SecGW Administration Guide, StarOS Release 21.17

First Published: 2019-12-19

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

About this Guide

This preface defines the Security Gateway, the organization of this guide and its document conventions.

Cisco Virtualized Packet Core Distributed Instance (VPC-DI) consists of a fully distributed network of multiple virtual machines (VMs) Grouped to form a single StarOS instance, with VMs performing management, input/output (I/O), and packet processing. The VMs run on commercial off-the-shelf (COTS) servers. This Guide describes how to configure and administer the various components of the VPC-DI instance.

To complete the SecGW configuration process you must also have at hand the following user documentation:

- *VPC-DI System Administration Guide*
- *IPSec Reference*

Conventions Used

The following tables describe the conventions used throughout this documentation.

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

Typeface Conventions	Description
Text represented as a `screen display`	This typeface represents displays that appear on your terminal screen, for example: `Login:`

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

Documents and Resources

Related Common Documentation

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

The following user documents are available:

- CommandLine InterfaceReference
- IPSec Reference
- AAA InterfaceAdministrationand Reference
- GTPPInterfaceAdministrationand Reference
- ReleaseChangeReference
- SNMP MIB Reference
- Statistics and Counters Reference
- Thresholding Configuration Guide
- Product-specificand feature-specificAdministrationguides

Obtaining Cisco VPC-DI Documentation

The most current Cisco documentation is available on the following website:

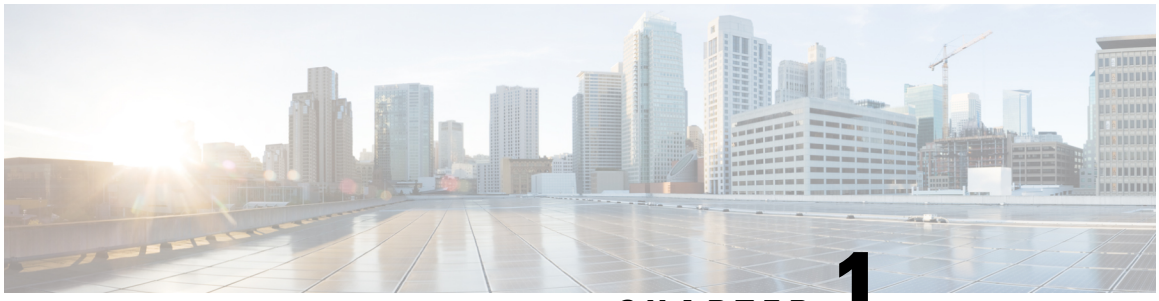
http://www.cisco.com/cisco/web/psa/default.html

Use the following path selectios to access the VPC-DI docuemntation.

Contacting Customer Support

Use the information in this section to contact customer support.

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



CHAPTER 1

Security Gateway Overview

This chapter contains general overview information about the Security Gateway (SecGW) running on an VPC-DI Virtualized Service Module (VSM) as a VPC-VSM instance.

The following topics are covered in this chapter:

Product Overview

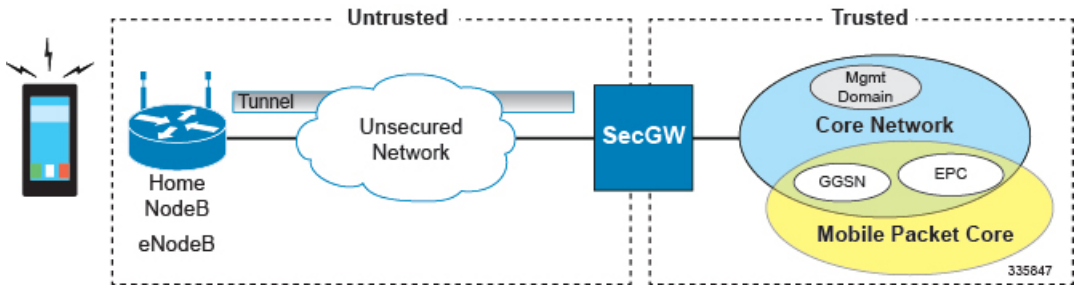
The SecGW is a high-density IP Security (IPSec) gateway for mobile wireless carrier networks. It is typically used to secure backhaul traffic between the Radio Access Network (RAN) and the operator core network.

