1. Configure Digi Connect WAN 3G VPN Tunnel with Certificates.

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

1.1 Software Requirements

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

1.2 Hardware Requirements

- Digi Connect WAN 3G
- VPN Appliance or Router with VPN functionalities

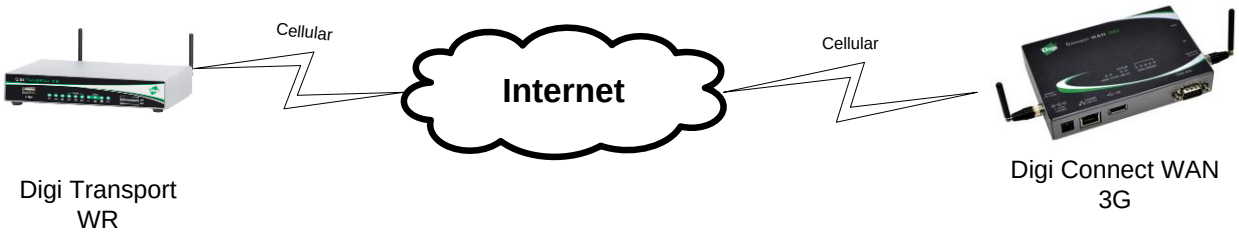
2. Introduction

The purpose of this document is to describe how to configure a Digi Connect WAN 3G to establish a VPN tunnel to a VPN appliance using custom certificates uploaded on the unit to use as the identity.

Once configured, the Digi Connect WAN 3G will establish a VPN tunnel to a VPN appliance.

In this example, the Digi Connect WAN 3G will establish a VPN tunnel to a Digi Transport router.

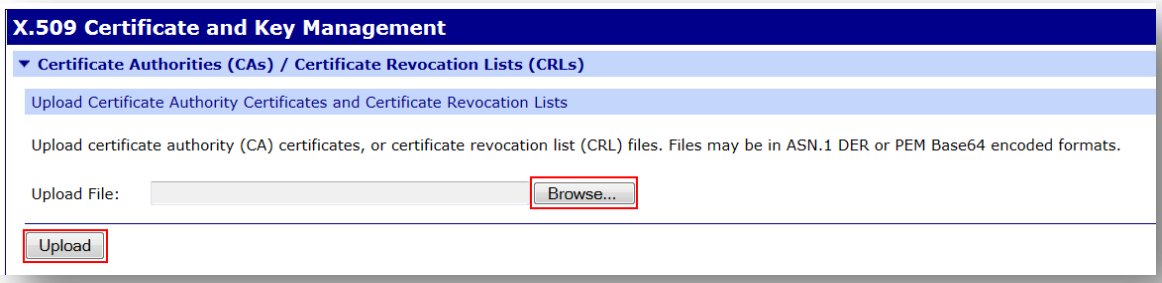
3. Sample Diagram



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

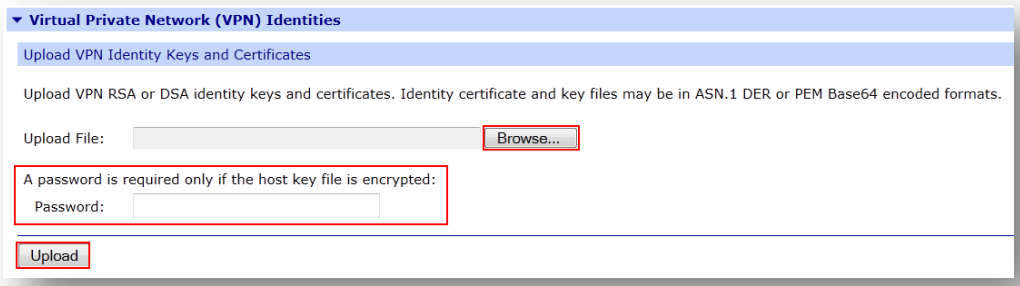
a) Open a web browser to the IP Address of the Digi Connect Wan 3G or use the Digi Device Discovery tool
b) Navigate to : **Administration>X.509 Certificate/Key Management** and click on **Certificate Authorities (CAs) / Certificate Revocation Lists (CRLs)**
c) Navigate to : **Upload Certificate Authority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



