Quick Note 041

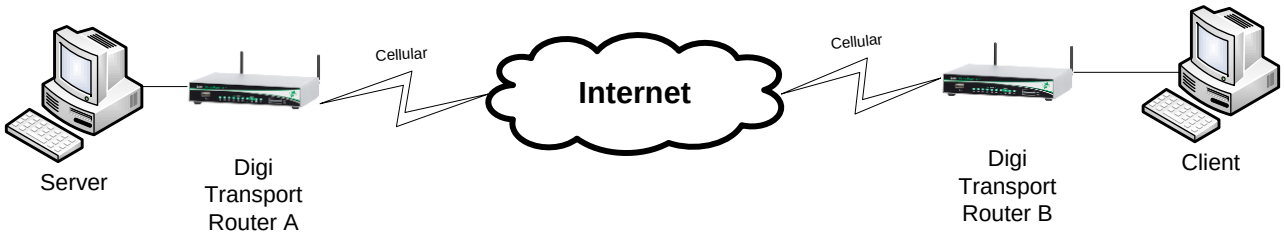
TransPort to TransPort VPN Tunnel using OpenSSL certificates.

November 2016

Contents

1 INTRODUCTION

1.1 Outline



This document describes how to create, upload SSL certificates and configure Digi TransPort WR routers to build a VPN tunnel.

1.2 Assumptions

This guide has been written for use by technically competent personnel with a good understanding of the communications technologies used in the product and of the requirements for their specific application. It also assumes a basic ability to access and navigate a Digi TransPort router.

This application note applies only to:

Model: DIGI TransPort WR41/44/21

Digi TransPort WR41 routers must have the "Encryption" option
Digi TransPort WR21 routers must run Enterprise firmware

Firmware versions: 5169 and later

Please note: This application note has been specifically rewritten for firmware release 5169 and later and will not work on earlier versions of firmware. Please contact tech.support@digi.com if your require assistance in upgrading the firmware of the TransPort router.

1.3 Corrections

Requests for corrections or amendments to this application note are welcome and should be addressed to: tech.support@digi.com
Requests for new application notes can be sent to the same address.

2 VERSION

Version Number	Status
1.0	Published
1.1	Branding and GUI update

3 CONFIGURATION

If you already have certificates available, you can skip to section 3.2

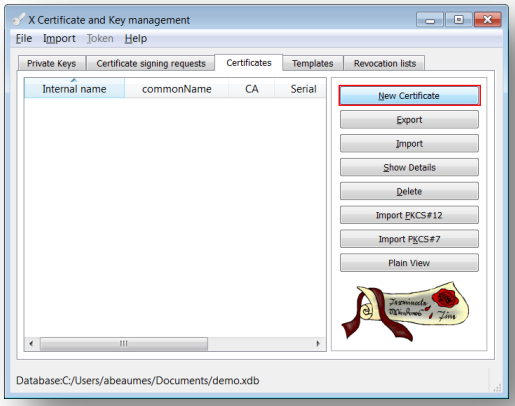
3.1 Generate Test certificates using OpenSSL and XCA

Download and install the latest release of XCA which can be found at: http://sourceforge.net/projects/xca/

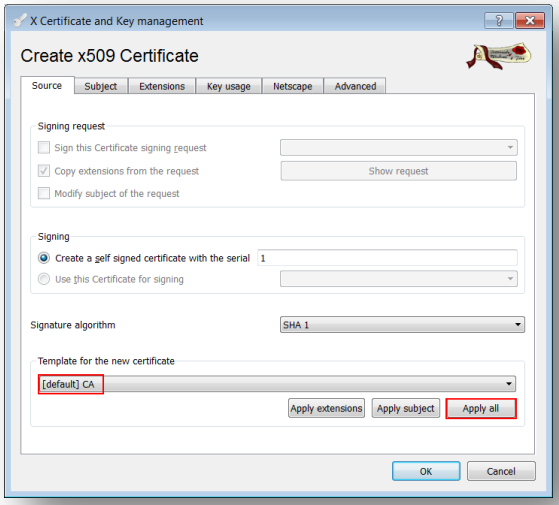
3.1.1 Create a Root CA Certificate

Open the XCA application

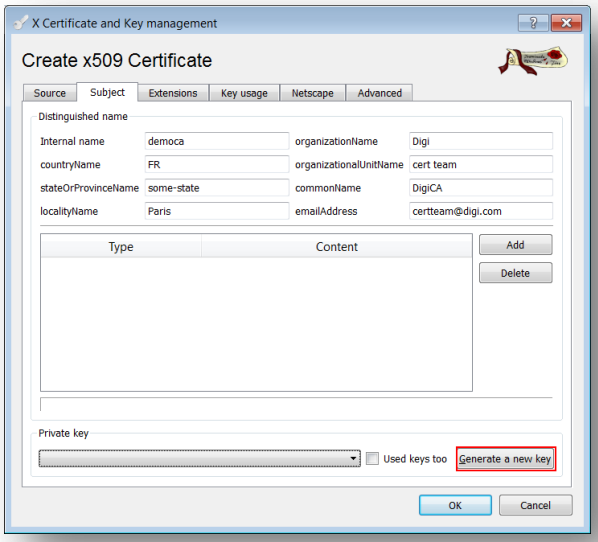
1. Click the **File** menu and select **New Database**, chose a name and click **Save.**
2. Chose a password and click **OK**
3. Click the **Certificates** tab
4. Click the **New Certificate** button