IPSec is an open standards set that provides confidentiality, integrity, and authentication for data between IP layer peers. The SecGW uses IPSec-protected tunnels to connect outside endpoints. SecGW implements the parts of IKE/IPSec required for its role in mobile networks.

The following types of LTE traffic may be carried over encrypted IPSec tunnels in the Un-trusted access domain:

- S1-C and S1-U: Control and User Traffic between eNodeB and EPC
- X2-C and X2-U: Control and User Traffic between eNodeBs during Handoff
- SPs typically carry only Control Traffic, however there exists a case for carrying non-Internet User traffic over secured tunnels

Figure 1: SecGW Implementation



SecGW Application

The StarOS-based Security Gateway (SecGW) application is a solution for Remote-Access (RAS) and Site-to-Site (S2S) mobile network environments. It is implemented via StarOS as a WSG (Wireless Security Gateway) service that leverages the IPSec features supported by StarOS.

For complete descriptions of supported IPSec features, see the *IPSec Reference*.

IPSec Capabilities

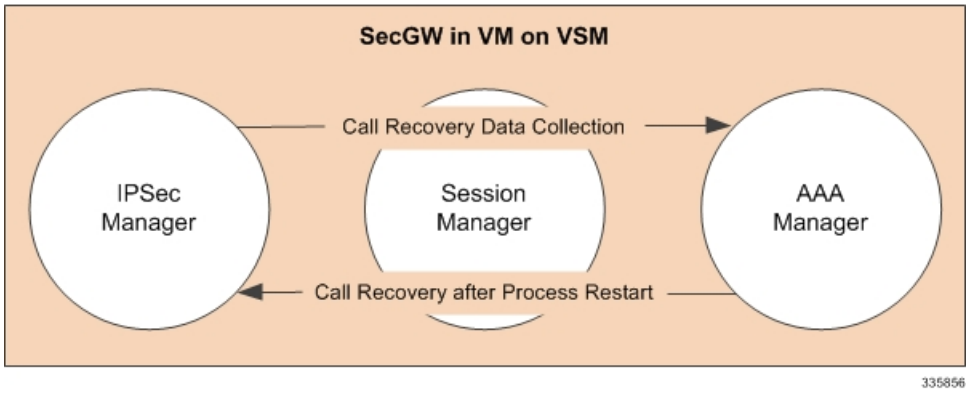
The following IPSec features are supported by StarOS for implementation in an SecGW application:

- Anti Replay
- Certificate Management Protocol (CMPv2)
- Session Recovery
- Support for IKE ID Type
- PSK support with up to 255 octets
- Online Certificate Status Protocol (OCSP)
- Blacklist/Whitelist by IDi
- Rekey Traffic Overlap
- CRL fetching with LDAPv3
- Sequence Number based Rekey
- PSK Support for up to 1000 Remote Secrets
- Certificate Chaining
- RFC 5996 Compliance
- Duplicate Session Detection
- Extended Sequence Number
- Support to provide DNS server address to the Peer

Process Recovery

The process recovery feature stores backup Security Association (SA) data in an AAA manager task. This manager runs on the SecGW where the recoverable tasks are located.

Figure 2: Process Recovery Diagram



Network Deployment

SecGW supports the following network deployment scenarios:

- Remote Access Tunnels, on page 3

Remote Access Tunnels

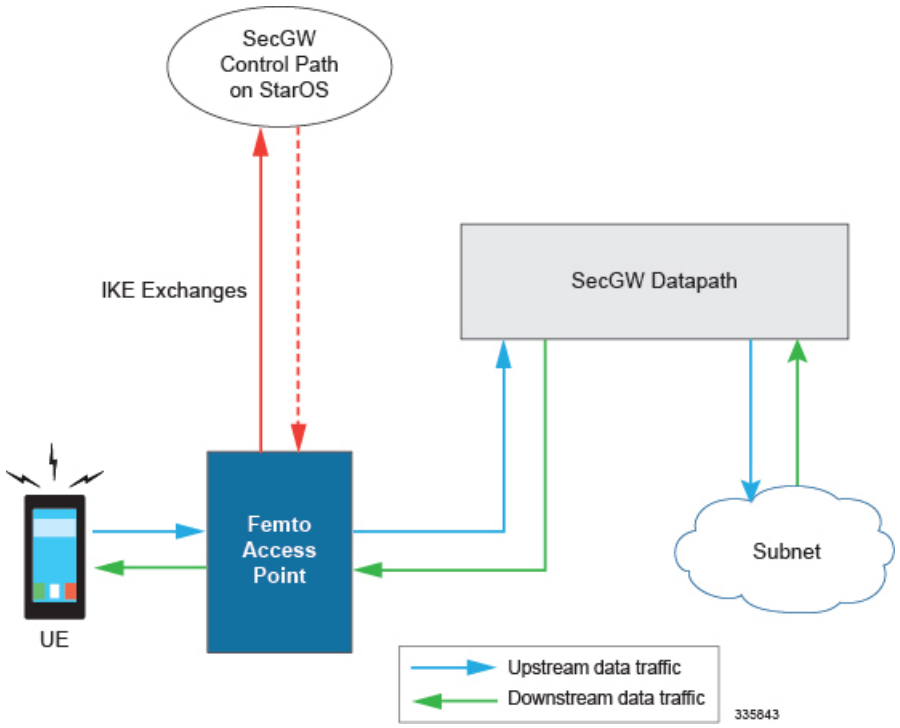
In a RAS scenario, a remote host negotiates a child SA with the SecGW and sends traffic inside the child SA that belongs to a single IP address inside the remote host. This is the inner IP address of the child SA. The outer IP address is the public IP address of the remote host. The addresses on the trusted network behind the SecGW to which the host talks could be a single IP or a network.

Figure 3: RAS Tunnel

Packet Flow

The figures below indicate traffic packet flows to and from the SecGW.

Figure 4: SecGW Packet Flow – RAS



Standards

Compliant

- RFC 1853 – IP in IP Tunneling
- RFC 2401 – Security Architecture for the Internet Protocol
- RFC 2402 – IP Authentication Header
- RFC 2406 – IP Encapsulating Security Payload (ESP)
- RFC 2407 – The Internet IP Security Domain of Interpretation for ISAKMP
- RFC 2408 – Internet Security Association and Key Management Protocol (ISAKMP)
- RFC 2409 – The Internet Key Exchange (IKE)
- RFC 3280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- RFC 3554 – On the Use of Stream Control Transmission Protocol (SCTP) with IPsec [Partially compliant, ID_LIST is not supported.]
- RFC 4210 – Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)
- RFC 4306 – Internet Key Exchange (IKEv2) Protocol

- RFC 4718 – IKEv2 Clarifications and Implementation Guidelines
- RFC 5996 – Internet Key Exchange Protocol Version 2 (IKEv2)
- Hashed Message Authentication Codes:
  - AES 96
  - MD5
  - SHA1/SHA2
- X.509 Certificate Support – maximum key size = 2048

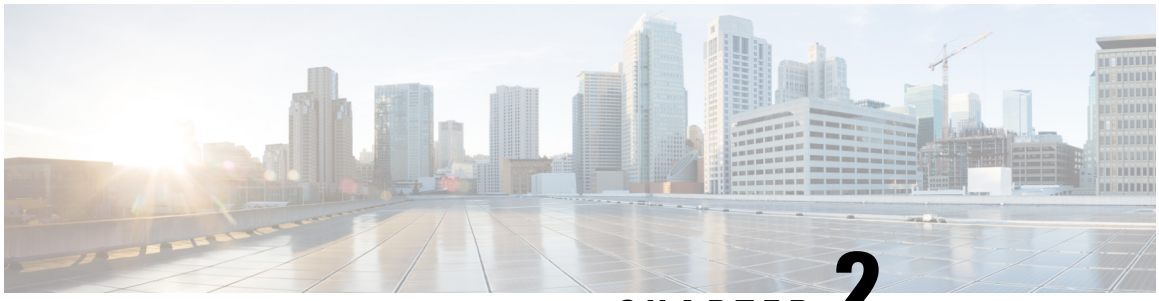
Supported Algorithms

SecGW supports the protocols in the table below, which are specified in RFC 5996.

