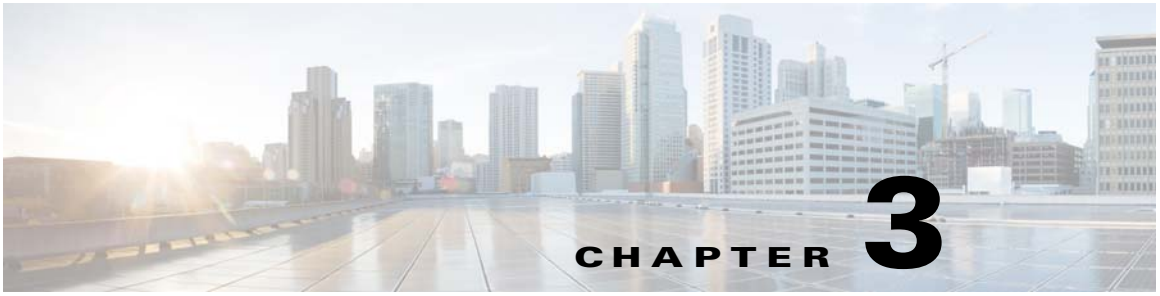

Command Reference for the WSG

The following sections provide details about WSG commands.

Commands appear in the submodes under which you enter them.

Crypto Address-Pool Submode Commands

Crypto Profile Submode Commands

EXEC Commands

Global Configuration Commands

ISAKMP/IKE Commands

Interface Submode Commands

IPSec Commands

Single OAM Commands

Resource Monitoring Commands

Show Commands

SNMP Traps Commands

Debug Commands

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

start-ip-address	First IP address in the address pool range. The format is either A.B.C.D or X:X:X::X.
end-ip-address	Last IP address in the address pool range. The format is either A.B.C.D or X:X:X::X.
netmask *netmask*	Netmask.
ipv6-prefix ***prefix***	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

ip_address	The *ip_address* is the DNS server IP address that is given to the endpoint by the WSG when requested. The *ip_address* format is either *A.B.C.D* or *X:X:X::X.*

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

vrf_name	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

vrf_name	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	**Caution** This is very destructive. Destroys all tunnels and SAs. • 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. 1. This command is supported for site-to-site profile types only. 2. 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

IP_address	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 throuhgput 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

src_file	Specifies the source file.
dst_file	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 commmand 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 specifiy 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 prompt 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

wsg_certificate	Current valid WSG certificate.
wsg_privatekey	Current valid private key corresponding to the certificate provided in the previous parameter.
modulus	Modulus of the generated certificate: 512, 1024, or 2048.
id-type	Type of ID: fqdn or ip.
id	ID can be a domain name. If ID type is ip, it can be an IPv4 or IPv6 address.
"subject_string"	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.
root_certificate	Filename of the CA root certificate (should be in DER format) present on the SUP bootflash disk.
url	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 exisiting 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

modulus	Modulus of the generated certificate: 512, 1024, or 2048.
id-type	Type of ID: fqdn or ip.
id	ID can be a domain name. If ID type is ip, it can be an IPv4 or IPv6 address.
subject_string	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.
reference-number:key	CA issued reference number and corresponding key value for CMPv2 operation.
root_certificate	Filename of the CA root certificate (should be in DER format) present on the SUP bootflash disk.
url	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

wsg_certificate	*C*urrent valid WSG certificate.
wsg_privatekey	Current valid private key corresponding to the certificate provided in the previous parameter.
root_certificate	Filename of the root certificate of the CA server (file present on SUP disk).
url	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

modulus_value	Enter the modulus value. The integer value is 1, 512, 1024, 2048, or 4096.
id-type	IKE identify of the client. The IKE identity is the identity the remote client uses when authenticating to the gateway. Valid values are: • **fqdn**—Fully-qualified domain name • **IP**—IP address
subject-name	Distinguished name (DN) that defines the entity associated with this certificate. 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: • 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 **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.

