Quick Note 054

Digi TransPort to Cisco VPN Tunnel using OpenSSL certificates.

February 2021

Contents

1 Introduction 3

1.1 Outline 3
1.2 Assumptions 3
1.3 Corrections 3

2 Version 3
3 certificates creation 4

If you already have certificates available, you can skip to section 3.2 4
3.1 Generate Test certificates using OpenSSL and XCA 4

3.1.1 Create a Root CA Certificate 4
3.1.2 Create a CA-Signed Host Certificate (Cisco Router, Responder) 7
3.1.3 Create a CA-Signed Client Certificate (Digi TransPort WR, initiator) 9
3.1.4 Export the certificates and keys in .PEM format 11

4 Digi transport configuration 14

4.1 Upload SSL certificates to the Digi TransPort WR (initiator) 14

4.1.1 Upload the certificates via FTP 14
4.1.2 Upload the certificates via the Web GUI 15

4.2 Configure the VPN Tunnel settings on the Digi TransPort WR (Initiator). 16

5 Cisco configuration 19

5.1 Import the certificates and private key 19

5.1.1 Create a trustpoint for the CA root certificate 19
5.1.2 Import the CA root certificate in the previously created trustpoint with copy and paste 19
5.1.3 Create a trustpoint for the public certificate and the private key 20
5.1.4 Import the public certificate in the previously created trustpoint with copy and paste 20

5.2 Configure the tunnel 21

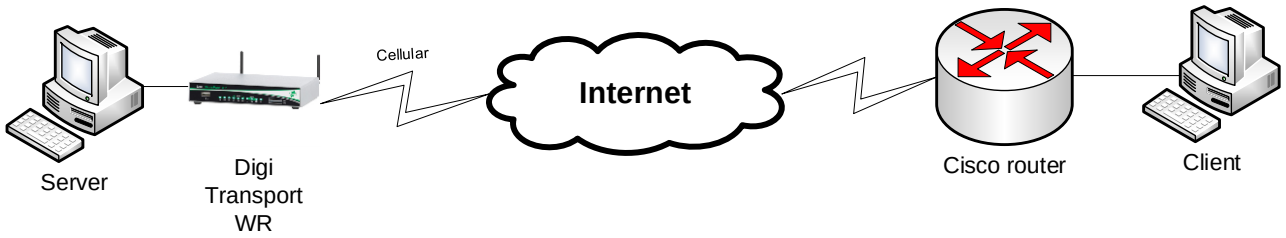
6 Testing 22

6.1 Confirm Traffic Traverses the IPSec Tunnels 23

7 Configuration files 24

1 INTRODUCTION

1.1 Outline



This document describes how to create, upload SSL certificates and configure Digi TransPort WR and Cisco routers to build an IPsec 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

Model: Cisco router running Advanced Enterprise Image.

Firmware versions: 15.9

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	Updated for new SarOS and Cisco firmware

3 CERTIFICATES CREATION

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

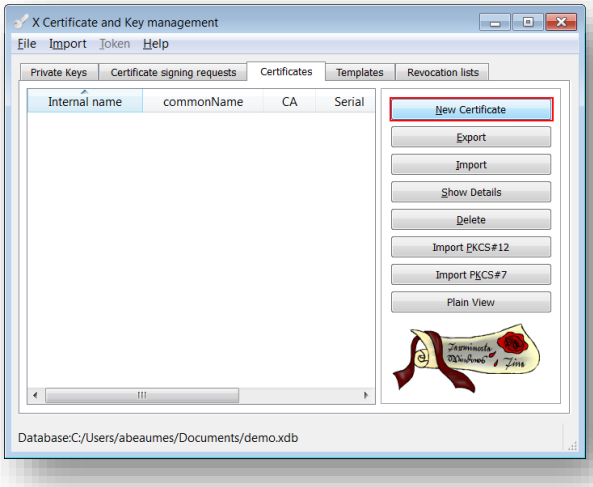
3.1 Generate Test certificates using OpenSSL and XCA