5. Under “Template for the new certificate”, select **default CA** and click **Apply all**

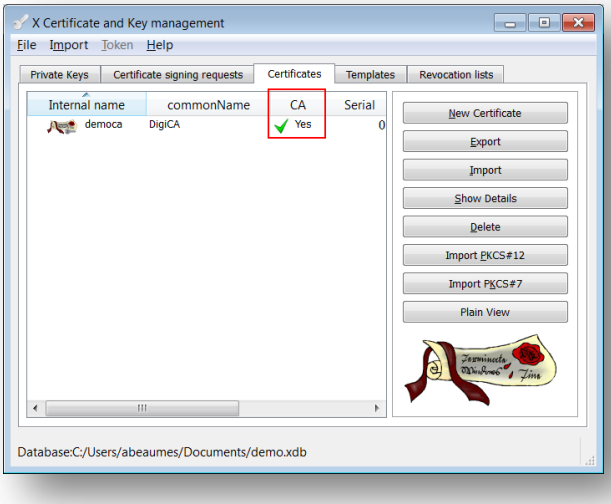


6. Go to the **Subject** tab, fill in all the information then click the **Generate a new key** button and click **OK**



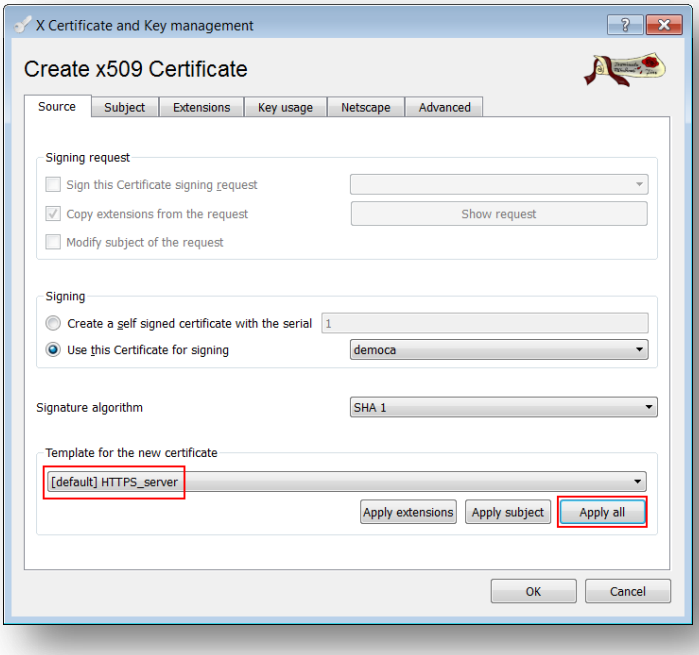
Parameter	Setting
Internal name	This is for display purposes in the tool, only
Country Name	The two-letter ISO 3166 abbreviation for your country.
State or Province Name	The state or province where your organization is legally located. Do not abbreviate. In this example: Some-State
Locality Name	The city where your organization is legally located. Do not abbreviate. In this example: Paris
Organization Name	The exact legal name of your organization. Do not abbreviate your organization name. In this example: Digi
Organizational Unit Name	Section of the organization. Examples of sections are Marketing, Research and Development, Human Resources or Sales.
Common Name	In this example DigiCA will be used.
Email Address	Enter your organization general email address. In this example certteam@digi.com

7. The certificate should now appear in the window with the **CA : YES** confirmation. If it does not say **CA: YES,** verify that you selected CA in the template and clicked Apply All.

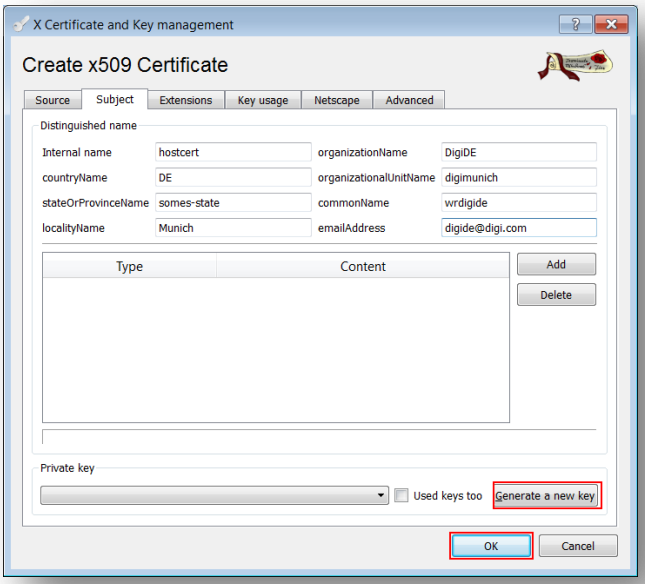


3.1.2 Create a CA-Signed Host Certificate (Router B, Responder)

1. Click the **Certificates** tab
2. Click the **New Certificate** button
3. Under Signing, make sure to select "**Use this Certificate for signing"** and chose the previously created CA.
4. Under "Template for the new certificate", select **default HTTPS_server** and click **Apply all**

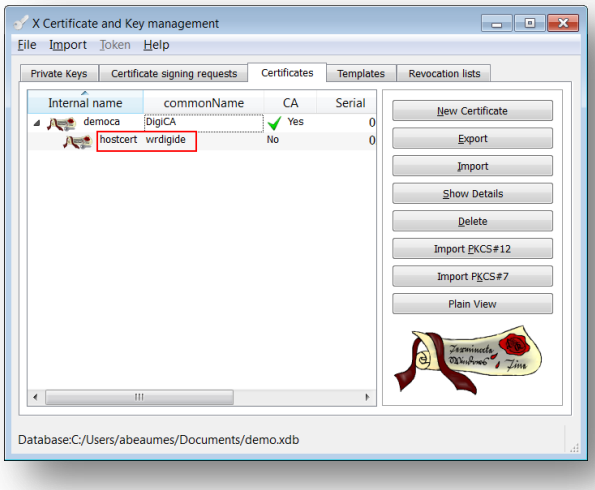


5. Go to the **Subject** tab, fill in all the information then click the **Generate a new key** button and click **OK**



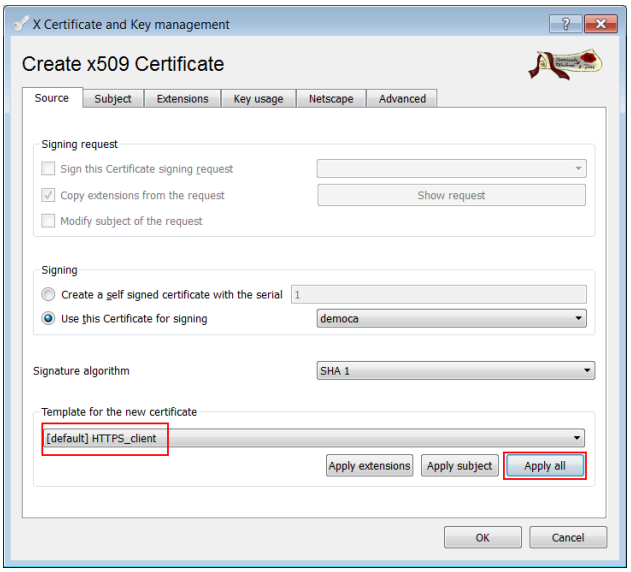
Parameter	Setting
Internal name	This is for display purposes in the tool, only
Country Name	The two-letter ISO 3166 abbreviation for your country.
State or Province Name	The state or province where your organization is legally located. Do not abbreviate. In this example: Some-State
Locality Name	The city where your organization is legally located. Do not abbreviate. In this example: Munich
Organization Name	The exact legal name of your organization. Do not abbreviate your organization name. In this example: DigiDE
Organizational Unit Name	Section of the organization. Examples of sections are Marketing, Research and Development, Human Resources or Sales.
Common Name	In this example **wrdigide** will be used. This will be used as the router Identity for the IPSec tunnel settings
Email Address	Enter your organization general email address. In this example digide@digi.com