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-----
MIIBrjCCARcCAQAwNTELMAkGA1UEBhMCVVMxDTALBgNVBAsTBFNNQlUxFzAVBgNV
BAMTDnNlZ3cuY2lzY28uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCr
xsJE11PDRytSqzGH7aVi4fmf8rXygmnYCcOPvnIQybMojt5PdOBtbXREJ2r4ON6Y
gh4E+IXbIe3yig6friBFMEkYgQJuLel3P8wELDdHyWA6vBLzVgZuwa34Me8B0nKa
LMaU7kZ47sConEOElc27NBl6mI5D4rVdBnacj4/GCQIDAQABoDkwNwYJKoZIhvcN
AQkOMSowKDALBgNVHQ8EBAMCBaAwGQYDVR0RBBIwEIIOc2Vndy5jaXNjby5jb20w
DQYJKoZIhvcNAQEFBQADgYEASEqXB00k1VfguVdUf9LU4Im1+3l+hWErFp/M5Nh4
r+h5ukmCW9ldPPIZxOkV2n2wedLf6mUKTcdzdOLUiwgrSozHSfLWgpXW+upxZDgn
Nk/LvIW3+NpwnjzCmYJEZKFpWglxKzzwMAe99AOpH+Z6yhrw5ffcc9qZCcWXkeHw
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

name of user	The name of the user.
unencrypted password	The unencrypted password.
encrypted password	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

ip_address netmask	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

pool_name	Name of the IPSec address pool.
start-ip	The starting IP address.
end-ip	The ending IP address.
netmask	The IPv4 netmask or IPv6 prefix.
ip_address	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 submode.
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

filename	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

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 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.

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

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 IXP0 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

transport protocol	Transport Protocol options are *http*, and *tcp*.
http	HTTP will be used as transport Protocol for all CMPv2 messages.
tcp	TCP will be used as transport Protocol for all CMPv2 messages.
no	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

interval	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

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:

WSG(config)# **crypto datapath icmp rate-limit 1000**

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

number	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 conjuction 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

number	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 conjuction 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

ip_address	Specifies the relay agent IP address.
server-port *port number*	Specifies the server port used on the WSG.
client-port *port number*	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

X:X:X::X	Specifies the DHCP-client link IPv6 address.
server-port *port number*	Specifies the server port used on the WSG.
client-port *port number*	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

A.B.C.D	Specifies the IPv4 dhcp-server address.
X:X:X::X	Specifies the IPv6 dhcp-server address.
port_number	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)# cypto 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 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 msecs. 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 msecs. 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

value	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 **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

interval	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

```
Router(config)# crypto ike-nat-keepalive ?
  <20-3600>  Enter the packet interval in seconds (default: 0 (Disabled))
Router(config)# crypto ike-nat-keepalive 3000
```

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 nameresolver

To enable the reverse DNS lookup feature, use the **crypto nameresolver** global configuration command. Use the **no** form of the command to disable this feature.

crypto nameresolver

no crypto nameresolver

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 nameresolver ?
enable Enable the name resolver(default: disable)
WSG(config)# crypto nameresolver enable
```

This example shows how to disable the reverse DNS lookup feature:

```
WSG(config)# no crypto nameresolver
```

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

cert_filename	Name of the WSG certificate on the SUP. Ensure certificate filenames end with a .crt file extension.
private-key-filename	(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

time	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

profile-name	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

identifier-string	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

ip	The IPv4 or IPv6 address of the RADIUS server. The format is either A.B.C.D or X:X:X::X.
keyword	The secret key that is used with the RADIUS server.
auth_port_#	The authentication port that the RADIUS server uses. The integer value is in the 0 to 65535 range. The default value is 1812.
acct_port_#	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

real_IP	Real IP address.
redirect_IP	Redirect IP address.
vrf_name	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

id_type	• **dn**—Distinguished name • **ip**—IP address • **fqdn**—Fully-qualified domain name. • **email**—Email address
id	Value of id_type.
secret	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 defualt 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 defualt 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

priority	Priority of this lookup. The range is 1 to 6.
src-netmask	Source IP network mask in format N. The N subnet mask format is increased from 0-32 to 0-128 for IPv6.
dst-netmask	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

number	Message levels from the WSG. Valid values are: • **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

threshold	WSG throughput utilization in percentage
interval	Number of sustained intervals where each interval is of 5 mins.

Defaults

By default the *threshold* value is 50.

By defalt 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
```

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

vlan_ID	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

vlan_ID	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
increment_vlan_ID	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.
primary	Set the preferred-role of the node to active.
secondary	Set the preferred-role of the node to standby.
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. 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.