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

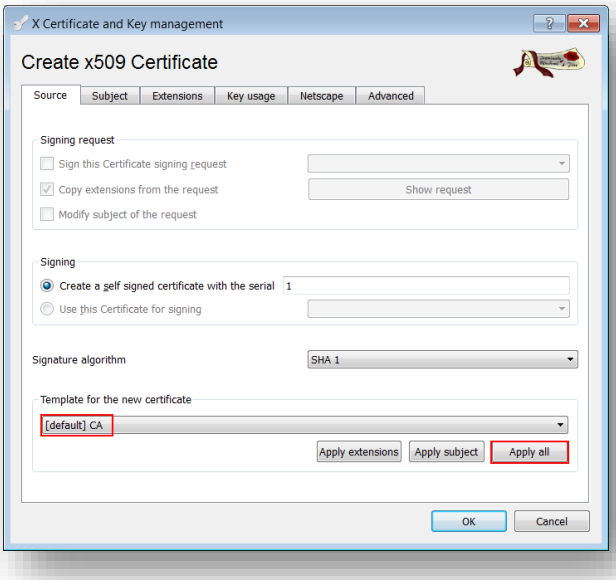
3.1.1 Create a Root CA Certificate

Open the XCA application

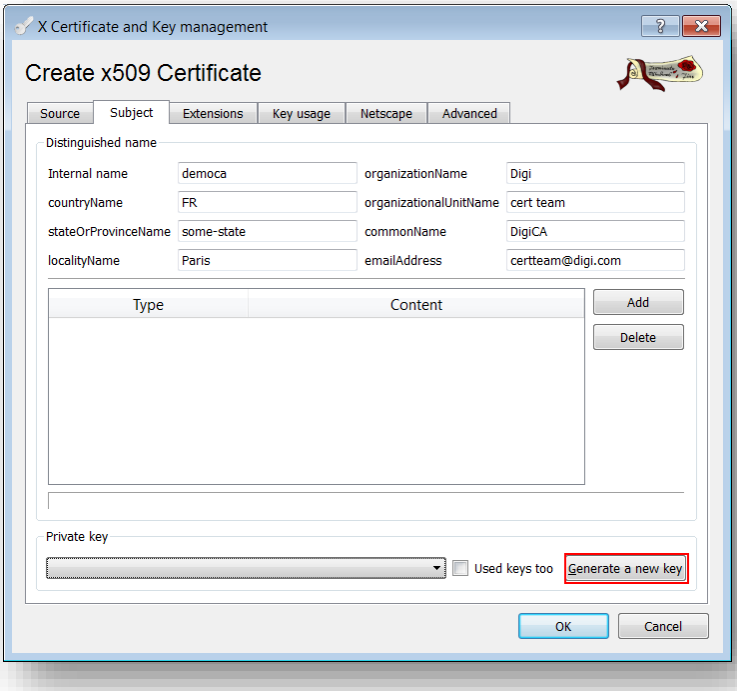
1. Click the **File** menu and select **New Database**, chose a name and click **Save.**
2. Chose a password and click **OK**
3. Click the **Certificates** tab
4. Click the **New Certificate** button



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

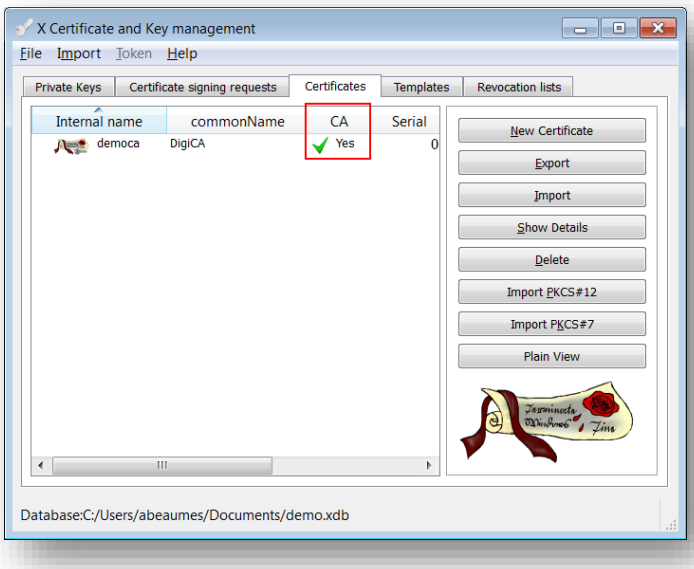


6. Go to the **Subject** tab, fill in all the information then click the **Generate a new key** button and click **OK**



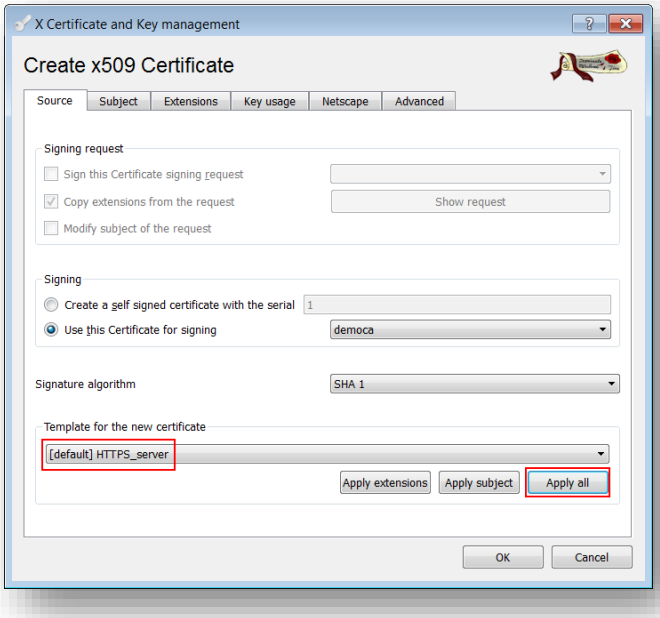
Parameter	Setting
Internal name	This is for display purposes in the tool, only
Country Name	The two-letter ISO 3166 abbreviation for your country.
State or Province Name	The state or province where your organization is legally located. Do not abbreviate. In this example: Some-State
Locality Name	The 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.

