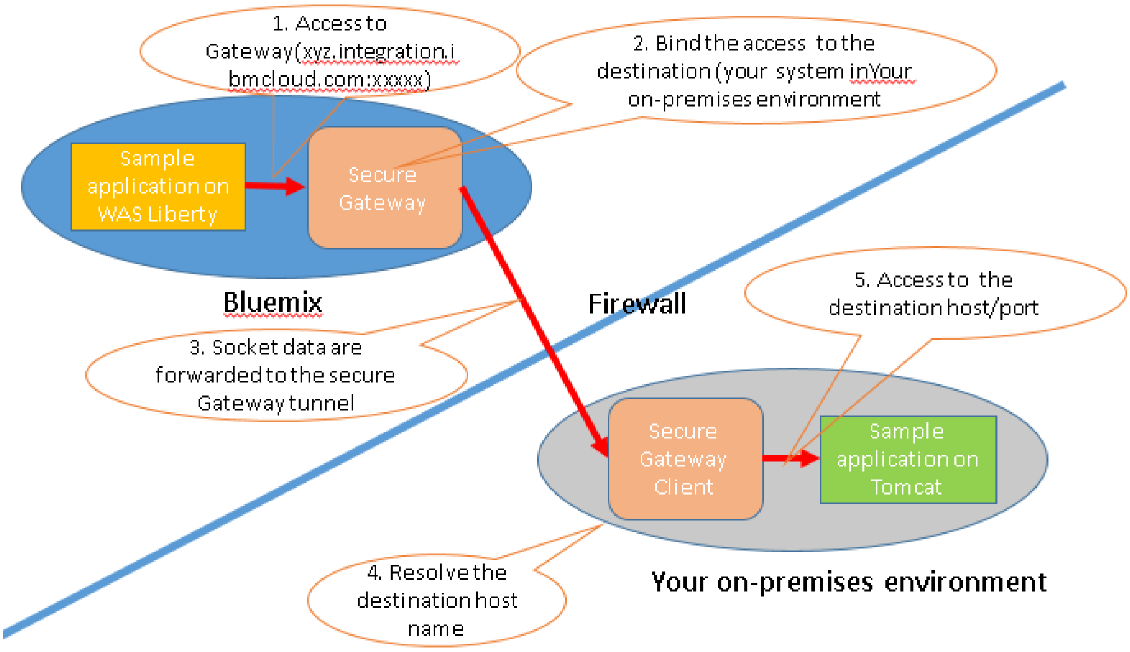
# How to setup Secure Gateway for the application on Bluemix to access services on your on-premises computing environment.

Dec 10, 2015 (updated: Mar 28, 2016)

1. Prerequisite
   1. Topology :


1. Access to Gateway(xyz.integration.ibmcloud.com:xxxxx)
2. Bind the access to the destination (your system in Your on-premises environment
Sample application on WAS Liberty
Secure Gateway
Bluemix
Firewall
5. Access to the destination host/port
3. Socket data are forwarded to the secure Gateway tunnel
Secure Gateway Client
Sample application on Tomcat
4. Resolve the destination host name
Your on-premises environment

   2. Need to obtain Bluemix account
   3. Optional : Two applications are necessary to verify that Secure Gateway would work
      1. One application on Bluemix which will access another application on your on-premises environment
      2. Another application which runs on your on-premises environment
   4. Optional: Eclipse to deploy and run two sample applications.
      1. For its setup, please follow : https://www.ng.bluemix.net/docs/manageapps/eclipsetools/eclipsetools.html