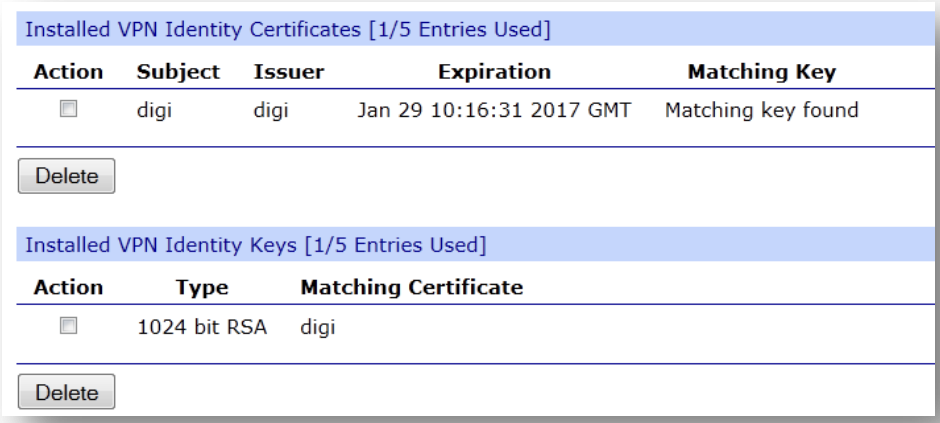
d) The CA certificate should now appear under "**Installed Certificate Authority Certificates**"

e) Navigate to : **Virtual Private Network (VPN) Identities**, click on **"Upload VPN identity Keys and Certificates"**, 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



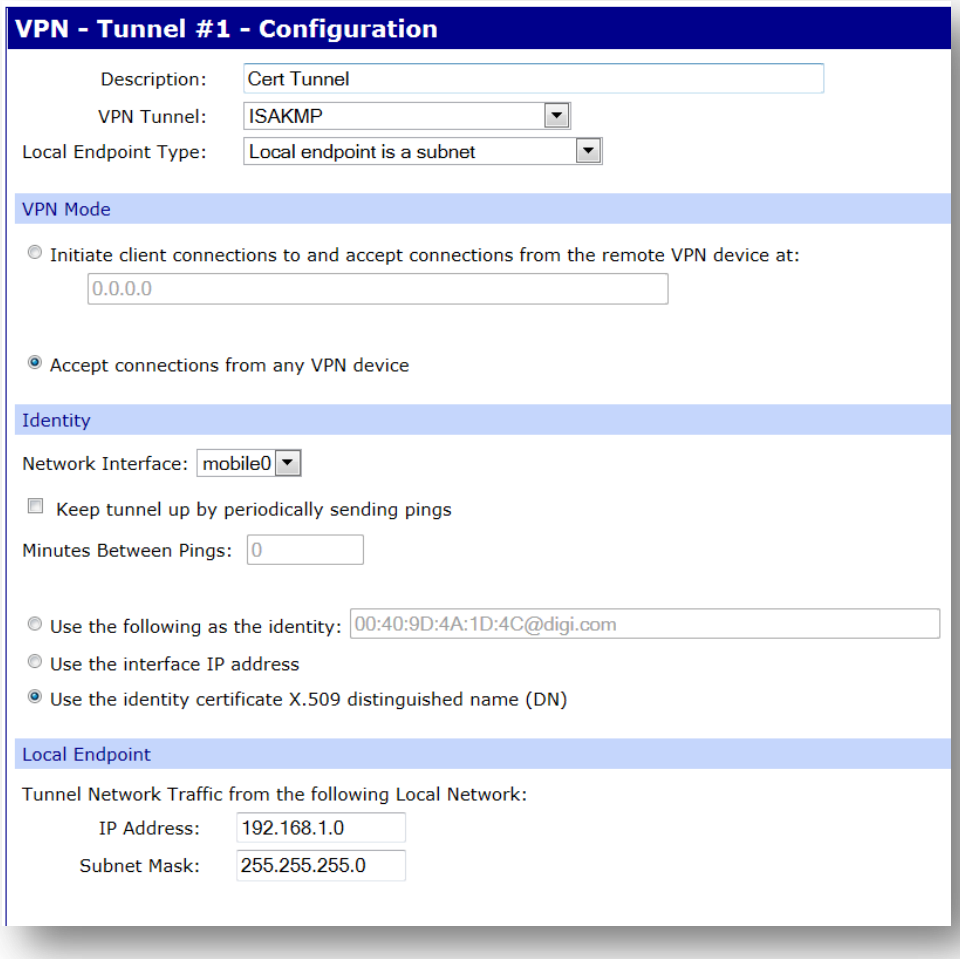
g) The Identity Certificates and Keys should now appear under each section

