

Quick Note 054

Digi TransPort to Cisco VPN Tunnel using OpenSSL certificates.

February 2021

Contents

1	Int	roduction	3
	1.1	Outline	3
	1.2	Assumptions	3
	1.3	Corrections	3
2	Ve	rsion	3
3	cer	tificates creation	4
	lf 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	Dig	i 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	Cis	co 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	Tes	iting	22
	6.1	Confirm Traffic Traverses the IPSec Tunnels	23
7	Со	nfiguration 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 <u>tech.support@digi.com</u> 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: <u>http://sourceforge.net/projects/xca/</u>

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**

		ions Key usage	Netscape Advanced	
Signing	request			
Sigr	this Certificate signing	g request		-
🗸 Сор	y extensions from the	request	Show request	
Mod	ify subject of the requ	est		
gnature	algorithm		SHA 1	•
Templat	e for the new certifica	te		
Templat [defau	e for the new certifica t] CA	te		•

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

	Extensions	Key usage	Netscape	Advanced		
vistinguished name						
nternal name	democa		organizatio	nName	Digi	
countryName FR		organizationalUnitName		cert team		
stateOrProvinceName	some-state		commonNa	ime	DigiCA	
ocalityName	Paris		emailAddre	ess	certteam@digi	.com
Туре			Conte	ent		Delete

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

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.

ate Keys Certifi	icate signing requests	Certificates	Templates	Revocation lists
Internal name	commonName	CA	Serial	New Cartificate
Network democa	DigiCA	🖌 Yes	0	<u>n</u> ew certificate
				<u>E</u> xport
				Import
				<u>S</u> how Details
				Delete
				Import <u>P</u> KCS#12
				Import PKCS#7
				Plain View
				Zerminecte Calundross, Zine
	11		P	

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**

ource Subject Extens	sions Key usage	Netscape Advanced
Signing request		
Sign this Certificate signin	g <u>r</u> equest	
Copy extensions from the	request	Show request
Modify subject of the requ	est	
Use this Certificate for sig nature algorithm	ning	democa
emplate for the new certifica	te	
[default] HTTPS_server		Apply extensions Apply subject Apply all

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

ource Subject	Extensions	Key usage	Netscape	Advanced			
Distinguished name							
Internal name	hostcert		organizationName		DigiDE		
countryName DE			organizatio	organizationalUnitName commonName		digimunich	
stateOrProvinceName	somes-state	es-state					
localityName	Munich		emailAddre	ess	digide@digi.com	n	
Type		Content				Add	

Parameter	Setting
Internal name	This is for display purposes in the tool, only
Country Name	The two-letter <u>ISO 3166</u> abbreviation for your country.
State or Province Name	The state or province where your organization is legally located. Do not abbreviate.
Locality Name	The city where your organization is legally located. Do not abbreviate.
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 <u>wrdigide</u> 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 <u>digide@digi.com</u>

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

ivate Keys Certi	ficate signing requests	Certificates	Templates	Revocation lists
Internal name	commonName	CA	Serial	New Certificate
Action democa	DigiCA	Yes	0	-
nosicer	t wraigide	NO		Export
				Import
				Show Details
				Delete
				Import PKCS#12
				Import P <u>K</u> CS#7
				Plain View
				Jarminecta Dingenes , Jine
	111			

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**

X Certificate and Key management	? 🔀
Create x509 Certificate	
Source Subject Extensions Key usage	vetscape Advanced
Signing request	
Sign this Certificate signing request	· · · · · · · · · · · · · · · · · · ·
Copy extensions from the request	Show request
Modify subject of the request	
Signing	
Use this Certificate for signing	democa 👻
Signature algorithm	SHA 1
Template for the new certificate	
	Apply extensions Apply subject Apply an
	OK Cancel

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

stinguished name nternal name puntryName tateOrProvinceName icalityName	clientcert UK some-state	organizationN organizational	ame	DigiUK	
nternal name puntryName tateOrProvinceName pcalityName	Clientcert UK some-state	organizationN organizational	ame	DigiUK	
ountryName tateOrProvinceName icalityName	UK some-state	organizationa		DigiUK	
tateOrProvinceName ocalityName	some-state		UnitName	digilondon	
icalityName T	Landan.	commonName		wrdigiuk	
-	London	emailAddress		digiuk@digi.com	ı
lvpe		Content			Add
ivate key					

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

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

vate Keys Certific	cate signing requests	Certificates	Templates	Revocation lists
Internal name	commonName	CA	Serial	New Certificate
Clientcert	wrdigiuk	V res	0	Export
hostcert	wrdigide	No	0	Import
			[Show Details
				Delete
			[Import <u>P</u> KCS#12
			[Import P <u>K</u> CS#7
				Plain View
				Zasuninceta das Dalundenos , Zina
II	1		4	

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

Internal name commonName CA Serial Mew Certificate Mew Certificate Mew Certificate Mew Certificate Export Import	
Memoca DigiCA Yes O Memoca DigiCA Yes O Memoca Clientc Wrdigiuk No O Memoca No O Export	
New O Export New hostcert wrdigide No 0 Import Import Import Import	
New hostcert wrdigide No 0	
Show Details	
Delete	
Import <u>P</u> KCS#12	
Import PKCS#7	
Plain View	
Jaminecta Juni	
Plain View	

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

🖉 X Certifi	cate and Key management		? ×
Certifil	ate export		Command The
Please ent	er the filename for the certificate.		
Filename	C:/Program Files (x86)/xca <mark>.cacert.pe</mark>	em	
DER is a b PEM is a b PKCS#7 is PKCS#12	nary format of the Certificate ase64 encoded Certificate an official Certificate exchange forma s an encrypted official Key-Certificate	at exchange format	
Export For	mat PEM		•
		ОК	Cancel