Table 1: Supported Algorithms

Protocol	Type	Supported Options
Internet Key Exchange version 2	IKEv2 Encryption	DES-CBC, 3DES-CBC, AES-CBC-128, AES-CBC-256
	IKEv2 Pseudo Random Function	PRF-HMAC-SHA1, PRF-HMAC-MD5, AES-XCBC-PRF-128
	IKEv2 Integrity	HMAC-SHA1-96, HMAC-SHA2-256-128, HMAC-SHA2-384-192. HMAC-SHA2-512-256, HMAC-MD5-96, AES-XCBC-96
	IKEv2 Diffie-Hellman Group	Group 1 (768-bit), Group 2 (1024-bit), Group 5 (1536-bit), Group 14 (2048-bit)

Protocol	Type	Supported Options
IP Security	IPSec Encapsulating Security Payload Encryption	NULL, DES-CBC, 3DES-CBC, AES-CBC-128, AES-CBC-256, AES-128-GCM-128, AES-128-GCM-64, AES-128-GCM-96, AES-256-GCM-128, AES-256-GCM-64, AES-256-GCM-96 **Note** AES-GCM algorithms are supported only on vPC-DI and vPC-SI Platform.
	Extended Sequence Number	Value of 0 or off is supported (ESN itself is not supported)
	IPSec Integrity	NULL, HMAC-SHA1-96, HMAC-MD5-96, AES-XCBC-96, HMAC-SHA2-256-128, HMAC-SHA2-384-192, HMAC-SHA2-512-256 **Important** HMAC-SHA2-384-192 and HMAC-SHA2-512-256 are not supported on vPC-DI and vPC-SI platforms if the hardware doesn't have crypto hardware.



CHAPTER 2

Pre-Tunnel Fragmentation

SecGW supports post-tunnel fragmentation for IPsec ESP data packets. If an encrypted packet exceeds an interface MTU size the packet is fragmented. Post-tunnel fragmentation can cause performance degradation and pre-tunnel fragmentation has better packet processing rate.

The following sections provide more detailed information:

Pre-Tunnel fragmentation at VPC-DI

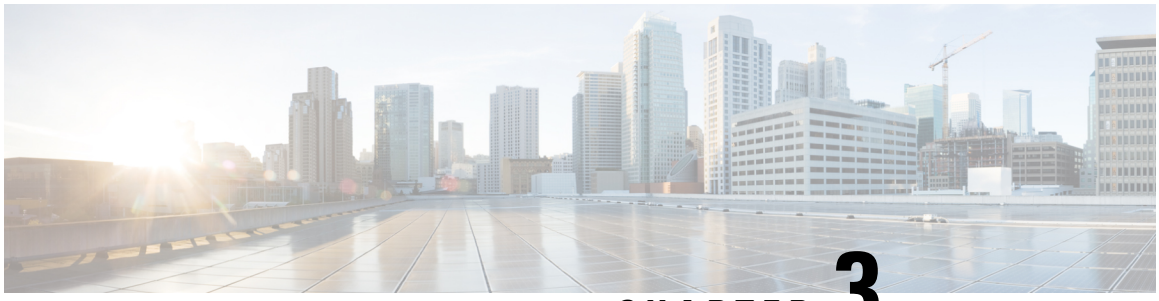
The pre tunnel fragmentation feature and its maximal MTU size will be defined under WSG service. This MTU size is stored with other WSG service parameters. During IPsec SA creation, the MTU is passed to crypto driver subsystem. The crypto driver will calculate the crypto overhead to determine the effective MTU size for plaintext based on given MTU size and SA information. When crypto driver receives a packet for encryption and packet length is longer than effective MTU, the packet will be fragmented before deliver to crypto chip.

MTU range is between intiger 576 to 2048, default is 1400.

Configuring IPsec Pre tunnel fragmentation

Use the below configuration to configure Pre-tunnel Fragmentation:

```
   config
      context context_name
        pre_fragment mtu mtu_size
        [ default | no ] pre_fragment
exit
```



CHAPTER 3

Config Payload extension for DHCP Address

This feature when implemented supports INTERNAL_IP4_DHCP, INTERNAL_IP6_DHCP as part of Configuration Attributes in Auth payloads. This instructs the host to send any internal DHCP requests to the address contained within the attribute. Multiple DHCP servers may be requested. SecGW may respond with zero or more DHCP server addresses.

• Config Payload Extension for DHCP Address Configuration, on page 9

Config Payload Extension for DHCP Address Configuration

Assumptions and Limitations

- In current release only 3 dhcp addresses per INTERNAL_IP4_DHCP or INTERNAL_IP6_DHCP requests will be supported.
- The DHCP addresses will be configured as part of wsg-service. 3 ipv4 and 3 ipv6 dhcp server addresses will be allowed per service.