6. The certificate should now appear in the window under the CA certificate.

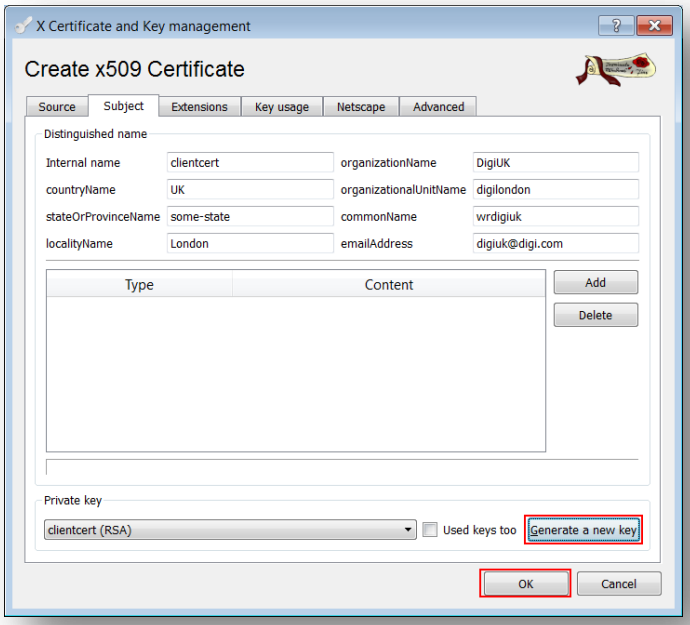


3.1.3 Create a CA-Signed Client Certificate (Router A, initiator)

1. Click the **Certificates** tab
2. Click the **New Certificate** button
3. Under Signing, make sure to select "**Use this Certificate for signing"** and chose the previously created CA.
4. Under "Template for the new certificate", select **default HTTPS_client** and click **Apply all**

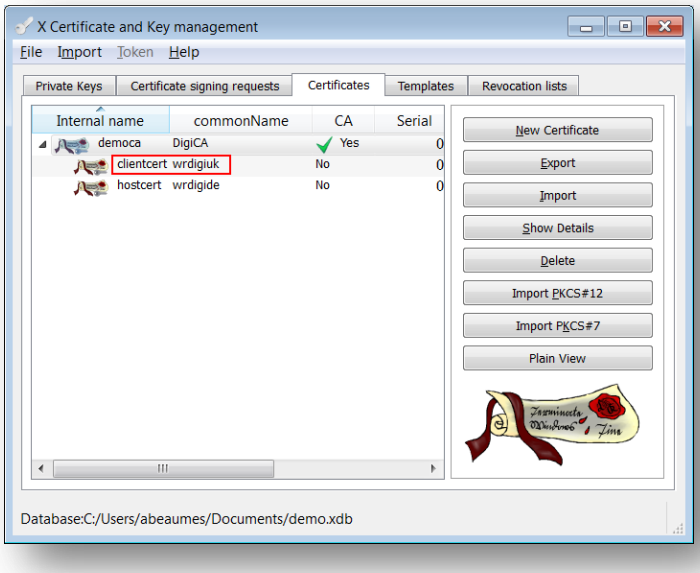


5. Go to the **Subject** tab, fill in all the information then click the **Generate a new key** button and click **OK**



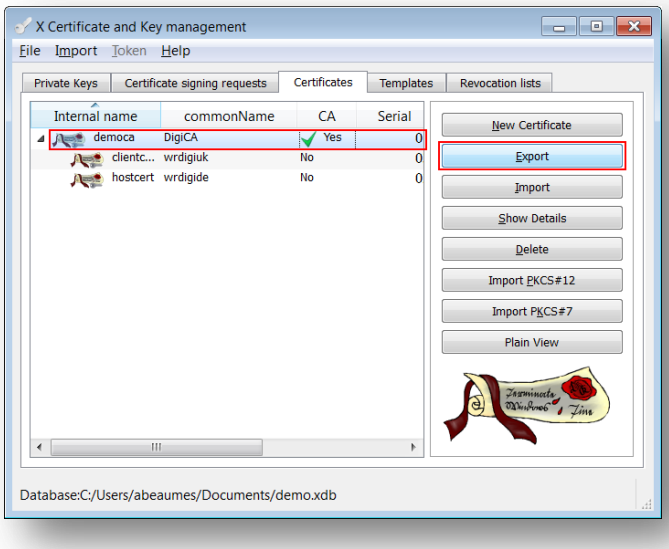
Parameter	Setting
Internal name	This is for display purposes in the tool, only
Country Name	The two-letter ISO 3166 abbreviation for your country.
State or Province Name	The state or province where your organization is legally located. Do not abbreviate. In this example: Some-State
Locality Name	The city where your organization is legally located. Do not abbreviate. In this example: Munich
Organization Name	The exact legal name of your organization. Do not abbreviate your organization name. In this example: DigiDE
Organizational Unit Name	Section of the organization. Examples of sections are Marketing, Research and Development, Human Resources or Sales.
Common Name	In this example **wrdigide** will be used. This will be used as the router Identity for the IPSec tunnel settings
Email Address	Enter your organization general email address. In this example digide@digi.com

1. The certificate should now appear in the window under the CA certificate.

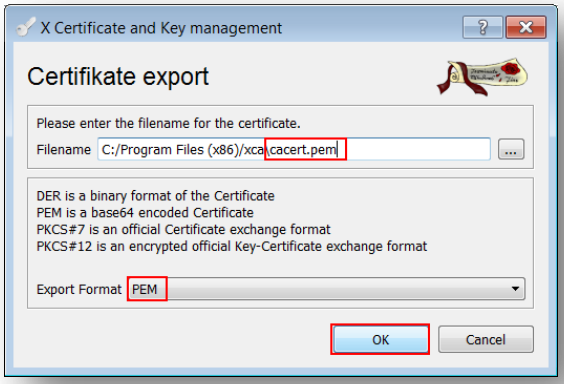


3.1.4 Export the certificates and keys in .PEM format

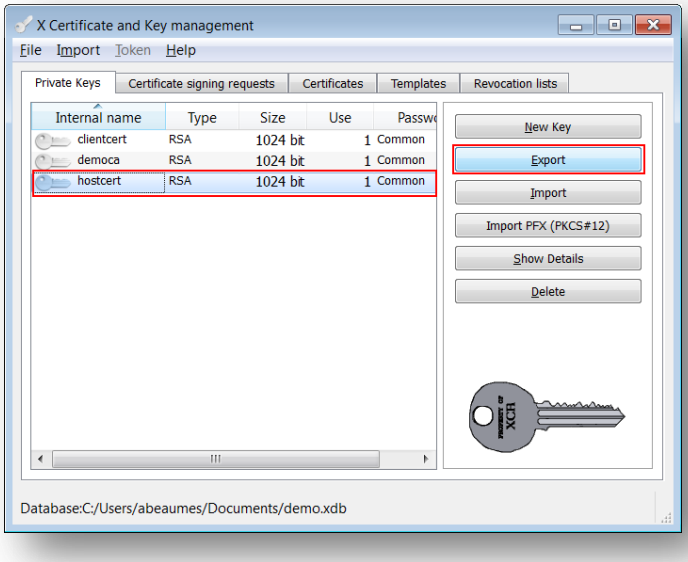
1. Select the **Certificates** Tab.
2. Highlight the DigiCA certificate and click the **Export** button



