6 addresses.
	WSG Release 4.0	Added hostname in reverse DNS lookup feature for IKE peer support.

Usage Guidelines Use the **show crypto ipsec sa** command to view all SAs on the WSG.

Examples This example shows how to view all SAs on the WSG:

```
WSG# show crypto ipsec sa ?
  remote-hostname  Show detailed stats for the remote SA with the hostname
  remote-ip        Show crypto ipsec sa detailed stats
  spi-in           Show crypto ipsec sa detailed stats with specified Inbound SPI
  |               Output modifiers.
  >               Output Redirection.
  <cr>            Carriage return.
```

show crypto ipsec sa

```
WSG# show crypto ipsec sa remote-hostname ?
<WORD> Enter hostname
```

```
WSG# show crypto ipsec sa remote-ip ?
<A.B.C.D>|<X:X:X::X> Enter IP address
```

```
WSG# show crypto ipsec sa remote-ip 184.0.155.74 ?
  ipv6-prefix Show crypto ipsec sa stats with in remote IPV6 prefix
  mask        Show crypto ipsec sa stats with in remote ip mask
  vrf-local   Show crypto ipsec sa detailed stats for an ip in a vrf
  |           Output modifiers.
  >           Output Redirection.
  <cr>        Carriage return.
```

```
WSG# show crypto ipsec sa remote-ip 184.0.155.74 SA Statistics
```

```
Packets
  Decrypted           : 843
  Encrypted           : 843
  Dropped Decrypted   : 0
  Dropped Encrypted   : 0
Bytes
  Decrypted           : 866604
  Encrypted           : 866604
Authentications
  Decrypted           : 843
  Encrypted           : 843
Authentications Failures
  Decrypted           : 0
  Encrypted           : 0
IXP Packet Stats
  Inbound             : 843
  Outbound            : 843
Failures
  Decryption          : 0
  Encryption          : 0
Anti-replay Drops Decrypted : 0
Up Time (seconds)    : 1687
Hardware SA Indices
  Nitrox Inbound Index : 0x16805551
  Nitrox Outbound Index : 0x1e03fed1
  IXP Table Index      : 0x5552
Path MTU              : 1400
SA Sequence Numbers
  Outbound Sequence Number : 34b
  Inbound Sequence Number  : 34b
ESP SPI
  SPI In              : 1669a16c
  SPI Out              : 000493e1
Rule Statistics
  Tunnel Type         : RAS
  Type                : Apply
  Precedence          : 411
  IP Protocol         : any
  Vrf Name            : global
  Source IP Low       : 172.60.0.0
  Source IP High      : 172.60.255.255
  Source Port Low     : 0
  Source Port High    : 65535
  Destination IP Low  : 10.133.0.1
  Destination IP High : 10.133.0.1
  Destination Port Low : 0
  Destination Port High : 65535
  Times Used          : 0
Last Packet Flow Statistics
```

```

Source IP Address      : 184.0.155.74
Source Hostname        :
Source Port Id        : 4500
Destination IP Address : 88.88.63.3
Destination Port Id    : 4500

```

WSG# **show crypto ipsec sa**

SA Id	ESP		Cipher	Algorithms		Compress
	SPI In	SPI Out		MAC		
1	44dc28be	00000001	aes-cbc/128	hmac-sha1-96/160		none
	Local IP Address	: 88.88.128.93				
	Remote IP Address/Host Name	: BXL123				
2	17d3d29d	00000006	aes-cbc/128	hmac-sha1-96/160		none
	Local IP Address	: 88.88.128.93				
	Remote IP Address/Host Name	: BXL123				
3	0ddcc17	0000000b	aes-cbc/128	hmac-sha1-96/160		none
	Local IP Address	: 88.88.128.93				
	Remote IP Address/Host Name	: BXL123				

This example shows how to view information on a specific SA:

```

WSG# show crypto ipsec sa remote-ip 50.0.0.1 ?
mask          Show crypto ipsec sa stats with in remote ip mask
vrf-local     Show crypto ipsec sa detailed stats for an ip in a vrf
|            Output modifiers.
>            Output Redirection.
<cr>        Carriage return.

```

```

WSG# show crypto ipsec sa remote-ip 50.0.0.1 vrf-local ?
<WORD> Enter the VRF Name as a string (Max Size - 63)

```

WSG# **show crypto ipsec sa remote-ip 50.0.0.1 vrf-local outsideB**

```

SA Statistics
Packets
  Decrypted      : 524625
  Encrypted      : 524012
  Dropped Decrypted : 0
  Dropped Encrypted : 0
Bytes
  Decrypted      : 252869250
  Encrypted      : 252573784
Authentications
  Decrypted      : 524625
  Encrypted      : 524012
Authentications Failures
  Decrypted      : 0
  Encrypted      : 0
IXP Packet Stats
  Inbound        : 524625
  Outbound       : 524012
Failures
  Decryption     : 0
  Encryption     : 0
Anti-replay Drops Decrypted : 0
Up Time (seconds) : 884
Hardware SA Indices
  Nitrox Inbound Index : 0x16805551
  Nitrox Outbound Index : 0x1e03fed1
  IXP Table Index      : 0x5552
Path MTU            : 1400
SA Sequence Numbers
  Outbound Sequence Number : 7feec
  Inbound Sequence Number  : 80151

```

■ show crypto ipsec sa

```
ESP SPI
  SPI In           : d9c35ce5
  SPI Out          : 8ae02c8b
Rule Statistics
  Tunnel Type      : S2S
  Type             : Apply
  Precedence       : 411
  IP Protocol      : any
  Vrf Name         : insideB
Negotiated Traffic Selectors
  Source IP Low    : 60.0.0.0
  Source IP High   : 60.0.0.255
  Source Port Low  : 0
  Source Port High : 65535
  Destination IP Low  : 44.44.33.1
  Destination IP High : 44.44.33.1
  Destination Port Low  : 0
  Destination Port High : 65535
  Source IP Low    : 60.1.0.0
  Source IP High   : 60.1.0.255
  Source Port Low  : 0
  Source Port High : 65535
  Destination IP Low  : 44.44.33.1
  Destination IP High : 44.44.33.1
  Destination Port Low  : 0
  Destination Port High : 65535
  Times Used       : 0
Last Packet Flow Statistics
  Source IP Address : 50.0.0.1
  Source Port Id    : 0
  Destination IP Address : 33.33.33.30
  Destination Port Id : 0
```


show crypto ipsec sa spi-in

To show information on a specific SA on the WSG, use the **show crypto ipsec sa spi-in** command in EXEC mode.

```
show crypto ipsec sa spi-in inbound_spi
```

Syntax Description	<i>inbound_spi</i>	Identifies the inbound SPI.
Command Default	None.	
Command Modes	EXEC	
Command History	Release	Modification
	WSG Release 1.1	This command was introduced.

Usage Guidelines Use the **show crypto ipsec sa spi-in** command to view information on a specific SA.