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

number	Assigns the VLAN to the context and accesses interface configuration mode commands for the VLAN. The *number* 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
```

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

ip_address	The starting IP address.
increment	The number of the incremental change of the IP address.
ip_address_netmask	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

A.B.C.D	Specifies the IPv4 name-server address.
X:X:X::X	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

ip_address	Specifies the IP address of the route you are adding.
subnet_mask	Specifies the subnet mask of the route.
gateway	Specifies the gateway of the route.
vrf_name	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
2hJOhwIVAPe7Tr4OTuwGoQPyQRIDXjQLTbuTAoGAXoc60iM52lFDGOZLgQm9JNWU/vV18YkeS8iCLpj2Y8zzJd0SCM
v42vtRDajFyf8I+0ahKzei8HNgmx1aRIYsHv6HrW0DtD+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

key	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
MIIBuwIBAAKBgQCecmWQsoFY8VYOCs0zEmI8VnlOMMSNxdr7RuLzhsHzTL3jhSW5bEpi9vprjC6JR774Dvr2rebP5m
tv8GhDebVEyqDFy0D1jijw6AxBd6Begu5PZy3zrHjlmxnOcGiCqM4GOW6qP1drj7aPYBxZzY9IXjFis7QXxmVCAovE
O95XtQIVAMIZuoiYMoYyLMEvvZJ91DVfz1pBAoGBAIJep7IWo1xhXByAc/iiUX0erJz0Qb64n+g5Hm3Y1Jg7mdn0BA
EBoOsZrdRHvowHp5gyufjDFztMYcWm1r07vEX0K5atuAhjacTwyH9zGuvK0HREu88UZa+M92o6JARYar5ip3luhmow
tZGnMcrLn49CZ8z0oIGzJtWclvfpOJjZAoGAY1D4CBRerptiTBHyCUPnNXfu3m7NVzSYIyxNf1pWFp+3Tp7DcqwASA
fncuvV9vXK3WuCgTle+jAFC2qdTvYJmI4At+sa8JmN9mR9Lc5Ryb2qJ/iRIWZIimZhleVLCc0wzfSMOWqFd77cm5TB
FRkNY19gI0lKNMdWi6Kk2Ce32v0CFCk5nas4jBwZ2KlHnn1ur+Kf7VKE
```

ip ssh port

To change the port used by SSH, use the **ip ssh port** global configuraion command. Use the **no** form of the command to remove this assignment.

ip ssh port *port_number*

no ip ssh port

Syntax Description

port_number	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

host_IP	IP address of the RADIUS server.
key_str	Shared key to authenticate with the RADIUS server.
port_number	Port number to be used with the RADIUS server. Default is port 1812.
timeout_number	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.
ipv6_prefix	Specifies the IPv6 prefix.
ipv6_gateway	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

vrf_name	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

A.B.C.D	Specifies the IPv4 address of the external logging server.
X:X:X::X	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

local-asn	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

ip_address	Specifies the IPv4 or IPv6 address of a neighboring BGP peer. Each address should be a unique identifier of a neighboring BGP peer.
remote_asn	Specifies the remote Autonomous System (AS) number of the BGP peer. The range is from 1 to 65535.
next_ip_address	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

timeout	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 *timeout* 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 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

id-type	IKE identify. The IKE identity is the identity sent to the remote client during IKE negotiation. Valid values are: • **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.
id	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

This example shows how to set the shared key name to ***foo***:

```
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
```

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	**1**—IKE version 1 **2**—IKE version 2 **both**—IKE version 1 and IKE version 2, use this if you are not sure which IKE version the client is using.

