WSG Service Configuration Mode Commands

Command Modes

The Wireless Security Gateway Configuration Mode is used to define the operating parameters for IPSec-based access control and handling of Encapsulating Security Payload (ESP) packets.

Exec > Global Configuration > Context Configuration > WSG-Service Configuration

configure > context *context_name* **> wsg-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-wsg-service)#
```

☞

Important

The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

☞

Important

Any changes made to a WSG service require that the service be restarted to apply any changed parameters. You restart the service by unbinding and binding the IP address to the service context.

associate subscriber-map

Binds the WSG service to the specified IPv4 or IPv6 address and crypto template (VPC only).

Product	SecGW (WSG)
Privilege	Security Administrator
Command Modes	Exec > Global Configuration > Context Configuration > WSG-Service Configuration
	configure > context *context_name* **> wsg-service** *service_name*
	Entering the above command sequence results in the following prompt:
	`[context_name]host_name(config-wsg-service)#`
Syntax Description	**associate subscriber-map** *subscriber_map_name*

subscriber_map_name

Specifies the name of an subscriber map as an alphanumeric string of 0 through 127 characters.

Usage Guidelines	Associates the WSG service to Subscriber Map.

Example

The following command associates SecGW to subscriber map1.

associate subscriber-map *subscriber_map1*

bind address

Binds the WSG service to the specified IPv4 or IPv6 address and crypto template (VPC only).

Product	SecGW (WSG)
Privilege	Security Administrator
Command Modes	Exec > Global Configuration > Context Configuration > WSG-Service Configuration
	configure > context *context_name* **> wsg-service** *service_name*
	Entering the above command sequence results in the following prompt:
	`[context_name]host_name(config-wsg-service)#`
Syntax Description	**bind address** *IPv4 / IPv6* **crypto-template** *template_name* | **Secure-tunnel** [**Max-sessions** *sessions*] **no bind address**

no

Unbinds the WSG service from the IP address.

IPv4 / IPv6

IPV4 ##.##.##.## or IPV6 ####:####:####:####:####:####:####:#### (IPV6 also supports :: notation).

template_name

Specifies the name of an existing crypto template as an alphanumeric string of 0 through 127 characters.

Usage Guidelines Bind the WSG service to an IPv4 or IPv6 address.

Example

The following command binds the WSG service to 10.1.1.1.

```
bind address 10.1.1.1 crypto template tplt01
```

deployment-mode

Specifies the deployment mode for the WSG service (VPC only).

Product	SecGW (WSG)
Privilege	Security Administrator
Command Modes	Exec > Global Configuration > Context Configuration > WSG-Service Configuration

configure > context *context_name* **> wsg-service** *service_name*

Entering the above command sequence results in the following prompt:

[*context_name*]*host_name*(config-wsg-service)#

Syntax Description
```
deployment-mode { remote-access | site-to-site }
no deployment-mode
```

no

Deletes deployment mode from the configuration.

{ remote-access | site-to-site }

Specifies the deployment mode as either:

- **remote-access** – support direct user communication with this WSG

- **site-to-site** – support bidirectional communication with two or more WSGs

Usage Guidelines Specify remote access or site-to-site communication as the deployment mode for this WSG.

Example

This command deploys this WSG for remote access:

deployment-mode remote-access

dhcp

Specifies the DHCPv4 context and service name to be used when the IP address allocation method is set **dhcp-proxy** (VPC only).

Product	SecGW (WSG)
Privilege	Security Administrator
Command Modes	Exec > Global Configuration > Context Configuration > WSG-Service Configuration
	configure > context *context_name* **> wsg-service** *service_name*
	Entering the above command sequence results in the following prompt:
	[*context_name*]*host_name*(config-wsg-service)#
Syntax Description	**dhcp { context-name** *context_name* **| service-name** *service_name* **}** **no dhcp { context-name	service-name }**

no

Deletes the specified parameter.

context-name *context_name*

Specifies the context in which the DHCPv4 service is configured as an alphanumeric string of 1 through 79 characters.

service-name *service_name*

Specifies which DHCPv4 service to use for the **dhcp-proxy** as an alphanumeric string of one through 63 characters. Only one DHCPv4 service can be configured as the **dhcp-proxy**.

Usage Guidelines	Specifies the DHCPv4 context and service name to be used when the IP address allocation method is set to **dhcp-proxy**. The specified DHCPv4 service is designated via the **ip address alloc-method dhcp-proxy** command.

The WSG service must be restarted to apply the parameters. You restart the service by doing an unbind and bind.

Example

The following command sequence enables a DHCPv4 service as an allocation method for IP addresses:

```
dhcp context-name wsg01
dhcp service-name dhcp1
```

dns-server

Enables the WSG service (SecGW) to send the IP Address of the DNS server to the peer. A new request will overwrite the existing entries.

Product	SecGW (WSG service)
Privilege	Security Administrator
Command Modes	Exec > Global Configuration > Context Configuration > WSG-Service Configuration

configure > context *context_name* **> wsg-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-wsg-service)#
```

Syntax Description
```
dns-server primary ip_address [ secondary ip_address ]
no dns-server primary ip_address
```

no

Disables sending the primary IP address of the DNS server.

primary *ip_address*

Specifies the IP Address, in IPv4 dotted-decimal or IPv6 colon-separated hexadecimal notation, of the primary DNS server to be sent to the peer.

secondary *ip_address*

Specifies the IP Address, in IPv4 dotted-decimal or IPv6 colon-separated hexadecimal notation, of the secondary DNS server to be sent to the peer.

Usage Guidelines Use this command to configure an IPv4 or IPv6 address of a DNS server. The same CLI can be configured twice with different IP address type. However, both primary and secondary IP address should be of the same type (IPv4 or IPv6) for a CLI.

A new request will overwrite the existing entries of the same IP address type.

Example

The following command enables the WSG service to send the IPv4 address of the primary DNS server to the peer:

```
dns-server primary 10.1.1.1 secondary 10.1.1.2
```

do show

Executes all **show** commands while in Configuration mode.

Product	All
Privilege	Security Administrator, Administrator
Syntax Description	```do show```
Usage Guidelines	Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command. The pipe character **|** is only available if the command is valid in the Exec mode.

⚠️

Caution   There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

duplicate-session-detection

Enables or disables allowing only one IKE-SA per remote IKE-ID. A new request will overwrite the existing tunnel.

Product	SecGW (WSG service)
Privilege	Security Administrator
Command Modes	Exec > Global Configuration > Context Configuration > WSG-Service Configuration **configure > context** *context_name* **> wsg-service** *service_name* Entering the above command sequence results in the following prompt: [*context_name*]*host_name*(config-wsg-service)#

Syntax Description	```duplicate-session-detection```
	```no duplicate-session-detection```
	
	no
	
	Disables duplicate session detection and allows multiple IKE-SAs per remote IKE-ID. This is the default behavior.

Usage Guidelines	Enables or disables allowing only one IKE-SA per remote IKE-ID. A new request will overwrite the existing tunnel. For a complete description of this feature, refer to the *IPSec Reference*.

Example

The following command enables duplicate session detection:

duplicate-session-detection

end

Exits the current configuration mode and returns to the Exec mode.

Product	All
Privilege	Security Administrator, Administrator
Syntax Description	**end**
Usage Guidelines	Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product	All
Privilege	Security Administrator, Administrator
Syntax Description	**exit**
Usage Guidelines	Use this command to return to the parent configuration mode.

initiator-mode-duration

Specifies the interval during which the WSG service (SecGW) will try to initiate a call with an IKE peer. A peer list must be configured in this WSG service for this command to be available (VPC only).

Product	SecGW (WSG)
Privilege	Security Administrator, Administrator
Command Modes	Exec > Global Configuration > Context Configuration > WSG-Service Configuration
	configure > context *context_name* **> wsg-service** *service_name*
	Entering the above command sequence results in the following prompt:
	[*context_name*]*host_name*(config-wsg-service)#

Syntax Description	**initiator-mode-duration** *seconds* **default initiator-mode-duration**

default

Sets the initiator mode duration to 10 seconds.

seconds

Specifies the duration interval in seconds as an integer from 5 through 250.

Usage Guidelines	Use this command to specify the interval during which the WSG service (SecGW) will try to initiate an IKE call when a peer list is activated (default is 10 seconds). This command is only available when a peer-list has been configured for the WSG service. See the *IPSec Reference* for additional information on configuring an SecGW as an IKE initiator.

Example

The following command sets the initiator mode duration to 15 seconds:

initiator-mode-duration 15

ip

Specifies the IPv4 access group and address allocation method for this WSG service (VPC only).

Product	SecGW (WSG)
Privilege	Security Administrator
Command Modes	Exec > Global Configuration > Context Configuration > WSG-Service Configuration **configure > context** *context_name* **> wsg-service** *service_name* Entering the above command sequence results in the following prompt: [*context_name*]*host_name*(config-wsg-service)#
Syntax Description	**ip { access-group** *group_name* **| address { alloc-method { dhcp-proxy	local }	pool name** *pool_name* **}** **no ip access-group** *group_name* **no ip address alloc-method** *pool_name* **no ip address pool name** *pool_name*

no

Deletes the specified parameter.

access-group *group_name*

Specifies an existing IPv4 ACL access group as an alphanumeric string of 1 through 47 characters. For additional information, see *ACL Configuration Mode Commands*.

address alloc-method { dhcp-proxy | local }

Specifies the method to be used when allocating IPv4 addresses:

- **dhcp-proxy** – allocates via a DHCP server
- **local** – allocates from a local pool (default)

pool name *pool_name*

Specifies an existing IPv4 access pool as an alphanumeric string of 1 through 31 characters. Up to 16 named IPv4 pools can be configured. For additional information, see *APN Configuration Mode Commands*.

Usage Guidelines	Use this command to specify the IPv4 access group and IPv4 address allocation method for this WSG service.

This command and its keywords are subject to the following limitations:

- The WSG service configuration takes precedence over the equivalent configuration in Subscriber mode or the template payload.

- The WSG service must be restarted to apply the parameters. You restart the service by doing an unbind and bind.

- Up to 16 named IPv4 pools can be configured. The list is sorted, and the addresses are allocated from the first pool in the list with available addresses.

- One IPv4 ACL can be configured.

- The IPv4 pools will only be used for IPv4 calls.

Example

This command specifies the IPv4 address pool named *pool401*:

```
ip address pool name pool401
```

This command specifies the use of a previously configure DHCPv4 service to allocate IPv4 addresses:

```
ip address alloc-method dhcp-proxy
```

ipv6

Specifies the IPv6 access group and prefix pool for this WSG service (VPC only).

Product	SecGW (WSG)
Privilege	Security Administrator
Command Modes	Exec > Global Configuration > Context Configuration > WSG-Service Configuration

WSG Service Configuration Mode Commands

peer-list

configure > context *context_name* **> wsg-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-wsg-service)#
```

Syntax Description

```
ipv6 { access-group group_name | address prefix-pool pool_name }
no ipv6 access-group group_name
no ipv6 address prefix-pool
```

no

Deletes the specified parameter.

access-group _group_name_

Specifies an existing IPv6 ACL access group as an alphanumeric string of 1 through 47 characters. For additional information, see *IPv6 ACL Configuration Mode Commands*.

address prefix-pool _pool_name_

Specifies an existing IPv6 prefix pool as an alphanumeric string of 1 through 31 characters. For additional information, see *Subscriber Configuration Mode Commands*.

Usage Guidelines

Specify the IPv6 access group and prefix pool for this WSG service.

This command and its keywords are subject to the following limitations:

- The WSG service configuration takes precedence over the equivalent configuration in Subscriber mode or the template payload.

- The WSG service must be restarted to apply the parameters. You restart the service by doing an unbind and bind.

- One named IPv6 pool can be configured.

- One named IPv6 ACL can be configured.

- The IPv6 pools will only be used for IPv6 calls.

Example

This command specifies the IPv6 prefix pool named pool601:

```
ipv6 prefix-pool name pool601
```

peer-list

Configures an SecGW to initiate an IKEv2 session setup request when the peer does not initiate a setup request within a specified time interval. This command is only available for a WSG service configured for site-to-site (S2S) deployment mode (VPC only).

Product

SecGW (WSG)

WSG Service Configuration Mode Commands

10

Privilege	Security Administrator, Administrator
Command Modes	Exec > Global Configuration > Context Configuration > WSG-Service Configuration
	configure > context *context_name* **> wsg-service** *service_name*
	Entering the above command sequence results in the following prompt:
	`[context_name]host_name(config-wsg-service)#`
Syntax Description	**peer-list** *peer_list_name* **no peer-list**

no

Disables the current peer list and SecGW as an IKE initiator functionality.

peer_list_name

Specifies the name of an existing peer list as an alphanumeric string of 1 through 79 characters. The crypto peer list must have been previously created using the Global Configuration mode **crypto peer-list** command.

Usage Guidelines	Enables the use of a peer list so that the SecGW can act as an initiator of an IKEv2 call session. The WSG service deployment mode must be configured as site-to-site for the **peer-list** command to execute.

The following limitations apply when the SecGW as initiator feature is enabled:

- The SecGW will only support up to 1,000 peers. This restriction is applied when configuring a crypto peer list.
- SecGW will not support the modification of an IPv4/IPv6 peer list on the fly (call sessions in progress). The modification will be allowed only after all the calls are removed.

When a peer list has been configured in the WSG service, the initiator and responder mode timer intervals each default to 10 seconds. The SecGW will wait for 10 seconds in the responder mode for a peer session initiation request before switching to the initiator mode and waiting 10 seconds for a peer response.

