1. Configure Digi Connect WAN 3G for SSL Tunnel with Certificates.

Objective: Configure a Digi Connect WAN 3G to build an SSL Socket tunnel using custom certificates.

1.1 Software Requirements

- Digi Device Discovery
- Latest 2.15.X firmware or newer
- Web browser
- SSL Certificates (CA,identity and key)

1.2 Hardware Requirements

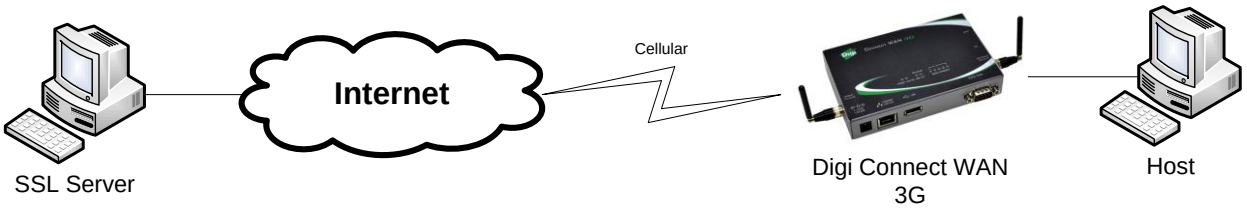
- Digi Connect WAN 3G
- SSL Server

2. Introduction

The purpose of this document is to describe how to configure a Digi Connect WAN 3G to establish a secure socket connection (SSL) using custom certificate uploaded on the unit.

Once configured, the Digi Connect WAN 3G will establish an SSL socket between a device connected on the Ethernet port and an SSL server.

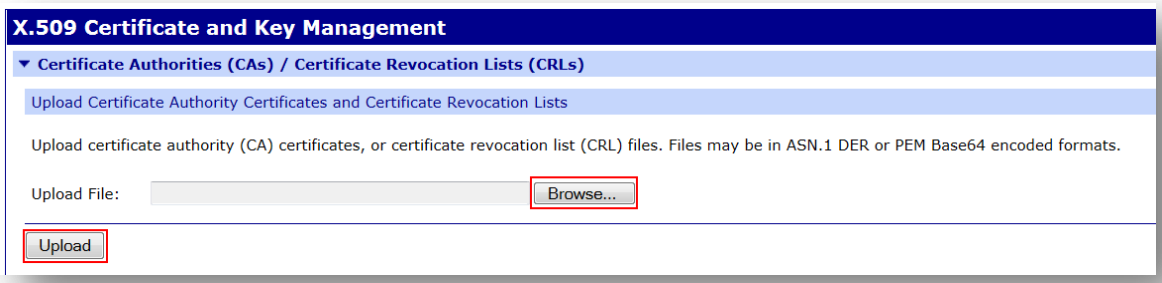
3. Sample Diagram



4. Installing Custom certificates in the Digi Connect WAN 3G

Note: It is possible to create certificates using OpenSSL and the integrated tools. For more information, please visit http://www.openssl.org

a) Open a web browser to the IP Address of the Digi Connect Wan 3G or use the Digi Device Discovery tool
b) Navigate to : **Administration>X.509 Certificate/Key Management** and click on **Certificate Authorities (CAs) / Certificate Revocation Lists (CRLs)**
c) Navigate to : **Upload Certificate Authority Certificates and Certificate Revocation Lists**, click the **Browse** button, select your CA certificate and click **Upload**



d) The CA certificate should now appear under "**Installed Certificate Authority Certificates**"

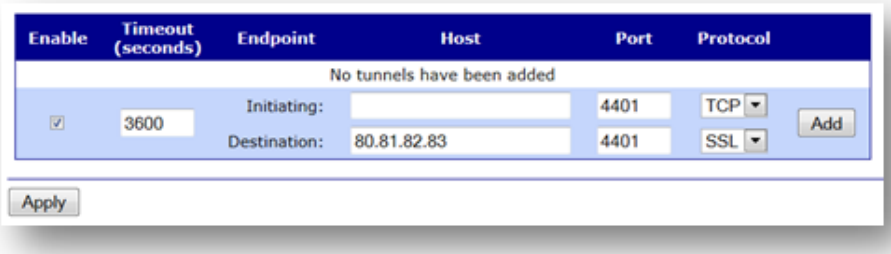
e) Navigate to : **Secure Sockets Layer (SSL) / Transport Layer Security (TLS) Certificates**, click on **"Identity Certificates and Keys**, click the **Browse** button, select your identity certificate (enter the password in the password field if the certificate is protected by a password) and click **Upload**

f) Repeat the same steps for the identity

g) The Identity Certificates and Keys should now appear under each section

5. Configuring the SSL Socket tunnel settings

a) Navigate to : **Configuration > Network > Socket Tunnel Settings**
b) Configure a new tunnel as follow and click **Add.**



Parameter	Setting	Description
Enable	Checked	Enable this Socket Tunnel
Timeout	3600	Inactivity timeout settings for this socket tunnel
Initiating		Host initiating the connection (Digi Connect WAN 3G local network side) Leave Blank.
Destination	80.81.82.83	SSL Server IP address (Public IP that can be reached from the Mobile WAN interface)
Port	4401	Port used for the Initiating (Port that the Digi Connect WAN 3G is listening on) and Destination (Port to send to)
Protocol	TCP / SSL	Protocol used on the Initiating and Destination side. Initiating side has to be TCP and destination has to be SSL (for the conversion to be done)

6. Testing

For this test, we will use the available binaries from OpenSSL and setup a listening server. Please visit http://www.openssl.org for more information on installing OpenSSL on your operating system.