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 123.234.345.567
```

Config Payload extension for DHCP Address Support Show Command Outputs

As part of " Config Payload extension for DHCP Address " feature below show commands output are introduced:

Show wsg-Service all Server:

- DHCP: ipv4 : <##.##.##.## > or NA(if not configured)

  <##.##.##.## >

  <##.##.##.## >

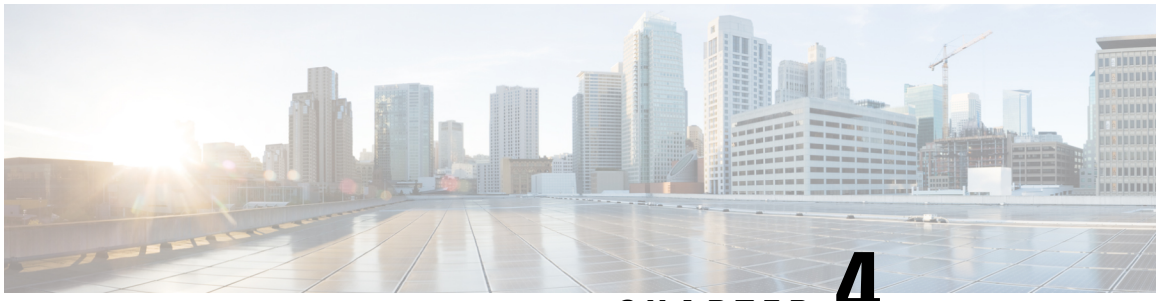
- ipv6 : < #:#:#:#:#:#:#:#> or NA(if not configured)

  <##.##.##.## >

  <##.##.##.## >

Show Configuration:

- server dhcp ipv4 <v4 address> <v4 address> <v4 address> <cr>
- server dhcp ipv6 <v6 address> <v6 address> <v6 address> <cr>



CHAPTER 4

SecGW TLS Support

This feature enables Secure Socket Layer (SSL) based connection endpoints in SecGW. Earlier only IKE/IPSEC based connection endpoints were supported in SecGW.

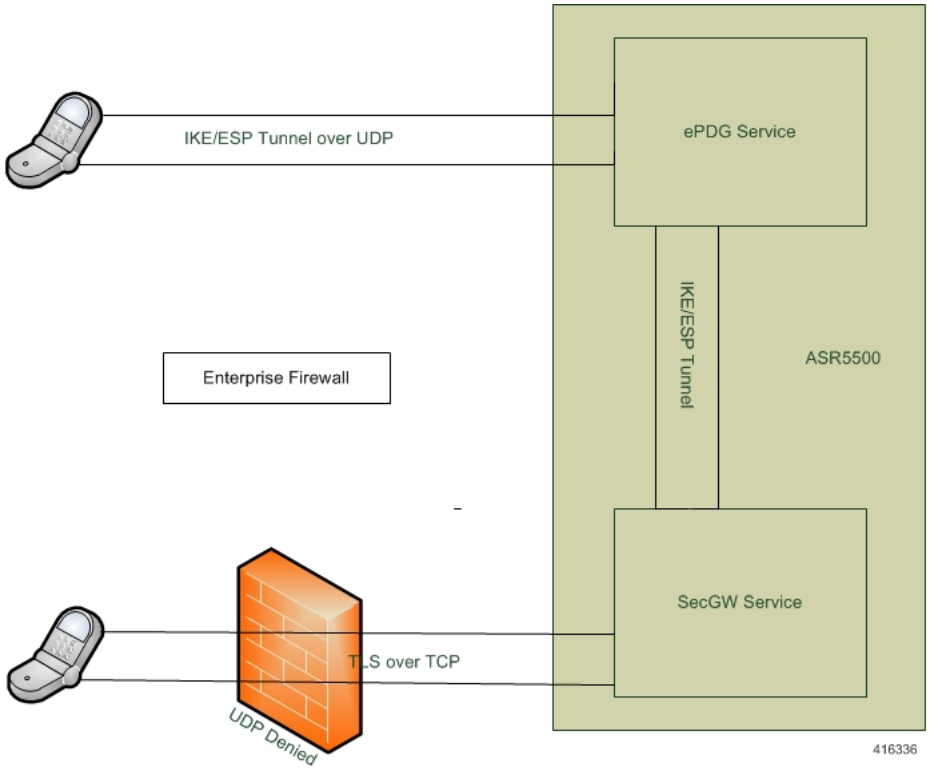
This support is added to facilitate UE in the enterprise networks to connect with security where the IKEv2 UDP ports are blocked and only TCP based connections are permitted.

SecGW TLS Support

SecGW TLS support enables peer devices to connect securely to SecGw using TLS/TCP based connections. The application data which is received on the TLS/TCP is IKE/ESP data which will be IP/UDP encapsulated and forwarded to local ePDG service. This will help UE penetrate enterprise firewalls while connecting to ePDG.

SecGW TLS Support

Figure 5: ***SecGW accessesing ePDG using TLS over TCP***



Assumptions and Limitations

- Only TLS/TCP data can be IP/UDP encapsulated and forwarded to local ePDG service
- It is possible that UE can send the IKE/ESP over SSL as application data
- IKE protocol is UDP encapsulated. But for this feature the IKE/ESP should be part for SSL data which is TCP based connection
- Ports supported for TLS/TCP connection is configurable in wsg-service
- TLS/TPC should be used as a fallback only when UDP is blocked in the firewall
- From SecGW point of view, network side is ePDG
- The SecGW supports both IKEv2/IPSec based as well SSL based connections simultaneously
- SecGW can be authenticated by UE based on a X.509 certificate. This is optional in TLS
- SSL should be used to provide data security between UE and SecGW
- SSL and TCP protocol stacks has been implemented at SecGW to support the authentication and connection security requirements