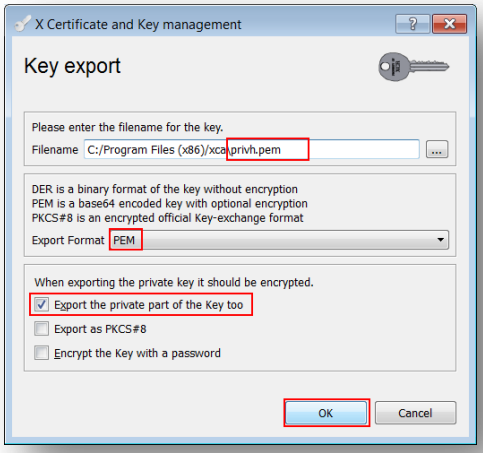
3. In the Certificate export window, select **PEM** as the export format and change the filename to **cacert.pem** and click **OK**



4. <u>Repeat the previous step for the Client and Host certificate. Rename them **certh.pem** and **certcl.pem**</u>.
5. Select the **Private Keys** tab.
6. Highlight the host certificate and click the **Export** button



7. In the Key export window, select **PEM** as the export format, check the box "**Export the private part of the key too**" and change the filename to **privh.pem** and click **OK**



8. <u>Repeat the previous step for the Client key and name it **privcl.pem**.</u>

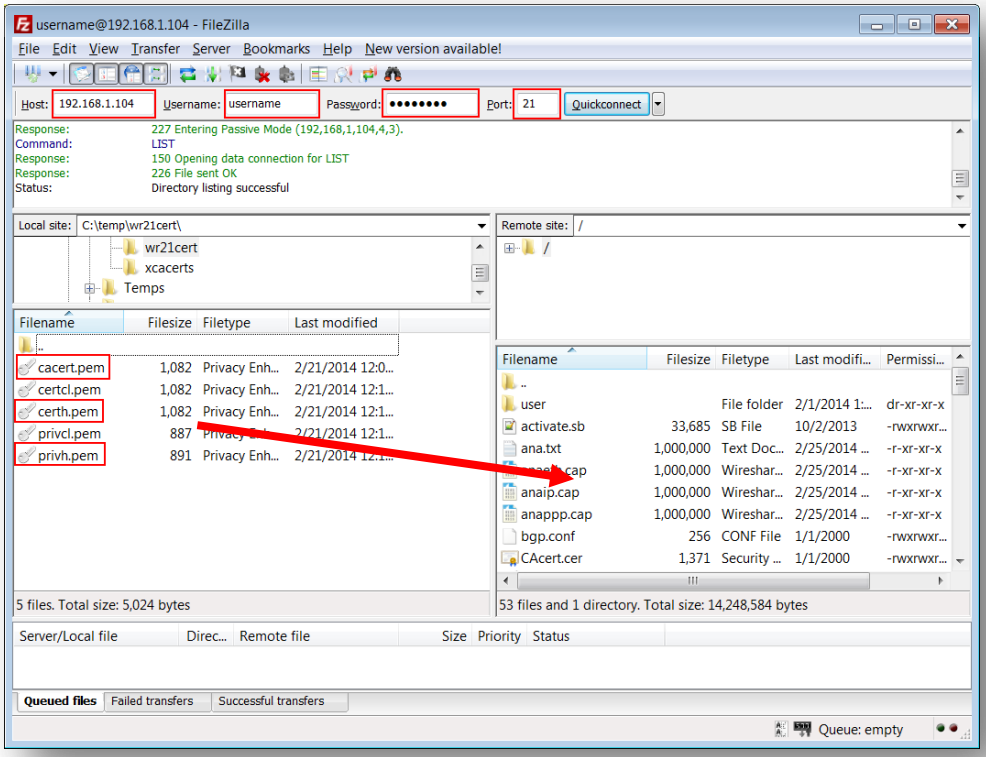
The following files should now be available:

- cacert.pem : CA root certificate
- certh.pem : Router B (responder) certificate
- certcl.pem : Router A (initiator) certificate
- privh.pem : Router B (responder) private key
- privcl.pem : Router A (initiator) private key

Please note: *It is important that the file name do not exceed the 8.3 file format and to keep the file type and naming as the TransPort router will be searching for these and load them in the certificate management automatically.*

3.2 Upload SSL certificates to the router B (responder)

3.2.1 Upload the certificates via FTP



Open an FTP connection to the TransPort router that you wish to update. In this example, using FileZilla.

Parameter	Setting	Description
Host	192.168.1.104	IP Address of the TransPort router
Username	username	Username with Access Level : Super to log in to the TransPort router (default : username)
Password	password	Password for the user with Access Level : Super to log in to the TransPort router (default : password)
Port	21	Default FTP port.
cacert.pem	-	CA Root certificate
certh.pem	-	Host Certificate
privh.pem	-	Host Private Key

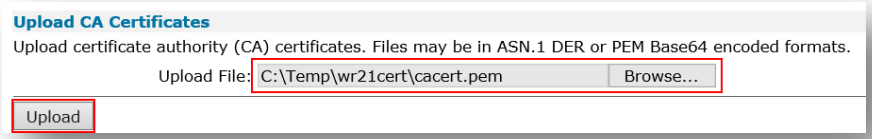
Transfer the certificates file to the root directory of the TransPort.

3.2.2 Upload the certificates via the Web GUI

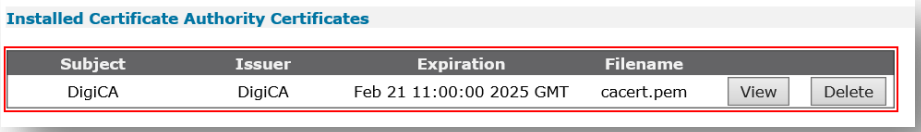
Open a web browser to the IP address of the Digi TransPort router B (responder)

Administration > X.509 Certificate Management > Certificate Authorities (CAs)

Click the browse button and select the file location where **cacert.pem** is located and click **Upload**

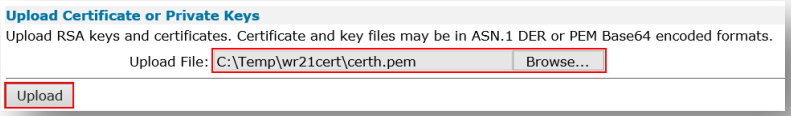


The CA Certificate should now appear under the **Installed Certificate Authority Certificates**

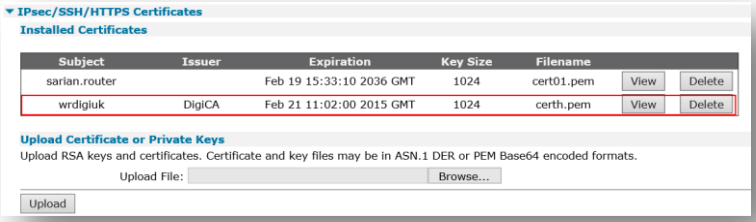


Administration > X.509 Certificate Management > IPSec/SSH/HTTPS Certificates

Click the browse button and select the file location where **certh.pem** is located and click **Upload**