    5. Linux, MacOS or Windows for Secure Gateway Client：One of the following OS
        1. Ubuntu Linux 14.04 Long Term Support (LTS) and greater
        2. Red Hat Linux 6.5 and greater
        3. SuSE Linux 11.0 and greater
        4. Mac OS 10.10 and grater
        5. Windows Desktop 8.1, 10 and greater
        6. Windows Server 2012 R2 and greater
2. Setup
    1. Login Bluemix
    2. Please follow https://www.ng.bluemix.net/docs/services/SecureGateway/index.html. The key steps are：
        1. Add Secure Gateway service
            1. Click：CATALOG > Secure Gateway
            2. Click：CREATE
        2. Add Gateway
            1. Click：ADD GATEWAY
            2. Type this gateway name to the text field（For example, “myscgateway”）
            3. Optional：Uncheck “Enforce security token on client” so that you don’t have to specify Security Token whenever starting Secure Gateway Client.
            4. Click：CONNECT IT
        3. Setup Secure Gateway Client
            1. Check：IBM Installer
                1. You can see some available installer. You can pick up one of them.
            2. Install Secure Gateway Client. Follow https://www.ng.bluemix.net/docs/services/SecureGateway/sg_021.html
            3. Copy Gateway ID,（and possibly Security Token） and start Secure Gateway Client.
                1. For example for linux,
                    1. cd /opt/ibm/securegateway
                    2. su secgwadmin
                    3. node lib/secgwclient.js <options> <gateway_ID>
                        1. options - Command line option. No option is fine if “Enforce security token on client” option was unchecked.

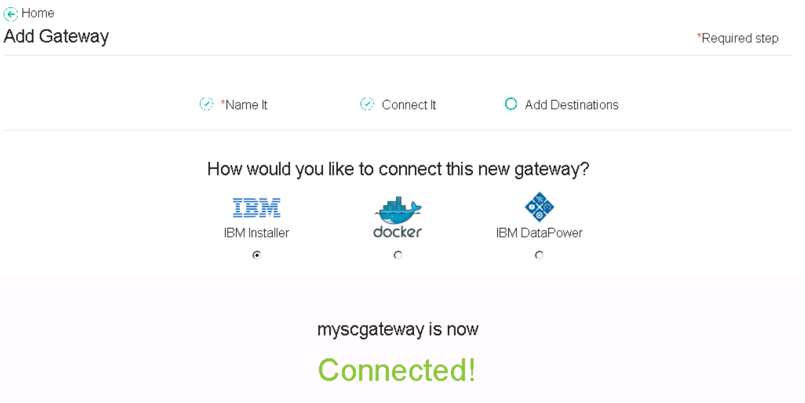
        If not, you need to use “--t” option with a given security token. See [https://www.ng.bluemix.net/docs/services/SecureGateway/sg_021.html#sg_037](https://www.ng.bluemix.net/docs/services/SecureGateway/sg_021.html#sg_037)

        2. gateway_id. The copied string. This is necessary.
        3. Option: If you will use IBM installer, then make sure that the client will say “The Secure Gateway tunnel is connected”

    4. Add ACL for the destination hostname and its port on your on-premises environment. For example,

```
cli> a allow :80
cli> a allow :9443
cli> S
---------------------------------------
-- Secure Gateway Client Access Control List --
 hostname                  port          value
 ALL                          80          Allow
 ALL                        9443          Allow
---------------------------------------
```

    5. On Blumix UI, you will see



How would you like to connect this new gateway?

myscgateway is now

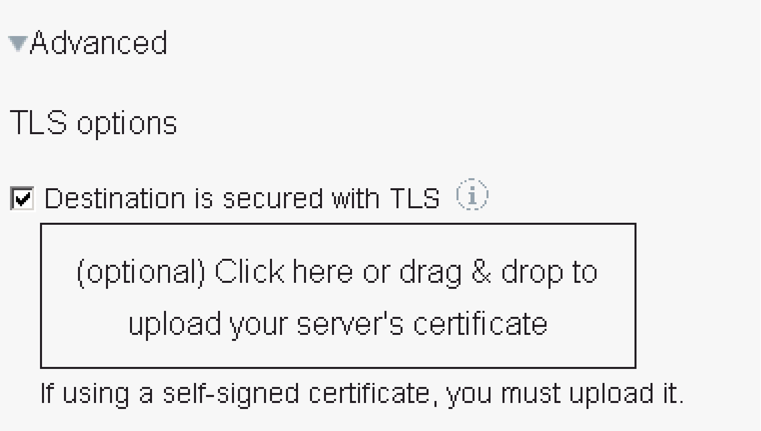
Connected!

4. Back to Bluemix UI
5. Click : ADD DESTINATION
6. Type

   Destination name : Any name is ok

   Hostname or IP Address/Port: This is a hostname or IP address and the port number of the apps on your on-premises computing environment.