SecGW TLS Support Configuration

Product

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`

Show Command Changes

As part of " TLS Support " feature below show commands output are introduced:

show wsg-service all

Secure tunnel parameters:

- Param 1
  - Protocol
  - Port

    - SSL template
    - WSG Application
- Param 1
    - Protocol
    - Port
    - SSL template
    - WSG Application

show configuration

- secure-tunnel protocol <type> port <port-num> ssl-template <template-name> wsg-application app1
- secure-tunnel protocol <type> port <port-num> ssl-template <template-name> wsg-application <application-name>
- bind address 176.0.10.167 secure-tunnel

show ssl statistics

WSG SSL Data Stats:

- Total Packets Rcvd from Nw:
- Total Bytes Rcvd from Nw:
- Total Packets Sent to User:
- Total Bytes Sent to User:
- Total Packets Rcvd from User:
- Total Bytes Rcvd from User:
- Total Packets Sent to Nw:
- Total Bytes Sent to Nw:

show ssl statistics

WSG TCP Data Stats:

- Total Buffer Rcvd from Nw:
- Total Bytes Rcvd from Nw:
- Total Buffer Sent to User:
- Total Bytes Sent to User:
- Total Buffer Rcvd from User :
- Total Bytes Rcvd from User:
- Total Buffer Sent to Nw:

• Total Bytes Sent to Nw:

show subscriber all

• USERNAME

show wsg-application

Displays wsg-application information.

Product

SecGW (WSG)

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

show wsg-application (all | name | *application_name* **[counter] [| { grep** *grep_options* **| more }] | statistics [all] [name] [| { grep** *grep options* **| more }] }**

all

Displays information for all configured application

name *application_name*

Displays specific application. Must be followed by application name which is a string of size 1 through 63.

counter

Displays information for all configured application.

statistics

Displays information for all configured application.

[| { grep *grep options* | more }] }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent. For details on the usage of the grep and more commands, refer to the Regulating a Command's Output section of the Command Line Interface Overview chapter.

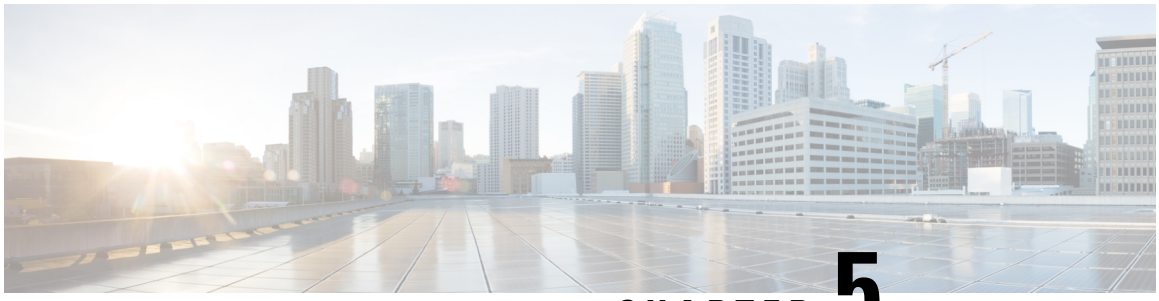
Usage Guidelines

Use this command to display wsg-application information.

Example

The following example displays information for all configured application:

```
show wsg-application statistics
```



CHAPTER 5

SecGW Support for EAP-MD5

Feature Description

SecGW uses RADIUS interface between AAA and SecGW for EAP-MD5 authentication of IPSec peer. Radius protocol is used between AAA Server and SecGW. SecGW will act as EAP-pass-through only.

Assumptions and Limitation

- The implementation will be valid only for SecGW RAS mode.
- EAP payload will not be validated only header will be validated.
- The prefix in Idi payload, which decides the EAP-Type to be performed for authentication is out of scope for this feature. As there is no prefix digit assigned to it, it will be decided by mutual agreement between SecGW peer (like FAP) and AAA server.

Configuring SecGW Support for EAP-MD5

Use the following configuration to configure SecGW Support for EAP-MD5.

associate subscriber-map *subscriber-map_name*

```
config
   context context_name
        wsg-service  service_name
            associate subscriber-map   subscriber_map_name
          end
```

Performance Indicator Changes

Below are the show commands outputs added as part of this feature SecGW Support for EAP-MD5:

show crypto stats ikev2:

EAP-MD5:

- Current: Failure:
- Attempt: Success:

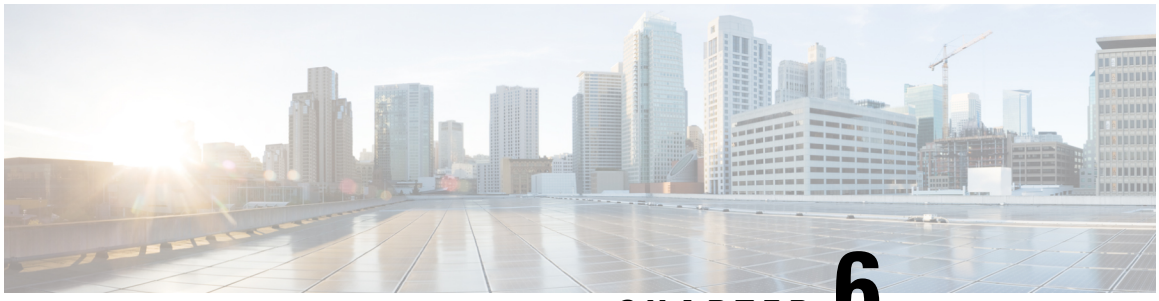
Existing Show command outputs significant to EAP-MD5 feature:

show wsg-service stats

- Auth failure:

show radius counters all

- Access-Request Sent:
- Access-Challenge Received:
- Access-Accept Received:
- Access-Reject Received:



CHAPTER 6

Authorization based on Certificate fields

This feature enables to authorize peer while IKEv2 tunnel establishment in case of SecGW product while using Certificate based authentication method.

Feature Description

Authorization of peer will be based on match of CN field in peer's certificate with list of configured allowed entries.

Assumptions and Limitations

- CN part will be such a way that it matches fully with one of the configured value.
- All peers are provided with the same Certificate or some set of known certificates. Hence CN will be same (or set of CN's) and will be limited in exclusive numbers. One such configuration can match all peers using said certificate.
- This feature is not applicable for non-certificate authentication method.
- Only 64 entries can be configured under one cert-policy and one cert-policy can be attached to one crypto template used for SecGW service.

Configuring Authorization based on Certificate fields

Use the following configuration to configure Authorization based on Certificate fields.

certificate policy

```
config
   context context_name
        [ no ]  certificate policy   ert-policy_name
          end
```

id