Examples This example shows how to view information on a specific SA:

```
ppc1# show crypto ipsec sa spi-in d9c35ce5
SA Statistics
  Packets
    Decrypted          : 524625
    Encrypted          : 524012
    Dropped Decrypted  : 0
    Dropped Encrypted  : 0
  Bytes
    Decrypted          : 252869250
    Encrypted          : 252573784
  Authentications
    Decrypted          : 524625
    Encrypted          : 524012
  Authentications Failures
    Decrypted          : 0
    Encrypted          : 0
  IXP Packet Stats
    Inbound            : 524625
    Outbound           : 524012
  Failures
    Decryption         : 0
    Encryption         : 0
  Anti-replay Drops Decrypted : 0
  Up Time (seconds)   : 884
  Hardware SA Indices
    Nitrox Inbound Index : 0x16805551
    Nitrox Outbound Index : 0x1e03fed1
    IXP Table Index      : 0x5552
```

■ show crypto ipsec sa spi-in

```
Path MTU : 1400
SA Sequence Numbers
  Outbound Sequence Number : 7feec
  Inbound Sequence Number : 80151
ESP SPI
  SPI In : d9c35ce5
  SPI Out : 8ae02c8b
Rule Statistics
  Tunnel Type : S2S
  Type : Apply
  Precedence : 411
  IP Protocol : any
  Vrf Name : insideB
  Source IP Low : 60.0.0.0
  Source IP High : 60.0.0.255
  Source Port Low : 0
  Source Port High : 65535
  Destination IP Low : 40.0.0.0
  Destination IP High : 40.0.0.255
  Destination Port Low : 0
  Destination Port High : 65535
  Times Used : 0
Last Packet Flow Statistics
  Source IP Address : 50.0.0.1
  Source Port Id : 0
  Destination IP Address : 33.33.33.30
  Destination Port Id : 0
```

show crypto isakmp info

To show IKE parameters, use the **show crypto isakmp info** command in EXEC mode.

show crypto isakmp info

Syntax Description This command has no keywords or arguments.

Defaults None.

Command Modes EXEC

Command History	Release	Modification
	WSG Release 1.1	This command was introduced.

Usage Guidelines Use the **show crypto isakmp info** command to view configured IKE parameters.

Examples This example shows how to view configured IKE parameters:

```
ppc1# show crypto isakmp info
```

```
Displayed Information for Profile: remote-access
```

```
Ike-version:                2
Encryption Algorithm:      AES
Hash Algorithm:            SHA1
Authentication Method:    rsa-sig
Diffie-Hellman group:     #2 (1024 bits)
Lifetime:                  28800 seconds
Sequence Number:          Short(32-bit)
Ike-retry-count:          1
Ike-retry-timeout:        Initial:5000 msec      Max:10000 msec
NAT Keepalive:            Disabled
DPD Timeout:              0 seconds (DPD turn-off)
EAP Type:                  none
```

```
Displayed Information for Profile: site-to-site
```

```
Ike-version:                2
Encryption Algorithm:      AES
Hash Algorithm:            SHA1
Authentication Method:    rsa-sig
Diffie-Hellman group:     #2 (1024 bits)
Lifetime:                  28800 seconds
Sequence Number:          Short(32-bit)
Ike-retry-count:          1
Ike-retry-timeout:        Initial:5000 msec      Max:10000 msec
NAT Keepalive:            Disabled
DPD Timeout:              2000 seconds
```

■ show crypto isakmp info

```
EAP Type:                none
```

```
ppc1# show crypto isakmp info remote-access
```

```
Displayed Information for Profile: remote-access
```

```
Ike-version:             2
Encryption Algorithm:    AES
Hash Algorithm:          SHA1
Authentication Method:   rsa-sig
Diffie-Hellman group:    #2 (1024 bits)
Lifetime:                28800 seconds
Sequence Number:         Short(32-bit)
Ike-retry-count:         1
Ike-retry-timeout:       Initial:5000 msec      Max:10000 msec
NAT Keepalive:           Disabled
DPD Timeout:             0 seconds (DPD turn-off)
EAP Type:                none
```

show crypto isakmp sa

To show IKE SA information and statistics, use the **show crypto isakmp sa** command in EXEC mode.

```
show crypto isakmp sa [remote-ip remote_ipv4_address mask remote_ipv4_mask]
  [remote-ip remote_ipv6_address ipv6-prefix ipv6_prefix_length] [remote-host remote_host]
  [vrf-local vrf_name]
```

Syntax Description		
remote_ipv4_address	Remote IPv4 address to be used with the mask to filter the set of ISAKMP SAs displayed.	
remote_ipv4_mask	Mask to be used with the IPv4 address to filter the set of ISAKMP SAs displayed.	
remote_ipv6_address	Remote IPv6 address to be used with the prefix length to filter the set of ISAKMP SAs displayed.	
ipv6_prefix_length	Prefix length to be used with the IPv6 address to filter the set of ISAKMP SAs displayed.	
remote_host	Remote hostname.	
vrf_name	Filters the set of IPsec SAs to display within a specific VRF.	

Defaults None.

Command Modes EXEC

Command History	Release	Modification
	WSG Release 1.1	This command was introduced.
	WSG Release 3.0	Added support for IPv6.
	WSG Release 4.0	Added hostname in reverse DNS lookup feature for IKE peer support.

Usage Guidelines Use the **show crypto isakmp sa** command to view IKE SA information and statistics.

Examples This example shows how to view IKE SA information and statistics:

```
WSG# show crypto isakmp sa ?
  remote-hostname Show detailed stats for the remote SA with the hostname
  remote-ip       Show crypto ike sa detailed stats
  |               Output modifiers.
  >               Output Redirection.
  <cr>            Carriage return.
```

show crypto isakmp sa

WSG# **show crypto isakmp sa**

SA Id	P1	IKE	Child	Encryption	Algorithm	Remote Auth	Tunnel	Type	VRF Name
	Done	Ver	SAs		Hash	PRF			
1	yes	2	1	aes128-cbc	hmac-sha1-96	hmac-sha1	rsa	RAS	global

Local IP Address:Port : 88.88.63.3:4500
 Remote IP Address:Port : 184.0.155.74:4500
 Remote Hostname :

This example shows how to view information on a specific SA by IP or hostname:

ppc1# **show crypto isakmp sa remote-ip 50.0.0.1**

```
IKE SA Detailed Statistics
  Profile Name           : s2s-one
  Tunnel Type            : S2S
  P1 Done                : yes
  IKE Version            : 2
  Child SAs              : 1
  Created                : Wed Sep 14 2011 21:29:28 UTC
  Up Time (seconds)     : 1480
  spi-i                  : 0xa19c4129b976af8b
  spi-r                  : 0x000251601676ed87
  VRF Name                : global
  IP Address Local       : 33.33.33.30
  Local Port             : 500
  IP Address Remote      : 50.0.0.1
  Host Remote            : BXL123
  Remote Port            : 500
  Identity Local         : ppc1@cisco.com (email)
  Identity Remote        : ixial@cisco.com (email)
  Algorithm Encryption   : aes128-cbc
  Algorithm Hash         : hmac-sha1-96
  Algorithm PRF          : hmac-sha1
  Local Auth Method      : rsa
  Remote Auth Method     : rsa
  Packets In             : 4
  Packets Out            : 4
  Bytes In                : 1580
  Bytes Out              : 1617
  Packets Dropped In    : 0
  Packets Dropped Out   : 0
```

ppc1# **show crypto isakmp sa remote-ip 50.0.0.1 vrf-local ?**

<WORD> Enter the VRF Name as a string (Max Size - 63)

ppc1# **show crypto isakmp sa remote-host BXL123**

```
IKE SA Detailed Statistics
  Profile Name           : s2s-one
  Tunnel Type            : S2S
  P1 Done                : yes
  IKE Version            : 2
  Child SAs              : 1
  Created                : Wed Sep 14 2011 21:29:28 UTC
  Up Time (seconds)     : 1480
  spi-i                  : 0xa19c4129b976af8b
  spi-r                  : 0x000251601676ed87
  VRF Name                : global
  IP Address Local       : 33.33.33.30
  Local Port             : 500
  IP Address Remote      : 50.0.0.1
  Host Remote            : BXL123
  Remote Port            : 500
  Identity Local         : ppc1@cisco.com (email)
  Identity Remote        : ixial@cisco.com (email)
  Algorithm Encryption   : aes128-cbc
  Algorithm Hash         : hmac-sha1-96
  Algorithm PRF          : hmac-sha1
```

```
Local Auth Method      : rsa
Remote Auth Method     : rsa
Packets In             : 4
Packets Out            : 4
Bytes In               : 1580
Bytes Out              : 1617
Packets Dropped In    : 0
Packets Dropped Out   : 0
```

show crypto isakmp summary

To show all global IKE statistics, use the **show crypto isakmp summary** command in EXEC mode.

show crypto isakmp summary

Syntax Description This command has no keywords or arguments.