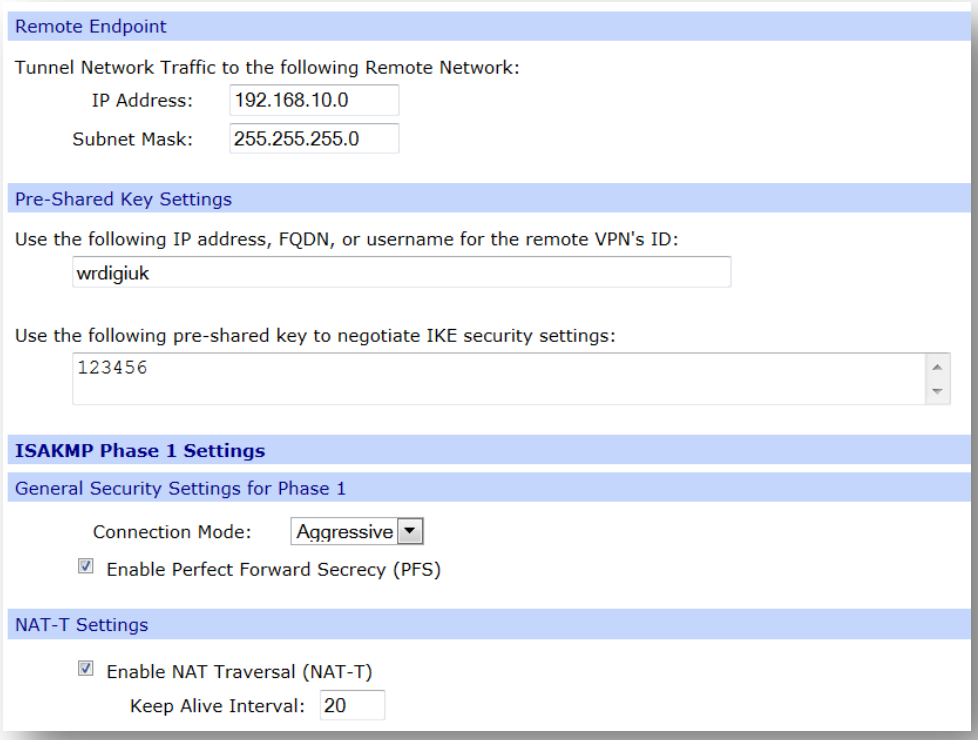


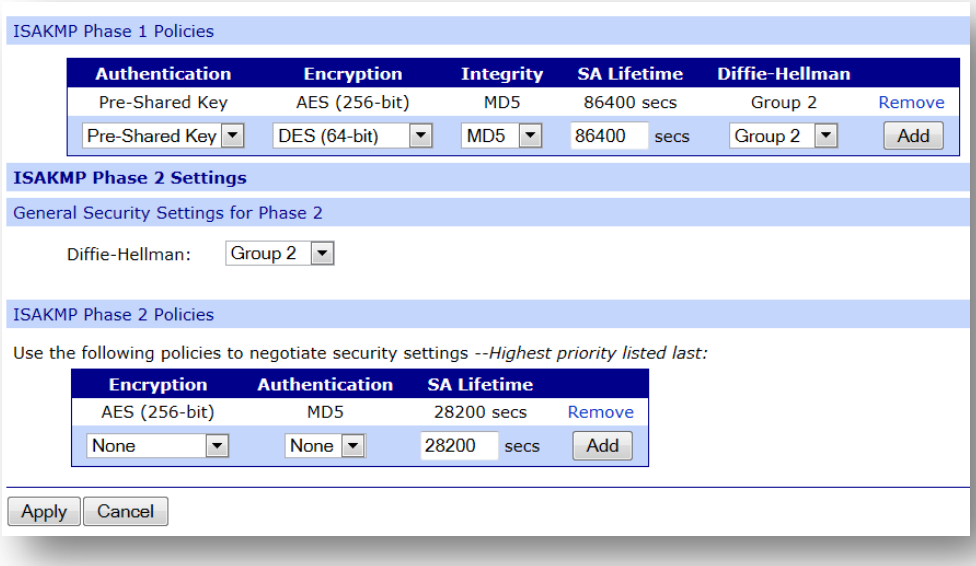
5. Configuring the VPN tunnel settings

Navigate to **Configuration > Network > Virtual Private Network (VPN) Settings > VPN Policy Settings**

a) Click on the **Add** button
b) Configure the tunnel with the following




Remote Endpoint
Tunnel Network Traffic to the following Remote Network:
IP Address: 192.168.10.0
Subnet Mask: 255.255.255.0
Pre-Shared Key Settings
Use the following IP address, FQDN, or username for the remote VPN's ID:
wrdigiuk
Use the following pre-shared key to negotiate IKE security settings:
123456
ISAKMP Phase 1 Settings
General Security Settings for Phase 1
Connection Mode: Aggressive
Enable Perfect Forward Secrecy (PFS)
NAT-T Settings
Enable NAT Traversal (NAT-T)
Keep Alive Interval: 20