```
config
   context context_name
        [ no ]  id  id
         id  id_value  match-criteria { common-name value comm-name_val  |
domain-name value dom_name_value }
          end
```

Performance Indicator Changes

Below are the show commands outputs added as part of this feature to support Authorization based on Certificate fields:

show crypto ikev2-ikesa certificate policy

Crypto Cert Policy Name cert_test

- ID 1 Match-Type common-name Match-Value wsg0@cisco.com
- ID 2 Match-Type common-name Match-Value wsg1@cisco.com
- ID 3 Match-Type common-name Match-Value wsg2@cisco.com

Crypto Cert Policy Name cert_test1

- ID 2 Match-Type common-name Match-Value wsg1@cisco.com

Crypto Cert Policy Name test

- ID 1 Match-Type common-name Match-Value wsg_test@cisco.com

show config

ikev2-ikesa certificate policy cert_test1

- id 2 match-criteria common-name value wsg1@cisco.com

ikev2-ikesa certificate policy cert_test

- id 1 match-criteria common-name value wsg0@cisco.com
- id 2 match-criteria common-name value wsg1@cisco.com
- id 2 match-criteria common-name value wsg1@cisco.com

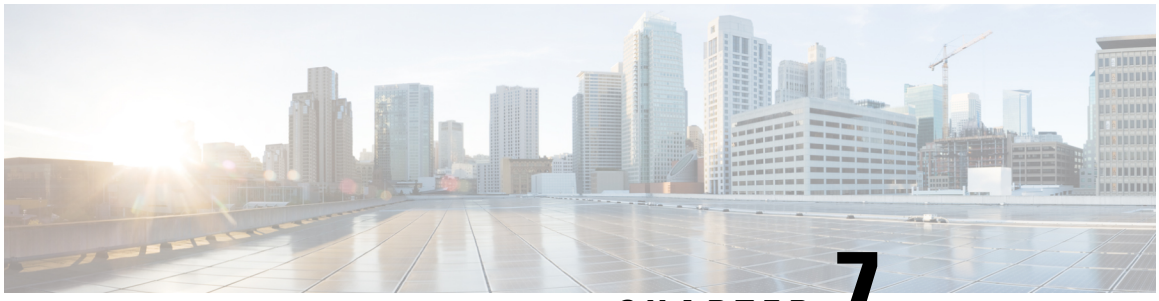
crypto template template-name ikev2-dynamic

- ikev2-ikesa cert-policy cert_test

Bulkstats

Below fields are added for Certificate Authentication Statistics:

- Authorisation policy failure



CHAPTER 7

IP Address stickiness for FAP

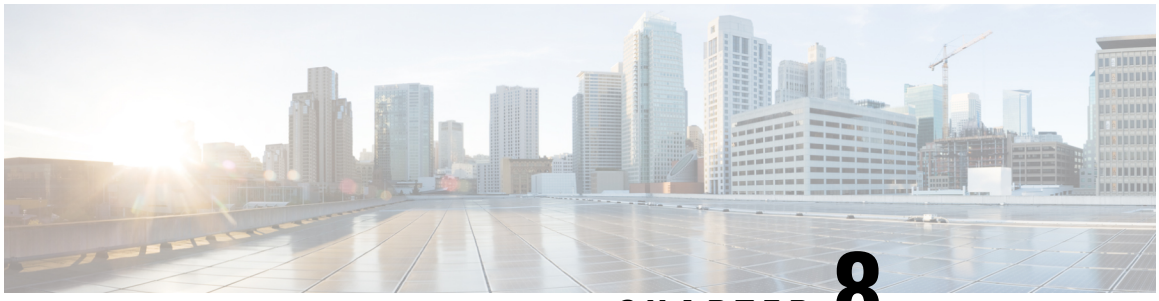
This feature allows to preserve allocated internal IP address for configured timer after tunnel tear down. Also helps to allocate same IP if new tunnel from same peer attaches within configured time.

Feature Description

If IPsec tunnel tear down happens and when a new tunnel is created with same peer, usually new IP gets allocated each time. With this in some case, there in-occurs a need to reconfigure peer's environment. In order to avoid such scenario**,** preservation of allocated internal IP is suggested for some configured timer.

IP preservation is with respect to WSG RAS mode only. IP Address Stickiness is not required for S2s mode.

IPv6 allocated IP will not be preserved and is out of scope of this feature.



CHAPTER 8

IPSec Large Support

Boost Crypto Performance

The IPSec Large feature boosts IPSec crypto performance by enabling the resource manager (RM) task to assign additional IPSec managers to packet processing cards that have sufficient processing capacity. The system can be configured to achieve a higher per SF scale by configuring the **[no] require ipsec-large** command. This configuration is effective during init time only, and system resources are adjusted accordingly for more number of ePDG sessions or IPSec tunnel establishments.

Important When IPSec large and demux on MIO are configured together, enable the IPSec large feature (using the **require ipsec-large** command) before enabling the demux on MIO (using the **require demux management-card** command).