Command Default None.

Command Modes EXEC

Command History	Release	Modification
	WSG Release 1.1	This command was introduced.
	WSG Release 3.0	The output of this command was modified with new information.

Usage Guidelines Use the **show crypto isakmp summary** command to view all global IKE statistics.

Examples This example shows how to view all global ISAKMP statistics:

```
switch# show crypto isakmp summary
SeGW Global Statistics

Started at: Mon Jun 27 2011 11:53:56
Uptime:    00:59:00

ISAKMP
  Active IKE SAs          : 17000
  Active IPSEC SAs       : 17000
  Total SAs
    Phase-1
      Done                 : 17002
      Failed               : 0
      Initiated            : 0
      Responded            : 17002
    Phase-2
      Done                 : 17007
      Failed               : 0
  IKE Errors
    Initiated
      Failures             : 0
      No Response          : 0
      Responded
        Failures           : 0
  Total Bytes In          : 28564912
  Total Bytes Out         : 29806186
  Total Packets In        : 34016
```



```
Total Packets Out      : 34016
Total Packets In Dropped : 0
Total Packets Out Dropped : 0
```

show crypto pki certificate

To display the certificate information, use the **show crypto pki certificate** command in EXEC mode.

show crypto pki certificate *certificate*

Syntax Description	none	Displays the certificate.
		Note This is a show command and does not affect the running configuration.
	certificate	The certificate name.

Defaults None.

Command Modes EXEC

Command History	Release	Modification
	WSG Release 1.2	This command was introduced.

Examples This example shows how to configure the **show crypto pki certificate** command:

```
WSG# show crypto pki certificate ppc1-cert.crt

Certificate =
  SubjectName = <C=US, ST=CA, L=San Jose, O=Cisco, OU=SMBU, CN=ppc1,
    MAILTO=ppc1@cisco.com>
  IssuerName = <C=US, ST=CA, L=San Jose, O=Cisco, OU=SMBU, CN=OPENSSSL CA,
    MAILTO=rootca@cisco.com>
  SerialNumber= 2
  SignatureAlgorithm = rsa-pkcs1-sha1
  Validity =
    NotBefore = 2009 Jan 22nd, 02:28:21 GMT
    NotAfter = 2019 Jan 20th, 02:28:21 GMT
  PublicKeyInfo =
    PublicKey =
      Algorithm name (SSH) : if-modn{sign{rsa-pkcs1-md5}}
      Modulus n (1024 bits) :
        12105435948033240350769679706089921111509427844907172607784507755496777
        33290642674006180643600266569660548777101038339032678599500242986426180
        52496238173469262228428095496931681549175135507918630237876156662298269
        60321021651738591123718624995852279161605794033250491563196782206945821
        6211824269443128225204287
      Exponent e ( 17 bits) :
        65537
    Extensions =
      Available = key usage, subject alternative name
      SubjectAlternativeNames =
        Following names detected =
          EMAIL (rfc822)
      Viewing specific name types =
```

```
EMAIL = ppc1@cisco.com
KeyUsage = DigitalSignature NonRepudiation KeyEncipherment
Public key SHA1 hash =
 12:c8:59:dc:79:b1:4f:72:c3:f4:33:56:15:df:c9:8a:49:1f:15:29
IKE Certificate hash =
 89:42:57:d3:c8:e8:4d:bb:81:ab:e8:56:c6:07:07:b0:f2:0a:d4:99
Fingerprints =
MD5 = 44:26:f6:15:31:60:e6:44:94:c9:a9:05:d4:21:57:02
SHA-1 = f1:9e:ae:ce:6d:c3:da:32:36:73:4e:aa:cb:95:08:1e:78:74:d1:4d
```

show crypto radius statistics

To display the count of different RADIUS messages sent and received, as well as the RADIUS timeout and retry counters, use the **show crypto radius statistics** command in EXEC mode.

show crypto radius statistics

Syntax Description This command has no keywords or arguments.

Command Default None.

Command Modes EXEC

Command History

Release	Modification
WSG Release 3.0	This command was introduced.

Usage Guidelines

Use the **crypto radius statistics** command to display the count of different RADIUS messages sent and received, as well as the RADIUS timeout and retry counters.

Examples

Here is sample output for the **show crypto radius statistics** command:

```
wsg# show crypto radius statistics
Radius Accounting Statistics
  Accounting requests sent           : 1
  Accounting-On requests sent       : 0
  Accounting-Off requests sent      : 0
  Accounting-Start requests sent    : 1
  Accounting-Stop requests sent     : 0
  Accounting Responses on received  : 0
  Accounting Invalid responses received : 0
  Accounting requests failed        : 0
  Accounting requests, Invalid IKE ID : 0
  Accounting requests timedout      : 1
  Accounting requests retransmission : 4
  Accounting requests cancelled     : 0
```

show crypto throughput

To display the throughput data for the last calculated 5 minute interval on the WSG, use the **show crypto throughput** command in EXEC mode.

show crypto throughput

Syntax Description This command has no keywords or arguments.

Command Default None.

Command Modes EXEC

Command History	Release	Modification
	WSG Release 4.2	This command was introduced.

- Usage Guidelines**
- Use the **show crypto throughput** command to display throughput data for the last calculated 5 minute interval on the WSG.
 - This CLI will display the “Throughput Utilization (%)” and “Peak Throughput Utilization (%)” value of highest IXP, either IXP 1 or IXP 2.

Examples Here is a sample output for the **show crypto throughput** command:

```
wsg# show crypto throughput
Throughput (Mbp/s)           : 4992
Throughput (Kpp/s)           : 626
Average Packet Size(bytes)   : 996
Throughput Utilization (%)   : 58
Peak Throughput Utilization (%) : 100 Sat Sep 06 15:39:50.012 UTC
  Peak Throughput (Mbp/s)    : 18400
  Peak Packet Size (bytes)   : 509
```

show crypto throughput ixp

Displays the throughput data for packets to/from Nitrox and the average throughput utilization for the last calculated interval on WSG for each IXP. IXP0 display also shows the packet data punted to IXP1.

show crypto throughput ixp <1/2>

Syntax Description

ixp	Selects IXP number
1	IXP0
2	IXP1

Command Default

None.

Command Modes

EXEC

Command History

Release	Modification
WSG Release 4.4	This command was introduced.

Usage Guidelines

Use the **show crypto throughput ixp** command to display throughput data for the last calculated 5 minute interval on the WSG.

Examples

Here are the sample outputs for the **show crypto throughput ixp <1/2>** command:

```
wsg# show crypto throughput ixp 1
Throughput - First Path (Mbp/s) : 3941
Throughput - First Path (Kpp/s) : 501
Average Packet Size - First Path (bytes) : 983
Throughput - Return Path (Mbp/s) : 1051
Throughput - Return Path (Kpp/s) : 125
Average Packet Size - Return Path (bytes) : 1051
Throughput Utilization (%) : 58
Peak Throughput Utilization (%) : 100 Sat Sep 06 15:39:50.012 UTC
Peak Throughput - First Path (Mbp/s) : 9200
Peak Packet Size - First Path (bytes) : 876
Peak Throughput - Return Path (Mbp/s) : 9200
Peak Packet Size - Return Path (bytes) : 1021
Punted to IXP2 (Mbp/s) : 2956
Punted to IXP2 (Kpp/s) : 376

wsg# show crypto throughput ixp 2
Throughput - First Path (Mbp/s) : 1051
Throughput - First Path (Kpp/s) : 125
Average Packet Size - First Path (bytes) : 1051
Throughput - Return Path (Mbp/s) : 4140
Throughput - Return Path (Kpp/s) : 501
```

```
Average Packet Size - Return Path (bytes) : 1032
Throughput Utilization (%) : 57
Peak Throughput Utilization (%) : 100 Sat Sep 06 15:39:50.012 UTC
Peak Throughput - First Path (Mbp/s) : 9200
Peak Packet Size - First Path (bytes) : 359
Peak Throughput - Return Path (Mbp/s) : 9200
Peak Packet Size - Return Path (bytes) : 359
```

show crypto throughput distribution history

To display the number of intervals the throughput fell in a certain bucket range with each Interval being 5 minutes, use the **show crypto throughput distribution history** command in EXEC mode.

show crypto throughput distribution history

Syntax Description This command has no keywords or arguments.