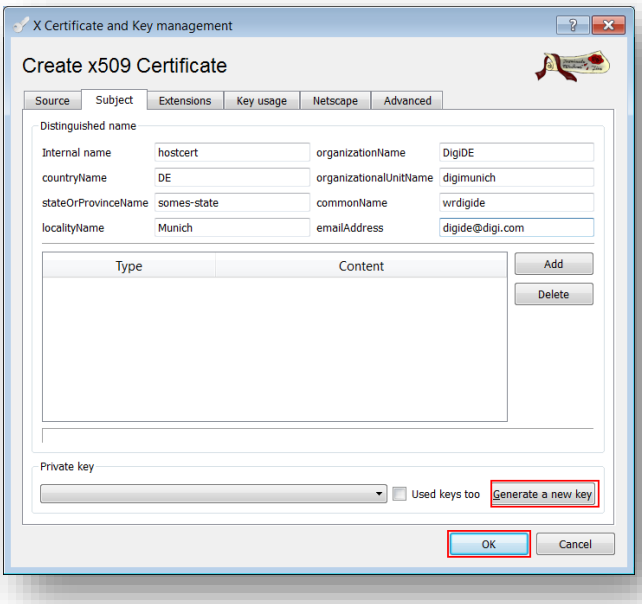


3.1.2 Create a CA-Signed Host Certificate (Cisco Router, Responder)

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**

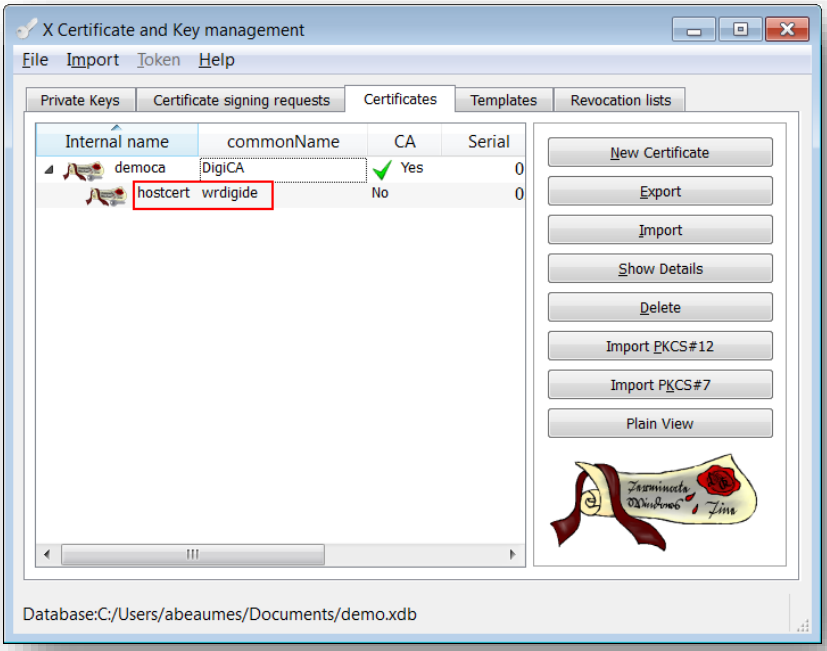


5. Go to the **Subject** tab, fill in all the information then click the **Generate a new key** button and click **OK**



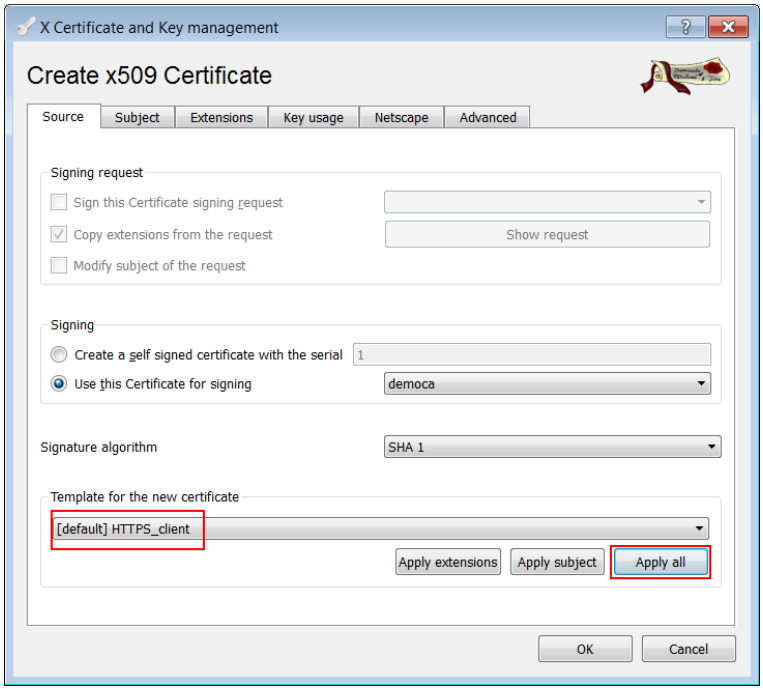
Parameter	Setting
Internal name	This is for display purposes in the tool, only
Country Name	The two-letter ISO 3166 abbreviation for your country.
State or Province Name	The state or province where your organization is legally located. Do not abbreviate. In this example: Some-State
Locality Name	The 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

