Edge Security

TLS for Edge UI

Google Cloud

Agenda

- Overview
- Create JKS keystore
- Run TLS configuration helper
- Test
- Force UI to use HTTPS to Management Server

Create and secure JKS Keystore

- Create the keystore as previously described.
- Copy the keystore to /opt/apigee/customer/application and name appropriately:

```
cp my_keystore.jks /opt/apigee/customer/application/ui_keystore.jks
```

- Set appropriate ownership and permissions for the keystore

```
chown apigee:apigee /opt/apigee/customer/application/ui_keystore.jks
chmod 600 /opt/apigee/customer/application/ui_keystore.jks
```

Configuring TLS using the apigee-service utility

TLS configuration for Edge UI is done via the `apigee-service` utility.

Example below:

```
apigee-service edge-ui configure-ssl

Checking for optional variables
Configuring HTTPS for UI services
Enter UI HTTPS port: 9443
Do you want to disable HTTP y/n (y): n
Enter SSL keystore algorithm (JKS): JKS
Enter SSL keystore absolute file path: /opt/apigee/customer/application/ui_keystore.jks
Enter SSL keystore password: TestMe
Enter SSL keystore password for verification: TestMe
```

Restart and Test

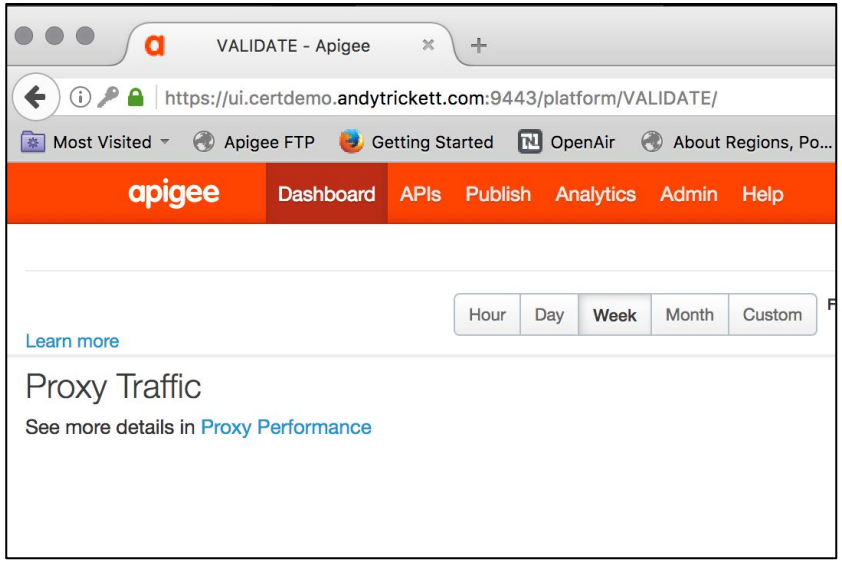
Once configuration is complete, restart the service:

```
apigee-service edge-ui restart
```

Test that the service has come up on the correct port:

```
ss -ltn | grep 9443
```

Check via browser and log on.



Force Edge UI to use TLS for Management API calls

It is possible to force Apigee Edge UI to make management calls exclusively over HTTPS (default is HTTP)
Check the Management API is accessible and configured to use HTTPS:

```
curl -u<admin@email> https://<MS_IP:SSL_PORT>/v1/o
```

On the server running Edge UI, add the following to `/opt/apigee/customer/application/ui.properties` and restart the service (`apigee-service edge-ui restart`):

```
conf_apigee_apigee.mgmt.baseurl="https://MS_IP:8443/v1"
```

Thank You

Google Cloud