Defaults

2

Command Modes

ISAKMP submode

Command History

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 submode

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.
address-pool-name	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

ip-address	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	Specifies the lifetime in megabytes. The minimum value is 4500MB. The default value is 36000MB.
seconds	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

ip-address	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.
subnet	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.
rule-name	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.
src_ip src_prefix	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.
start_src_port *end_src_port*	Applies only to site-to-site. The start and end source port numbers. The range is 0 to 65535.
dst_ip dst_prefix	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.
start_dst_port *end_dst_port*	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. • rule-name • **protocol** *protocol* • **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*
WSG Release 2.0	The following keywords and arguments were changed for site-to-site scalability improvements: • **src-ip** *src ip/subnet mask* • **dst-ip** *dst ip/subnet mask*
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 3-108
aes-xcbc | md5 | sha1	See hash, page 3-110 **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	This command was introduced.
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

vlan_number	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

ip_address	Specifies the IP address of the route you are adding.
subnet_mask	Specifies the subnet mask of the route.
gateway	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 *percentage* **interval** *seconds*	Establishes the rising percentage threshold values. Threshold values: minimum 1% to maximum 100%. Threshold interval: 5 – 86400 seconds.
falling *percentage* **interval** *seconds*	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

threshold	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 to1996000KB.

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-sha1
Pfs Group:              Disabled
Sa lifetime:             25200 seconds
Sa anti-replay:        enable, Window 32

Displayed Information for Profile: remote-access
Transform:              esp-aes128-sha1
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-sha1
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
```

```
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
    Reassmebly                  : 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.
```

```
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 Indicies
  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                              Algorithms
          SPI In   SPI Out       Cipher              MAC              Compress
     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  0dddcc17  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 Indicies
  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
```

```
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

inbound_spi	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 Indicies
  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
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
```

```
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.
```

```
WSG# show crypto isakmp sa
 SA Id   P1   IKE  Child                    Algorithm              Remote Auth    Tunnel Type VRF Name
        Done  Ver   SAs       Encryption         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             : ixia1@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             : ixia1@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=OPENSSL 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) :
        121054359480332403507696797060899211115094278449071726077845077554967777
        332906426740061806436002665696605487771010383390326785995002429864261800
        524962381734692622284280954969316815491751355079186302378761566622982690
        603210216517385911237186249958522791616057940332504915631967822069458210
        621182426944312822520428 7
      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 timeouted         : 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.

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
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 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
```

```
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

interval	Duration of history of throughput. Valid values are: • **1** - 5minutes • **2** - 1hour • **3** - 3hours
type	Type of unit value to display the throughput. Valid values are: – 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
```

```
.... ....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
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 #
```

```
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
Icmp6InDestUnreachs                     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
Icmp6OutDestUnreachs                    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

number	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
   iftype:         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

number	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

Command History

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

vrf_name	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 tunl0 sit0 ip6tnl0 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** [|] [**>**] | **message** {**all cpuid** *cpu-id* | **module** *mod-id*}}

Syntax Description

config	Displays syslog configuration.
message	Displays syslog messages.
cpu-id	Displays syslog messages for a specific CPU id.
mod-id	Displays sysog 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**]

no snmp-server enable traps ipsec [**address-pool-exhaust | too-many-sas | tunnel** {**start | stop**} | **cert-expiry | cert-renewal | throughput-threshold**]

Syntax Description

snmp-server enable traps ipsec	Enable all SNMP IPSec 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.
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

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** keywords were added.

Usage Guidelines

Use the **snmp-server enable traps ipsec** command to enable SNMP IPSec 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

A.B.C.D	Specifies the IPv4 address of the SNMP server host.
X:X:X::X	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

ip_address	Remote peer IPv4 or IPv6 address.
netmask	Remote IPv4 network subnet.
prefix	Remote IPv6 network prefix.
vrf_name	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 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
```