Defaults None.

Command Modes EXEC

Command History	Release	Modification
	WSG Release 4.2	This command was introduced as the crypto throughput distribution history command.

Usage Guidelines Use the **show crypto throughput distribution history** command display the history of throughput.

Examples Here is a sample output for the **show crypto throughput distribution history** command:

```
wsg# show crypto throughput distribution history
% Throughput Utilization bucket          Number of Intervals
 1 - 25                                   1
26 - 50                                   0
51 - 60                                   4
61 - 65                                   0
66 - 70                                   0
71 - 75                                   0
76 - 80                                   0
81 - 82                                   0
83 - 84                                   0
85 - 86                                   0
87 - 88                                   0
89 - 90                                   0
91 - 92                                   0
93 - 94                                   0
95 - 96                                   0
97 - 98                                   0
99 - 100                                  1
```


show crypto throughput distribution history ixp

To display the number of intervals the throughput fell in a certain bucket range for each IXP, with each Interval being 5 minutes, use the **show crypto throughput distribution history ixp <1/2>** command in EXEC mode.

show crypto throughput distribution history ixp <1/2>

Syntax Description

ixp	Selects IXP number
<i>1</i>	IXP0
<i>2</i>	IXP1

Defaults

None.

Command Modes

EXEC

Command History

Release	Modification
WSG Release 4.4	This command was introduced.

Usage Guidelines

Use the **show crypto throughput distribution history ixp** command to display the history of throughput.

Examples

Here are the sample outputs for the **show crypto throughput distribution history ixp** commands:

```
wsg# show crypto throughput distribution history ixp 1
% Throughput Utilization bucket          Number of Intervals
 1 - 25                                   1
26 - 50                                   0
51 - 60                                   4
61 - 65                                   0
66 - 70                                   0
71 - 75                                   0
76 - 80                                   0
81 - 82                                   0
83 - 84                                   0
85 - 86                                   0
87 - 88                                   0
89 - 90                                   0
91 - 92                                   0
93 - 94                                   0
95 - 96                                   0
97 - 98                                   0
99 - 100                                  1
```

■ show crypto throughput distribution history ixp

```
wsg# show crypto throughput distribution history ixp 2
% Throughput Utilization bucket          Number of Intervals
 1 - 25                                 0
26 - 50                                 0
51 - 60                                 4
61 - 65                                 0
66 - 70                                 0
71 - 75                                 0
76 - 80                                 0
81 - 82                                 0
83 - 84                                 0
85 - 86                                 0
87 - 88                                 0
89 - 90                                 0
91 - 92                                 0
93 - 94                                 0
95 - 96                                 0
97 - 98                                 0
99 - 100                                1
```

show crypto throughput history

To display the history of throughput in Mbp/s and Packets/s from 3 hours, 1 day to 1 week history, use the **show crypto throughput history** command in EXEC mode.

show crypto throughput history interval *interval type*

Syntax Description	<i>interval</i>	Duration of history of throughput. Valid values are: <ul style="list-style-type: none"> • 1 - 5minutes • 2 - 1hour • 3 - 3hours
	<i>type</i>	Type of unit value to display the throughput. Valid values are: <ul style="list-style-type: none"> - Mbps - Kpps (Kilo-Packets-per-second)

Defaults None.

Command Modes EXEC

Command History	Release	Modification
	WSG Release 4.2	This command was introduced as the crypto throughput history command.

Usage Guidelines Use the **show crypto throughput history** command to display the history of throughput.

Examples Here are the sample outputs for the **show crypto throughput history** commands:

```
wsg# show crypto throughput history interval 5minutes Kpps
3200 #
3000
2800
2600
2400
2200
2000
1800
1600
1400
1200
1000
800
600 #####
400
200
```

show crypto throughput history

```

....  ....1....1....2....2....3....3....4....4....5....5....6....6....7..
0 5 0 5 0 5 0 5 0 5 0 5 0 5 0 5 0
Kpps per five min (last 6 hrs)

```

```
wsg# show crypto throughput history interval 5minutes Mbps
```

```

9200 #
8700
8200
7700
7200
6700
6200
5700
5200 ####
4700
4200
3700
3200
2700
2200
1700
1200
700
200 #
....  ....1....1....2....2....3....3....4....4....5....5....6....6....7..
0 5 0 5 0 5 0 5 0 5 0 5 0 5 0
Mbps per five min (last 6 hrs)

```

show crypto throughput history ixp

To display the history of throughput in Mbp/s and Packets/s separately for each IXP, use the **show crypto throughput history** command in EXEC mode.

show crypto throughput history interval *interval type* ixp <1/2>

Syntax Description	ixp	Selects IXP number
	1	IXP0
	2	IXP1

Defaults None.

Command Modes EXEC

Command History	Release	Modification
	WSG Release 4.4	This command was introduced.

Usage Guidelines Use the **show crypto throughput history interval *interval type* ixp** command to display the history of throughput.

Examples Here is a sample output for the **show crypto throughput history interval *interval type* ixp** command:

```
wsg# show crypto throughput history interval 5minutes Kpps ixp 1
3200
3000
2800
2600
2400
2200
2000
1800
1600
1400
1200 #
1000
800
600
400 ####
200
.... 1...1...2...2...3...3...4...4...5...5...6...6...7..
0 5 0 5 0 5 0 5 0 5 0 5 0 5 0
Kpps per five min (last 6 hrs)
```

```
wsg# show crypto throughput history interval 5minutes Kpps ixp 2
3200 #
```

■ **show crypto throughput history ixp**

```

3000
2800
2600
2400
2200
2000
1800
1600
1400
1200
1000
800
600
400 #####
200
.... 1....1....2....2....3....3....4....4....5....5....6....6....7..
0 5 0 5 0 5 0 5 0 5 0 5 0 5 0
Kpps per five min (last 6 hrs)

```

```

wsg# show crypto throughput history interval 5minutes Mbps ixp 1
9200 #
8700
8200
7700
7200
6700
6200
5700
5200
4700
4200
3700
3200
2700 #####
2200
1700
1200
700
200 #
.... 1....1....2....2....3....3....4....4....5....5....6....6....7..
0 5 0 5 0 5 0 5 0 5 0 5 0 5 0
Mbps per five min (last 6 hrs)

```

```

wsg# show crypto throughput history interval 5minutes Mbps ixp 2
9200 #
8700
8200
7700
7200
6700
6200
5700
5200
4700
4200
3700
3200
2700 #####
2200
1700
1200
700

```

```
200 #  
... ..1...1...2...2...3...3...4...4...5...5...6...6...7..  
0 5 0 5 0 5 0 5 0 5 0 5 0 5 0  
Mbps per five min (last 6 hrs)
```

show debug crypto

To view crypto debug information on the WSG, use the **show debug crypto** command in EXEC mode.

show debug crypto

Syntax Description This command has no keywords or arguments.

Command Default None.

Command Modes EXEC

Command History	Release	Modification
	WSG Release 1.2	This command was introduced.

Usage Guidelines Use the **show debug crypto** command to view crypto debug information.



Note

The **show debug** command does not show the debugs related to the crypto module.