7. Select TCP(or HTTP) (Note: Don’t specify TLS* or HTTPS. We don’t use Application-side TLS ).
    1. If the destination is https, check Advanced > Destination is secured with TLS.

       ▼Advanced

       TLS options

       ☑ Destination is secured with TLS

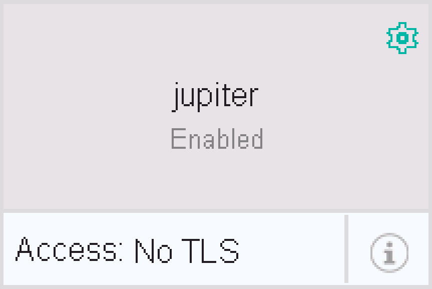
       (optional) Click here or drag & drop to upload your server's certificate

       If using a self-signed certificate, you must upload it.

    2. If the destination system uses a self-signed certificate, we need to upload it..
        1. Open Browser and try to access the destination application so that Browser will have its certificate.
        2. Tools > Options > Advanced > View Certificates
        3. Select the destination host’s certificate
        4. Export it as “X.509 Certificate (PEM)”
        5. Drag & drop it
    3. Make sure that the system’s date and time for Secure Gateway Client and the destination server must be same. Otherwise, you will see CERT_NOT_YET_VALID error from SSL connection.
    4. Note: If the destination server is CLM server, its certificate usually uses “localhost” as CN which causes an error. So you need to recreate keystore by yourself.
        1. Stop CLM
        2. Remove an old certificate from your browser
            1. Start Browser
            2. Tools > Options > Advanced > View Certificates
            3. Select the destination host’s certificate
            4. Delete…
        3. cd <CLM install location>¥JazzTeamServer¥server¥liberty¥servers¥clm¥resources¥security

   4. rename ibm-team-ssl.keystore ibm-team-ssl.keystore.ORG as a backup.
   5. Generate new keystore, self-sign it and export its certificate as PEM(RFC1421). For example,
      1. PATH=<CLM install location>¥JazzTeamServer¥server¥jre¥bin;%PATH%
      2. set MYHOST=<the destination server name. No “localhost” please>
      3. keytool.exe -genkey -v -alias %MYHOST% -dname "CN=%MYHOST%,OU=IBM Rational,O=IBM" -keyalg RSA -sigalg SHA1WithRSA -keysize 1024 -validity 365 -storetype JCEKS -keystore ibm-team-ssl.keystore -storepass ibm-team -keypass ibm-team -J-Duser.language=en
      4. keytool.exe -selfcert -v -alias %MYHOST% -dname "CN=%MYHOST%,OU=IBM Rational,O=IBM" -sigalg SHA1WithRSA -validity 365 -storetype JCEKS -keystore ibm-team-ssl.keystore -storepass ibm-team -keypass ibm-team -J-Duser.language=en

         Note: If you don’t self-cert it here, you will see DEPTH_ZERO_SELF_SIGNED_CERT error.
      5. keytool.exe -exportcert -rfc -v -alias %MYHOST% -storetype JCEKS -keystore ibm-team-ssl.keystore -storepass ibm-team -file ibm-team-ssl.pem -J-Duser.language=en
   6. Upload the generated PEM file to Secure Gateway Destination above.
   7. Update <CLM install location>¥JazzTeamServer¥server¥liberty¥servers¥clm¥server.xml accordingly. For example,
      1. <keyStore id="defaultKeyStore" location="ibm-team-ssl.keystore" type="JCEKS" password="***<password: for example, ibm-team>***"/>
   8. Start CLM again, then export a new certificate.
8. Click + icon
9. You should see something like