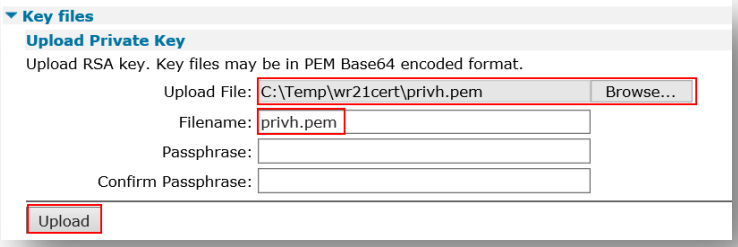


The Certificate should now appear under the **Installed Certificates**



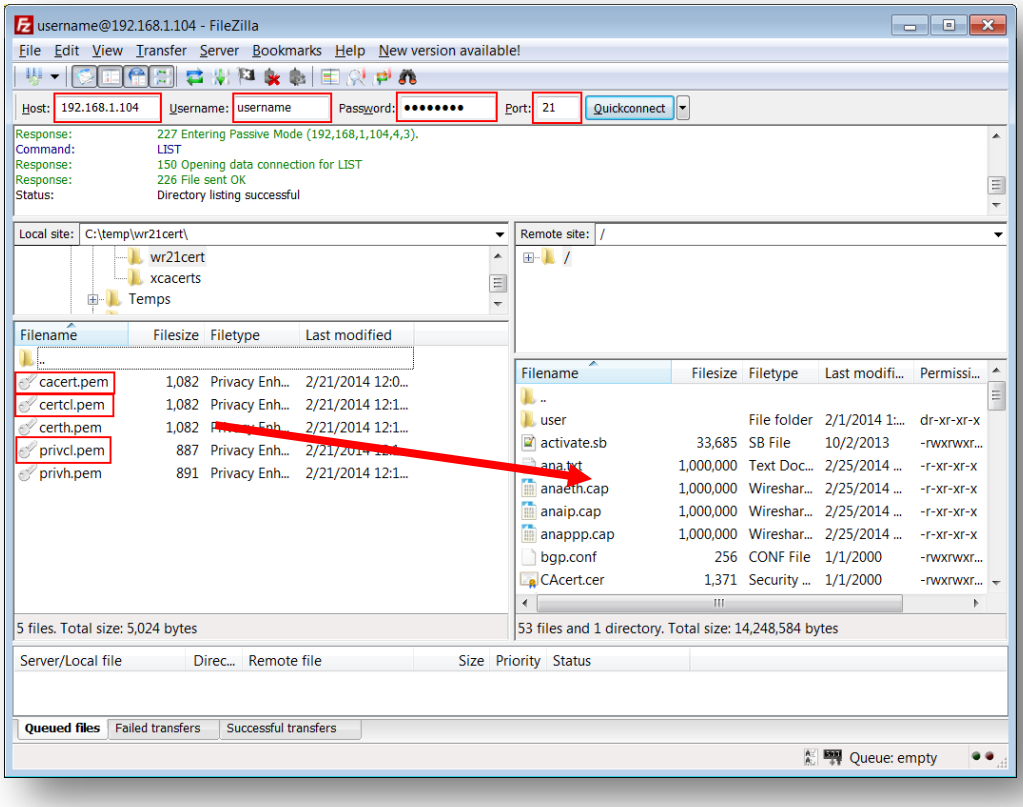
Administration > X.509 Certificate Management > Key Files

Click the browse button and select the file location where **privh.pem** is located.
Under filename, type **privh.pem** and click **Upload**.



3.3 Upload SSL certificates to the router A (initiator)

3.3.1 Upload the certificates via FTP



Open an FTP connection to the TransPort router that you wish to update. In this example, using FileZilla.

Parameter	Setting	Description
Host	192.168.1.105	IP Address of the TransPort router
Username	username	Username with Access Level : Super to log in to the TransPort router (default : username)
Password	password	Password for the user with Access Level : Super to log in to the TransPort router (default : password)
Port	21	Default FTP port.
cacert.pem	-	CA Root certificate
certcl.pem	-	Client Certificate
privcl.pem	-	Client Private Key

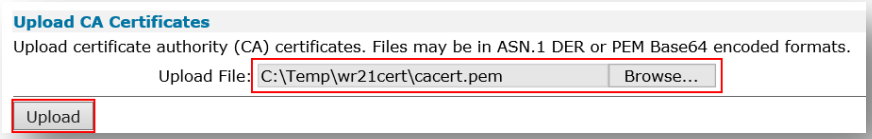
Transfer the certificates file to the root directory of the TransPort.

3.3.2 Upload the certificates via the Web GUI

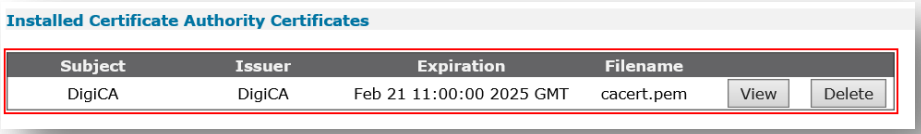
Open a web browser to the IP address of the Digi TransPort router A (initiator)

Administration > X.509 Certificate Management > Certificate Authorities (CAs)

Click the browse button and select the file location where **cacert.pem** is located and click **Upload**

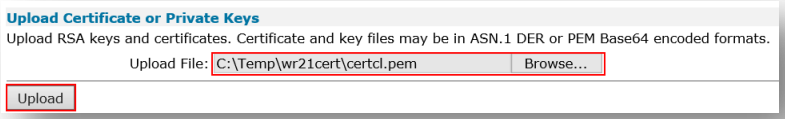


The CA Certificate should now appear under the **Installed Certificate Authority Certificates**

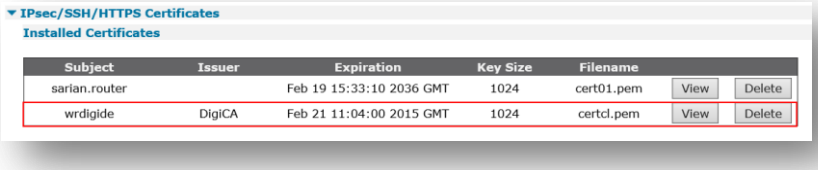


Administration > X.509 Certificate Management > IPSec/SSH/HTTPS Certificates

Click the browse button and select the file location where **certcl.pem** is located and click **Upload**

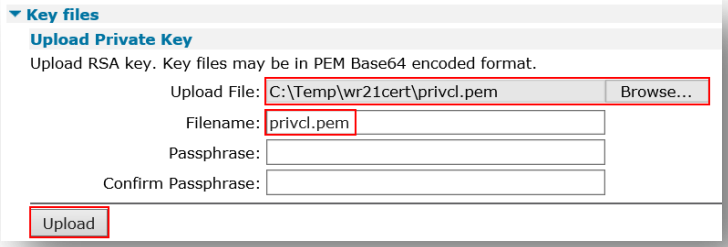


The Certificate should now appear under the **Installed Certificates**



Administration > X.509 Certificate Management > Key Files

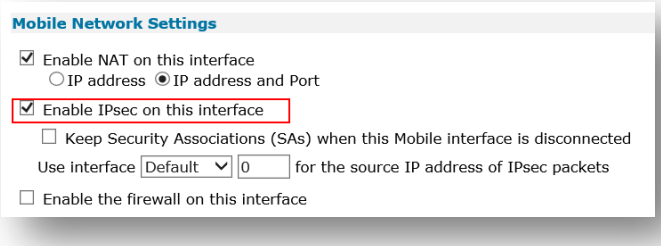
Click the browse button and select the file location where **privcl.pem** is located.
Under filename, type **privcl.pem** and click **Upload**.