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

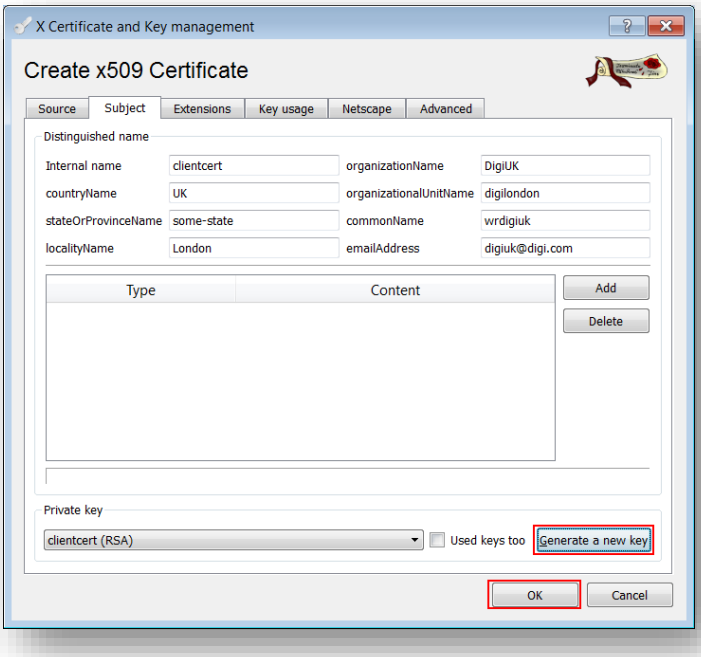


3.1.3 Create a CA-Signed Client Certificate (Digi TransPort WR, initiator)

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**

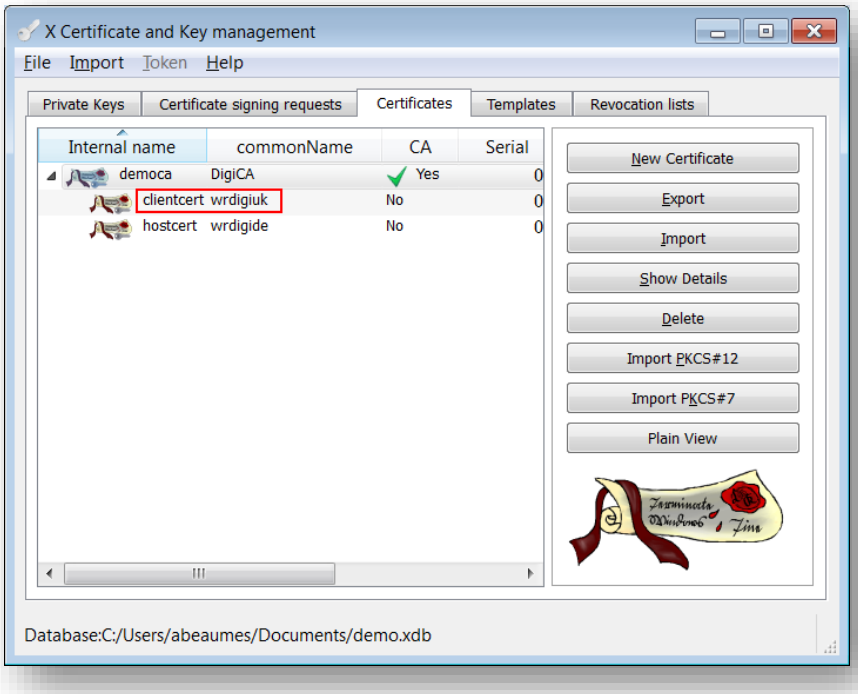


5. Go to the **Subject** tab, fill in all the information then click the **Generate a new key** button and click **OK**



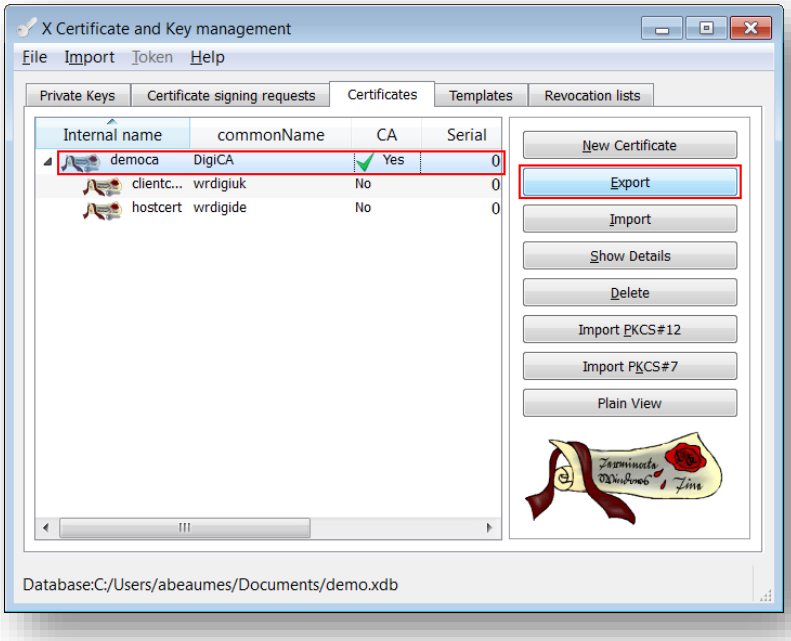
Parameter	Setting
Internal name	This is for display purposes in the tool, only
Country Name	The two-letter ISO 3166 abbreviation for your country.
State or Province Name	The state or province where your organization is legally located. Do not abbreviate. In this example: Some-State
Locality Name	The 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.



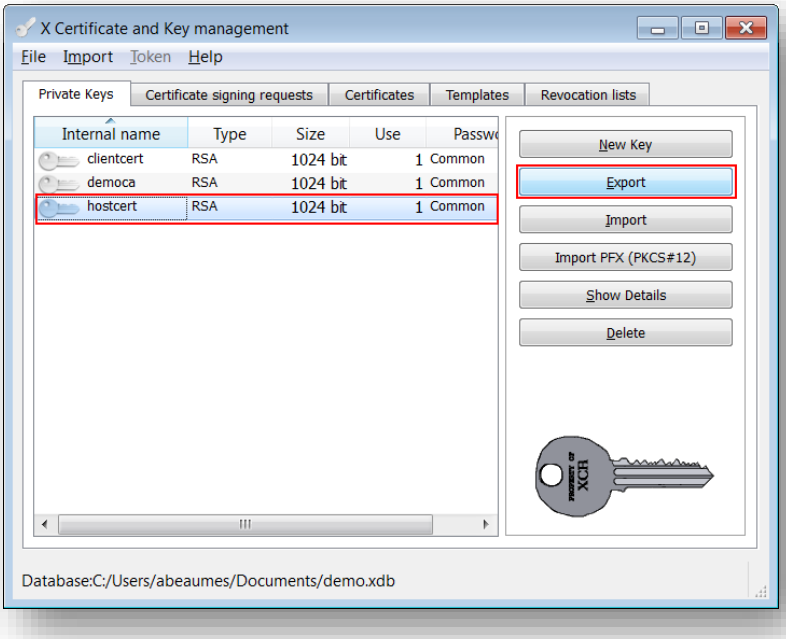
3.1.4 Export the certificates and keys in .PEM format

