Edge Security

Configuring TLS on an Edge Management ServerEdge Security

Agenda

- Overview
- Create obfuscated password
- Update management server configuration
- Test

Agenda

By default, TLS is disabled for the management API and you access the Edge management API over HTTP by using the IP address of the Management Server node and port 8080.

TLS can be configured on the management server to permit access via HTTPS.

Additionally, it is possible to force the Edge UI component to make management API calls over HTTPS (HTTP is the default)

Create an Obfuscated Password

Some parts of the Edge TLS configuration procedure require you to enter an obfuscated password in a configuration file. An obfuscated password is a more secure alternative to entering your password in plain text.

You can generate an obfuscated password in Java by using the Jetty .jar files installed with Edge.
Example with output : (jar versions will be specific to installed version of Edge)

```
java -cp \
/opt/apigee/edge-gateway/lib/thirdparty/jetty-http-8.0.4.v20111024.jar:/opt/apigee/edge-gateway/
lib/thirdparty/jetty-util-8.0.4.v20111024.jar org.eclipse.jetty.http.security.Password TestMe
```

Output:

```
TestMe
OBF:1ppq1od31yta1ytc1obr1pqo
MD5:2c539f7b23fc3fb3b8ec52d3bfa58834
```

Configuring TLS

Procedure

- Create JKS keystore containing private key and certificate (or chain)
- Copy keystore to an Apigee accessible directory on the management server e.g: `/opt/apigee/customer/application`
- Create or edit: `/opt/apigee/customer/application/management-server.properties`
- Restart Management Server: `apigee-service edge-management-server restart`

management-server.properties

```
conf_webserver_ssl.enabled=true
# http.turn.off=true if all comms should be over HTTPS.
# Not recommended as many Edge internal calls use HTTP.

conf_webserver_http.turn.off=false
conf_webserver_ssl.port=8443
conf_webserver_keystore.path=/tmp/keystore.jks
# Enter the obfuscated keystore password below.
conf_webserver_keystore.password=OBF:obfuscatedPassword
conf_webserver_cert.alias=apigee-devtest
```

Test

The Edge Management API is now accessible over HTTPS:

Test - should return list of configured Orgs for your planet:

```
curl https://mapi.certdemo.yourdomain.xyz:8443/v1/o -u<apigee-opdk@google.com>

[ "VALIDATE", "tisdemo" ]
```

Note: If using your own CA you may have to append --cacert /path/to/ca/chain/cert to your curl command

Overview

By default, TLS is disabled for the management API and you access the Edge management API over HTTP by using the IP address of the Management Server node and port 8080.

TLS can be configured on the management server to permit access via HTTPS.

Additionally, it is possible to force the Edge UI component to make management API calls over HTTPS (HTTP is the default)

Creating an obfuscated password

Some parts of the Edge TLS configuration procedure require you to enter an obfuscated password in a configuration file. An obfuscated password is a more secure alternative to entering your password in plain text.

You can generate an obfuscated password in Java by using the Jetty .jar files installed with Edge.
Example with output : (jar versions will be specific to installed version of Edge)

```
java -cp \
/opt/apigee/edge-gateway/lib/thirdparty/jetty-http-8.0.4.v20111024.jar:/opt/apigee/edge-gateway/
lib/thirdparty/jetty-util-8.0.4.v20111024.jar org.eclipse.jetty.http.security.Password TestMe
```

Output:

```
TestMe
OBF:1ppq1od31yta1ytc1obr1pqo
MD5:2c539f7b23fc3fb3b8ec52d3bfa58834
```

Configuring TLS

- Create JKS keystore containing private key and certificate (or chain)
- Copy keystore to an Apigee accessible directory on the management server e.g:
  /opt/apigee/customer/application
- Create or edit: /opt/apigee/customer/application/management-server.properties
- Restart Management Server: apigee-service edge-management-server restart

```
conf_webserver_ssl.enabled=true
# http.turn.off=true if all comms should be over HTTPS.
# Not recommended as many Edge internal calls use HTTP.

conf_webserver_http.turn.off=false
conf_webserver_ssl.port=8443
conf_webserver_keystore.path=/opt/apigee/customer/application/ms-keystore.jks
# Enter the obfuscated keystore password below.
conf_webserver_keystore.password=OBF:obfuscatedPassword
conf_webserver_cert.alias=apigee-ms-server
```

Test

The Edge Management API is now accessible over HTTPS:

Test - should return list of configured Orgs for your planet:

```
curl https://mapi.certdemo.yourdomain.xyz:8443/v1/o
-u<apigee-opdk@google.com>

[ "VALIDATE", "tlsdemo" ]
```

Note: If using your own CA you may have to append --cacert /path/to/ca/chain/cert to your curl command

Thank You