Transport Gateway Communication over HTTPs

Devices in order to communicate with TG via HTTPS, SSL certificates need to be installed on devices. In addition to the TG SSL Certificate option there is also a provision for Self-signed certificates.

The Transport Gateway is shipped with Self-signed certificates that works for IOS devices. The below use case explains the process to setup Self-signed SSL certificates to enable HTTPS communication between devices and TG.

Usecase

Customer Using Self-signed certificates shipped with TG

TG is shipped with self-signed certificate and configured by default. Customer needs to import the certificate in device following the standard instructions on device. A section (Using HTTPS for device to TG communication) in the TG user guide document entails this information.

Reference: Using HTTPS for device to TG communication

Customer installs own certificate on TG

We shall consider below scenario in this use case:

- Creating and Installing Self-signed certificates with Subject Alternative Name (SAN) (mandatory for IOS-XR devices).

Creating and Installing Self-signed certificates with Subject Alternative Name (mandatory for IOS-XR devices)

Note

- Ensure JDK 1.7 or higher is installed on the system where the below commands are executed.
- If you are trying to install the certificates, using Cisco Smart Software Manager Satellite, contact Cisco Support team for support.

1. Generate the keystore. (Please enter relevant values being asked by java keytool. Replace "1.1.1.1" with the actual IP address of the system where TG is installed). Remember the keystore password/note down.

keytool -genkey -alias tgservernew -keyalg RSA -sigalg SHA256withRSA -keysize 2048 -keystore tgservernew.jks -ext SAN= ip:1.1.1.1 -validity 3650

2. Export the certificate (tgservernew.cer) and install it onto the device.

keytool -keystore tgservernew.jks -exportcert -alias tgservernew -rfc -file tgservernew.pem

This will generate the java keystore (*tgservernew.jks*) and the certificate *(tgservernew.pem*) file.

Follow the below steps to add the keystore to TG and install the certificate onto the device:

Step:1 Copy the *tgservernew.jks* file to *<TG_INSTALL_DIR>/CSCOSchtg/tg/resources/security*

Step:2 Open the file *<TG_INSTALL_DIR>/CSCOSchtg/tg/conf/properties/jettyconfig.properties*

Step:3 Edit the below line so that it becomes like below

jettyconfig.pki.certclient.keystore_file= tgservernew.jks
jettyconfig.pki.certclient.keystore_pass=<key store password>
jettyconfig.sslCertificateExists=false

Step:4 Restart TG

Step:5 Open the certificate file "*tgservernew.pem*" using a text editor and follow the commands given in step 3 in below user guide in order to install it onto the device.

Reference: Using HTTPS for device to TG communication