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

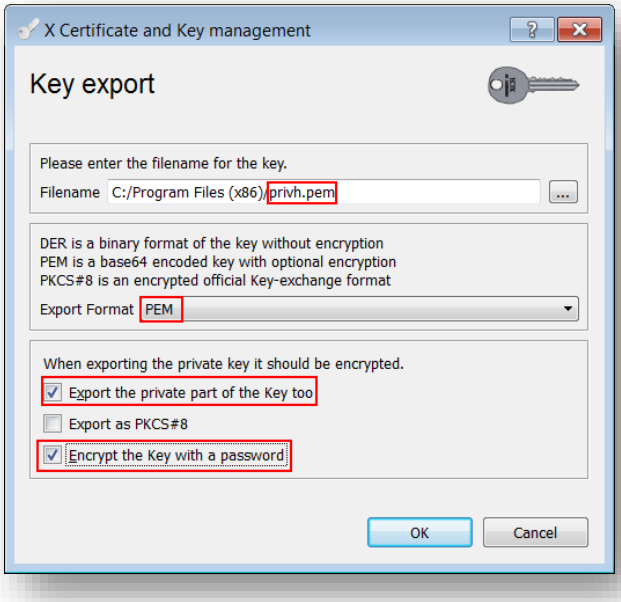


3. In the Certificate export window, select **PEM** as the export format and change the filename to **cacert.pem** and click **OK**

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**



Please note: Cisco routers require the private key to be encrypted. Make sure to check the box "**Encrypt the key with a password**" when export the key for the Cisco device (**privh.pem** below) and specify a passphrase.
In the next step, we will convert the private key, which is encrypted in AES by default (in the case of XCA software), and for Cisco we need DES or DES3. Therefore, you have to convert. Let's do it on the nearest Linux server with openssl installed with the following command.

openssl rsa -in privh.pem -out privh.pem -des3

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

The following files should now be available:

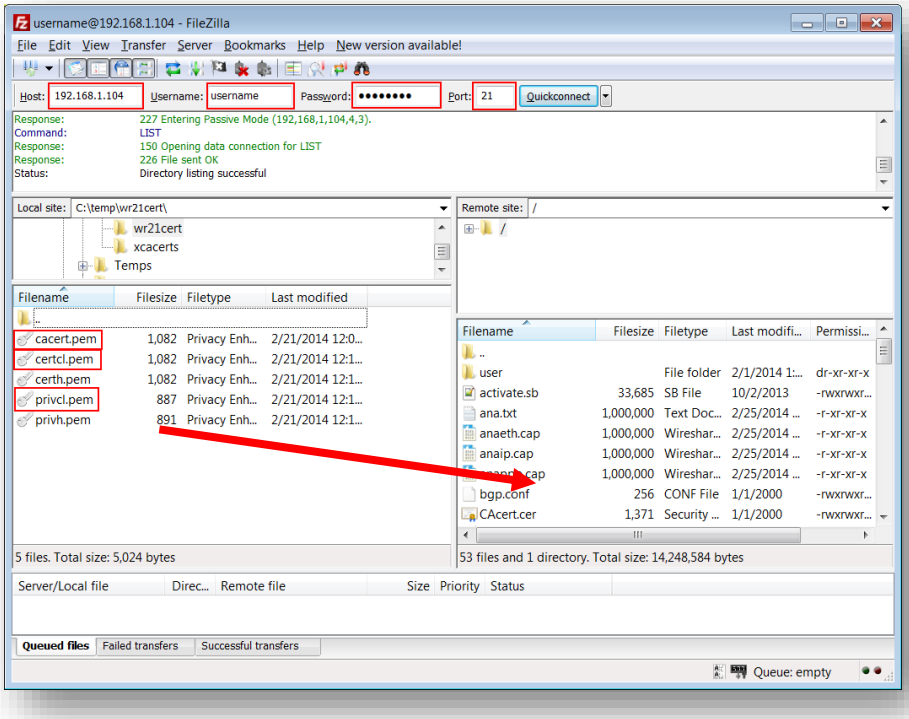
- cacert.pem : CA root certificate
- certh.pem : Cisco (responder) certificate
- certcl.pem : TransPort WR (initiator) certificate
- privh.pem : Cisco (responder) private key (password encrypted)
- privcl.pem : TransPort WR (initiator) private key

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.*

4 DIGI TRANSPORT CONFIGURATION

4.1 Upload SSL certificates to the Digi TransPort WR (initiator)

4.1.1 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

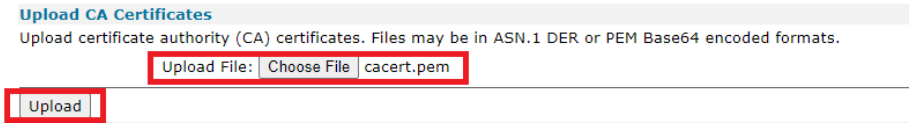
Transfer the certificates file to the root directory of the TransPort.

