Edge Security

Configuring TLS on an Edge Router

Google Cloud

Agenda

- Overview
- Create the JAR for the keystore
- Creating a keystore and uploading JAR
- Creating a secure virtual host

apigee

Overview

- TLS encryption may be terminated at the Edge Router if desired.
  - A common case is to terminate at the load balancer closest to the data center boundary.

- To enable TLS for incoming API requests, the virtual host associated with an environment must be created and configured to accept encrypted connections.

- TLS keys and certificates are stored in keystores via the management API.
  - Keys and certificates are bundled in a specially-formatted JAR file and uploaded to: `/v1/o/<org>/e/<env>/keystores/<keystore>`
  - Once complete, keystore and key name are referenced in virtual host definition.

Creating the keystore jar

JAR file must contain:

- Certificate (or chain if including CA/Intermediate CA) - `mycert.pem`
- Private Key - `myKey.pem`
- Manifest - `META-INF/descriptor.properties`

Package using JAR

```
jar -cf myKeystore.jar myCert.pem myKey.pem
jar -uf myKeystore.jar META-INF/descriptor.properties
```

Note : Only one certificate is allowed per JAR file.

Creating and uploading the Keystore

Create the keystore:

```
curl -H "Content-Type: text/xml" \
https://api.enterprise.apigee.com/v1/o/{org_name}/environments/{env_name}/keystores \
-X POST -d '<KeyStore name="myTestKeystore"/>' -u email:password
```

Upload the jar file:

```
curl -X POST -H "Content-Type: multipart/form-data" -F file="@myKeystore.jar" \
"https://tlsdemo.apigee-training.google.com/v1/o/{org_name}/e/{env_name}/keystores/{myTestKeysto
re}/keys?alias=myKeyAlias&password={key_pass}" -u email:password
```

Agenda

With a keystore in place, it is simply added to the configuration when creating a new, secure virtual host:

```
curl -X POST -H "Content-Type:application/xml" -u email:password
http://<ms-IP>:8080/v1/o/{org}/e/{env}/virtualhosts
-d '<VirtualHost  name="securevhost">
      <HostAliases>
        <HostAlias>tlsdemo.apigee-training.google.com</HostAlias>
      </HostAliases>
      <Interfaces/>
      <Port>9443</Port>
      <SSLInfo>
        <Enabled>true</Enabled>
        <ClientAuthEnabled>false</ClientAuthEnabled>
        <KeyStore>myTestKeystore</KeyStore>
        <KeyAlias>myKeyAlias</KeyAlias>
      </SSLInfo>
  </VirtualHost>'
```

Thank You

Google Cloud