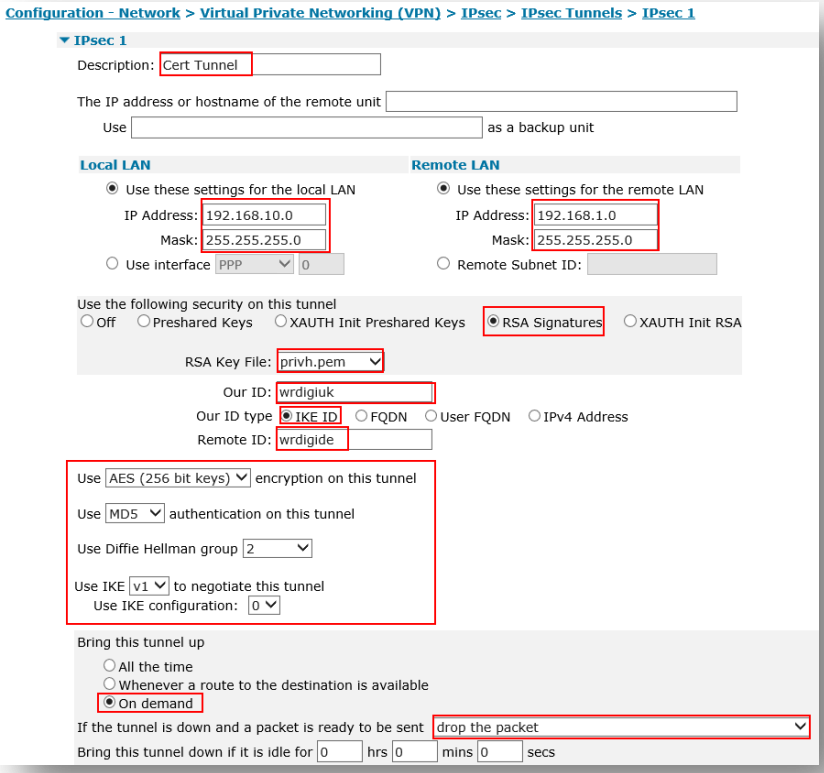
3.4 Configure the VPN Tunnel settings on router B (responder).

Enable IPSec on PPP 1 (mobile interface) :

Configuration – Network > Interfaces > Mobile



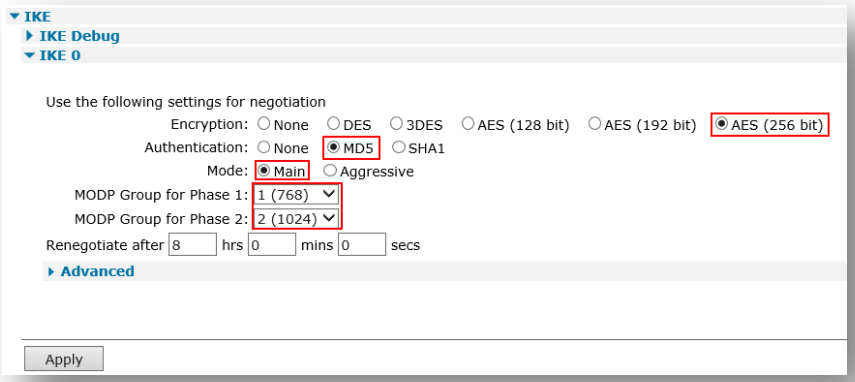
Configuration – Network > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec 0-9 > IPsec 0



Parameter	Setting	Description
Description	Cert Tunnel	Description of the IPsec tunnel
Local Lan IP Address	192.168.1.0	Local Lan IP address
Local Lan Mask	255.255.255.0	Local Lan subnet mask
Remote Lan IP Address	192.168.10.0	Remote Lan IP address
Remote Lan Mask	255.255.255.0	Remote Lan subnet mask
Use the Following security on this tunnel	RSA Signatures	Select RSA signature security for this tunnel to use the uploaded certificates
RSA Key File	privh.pem	Private key file used for router B (responder)
Our ID	wrdigiuk	ID that is matching the CN of the certificate in the first router (responder)
Our ID type	IKE ID	IKE ID for the ID type (to match the information used in the certificate)
Remote ID	wrdigide	Remote ID that is matching the CN in the second router certificate (initiator)
Encryption on this tunnel	AES 256	Encryption type used on this tunnel
Authentication on this tunnel	MD5	Authentication type used on this tunnel
Use Diffie Hellman Group	2	Use DH Group 2
Use IKE configuration	1	IKE settings used to setup the tunnel
Bring this tunnel up	On demand	Settings to bring the IPsec tunnel up
If the tunnel is down and a packet is ready to be sent	Drop the backup	Drop the packet if the tunnel is down.

Click **Apply** and **Save** to save the settings.

Configuration – Network > Virtual Private Networking (VPN) > IPsec > IKE > IKE 1

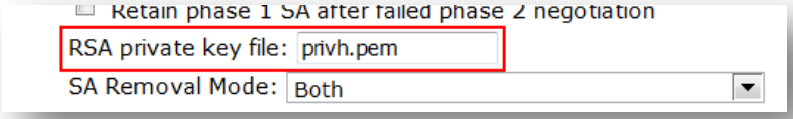


Parameter	Setting	Description
Encryption	AES (256 bit)	Encryption settings used on the tunnel
Authentication	MD5	Authentication settings used on the tunnel
Mode	Main	Phase 1 negotiation type
MODP Group for Phase 1	1 (758)	DH Phase 1
MODP Group for Phase 2	2 (1024)	DH Phase 2

Click **Apply** and **Save** to save the settings.

Configuration – Network > Virtual Private Networking (VPN) > IPsec > IKE > IKE 1 > Advanced

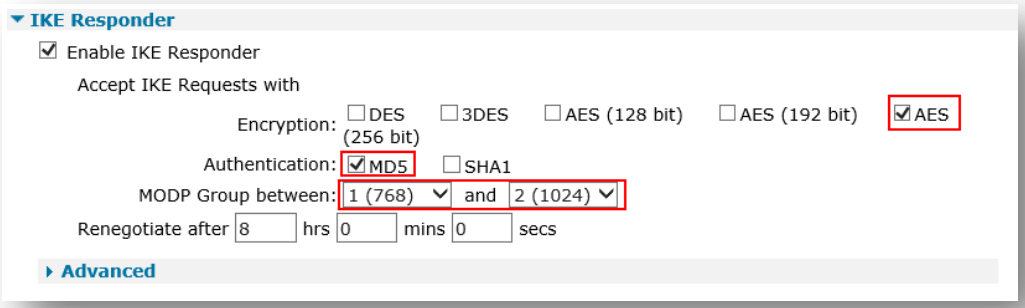
Enter the private key file name



Click **Apply** and **Save** to save the settings.