4.1.2 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)

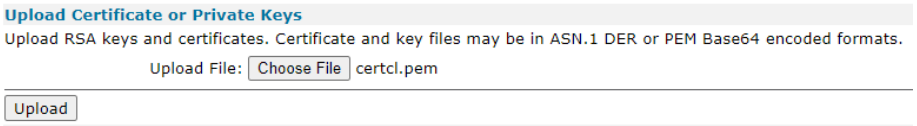
Click the browse button and select the file location where **cacert.pem** is located and click **Upload**



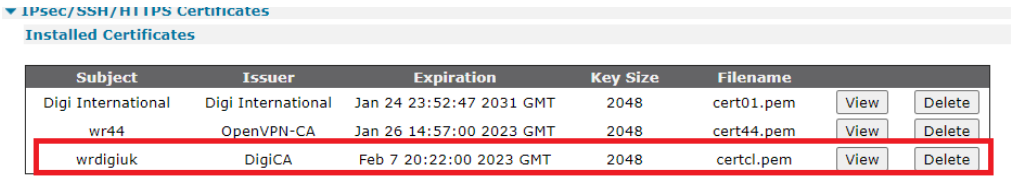
The CA Certificate should now appear under the **Installed Certificate Authority Certificates**

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**

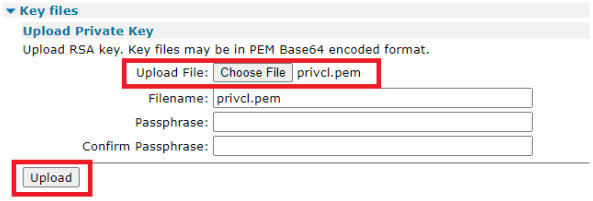


The Certificate should now appear under the **Installed Certificates**



Administration > X.509 Certificate Management > Key Files

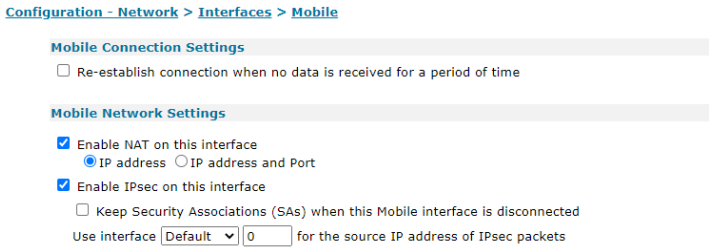
Click the browse button and select the file location where **privcl.pem** is located.
Under filename, type **privcl.pem** and click **Upload**.



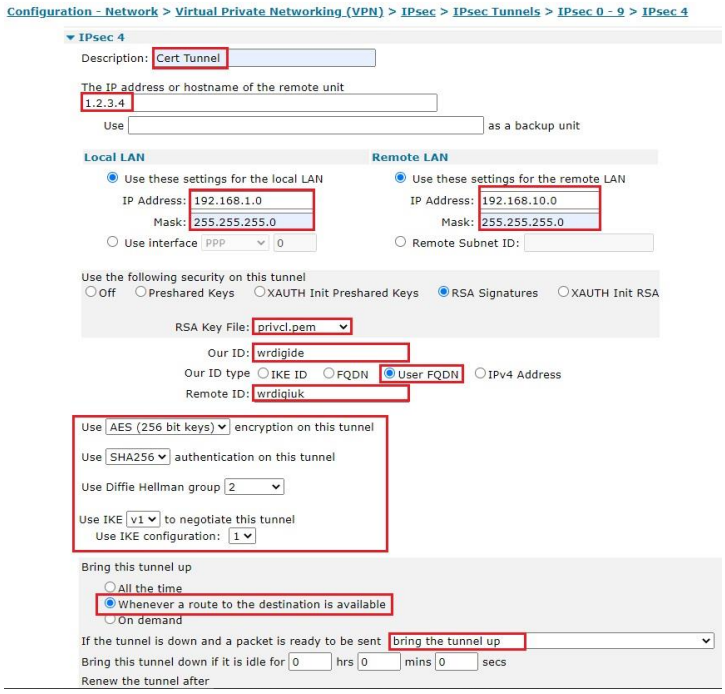
4.2 Configure the VPN Tunnel settings on the Digi TransPort WR (Initiator).

Enable IPSec on PPP 1 (mobile interface) :

Configuration – Network > Interfaces > Mobile



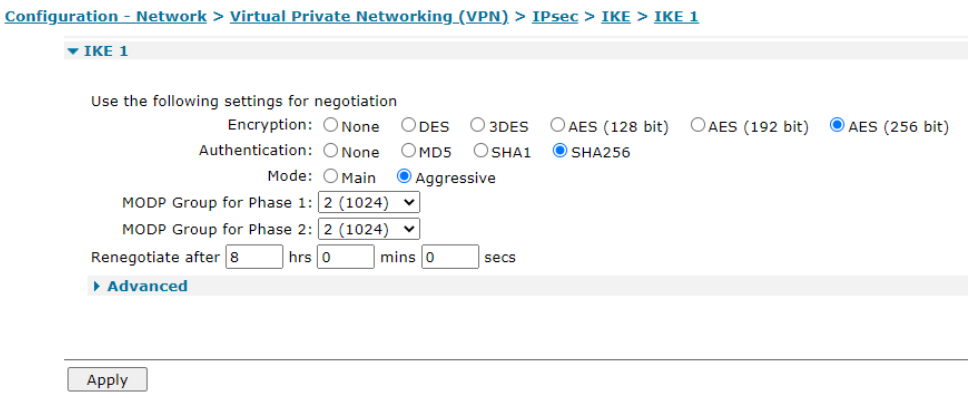
Configuration – Network > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec 0-9 > IPsec 0