Examples This example shows how to configure the show debug crypto command:

```
WSG# show debug crypto
debug crypto config events
```


show ha info

To display the configuration, states, and statistics of the local node and its peer, use the **show ha info** command in EXEC mode.

show ha info [brief | detail]

Syntax Description	brief	Displays the configuration and the state of the local node.
	detail	Display includes extra information about the cluster and the node names.

Defaults None.

Command Modes EXEC

Command History	Release	Modification
	WSG Release 2.0	This command was introduced.

Examples The **show ha info** command shows the configuration, states, and statistics of the local node and its peer:

```
WSG# show ha info
Redundancy mode (configured) : active-standby
Redundancy state : Redundant
My Node
  Current State : Active
  Preferred Role : Primary
  IP Address   : 51.51.51.43
  Slot/PPC    : 4/3
Peer Node
  IP Address   : 51.51.51.53
  Slot/PPC    : 5/3
Bulk Sync Status : Success
Bulk Sync done  : Thu Sep 15 01:24:36 2011
HA Revertive   : Disabled
```

The **show ha info brief** command shows the configuration and the state of the local node:

```
WSG# show ha info brief
Interface  IP-Address  Redundancy-State  Mode           Current-State  Preferred-Role  HA-Revertive
VLAN51    51.51.51.43  Redundant         active-standby Active          Primary         Disabled
```

The **show ha info detail** command includes extra information about the cluster and node names:

```
WSG# show ha info detail
Redundancy mode (configured) : active-standby
Redundancy state : Redundant
My Node
  nodename      : node1
  Current State : Active
  Last State    : Un-assigned
  Preferred Role : Primary
  IP Address    : 51.51.51.43
  Slot/PPC     : 4/3
Peer Node
  nodename      : node2
  IP Address    : 51.51.51.53
  Slot/PPC     : 5/3
Bulk Sync Status : Success
Bulk Sync done   : Thu Sep 15 01:24:36 2011
HA Revertive    : Disabled
ISync Counters
  Total Request Sent : 0
  Total Response Rcvd : 0
  Total Fail Count   : 0
  Total Request Rcvd : 0
  Total Response Sent : 0
Cluster         : cluster12
  Active Mgr      : node1
  Standby Mgr     : node2
```

show hosts

To display the hosts on a PPC, use the **show hosts** command in EXEC mode.

show hosts

Syntax Description This command has no arguments or keywords.

Defaults None.

Command Modes EXEC

Command History	Release	Modification
	COSLI 1.0	This command was introduced.
	WSG Release 3.0	IPv6 statistics were added.

Usage Guidelines The **show hosts** command lists the name servers and their corresponding IP addresses. It also lists the hostnames, their corresponding IP addresses, and their corresponding aliases (if applicable) in a host table summary.

Examples To display a list of hosts on a PPC, enter:

```
switch# show hosts
Default domain is not set
Name/address lookup uses domain service
Name servers are 51.51.51.1 2001:88:88:94::1
```

show icmp6 statistics

To display the ICMP6 statistics, use the **show icmp6 statistics** command in EXEC mode.

show icmp6 statistics

Syntax Description There are no keywords or arguments for this command.

Defaults None.

Command Modes EXEC

Command History	Release	Modification
	WSG Release 3.0	This command was introduced.

Usage Guidelines None.

Examples This example shows how to enable the **show icmp6 statistics** command:

```
wsg# show icmp6 statistics
Icmp6InMsgs                352
Icmp6InErrors              0
Icmp6OutMsgs               350
Icmp6InDestUnreaches      0
Icmp6InPktTooBigs         0
Icmp6InTimeExcds          0
Icmp6InParmProblems       0
Icmp6InEchos               0
Icmp6InEchoReplies        231
Icmp6InGroupMembQueries   28
Icmp6InGroupMembResponses 0
Icmp6InGroupMembReductions 0
Icmp6InRouterSolicits     0
Icmp6InRouterAdvertisements 34
Icmp6InNeighborSolicits   52
Icmp6InNeighborAdvertisements 7
Icmp6InRedirects          0
Icmp6InMLDv2Reports       0
Icmp6OutDestUnreaches    0
Icmp6OutPktTooBigs        0
Icmp6OutTimeExcds         0
Icmp6OutParmProblems      0
Icmp6OutEchos              231
Icmp6OutEchoReplies       0
Icmp6OutGroupMembQueries  0
Icmp6OutGroupMembResponses 0
Icmp6OutGroupMembReductions 0
Icmp6OutRouterSolicits    15
Icmp6OutRouterAdvertisements 0
```

Icmp6OutNeighborSolicits	6
Icmp6OutNeighborAdvertisements	56
Icmp6OutRedirects	0
Icmp6OutMLDv2Reports	42
Icmp6InType129	231
Icmp6InType130	28
Icmp6InType134	34
Icmp6InType135	52
Icmp6InType136	7
Icmp6OutType128	231
Icmp6OutType133	15
Icmp6OutType135	6
Icmp6OutType136	56
Icmp6OutType143	42

show interface

To display interface information, use the **show interface** command in EXEC mode.

show interface [*vlan number*]

Syntax Description	<i>number</i>	Displays the statistics for the specified VLAN.
--------------------	---------------	---

Defaults	None.
----------	-------

Command Modes	EXEC
---------------	------

Command History	Release	Modification
	WSG Release 1.0	This command was introduced.
	WSG Release 3.0	Added support for IPv6.

Usage Guidelines	To display all of the interface statistical information, enter the show interface command without using the optional vlan keyword.
------------------	--

Examples	To display all of the interface statistical information, enter:
----------	---

```
switch# show interface
eth0      Link encap:Ethernet  HWaddr 00:1F:CA:08:89:2E
          inet addr:127.0.0.23  Bcast:127.0.0.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:9560  Metric:1
          RX packets:376394 errors:0 dropped:0 overruns:0 frame:0
          TX packets:35455 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:109038474 (103.9 MiB)  TX bytes:4452754 (4.2 MiB)
          Base address:0x4000

eth0.121  Link encap:Ethernet  HWaddr 00:1F:CA:08:89:2E
          inet addr:1.5.31.122  Bcast:1.5.255.255  Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5405 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:324300 (316.6 KiB)
```

To display the details, statistics, or IP information for all or a specified VLAN interface (51 in this example), enter:

```
wsg# show interface vlan 51
vlan [51] is administratively up
Hardware type: VLAN
MODE: UNKNOWN
IP Address = [51.51.51.4] netmask = [255.255.255.0]
IPv6 Address = fe80::21b:2aff:fe65:fa56/64
```

```
FT Status: non redundant
Description:
MTU: 1500 bytes
```

```
295165 unicast packets input, 23950072 bytes
0 multicast, 84326 broadcast
0 input errors, 0 unknown, 0 ignored
6 unicast packets output, 468 bytes
0 multicast, 0 broadcast
0 output errors, 0 ignored
```

show interface internal iftable

To display internal iftable statistics, use the **show interface internal iftable** command in EXEC mode.

show interface internal iftable

Syntax Description There are no keywords or arguments for this command.

Defaults None.

Command Modes EXEC

Command History	Release	Modification
	WSG Release 3.0	This command was introduced.

Usage Guidelines None.

Examples This example shows how to enable the **show interface internal iftable** command:

```
wsg# show interface internal iftable
vlan39
-----
Context:          0
physid:           39
iftyp:            0 (vlan)
IP:               (11.11.39.43)
IPv6:             (2001:88:88:94::43/96)
IPv6:             (2001:88:88:94::11/96)
MTU:              1500
MAC:              00:1B:2A:65:FA:56
LastChange:      Thu Sep 15 01:21:04 2011
```


show ip bgp

To display general information about bgp routing processes, use the **show ip bgp** command in EXEC mode.

show ip bgp

Syntax Description There are no keywords or arguments for this command.

Defaults None.

Command Modes EXEC

Command History	Release	Modification
	WSG Release 3.0	This command was introduced.