You can change the default settings for the initiator and/or responder mode intervals using the WSG Service mode **initiator-mode-duration** and **responder-mode-duration** commands.

See the *IPSec Reference* for additional information on configuring an SecGW as an IKE initiator.

Example

The following command enables the user of a peer list named *peer1*.

peer-list peer1

pre_fragment mtu

Specifies the Maximum Transmission Unit (MTU) size which when exceeded initiates pre-tunnel (before encryption) fragmentation of IPSec Encapsulated Security Payload (ESP) packets within this WSG service (VPC only).

Product	SecGW (WSG)

Privilege	Security Administrator
Command Modes	Exec > Global Configuration > Context Configuration > WSG-Service Configuration
	configure > context *context_name* **> wsg-service** *service_name*
	Entering the above command sequence results in the following prompt:
	`[`*context_name*`]`*host_name*`(config-wsg-service)#`
Syntax Description	`pre_fragment mtu` *size* `no pre_fragment` *size* `default pre_fragment` *size*

no

Disables this function.

default

Sets the MTU size to the default value of 1400 bytes.

mtu *size*

Specifies the MTU size in bytes as an integer from 576 through 2048. Default = 1400

Usage Guidelines	Specify the MTU size which when exceeded initiates pre-tunnel fragmentation of IPSec ESP packets within this WSG service.

Pre-Tunnel-Fragmentation improves packet processing performance as compared to post-tunnel-fragmentation.

If a clear IPv4 packet is longer than the predefined MTU size, it will be fragmented before the packet is encrypted and transmitted to internet.

If a clear IPv6 packet is longer than the predefined MTU size, it is dropped and an ICMP packet with the maximum length is sent back to the source. The source will then fragment the IPv6 packet and retransmit.

Example

The following command sets MTU size to 2048 bytes.

`pre_fragment mtu 2048`

responder-mode-duration

Specifies the interval during which the WSG service (SecGW) will wait for a response from an IKE peer before switching to initiator mode. A peer list must be configured in this WSG service for this command to be available (VPC only).

Product	SecGW (WSG)
Privilege	Security Administrator, Administrator

Command Modes	Exec > Global Configuration > Context Configuration > WSG-Service Configuration
	configure > context *context_name* **> wsg-service** *service_name*
	Entering the above command sequence results in the following prompt:
	[*context_name*]*host_name*(config-wsg-service)#
Syntax Description	**responder-mode-duration** *seconds* **default responder-mode-duration**

default

Sets the responder mode duration to 10 seconds.

seconds

Specifies the duration interval in seconds as an integer from 5 through 250.

Usage Guidelines	Use this command to specify the interval during which the WSG service (SecGW) will wait or a response from an IKE peer before switching to initiator mode (default is 10 seconds).
	This command is only available when a peer-list has been configured for the WSG service.
	See the *IPSec Reference* for additional information on configuring an SecGW as an IKE initiator.

Example

The following command sets the responder mode duration to 15 seconds:

responder-mode-duration 15

Server dhcp

Specifies the dhcp server addresses to be sent to the peer in authentication response.

Product	SecGW (WSG)
Privilege	Security Administrator
Command Modes	Exec > Global Configuration > Context Configuration > WSG-Service Configuration
	configure > context *context_name* **> wsg-service** *service_name*
	Entering the above command sequence results in the following prompt:
	[*context_name*]*host_name*(config-wsg-service)#
Syntax Description	**server dhcp { ipv4** *ipv4_address* **[IP-ADDRESS	IP-ADDRESS]	ipv6** *ipv6_address* **[IPv6-ADDRESS	IPv6-ADDRESS] }** **no server dhcp { ipv4 [ipv6]	ipv6 [ipv4] }**

no

Deletes the specified parameter.

ipv4_address

Specifies the ipv4 address of the dhcp-server to be sent to the peer. The IPV4 address should be in the format ##.##.##.## which is the first ipv4 dhcp-server's address.

IP-ADDRESS

Specifies ipv4 address of the dhcp-server to be sent to the peer.

ipv6_address

Specifies the ipv6 address of the dhcp-server to be sent to the peer. The IPV6 address should be in the format ####:####:####:####:####:####:####:#### (IPv6 also supports :: notation).

IPv6-ADDRESS

Specifies ipv6 address of the dhcp-server to be sent to the peer.

Usage Guidelines   This command specifies the dhcp server addresses to be sent to the peer in authentication response

Example

The following command specifies the dhcp server ipv4 addresses to be sent to the peer in authentication response:

```
server dhcp ipv4 209.165.200.242
```