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	User FQDN	User FQDN for the ID type (to match the CN 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	0	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

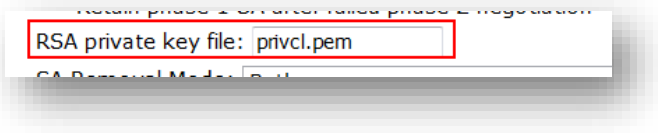


Parameter	Setting	Description
Encryption	AES (256 bit)	Encryption settings used on the tunnel
Authentication	MD5	Authentication settings used on the tunnel
Mode	Main	Phase 1 negotiation type
MODP Group for Phase 1	1 (758)	DH Phase 1
MODP Group for Phase 2	2 (1024)	DH Phase 2

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.

5 CISCO CONFIGURATION

5.1 Import the certificates and private key

5.1.1 Create a trustpoint for the CA root certificate

```
cisco (config)#crypto ca trustpoint digiroot
cisco (ca-trustpoint)#enrollment terminal pem
cisco (ca-trustpoint)#exit
```

5.1.2 Import the CA root certificate in the previously created trustpoint with copy and paste

```
cisco (config)#crypto ca authenticate digiroot

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
XXXXXXXXXXXXXXXXXXXXXXXXXXX
-----END CERTIFICATE-----
quit

Certificate has the following attributes:
Fingerprint: xxxxxxx
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

Make sure that the certificate starts and ends like shown.

5.1.3 Create a trustpoint for the public certificate and the private key

```
cisco (config)#crypto ca trustpoint digitest
cisco (ca-trustpoint)#enrollment terminal pem
cisco (ca-trustpoint)#exit
```

5.1.4 Import the public certificate in the previously created trustpoint with copy and paste

```
cisco (config)#crypto pki import digitest pem terminal password digi


% Enter PEM-formatted CA certificate.
% End with a blank line or "quit" on a line by itself.
-----BEGIN CERTIFICATE-----
xxxxxx
-----END CERTIFICATE-----
quit

% Enter PEM-formatted encrypted private General Purpose key.
% End with "quit" on a line by itself.
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,XXXXXXXXXXXX
-----BEGIN CERTIFICATE-----
xxxxx
-----END CERTIFICATE-----
quit

% Enter PEM-formatted General Purpose certificate.
% End with a blank line or "quit" on a line by itself.
-----BEGIN CERTIFICATE-----
xxxxx
-----END CERTIFICATE-----
quit

% PEM files import succeeded.
```

The last part of the command is the password used for the private key during certificates creation.

First, re-enter the CA certificate. Second, enter the private key . Third, enter the public certificate .

5.2 Configure the tunnel

Set “our ID” type and configure use for IKE.

```
cisco (config)#crypto pki trustpoint digiroot
cisco (ca-trustpoint)# enrollment terminal pem
cisco (ca-trustpoint)# usage ike
cisco (ca-trustpoint)# revocation-check none
```

Set Phase 1 and Phase 2 policy to match the configuration of the TransPort

```
cisco (config)#crypto isakmp policy 1
cisco (config-isakmp)# encr aes 256
cisco (config-isakmp)# hash sha256
cisco (config-isakmp)# group 2
cisco (config-isakmp)#crypto isakmp identity hostname
cisco3 (config)#crypto isakmp keepalive 10
```

Tunnel Mode and phase 2 set

```
cisco (config)#crypto ipsec transform-set myset esp-aes 256 esp-sha-hmac
cisco (cfg-crypto-trans)# mode tunnel
```

Configure SA timers and create dynamic map

```
cisco (cfg-crypto-trans)#crypto call admission limit ike sa 6000
cisco (config)#crypto call admission limit ike in-negotiation-sa 3000
cisco (config)#crypto dynamic-map mydynmap 1
cisco (config-crypto-map)# set security-association lifetime seconds 86400
cisco (config-crypto-map)# set security-association idle-time 28200
cisco (config-crypto-map)# set transform-set myset
cisco (config-crypto-map)#set pfs group2
cisco (config-crypto-map)#crypto map mymap1 10 ipsec-isakmp dynamic mydynmap
```

Configure the WAN interface and enable IPsec

```
cisco (config)#interface FastEthernet0/1
cisco (config-if)# ip address 192.168.10.254 255.255.255.248
cisco (config-if)# speed auto
cisco (config-if)# duplex auto
cisco (config-if)# crypto map mymap1
```

Configure the default route