Examples

Here is an example to display BGP-related information:

```
wsg# sh ip bgp
BGP router identifier 127.0.0.23, local AS number 7675 RIB entries 1, using 64 bytes of
memory Peers 1, using 2508 bytes of memory

Neighbor      V    AS MsgRcvd MsgSent   TblVer  InQ  OutQ  Up/Down  State/PfxRcd
33.33.33.3    4   7675   1239   1130     0    0    0 18:46:42      0

Total number of neighbors 1
BGP scan is running
BGP scan interval is 60
Current BGP nexthop cache:
BGP connected route:
 33.0.0.0/8
 33.33.33.0/24
 70.70.70.0/24
 77.0.0.0/8
 77.77.77.0/24
127.0.0.0/24
BGP table version is 0, local router ID is 127.0.0.23 Status codes: s suppressed, d
damped, h history, * valid, > best, i - internal,
                r RIB-failure, S Stale, R Removed Origin codes: i - IGP, e - EGP, ? -
incomplete

      Network          Next Hop           Metric LocPrf Weight Path
*> 40.0.0.0/24        0.0.0.0             0         32768  ?

Total number of prefixes 1
```

show ip interface brief

To display a brief configuration and status summary of all interfaces or a specified VLAN, enter:

```
show ip interface brief [vlan number]
```

Syntax Description	<i>number</i>	Displays the statistics for the specified VLAN.
--------------------	---------------	---

Defaults	None.
----------	-------

Command Modes	EXEC
---------------	------

Command History	Release	Modification
	WSG Release 1.0	This command was introduced.
	WSG Release 3.0	Added support for IPv6.

Usage Guidelines	Use the show ip interface brief command to display a brief configuration and status summary of all the interfaces or a specified VLAN.
------------------	---

Examples	To display a brief configuration and status summary of all the interfaces, enter:
----------	---

```
switch# show ip interface brief
Interface    IP-Address      IPv6-Address      Status           Protocol
vlan 51     51.51.51.4      fe80::21b:2aff:fe65:fa56/64  administratively up  up
```

show ip route

To display the IPv4 destination routes, use the **show ip route** command in EXEC mode.

show ip route

Syntax Description There are no keywords or arguments for this command.

Defaults None.

Command Modes EXEC

Command History	Release	Modification
	WSG Release 3.0	This command was introduced.

Usage Guidelines None.

Examples This example shows how to display the IPv4 destination routes:

```
switch# show ip route
 99.99.99.0/24 via 11.11.36.1 dev eth0.36 vrf global
 52.52.52.0/24 dev eth0.52 proto kernel scope link src 52.52.52.43 vrf global
 51.51.51.0/24 dev eth0.51 proto kernel scope link src 51.51.51.43 vrf global
 default via 11.11.39.1 dev eth0.39 vrf global
```

show ip route np

To display the IPv4 routes configured on the Network Processor, use the **show ip route np** command in EXEC mode.

show ip route np

Syntax Description There are no keywords or arguments for this command.

Defaults None.

Command Modes EXEC

Command History	Release	Modification
	WSG Release 3.0	This command was introduced.

Usage Guidelines None.

Examples This example shows how to display the IPv4 routes configured on the Network Processor:

```
switch# show ip route np
Routes in NP:
 99.99.99.0/24 via 11.11.36.1 vrf global: MAC 00:18:74:2e:0d:40 VLAN 36 vrfId 0
 88.88.88.0/24 via 11.11.36.1 vrf global: MAC 00:18:74:2E:0D:40 VLAN 36 vrfId 0
 20.20.20.0/24 via 11.11.36.1 vrf global: MAC 00:18:74:2E:0D:40 VLAN 36 vrfId 0
 0.0.0.0/0 via 11.11.39.1 vrf global: MAC 00:18:74:2E:0D:40 VLAN 39 vrfId 0
Routes NOT in NP:
 88.88.88.0/24 via 11.11.36.1 vrf clear1
 88.88.88.0/24 via 11.11.36.2 vrf clear2
 88.88.88.0/24 via 11.11.36.1 vrf clear3
Route commands to NP:
 IPv4 static route add = 4
 IPv4 static route delete = 0
 static route add failure (exceeding limit) = 0
```

show ip ssh

To display the SSH information, use the **show ip ssh** command in EXEC mode.

show ip ssh

Syntax Description There are no keywords or arguments for this command.

Defaults None.

Command Modes EXEC

Release	Modification
WSG Release 4.0	This command was introduced.

Usage Guidelines None.

Examples This example shows how to display the SSH information:

```
switch# show ip ssh
```

```
sshd pid(s) 1844 are running...
```

```
USER      TTY      IDLE      TIME      HOST
test2     pts/0    00:04    Jun 25 13:58:3 22.22.110.100
```

show ipv6 neighbors

To display information about IPv6 neighbors, use the **show ipv6 neighbors** command in EXEC mode.

show ipv6 neighbors

Syntax Description There are no keywords or arguments for this command.

Defaults None.

Command Modes EXEC

Command History	Release	Modification
	WSG Release 3.0	This command was introduced.

Usage Guidelines None.

Examples This example displays the output of the **show ipv6 neighbors** command:

```
wsg# show ipv6 neighbors
2001:88:88:94::4 dev eth0 lladdr 00:a9:40:0f:84:6a REACHABLE
2001:88:88:94::2 dev eth0 lladdr 00:0a:b7:cf:9f:00 REACHABLE
```

show ipv6 route

To display the IPv6 destination route, use the **show ipv6 route** command in EXEC mode.

show ipv6 route

Syntax Description There are no keywords or arguments for this command.

Defaults None.

Command Modes EXEC

Command History	Release	Modification
	WSG Release 3.0	This command was introduced.

Usage Guidelines None.

Examples This example displays the output of the **show ipv6 route** command:

```
wsg# show ipv6 route
Destination                Next Hop    Flags Metric Ref    Use Iface
2001:88:88:94::/96        ::          U        256   0      0      eth0.39
2001:88::/32              ::          U        256   0      0      eth0.5
fe80::/64                 ::          U        256   0      0      eth0
```

show ipv6 route np

To display the IPv6 routes configured on the Network Processor, use the **show ipv6 route np** command in EXEC mode.

show ipv6 route np

Syntax Description There are no keywords or arguments for this command.

Defaults None.

Command Modes EXEC

Command History

Release	Modification
WSG Release 3.0	This command was introduced.

Usage Guidelines

None.

Examples

This example shows how to display the IPv6 routes configured on the Network Processor:

```
switch# show ipv6 route np
Routes in NP:
  2001:88:88:94::/96 via 2001:88:88:94::1 vrf global: MAC 00:18:74:2e:0d:40 VLAN 39
    vrfId 0
  2001:77:77:94::/96 via 2001:88:88:94::1 vrf global: MAC 00:18:74:2e:0d:40 VLAN 39
    vrfId 0
  ::/0 via 2001:77:77:94::1 vrf global: MAC 00:18:74:2e:0d:40 VLAN 36 vrfId 0
Route commands to NP:
  IPv6 static route add = 3
  IPv6 static route delete = 0
  static route add failure (exceeding limit) = 0
```


show ip vrf

To display all VRFs in the system, use the **show ip vrf** command. To display a specific VRF, use the **show ip vrf vrf_name** command.

show ip vrf vrf_name

Syntax Description	<i>vrf_name</i>	Specifies the VRF to display.
Defaults	None.	
Command Modes	EXEC	
Command History	Release	Modification
	WSG Release 3.0	This command was introduced.

Usage Guidelines To display all VRFs in the system, use the **show ip vrf** command.