ISAKMP Phase 1 Policies
Authentication Encryption Integrity SA Lifetime Diffie-Hellman
Pre-Shared Key AES (256-bit) MD5 86400 secs Group 2 Remove
Pre-Shared Key DES (64-bit) MD5 86400 secs Group 2 Add
ISAKMP Phase 2 Settings
General Security Settings for Phase 2
Diffie-Hellman: Group 2
ISAKMP Phase 2 Policies
Use the following policies to negotiate security settings --Highest priority listed last:
Encryption Authentication SA Lifetime
AES (256-bit) MD5 28200 secs Remove
None None 28200 secs Add
Apply Cancel

Parameter	Setting	Description
Description	Cert Tunnel	Description/name of tunnel
VPN Tunnel	ISAKMP	VPN Tunnel type
Local Endpoint Type	Local endpoint is a subnet	Endpoint type
VPN Mode	Accept connections from any VPN device	Setup device as Initiator or listener
Network Interface	Mobile0	Network interface used to create the tunnel
Identity	Use the indentiy certificate X.509 distinguished name (DN)	Type of identity used
Local Endpoint IP Address	192.168.1.0	Local network subnet
Local Endpoint Subnet Mask	255.255.255.0	Local network subnet mask
Remote Endpoint IP Address		Remote network subnet
Remote Endpoint Subnet Mask	255.255.255.0	Remote network subnet mask
Use The following IP address,FQDN or username for the remote VPN's ID	wrrouter	Remote VPN's ID, should match the CN in the certificate
Use the following pre-shared key to negotiate IKE security settings	123456	IKE pre-share key
Connection Mode	Aggressive	Connect Method for phase 1
Enable Perfect Forward Secrecy (PFS)	Checked	Enable PFS
Enable NAT Traversal (NAT-T)	Checked	Enable NAT-T
ISAKMP Phase 1 Policies	AES (256), MD5, 86400, Group 2	Phase 1 policies
Diffie-Hellman	Group 2	General Security settings for phase 2
ISAKMP Phase 2 Policies	AES (256), MD5, 28200	Phase 2 policies

Click **Apply** to validate the settings. The tunnel is now created.

*Note: In this example, the certificates are only used for Identity. It is possible to also use the certificates for authentication on phase 1 (and not use a pre-shared key) by selecting **RSA Signature** in the ISAKMP Phase 1 policy Authentication settings.*

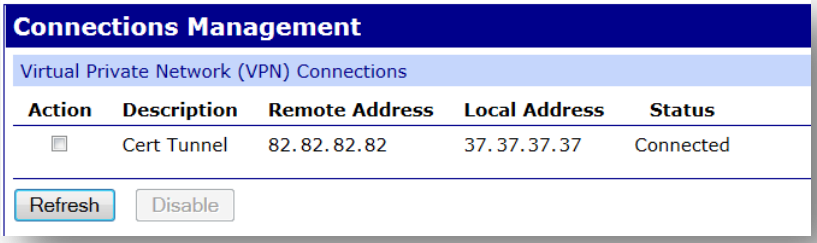
6. Important info

a) When building a tunnel with certs between a Digi Connect WAN 3G and a Digi Transport, a few configurations points need to be checked :
   a. The "**Our ID type**" option should be "**FQDN**"
   b. If the Digi Transport is the Responder, it is not required to enter an IP address or hostname for the remote unit in the IPSec tunnel settings.
   c. The "**AH authentication**" should be set to **No**
   d. **Dead Pear Detection** must be turned **Off**

7. Testing

Make sure the Digi Connect WAN 3G and Digi Transport are both connected to the internet.

The Tunnel should be built from the Digi Connect WAN 3G as soon as the interface comes up. To verify, navigate to **Management > Connections**. Under **Virtual Prviate Network (VPN) Connections**, the Tunnel should be show with a status "**Connected**"



Navigate to **Administration > System Information > Diagnostics** and ping an IP address from the remote end, for example the local Ethernet ip of the Digi Transport:

```
PING 192.168.10.254: 64 data bytes

64 bytes from 192.168.10.254: icmp_seq=0 time=2391 ms
64 bytes from 192.168.10.254: icmp_seq=1 time=1894 ms
64 bytes from 192.168.10.254: icmp_seq=2 time=1335 ms

--- 192.168.10.254 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss
round-trip min/avg/max = 1335/1873/2391 ms
```