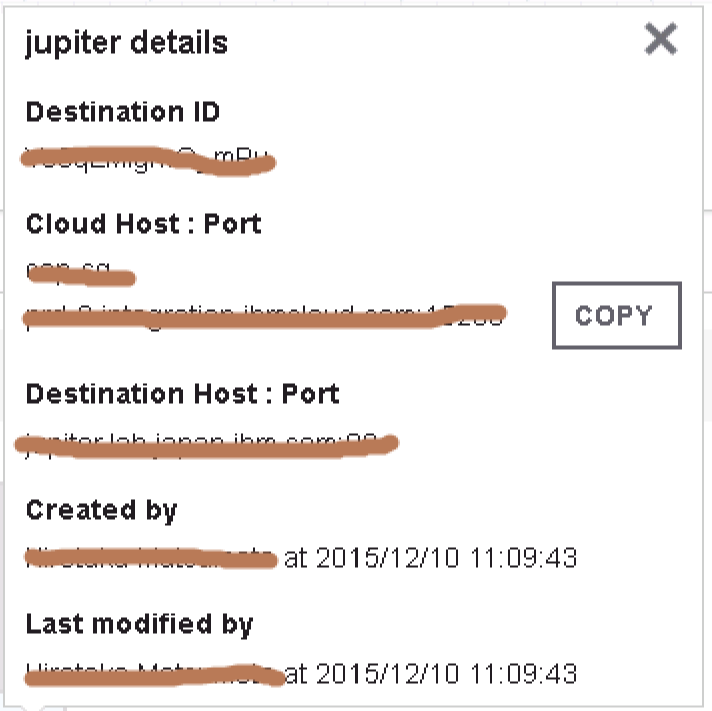


jupiter

Enabled

Access: No TLS

10. If you click I icon, you can see something like



**jupiter details**

**Destination ID**

[redacted]

**Cloud Host : Port**

[redacted]

COPY

**Destination Host : Port**

[redacted]

**Created by**

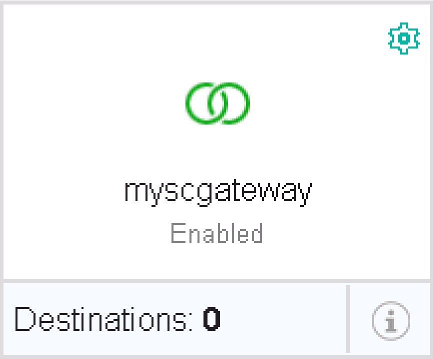
[redacted] at 2015/12/10 11:09:43

**Last modified by**

[redacted] at 2015/12/10 11:09:43

   1. This means that all access to Cloud Host:Port will be redirected to Destination Host:Port

11. Click : I'M DONE
12. Go back to Secure Gateway UI and make sure that you will see a green icon

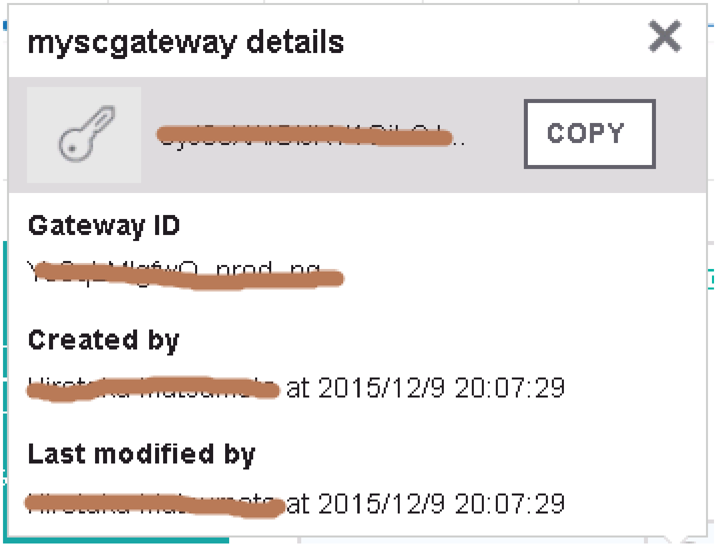


myscgateway

Enabled

Destinations: **0**

Note: If you will click I icon, you can verify the gateway id



myscgateway details

[redacted]

Gateway ID

[redacted]

Created by

[redacted] at 2015/12/9 20:07:29

Last modified by

[redacted] at 2015/12/9 20:07:29

13. Sometimes you won't see a green icon for Secure Gateway. Even if so, let's try to access your application on your on-premises environment through Secure Gateway. If that doesn't work, let's try to restart Secure Gateway Client. If still not, let's create Secure Gateway and its destination again as well as restart Secure Client Gateway Client. You may need to repeat these actions.

3. Optional : Test
   1. You can try to access your application on your on-premises environment from another application in Bluemix