Configuration – Network > Virtual Private Networking (VPN) > IPsec > IKE > IKE Responder

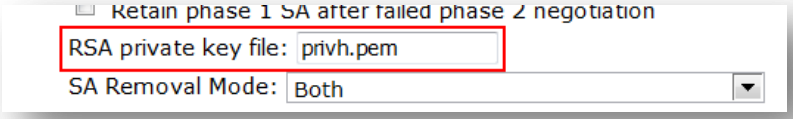
By default the Digi TransPort will accept any type of IKE requests. It is recomended to enable only the ones that are used in the tunnel.



Parameter	Setting	Description
Enable IKE Responder	Checked	Enable IKE responder
Encryption	AES (256 bit)	Encryption type used on this tunnel
Authentication	MD5	Authentication type used on this tunnel
MODP Group Between	1 (768) and 2 (1024)	DH groups used on this tunnel

Configuration – Network > Virtual Private Networking (VPN) > IPsec > IKE > IKE Responder

Enter the private key file name

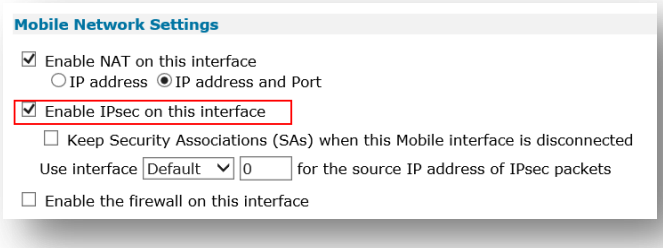


Click **Apply** and **Save** to save the settings.

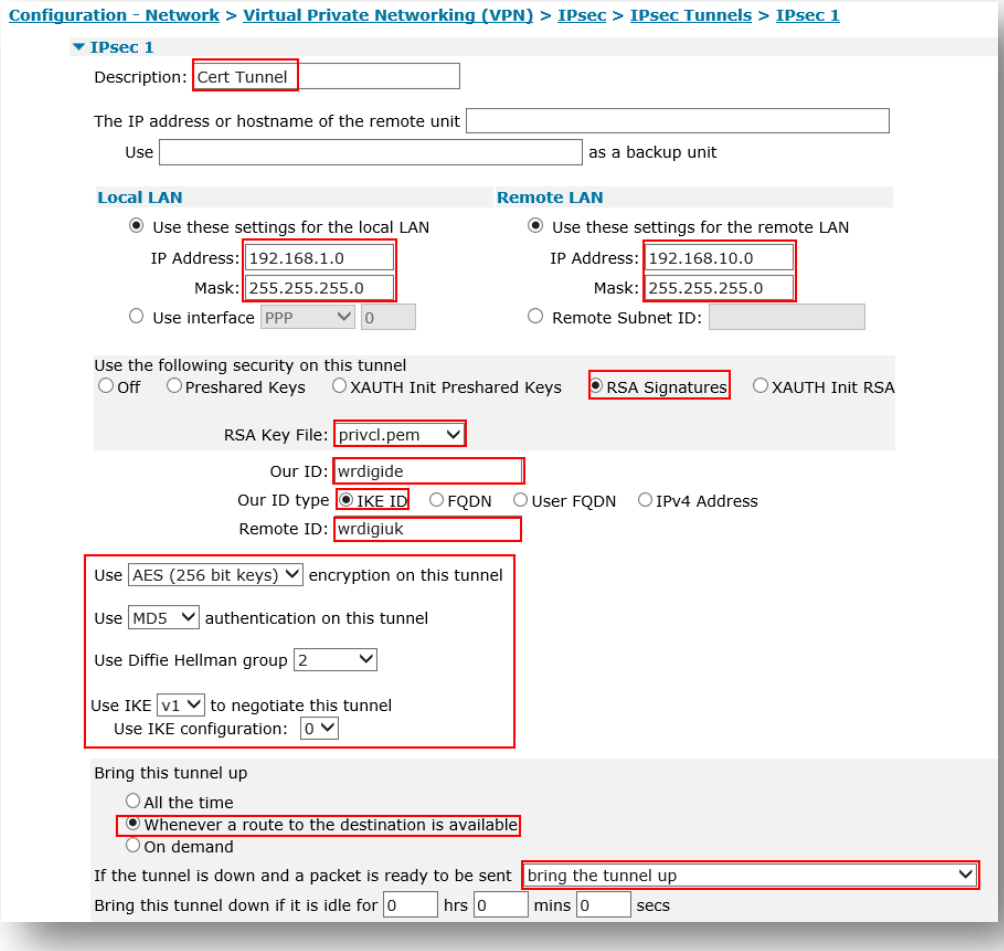
3.5 Configure the VPN Tunnel settings on router A (Initiator).

Enable IPSec on PPP 1 (mobile interface) :

Configuration – Network > Interfaces > Mobile



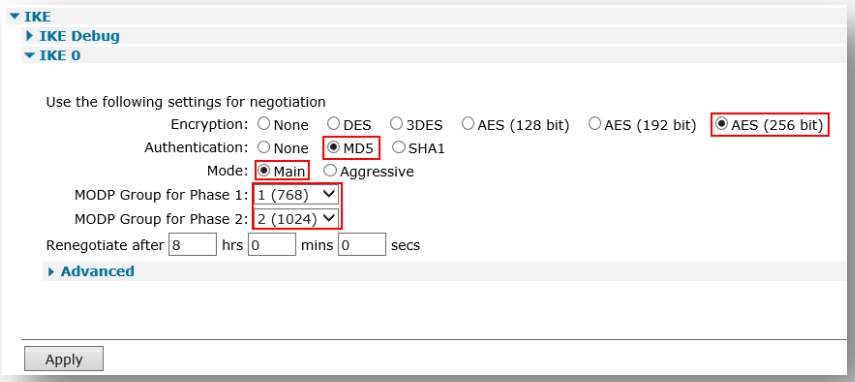
Configuration – Network > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec 0-9 > IPsec 0