Make sure to copy the host/server certificates in the openssl\bin directory or any other accessible path.

After installation, open a command prompt to the bin directory of OpenSSL, by default: **c:\openssl\bin**

Configure the OpenSSL Server as follow:

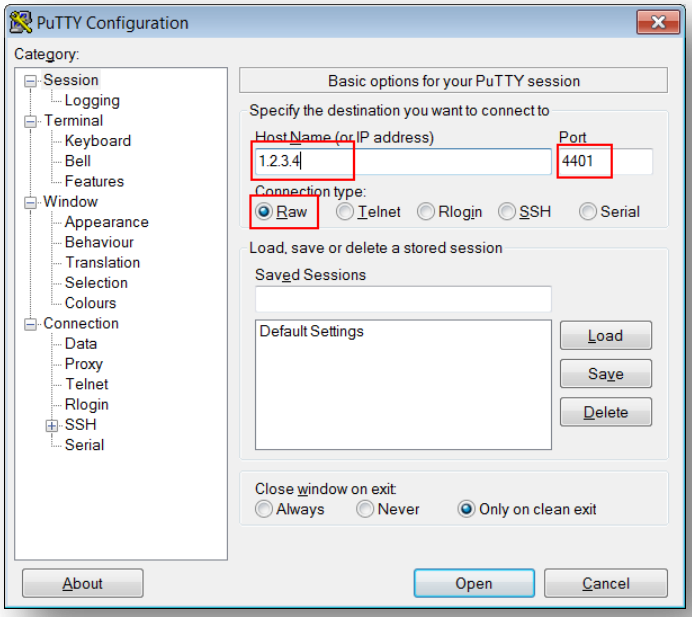
C:\OpenSSL-Win32\bin>**openssl s_server –accept 4401 –cert certh.pem –key privh.pem –CAfile cacert.pem –debug**

Parameter	Setting	Description
-accept	4401	Port to listen to (matching the port set in the Transport configuration)
-cert	certh.pem	Host certificate filename/path (if in another folder)
-key	privh.pem	Host private key filename/path (if in another folder)
-CAfile	cacert.pem	CA certificate filename/path (if in another folder)
-accept	4401	Port to listen to (matching the port set in the Transport configuration)
-cert	certh.pem	Host certificate filename/path (if in another folder)
-debug	-debug	Will output debug information from the OpenSSL server during connection and data transfer. (Helpful during testing. can be removed after.)

The OpenSSL server should now be up and running and in listening mode on port:

```
Loading 'screen' into random state - done
Using default temp DH parameters
Using default temp ECDH parameters
ACCEPT
```

On the Computer/Host connected to the Etherport of the Digi Transport, open a terminal application such as PuTTy and configure the following:



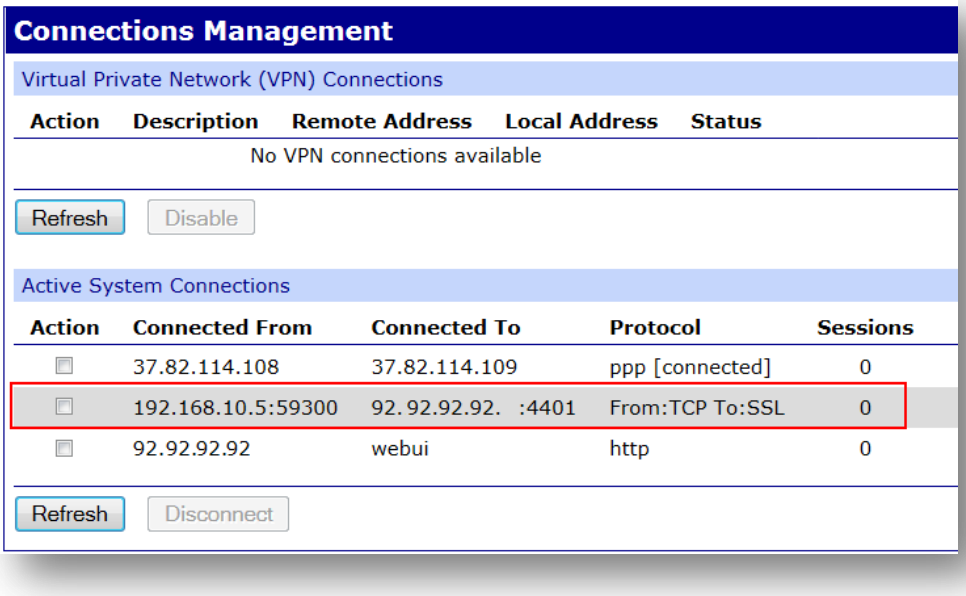
Parameter	Setting	Description
Host name or IP address	1.2.3.4	Host Name or IP Address of the OpenSSL Server
Port	4401	Listening port on the Digi Transport
Connection Type	Raw	Raw TCP connection type (TCP to SSL conversion being done by the Protocol switch on the Digi Transport)