Examples The following is an example of how to display all VRFs in the system:

WSG# **show ip vrf**

vrf: id - 0, name - global

member devices: eth0 lo dummy0 tun10 sit0 ip6tn10 eth0.70 eth0.32 eth0.72

vrf: id - 1, name - insideRed

member devices: eth0.77

vrf: id - 2, name - insideBlue

member devices: eth0.78

vrf: id - 3, name - outsideRed

member devices: eth0.33

vrf: id - 4, name - outsideBlue

member devices: eth0.34

Max VRFs supported: 1000

The following is an example of how to display the specific VRF named *insideRed*:

WSG# **sh ip vrf insideRed**

vrf: id - 1, name - insideRed

member devices: eth0.77

show logging

To display the current syslog configuration and syslog messages, use the **show logging** command.

```
show logging { config [l] [>] | message { all cpuid cpu-id | module mod-id }
```

Syntax Description	
config	Displays syslog configuration.
message	Displays syslog messages.
<i>cpu-id</i>	Displays syslog messages for a specific CPU id.
<i>mod-id</i>	Displays syslog messages for a specific module id.
	(Optional) Pipe character () for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the show command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the show command.

Defaults None.

Command Modes EXEC

Command History	Release	Modification
	COSLI 1.0	This command was introduced.
	WSG Release 3.0	Added support for IPv6.
	WSG Release 3.1	Adds configured hostname along with CPU ID to the syslog.

Usage Guidelines To enable system logging, use the **logging** configuration command. The **show logging** command lists the current syslog messages and identifies which **logging** command options are enabled.

Prior to WSG Release 3.1, syslog messages display the CPU ID as the name of the source host where messages originated from. The enhancement in WSG Release 3.1 adds the configured hostname along with the CPU ID to the syslog in order to make management easier.

Examples To display the syslog configuration, enter:

```
wsg# show logging config
  Ext logging server IP: 1.1.1.1
  Ext logging server IPv6: 2001:88:88:94::1
  Number of lines read log: 100
wsg# show logging
Feb 14 21:47:58 172.29.99.4 alert VF-D2 cpu3:root: this is a test msg from PPC3
Feb 14 21:52:18 172.29.99.4 notice VF-D2 cpu3:root: this is a test msg from PPC3
```

snmp-server enable traps ipsec

To enable SNMP IPsec traps, use the **snmp-server enable trap ipsec** global configuration command. To disable traps, use the **no** form of this command.

```
snmp-server enable traps ipsec [ address-pool-exhaust | too-many-sas | tunnel { start | stop } |
cert-expiry | cert-renewal | throughput-threshold | tunnel-rate { create <1-1000> | delete
<1-1000> } | decrypt auth-failure ]
```

```
no snmp-server enable traps ipsec [ address-pool-exhaust | too-many-sas | tunnel { start | stop
} | cert-expiry | cert-renewal | throughput-threshold | tunnel-rate { create <1-1000> | delete
<1-1000> } | decrypt auth-failure ]
```

Syntax Description

snmp-server enable traps ipsec	Enables all SNMP IPsec traps except “ tunnel-rate create ” and “ tunnel-rate delete ” traps.
address-pool-exhaust	Enable only Insufficient IP Address Pool notification event.
too-many-sas	Enable only Too Many SAs notification event.
tunnel start	Enable only 1000 IPsec tunnel start notification event.
tunnel stop	Enable only 1000 IPsec tunnel stop notification event.
tunnel-rate	Enable tunnel event notification (25 secs rate interval).
tunnel-rate create	Generate trap on created tunnels for configured tunnel count.
tunnel-rate delete	Generate trap on deleted tunnels for configured tunnel count.
<1-1000>	Number of tunnels.
cert-expiry	Enable only certificate expiration notification event.
cert-renewal	Enable only certificate renewal notification event.
throughput-threshold	Enable SNMP trap when WSG throughput utilization goes above the configured or default value for a sustained number of intervals
decrypt auth-failure	Enable authentication decryption failure notification event. Sends a trap when the authentication decryption failure for a particular IPsec tunnel increases at a configurable rate (using CLI “ crypto decrypt auth-failure rate <> ”) in an interval of 5 minutes.

Defaults

SNMP traps are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
WSG Release 1.1	This command was introduced.
WSG Release 3.0	The cert-expiry and cert-renewal keywords were added.
WSG Release 4.2	The throughput-threshold keyword was added.

Release	Modification
WSG Release 4.4.3	The tunnel-rate keyword was added.
WSG Release 4.4.8	The decrypt auth-failure keyword was added.

Usage Guidelines

Use the **snmp-server enable traps ipsec** command to enable SNMP IPsec traps, except “**tunnel-rate create**” and “**tunnel-rate delete**” traps.

Examples

Here is an example showing how to enable all SNMP IPsec traps:

```
WSG# config  
Enter configuration commands, one per line. End with CNTL/Z.  
WSG (config)# snmp-server enable traps ipsec
```

snmp-server host

To specify the hosts to receive SNMP notifications, use the **snmp-server host** global configuration command. Use the **no** form of the command to disable this functionality.

```
snmp-server host A.B.C.D | X:X:X::X
```

Syntax Description

<i>A.B.C.D</i>	Specifies the IPv4 address of the SNMP server host.
<i>X:X:X::X</i>	Specifies the IPv6 address of the SNMP server host.

Defaults

By default this command is not configured.

Command Modes

Global configuration

Command History

Release	Modification
WSG Release 2.0	This command was introduced.
WSG Release 3.0	The IPv6 address argument was added.

Examples

This example shows how to enable the **snmp-server host** command:

```
wsg(config)# snmp-server host ?
```

```
<A.B.C.D>|<X:X:X::X> Enter an IP address
```

```
wsg(config)# snmp-server host 44.44.44.16 traps version 2c public
```

```
wsg(config)# snmp-server host 2001:88:88:94::1 traps version 2c public
```

Debug Commands

This section lists the debug commands for the WSG. Please be aware of the following cautions and restrictions:



Caution

Be sure to turn on debugs from within a telnet session and not a console session.



Caution

Be sure to deactivate session-timeout on the PPC debug terminal.



Caution

Ensure that you turn off debugs before you exit a terminal session. If you exit a terminal session that has debugs on, be sure to turn off the debugs from the console before opening a new PPC terminal session.

**Note**

Debugs are activated on a per-terminal basis. You must turn off debugs from the same terminal you turned them on for them to be deactivated.

**Note**

Turning debugs off from a different terminal will deactivate the application debugs, but it will not deactivate the internal debugging flags.

debug crypto

To enable debugging for various crypto parameters, use the **debug crypto** command in EXEC mode. Use the **no** form of the command to disable debugging.

```
debug crypto {config | snmp | stats | dhcp | eap | engine | fastapi | ha | ike | pki | policy}
             {errors | events} [trace]
```

```
no debug crypto {config | snmp | stats | dhcp | eap | engine | fastapi | ha | ike | pki | policy}
               {errors | events} [trace]
```

Syntax Description

config	Debug crypto configuration.
snmp	Debug crypto SNMP configuration.
stats	Debug crypto statistics configuration.
dhcp	Debug crypto DHCP configuration.
eap	Debug crypto EAP module.
engine	Debug crypto engine module.
fastapi	Debug crypto fastapi module.
ha	Debug crypto HA.
ike	Debug crypto IKE module.
pki	Debug crypto PKI module.
policy	Debug crypto policy module.
errors	Debug crypto module errors.
events	Debug crypto module events.
trace	If trace option is enabled.

Defaults

Debugging is disabled by default.

Command Modes

EXEC

Command History

Release	Modification
WSG Release 1.2	This command was introduced.
WSG Release 2.2	Added dhcp option.
WSG Release 3.0	Added eap , engine , fastapi , ha , ike , pki , and policy options.