```
ip route 0.0.0.0 0.0.0.0 82.82.182.182
```

Configuring Certificate Security Attribute-Based Access Control

cisco (config)#crypto pki certificate map digitest 10
cisco (ca-certificate-map)# subject-name co o = digi
cisco (ca-certificate-map)#subject-name co ou = support
cisco (ca-certificate-map)# subject-name co cn = wrdigiuk

The cisco is now configured and the tunnel should come up.

6 TESTING

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

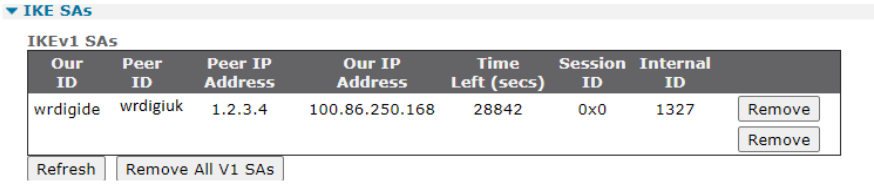
The Event log will show the IPSec tunnel is up.

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.

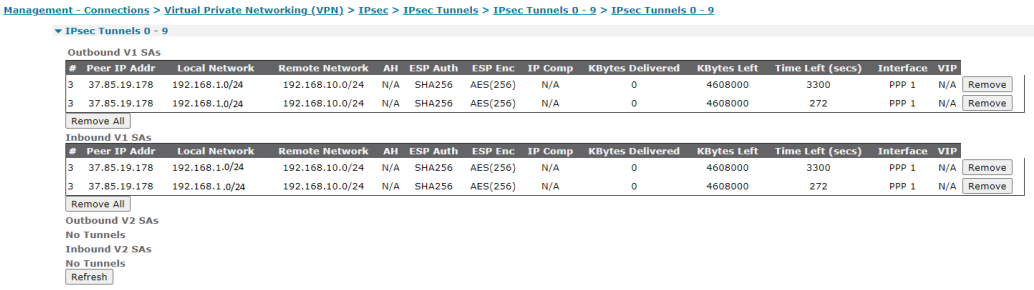


IKE SAs

IKEv1 SAs

Our ID	Peer ID	Peer IP Address	Our IP Address	Time Left (secs)	Session ID	Internal ID	
wrdigide	wrdigiuk	1.2.3.4	100.86.250.168	28842	0x0	1327	Remove
							Remove

Refresh | Remove All V1 SAs



Management - Connections > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec Tunnels 0 - 9 > IPsec Tunnels 0 - 9

IPsec Tunnels 0 - 9

Outbound V1 SAs

#	Peer IP Addr	Local Network	Remote Network	AH	ESP Auth	ESP Enc	IP Comp	KBytes Delivered	KBytes Left	Time Left (secs)	Interface	VIP	
3	37.85.19.178	192.168.1.0/24	192.168.10.0/24	N/A	SHA256	AES(256)	N/A	0	4608000	3300	PPP 1	N/A	Remove
3	37.85.19.178	192.168.1.0/24	192.168.10.0/24	N/A	SHA256	AES(256)	N/A	0	4608000	272	PPP 1	N/A	Remove

Remove All

Inbound V1 SAs

#	Peer IP Addr	Local Network	Remote Network	AH	ESP Auth	ESP Enc	IP Comp	KBytes Delivered	KBytes Left	Time Left (secs)	Interface	VIP	
3	37.85.19.178	192.168.1.0/24	192.168.10.0/24	N/A	SHA256	AES(256)	N/A	0	4608000	3300	PPP 1	N/A	Remove
3	37.85.19.178	192.168.1.0/24	192.168.10.0/24	N/A	SHA256	AES(256)	N/A	0	4608000	272	PPP 1	N/A	Remove

Remove All

Outbound V2 SAs

No Tunnels

Inbound V2 SAs

No Tunnels

Refresh

6.1 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
```

7 CONFIGURATION FILES

Digi TransPort WR 21

```
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
```

Cisco

```
version 15.9
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname cisco
!
boot-start-marker
boot-end-marker
!
!
enable password cisco
!
!
!
!
!
!
!
!
!
multilink bundle-name authenticated
!
crypto pki trustpoint digiroot
 enrollment terminal pem
 usage ike
 revocation-check none
!
crypto pki trustpoint digitest
 enrollment pkcs12
 revocation-check none
 rsakeypair digitest
```

```
 match certificate digitest
!
!
!
crypto pki certificate map digitest 10
 subject-name co o = digi
 subject-name co ou = support
 subject-name co cn = wrdigiuk
!
crypto pki certificate chain digiroot
 certificate ca 01
  xxxxx
        quit
crypto pki certificate chain digitest
 certificate 02
xxxx
        quit
 certificate ca 01
xxx
        quit
!
!
!
!
!
!
!
!
!
!
ip tcp synwait-time 5
!
!
crypto isakmp policy 1
 encr aes 256
 hash sha256
 group 2
crypto isakmp identity hostname
crypto isakmp keepalive 10
!
crypto ipsec security-association lifetime seconds 900
crypto ipsec security-association idle-time 910
!
crypto ipsec transform-set myset esp-aes 256 esp-sha-hmac
 mode tunnel
!
!
!
crypto call admission limit ike sa 6000
!
crypto call admission limit ike in-negotiation-sa 3000
!
crypto dynamic-map mydynmap 1
 set security-association lifetime seconds 86400
 set security-association idle-time 28200
 set transform-set myset
 set pfs group2
!
!
!
crypto map mymap1 10 ipsec-isakmp dynamic mydynmap
!
!
!
```

```
!
!
interface Loopback0
 ip address 10.100.0.1 255.255.255.255
!
interface FastEthernet0/0
 ip address 10.0.0.1 255.255.255.0
 speed auto
 duplex auto
!
interface FastEthernet0/1
 ip address 192.168.10.0 255.255.255.248
 speed auto
 duplex auto
 crypto map mymap1
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 82.82.182.182
!
!
!
!
!
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 password cisco
 login
line vty 5 10
 password cisco
 login
!
!
end
```