Press **Open**

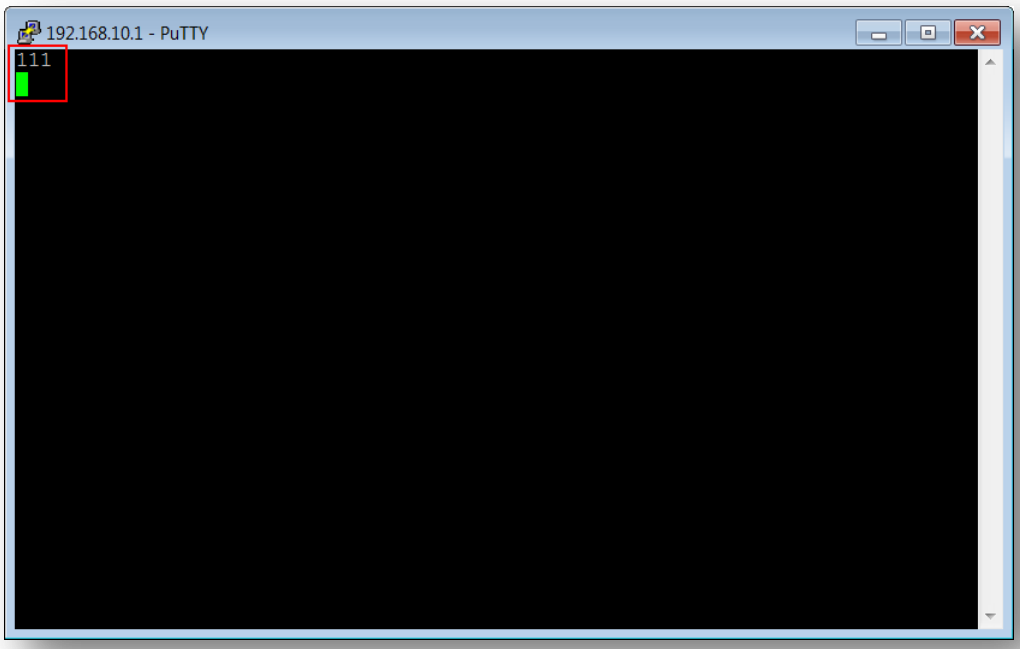
If the **debug** parameter was used, a lot of information should start to be displayed on the screen, which is the certificate exchange. This part will confirm that the tunnel is now established:

```
-----BEGIN SSL SESSION PARAMETERS-----
MHUCAQECAgMBBAIALwQgUw78/NisMM/adoQF43wa+ROkx1Bo17Eav4iPrm6IYl0E
MMfr2hGQyg4VDaouYLb3cV5ca69kNBnvlDT+ijcOEs83Sscgv4pEY9Y1Shh1QoKQ
96EGAgRTFddqogQCAgEspAYEBAEAAAA=
-----END SSL SESSION PARAMETERS-----
Shared ciphers:AES128-SHA:AES256-SHA:DES-CBC3-SHA:DES-CBC-SHA:DHE-DSS-AES128-
SHA
:DHE-DSS-AES256-SHA:EDH-DSS-DES-CBC3-SHA:EDH-DSS-DES-CBC-SHA
CIPHER is AES128-SHA
Reused session-id
Secure Renegotiation IS NOT supported
```

Check the Digi Connect Wan 3G Connection status:



Sending data in the Terminal/PuTTy Window will appear in the debug window of the OpenSSL server




```
read from 0x727ff8 [0x73369b] (5 bytes => 5 (0x5))
0000 - 17 03 01                                           ...
0005 - <SPACES/NULS>
read from 0x727ff8 [0x7336a0] (32 bytes => 32 (0x20))
0000 - 4a 6f eb 6e a4 3f 66 8c-19 32 01 54 f7 3a 39 77   Jo.n.?f..2.T.:9w
0010 - 05 4e 6d 79 a5 48 4e b7-4d 9b 6b d1 de de c9 8c   .Nmy.HN.M.k.....
111
```

Closing the Terminal/PuTTy window will close the OpenSSL Tunnel:

```
read from 0x727ff8 [0x73369b] (5 bytes => 0 (0x0))
ERROR
shutting down SSL
CONNECTION CLOSED
ACCEPT
```