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.

Figure 1: *SecGW accessesing ePDG using TLS over TCP*
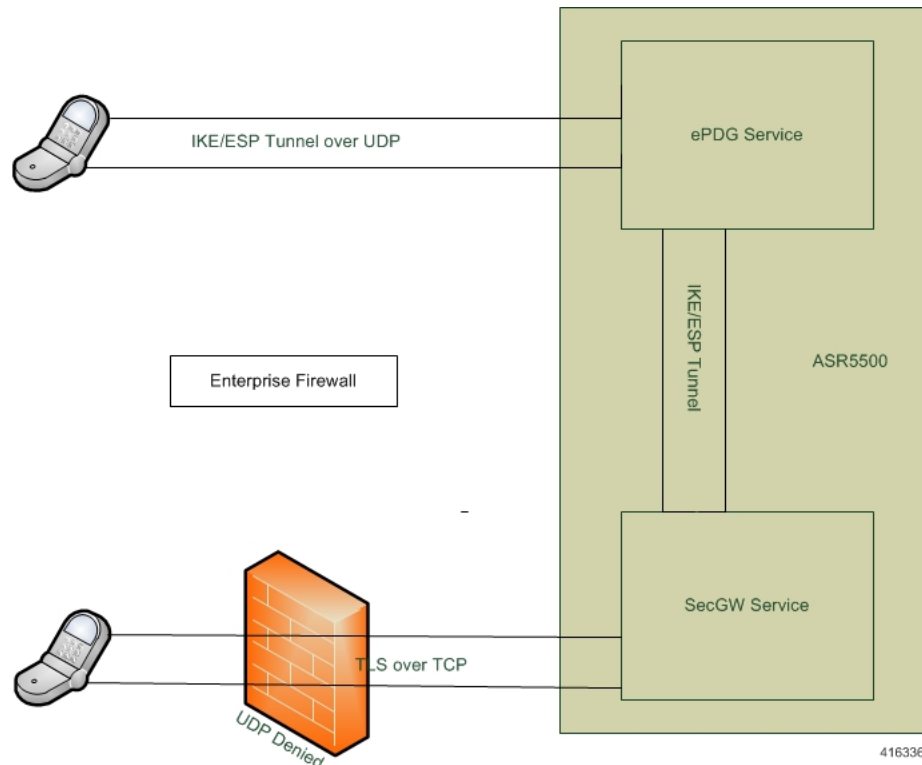
Assumptions and Limitations

- 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