Examples

This example displays how to use the **debug crypto ike events** command:

```
wsg# debug crypto ike events
```


debug crypto ike remote-ip

To enable debugging of tunnel setup and IKE protocol exchanges by peer IP address, use the **debug crypto ike remote-ip** command in EXEC mode. Use the **no** form of the command to disable crypto IKE debugging.

```
debug crypto ike remote-ip ip_address {netmask netmask | ipv6_prefix prefix} [vrf vrf_name]
{errors | events | info | verbose} [trace]
```

```
no debug crypto ike remote-ip ip_address {netmask netmask | ipv6_prefix prefix} [vrf
vrf_name] {errors | events | info | verbose} [trace]
```

Syntax Description		
<i>ip_address</i>		Remote peer IPv4 or IPv6 address.
<i>netmask</i>		Remote IPv4 network subnet.
<i>prefix</i>		Remote IPv6 network prefix.
<i>vrf_name</i>		Name of VRF up to 60 characters.
errors		Debug tunnel exchange failures.
events		Debug tunnel establishment and removal.
info		Debug tunnel initiation and short decodes.
verbose		Debug tunnel detailed decodes.
trace		If trace option is enabled.

Defaults Debugging is disabled by default.

Command Modes EXEC

Command History	Release	Modification
	WSG Release 3.0	This command was introduced.

Usage Guidelines The **debug crypto ike remote-ip** command requires at least one active profile. You can configure up to 4 tunnel sets.

debug crypto ike remote-ip

Debug Level	Description	Messages Included
1—errors	IKE exchange failure	Level 1
2—events	IKE and IPSec SA establishment and removal	Level 1-2
3—info	IKE exchange initiation, successful completions, and short packet decodes	Level 1-3
4—verbose	Detailed packet decodes	Level 1-4

Examples

This example shows the use of the **debug crypto ike remote-ip** command:

```
wsg# debug crypto ike remote-ip 10.10.10.10 netmask 255.255.255.0 vrf VRF1 events
wsg# debug crypto ike remote-ip 2000:1:2::3 ipv6_prefix 64 vrf VRF2 info
```



Upgrading to WSG Release 4.0

WSG Release 4.0 and later supports inter-chassis, stateful 1:1 redundancy for high availability. The PPC of the active WSG syncs its state to the corresponding PPC of the redundant WSG. An upgrade to the software image can be performed on both the active and the standby WSG in a redundant setup with minimal to no service disruption.

This appendix describes the recommended procedure for upgrading from WSG Release 3.0 to WSG Release 4.0 software. WSG Release 4.0 also provides a path for a graceful downgrade in the event that the attempted upgrade was not successful. However, the graceful downgrade is only available when all the existing tunnels and their respective states are still intact. Otherwise, the downgrade is not graceful.



Note

Graceful upgrade and downgrade are only available between WSG Release 3.0 and Release 4.0. There is no support for graceful upgrade and downgrade between WSG Release 2.0 and Release 4.0.



Note

Do not execute the **copy running-config startup-config** command at any time during the upgrade or downgrade process. Only execute the command when the upgrade or downgrade process is complete.



Note

When there is an **ha-revertive** configuration active, the revertive action will not kick in during an upgrade or downgrade process. Once the upgrade or downgrade process is complete, re-configure **ha-revertive** in the running configuration on the active card, and execute the **copy running-config startup-config** command.

Perform the following steps to upgrade from WSG Release 3.0 to WSG Release 4.0 software:

- Step 1** Copy the running configuration to the startup configuration by executing the **copy running-config startup-config** command on all SAMIs.

```
WSG# copy run start
running config of context Admin saved
Copying operation succeeded.
```

This will save the configurations on the SUP bootflash as a `SLOT<slot>SAMI<processor>.cfg` file.

```
WSG# dir bootflash:SLOT4SAMIC3.cfg
Directory of bootflash:/SLOT4SAMIC3.cfg
243  -rw-          1697  Aug 16 2011 23:05:28 -08:00  SLOT4SAMIC3.cfg
65536000 bytes total (62448108 bytes free)
```




Fast Path Stats Counters

This appendix describes the Fast Path stats counters.

[Table B-1](#) and [Table B-2](#) lists the Fast Path Stats supported by the WSG:

Table B-1 Global IPsec Fast Path Stats Supported by the WSG

Stats	Source	Description
ceipSecGlobalInDrops	NPU	<p>The total number of packets dropped during receive processing by all current and previous IPsec Phase-2 Tunnels. This count does NOT include packets dropped due to Anti-Replay processing.</p> <p>Possible causes of this error:</p> <ul style="list-style-type: none"> • Incorrect IP version • TTL field is zero • ESP packet's Next Header field does not match the IP protocol of the encapsulated packet
ceipSecGlobalOutDrops	NPU	<p>The total number of packets dropped during send processing by all current and previous IPsec Phase-2 Tunnels</p> <p>Possible cause of this error:</p> <ul style="list-style-type: none"> • Fragmentation errors; E.g., packet larger than the WSG's configured pre-fragmentation MTU with DF bit set.
ceipSecGlobalInReplayDrops	Crypto chip	<p>The total number of packets dropped during receive processing due to Anti-Replay processing by all current and previous IPsec Phase-2 Tunnels</p> <p>Possible causes of this error:</p> <ul style="list-style-type: none"> • WSG recives an ESP packet with sequence number out of the replay window. • Simulated by capturing and reply the ESP packet.

Table B-1 Global IPsec Fast Path Stats Supported by the WSG (continued)

Stats	Source	Description
ceipSecGlobalInAuthFails	Crypto chip	The total number of decrypt packet authentications which ended in failure by all current and previous IPsec Phase-2 Tunnels.
ceipSecGlobalOutAuthFails	NPU	The total number of encrypt packet authentications which ended in failure by all current and previous IPsec Phase-2 Tunnels. Possible cause of this error: <ul style="list-style-type: none"> Failures during encryption of the packets for any tunnel on the card.

Table B-2 IPsec Tunnel Fast Path Stats Supported by the WSG

Stats	Source	Description
ceipSecTunInDropPkts	NPU	The total number of packets dropped during receive processing by this IPsec Phase-2 Tunnel. This count does NOT include packets dropped due to Anti-Replay processing. Possible causes of this error: <ul style="list-style-type: none"> Incorrect IP version TTL field is zero ESP packet's Next Header field does not match the IP protocol of the encapsulated packet
ceipSecTunOutDropPkts	NPU	The total number of packets dropped during send processing by this IPsec Phase-2 Tunnel. Possible cause of this error: <ul style="list-style-type: none"> Fragmentation errors; E.g., packet larger than the WSG's configured pre-fragmentation MTU with DF bit set.
ceipSecTunInAuthFails	NPU	The total number of inbound authentication's which ended in failure by this IPsec Phase-2 Tunnel. Possible cause of this error: <ul style="list-style-type: none"> Failures during decryption of the packet because of mis-comparison in the hash mac.
ceipSecTunOutAuthFails	NPU	The total number of outbound authentication's which ended in failure by this IPsec Phase-2 Tunnel.

Table B-2 IPsec Tunnel Fast Path Stats Supported by the WSG (continued)

Stats	Source	Description
ceipSecTunInDecryptFails	NPU	<p>The total number of inbound decryption's which ended in failure by this IPsec Phase-2 Tunnel.</p> <p>Possible causes of this error:</p> <ul style="list-style-type: none"> • Tunnel decryption failed due to next header mismatch in the decrypted packet • Bad IP version • Bad IP checksum • TTL expiry
ceipSecTunOutEncryptFails	NPU	<p>The total number of outbound encryption's which ended in failure by this IPsec Phase-2 Tunnel.</p> <p>Possible cause of this error:</p> <ul style="list-style-type: none"> • Badly formed IP packet getting encrypted; e.g. wrong checksum, bad IP version, etc.
ceipSecTunInReplayDropPkts	NPU	<p>The total number of packets dropped during receive processing due to Anti-Replay processing by this IPsec Phase-2 Tunnel.</p> <p>Possible cause of this error:</p> <ul style="list-style-type: none"> • Receiving packets with ESP sequence numbers within the replay window.