Parameter	Setting	Description
Description	Cert Tunnel	Description of the IPsec tunnel
IP Address / Hostname of Remote Endpoint	1.2.3.4	IP Address of the remote endpoint router B (responder)
Local Lan IP Address	192.168.10.0	Local Lan IP address
Local Lan Mask	255.255.255.0	Local Lan subnet mask
Remote Lan IP Address	192.168.1.0	Remote Lan IP address
Remote Lan Mask	255.255.255.0	Remote Lan subnet mask
Use the Following security on this tunnel	RSA Signatures	Select RSA signature security for this tunnel to use the uploaded certificates
RSA Key File	Privcl.pem	Private key file used for router A (initiator)
Our ID	wrdigide	ID that is matching the CN of the certificate in the first router (initiator)
Our ID type	IKE ID	IKE ID for the ID type (to match the information used in the certificate)
Remote ID	wrdigiuk	Remote ID that is matching the CN in the second router certificate (responder)
Encryption on this tunnel	AES 256	Encryption type used on this tunnel
Authentication on this tunnel	MD5	Authentication type used on this tunnel
Use Diffie Hellman Group	2	Use DH Group 2
Use IKE configuration	1	IKE settings used to setup the tunnel
Bring this tunnel up	Whenever a route to the destination is available	Settings to bring the IPsec tunnel up
If the tunnel is down and a packet is ready to be sent	Bring the tunnel up	Drop packets to the remote side if the tunnel is down

Click **Apply** and **Save** to save the settings.

Configuration – Network > Virtual Private Networking (VPN) > IPsec > IKE > IKE 1



Parameter	Setting	Description
Encryption	AES (256 bit)	Encryption settings used on the tunnel
Authentication	MD5	Authentication settings used on the tunnel
Mode	Main	Phase 1 negotiation type
MODP Group for Phase 1	1 (758)	DH Phase 1
MODP Group for Phase 2	2 (1024)	DH Phase 2

Click **Apply** and **Save** to save the settings.

Configuration – Network > Virtual Private Networking (VPN) > IPsec > IKE > IKE 1 > Advanced

Enter the private key file name

Click **Apply** and **Save** to save the settings.

4 TESTING

This section will show that the IPSec tunnel has been established.

The Event log will show the IPSec tunnel is up.

Management – Event Log

```
14:49:48, 25 Feb 2014,(2) IKE SA Removed. Peer: wrdigiuk,Successful Negotiation
14:49:18, 25 Feb 2014,Eroute 0 VPN up peer: wrdigiuk
14:49:18, 25 Feb 2014,New IPSec SA created by wrdigiuk
```

MANAGEMENT - CONNECTIONS > VIRTUAL PRIVATE NETWORKING (VPN) > IPSEC > IPSEC TUNNELS > IPSEC TUNNELS 0 - 9 > IPSEC TUNNELS 0 - 9

Navigate to the above link where the status of the newly established IPSec tunnel/s can be seen. The first column shows which tunnel number the tunnel is connected to.

4.1 Confirm Traffic Traverses the IPSec Tunnels

This section will show traffic passing across the tunnel. To test this easily, an ICMP Echo Request/Reply (or PING) will pass from the Router A lan (initiator) to Router B Ethernet interface side (responder)

Administration > Execute a command

```
Ping 192.168.10.254 -e0
```

Using –e0 specifies that the source address is taken from Ethernet 0 which is the negociated LAN settings in the IPSec tunnel.

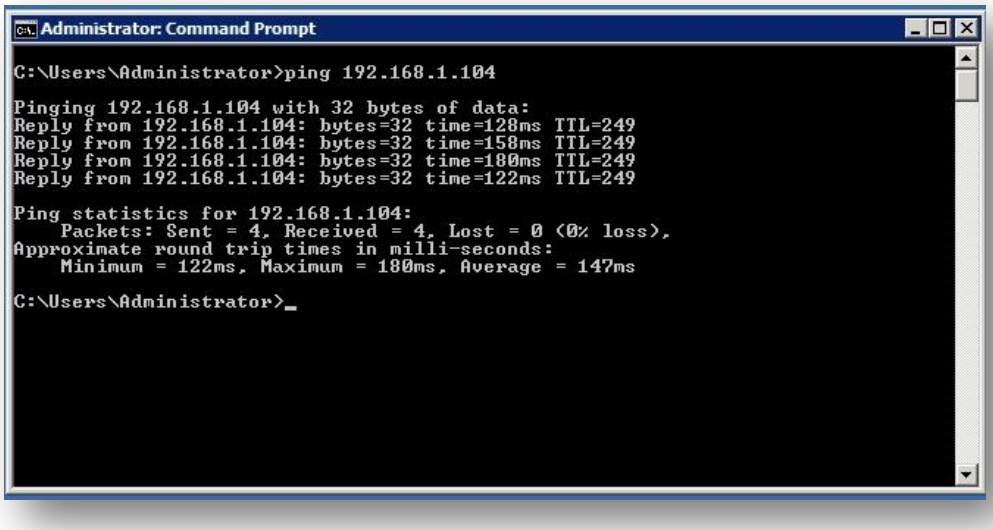
```
Command: ping 192.168.10.254 -e0
Command result

Pinging Addr [192.168.10.254]

sent PING # 1
PING receipt # 1 : response time 0.26 seconds
Iface: PPP 1
Ping Statistics
Sent        : 1
Received    : 1
Success     : 100 %
Average RTT : 0.26 seconds

OK
```

Pinging from Computer on Ethernet side of Router B:



5 CONFIGURATION FILES

Digi TransPort WR 21 Router B (Responder)

```
eroute 1 descr "Cert Tunnel"
eroute 1 peerid "wrdigide"
eroute 1 ourid "wrdigiuk"
eroute 1 locip "192.168.10.0"
eroute 1 locmsk "255.255.255.0"
eroute 1 remip "192.168.1.0"
eroute 1 remmsk "255.255.255.0"
eroute 1 ESPauth "MD5"
eroute 1 ESPenc "AES"
eroute 1 authmeth "RSA"
eroute 1 ikecfg 1
eroute 1 dhgroup 2
eroute 1 enckeybits 256
eroute 1 privkey "privh.pem"
eroute 1 debug ON
ike 1 encalg "AES"
ike 1 keybits 256
ike 1 aggressive ON
ike 1 ipsecgroup 2
ike 1 dpd OFF
ike 1 privrsakey "privh.pem"
ike 1 delmode 3
```

Digi TransPort WR 21 Router A (initiator)

```
eroute 1 descr "Cert Tunnel"
eroute 1 peerip "1.2.3.4"
eroute 1 peerid "wrdigiuk"
eroute 1 ourid "wrdigide"
eroute 1 locip "192.168.1.0"
eroute 1 locmsk "255.255.255.0"
eroute 1 remip "192.168.10.0"
eroute 1 remmsk "255.255.255.0"
eroute 1 ESPauth "MD5"
eroute 1 ESPenc "AES"
eroute 1 authmeth "RSA"
eroute 1 nosa "TRY"
eroute 1 autosa 2
eroute 1 ikecfg 1
eroute 1 dhgroup 2
eroute 1 enckeybits 256
eroute 1 privkey "privcl.pem"
eroute 1 debug ON
ike 1 encalg "AES"
ike 1 keybits 256
ike 1 ikegroup 2
ike 1 privrsakey "privcl.pem"
ike 1 delmode 3
```