- 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

tternal name Type Size Use Passwi clientcert RSA 1024 bit 1 Common democa RSA 1024 bit 1 Common hostcert RSA 1024 bit 1 Common Mew Key Export Import Import PFX (PKCS#12) Show Details Delete		ertificate signing requ	ests Certificates	Templates	Revocation lists
clientcert RSA 1024 bit 1 Common democa RSA 1024 bit 1 Common hostcert RSA 1024 bit 1 Common Import Import PFX (PKCS#12) Show Details Delete	Internal name	Туре	Size Use	Passwo	Now Koy
democa RSA 1024 bit 1 Common Export hostcert RSA 1024 bit 1 Common Jmport Jmport PFX (PKCS#12) Show Details Delete	clientcert	RSA	1024 bit 1	Common	<u>H</u> ew Key
hostcert RSA 1024 bit 1 Common Import Import PFX (PKCS#12) Show Details Delete	emoca	RSA	1024 bit 1	Common	<u>E</u> xport
Import PFX (PKCS#12) Show Details Delete	bostcert	RSA	1024 bit 1	Common	Import
Show Details Delete					Import PEX (PKCS#12)
					Chew Dataila
					Show Details
					Delete

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**

X Certif	icate and Key managen	nent	? ×
Key ex	kport		
Please er	ter the filename for the key	y.	
Filename	C:/Program Files (x86)/pr	rivh.pem	
DER is a PEM is a PKCS#8 i Export Fo	binary format of the key with base64 encoded key with o s an encrypted official Key- rmat PEM	thout encryption ptional encryption exchange format	
When ex	porting the private key it sh rt the private part of the Ke	ould be encrypted. y too	
Encry	pt the Key with a password		
		ОК	Cancel

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

octu 102 169 1 10/	Ucoroamou Ucoroam	0 Doogword		Dorts 21		lickconnect					
sponse:	227 Entering Passive M	e Fass <u>w</u> ord.	4.2)	Fort. 21		lickconnect	Ŀ				
mmand:	LIST		4,5) .								Î
sponse: sponse:	150 Opening data conn 226 File sent OK	ection for LIST									-
itus:	Directory listing succes	ful									-
cal site: C:\temp\	wr21cert\			Remote	site: /						-
	wr21cert				1						_
	xcacerts		:	1							
њ- 📜 Т	emps			-							
lanama	Filosizo Filotuno	Last modified		-							
	ritesize ritetype	Last moumeu		- L							
cacert nem	1 082 Privacy Enh	2/21/2014 124	i n	Filena	me 🔷		Filesize	Filetype	Last modifi	Permissi	*
certcl pem	1.082 Privacy Enh	2/21/2014 12:	1	1.							Ξ
certh pem	1 082 Privacy Enh	2/21/2014 12:	1	👢 use	r			File folder	2/1/2014 1:	dr-xr-xr-x	
privel.pem	887 Privacy Enh.	. 2/21/2014 12:	1	🖹 act	ivate.sb		33,685	SB File	10/2/2013	-rwxrwxr	
privh.pem	891 Privacy Enh.	2/21/2014 12:	1	📄 ana	a.txt		1,000,000	Text Doc	2/25/2014	-r-xr-xr-x	
				iii ana	aeth.cap)	1,000,000	Wireshar	2/25/2014	-r-xr-xr-x	
				iii ana	aip.cap		1,000,000	Wireshar	2/25/2014	-r-xr-xr-x	
				1000	on ca	р	1,000,000	Wireshar	2/25/2014	-r-xr-xr-x	
				bg	p.conf		256	CONF File	1/1/2000	-rwxrwxr	
				L CA	cert.cer		1,371	Security	1/1/2000	-rwxrwxr	Ŧ
				-						•	
iles. Total size: 5,	024 bytes			53 files	s and 1	directory. T	otal size: 1	4,248,584 by	/tes		
erver/Local file	Direc Remo	te file	Size	Priority S	tatus						

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

Installed Certificate	Authority Certifie	cates			
Subject	Issuer	Expiration	Filename		
DigiCA	DigiCA	Feb 7 20:17:00 2031 GMT	cacert.pem	View	Delete

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

Upload Certificate or Private Keys
Upload RSA keys and certificates. Certificate and key files may be in ASN.1 DER or PEM Base64 encoded formats.
Upload File: Choose File certcl.pem
Upload

The Certificate should now appear under the Installed Certificates

IPsec/SSH/HTTPS C	ertificates					
Installed Certificate	5					
Subject	Issuer	Expiration	Key Size	Filename		
Digi International	Digi International	Jan 24 23:52:47 2031 GMT	2048	cert01.pem	View	Delete
wr44	OpenVPN-CA	Jan 26 14:57:00 2023 GMT	2048	cert44.pem	View	Delete
wrdigiuk	DigiCA	Feb 7 20:22:00 2023 GMT	2048	certcl.pem	View	Delete

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**.

▼ Key files				
Upload Private	Key			
Upload RSA key.	Key files may	be in PEM Base64 encoded	format.	
	Upload File:	Choose File privcl.pem		
	Filename:	privcl.pem		
	Passphrase:			
Confirm	n Passphrase:			
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

<u>Configuration - Network > Interfaces > Mobile</u>
Mobile Connection Settings
Re-establish connection when no data is received for a period of time
Mobile Network Settings
 Enable NAT on this interface IP address
Enable IPsec on this interface
\square Keep Security Associations (SAs) when this Mobile interface is disconnected
Use interface Default 🗸 0 for the source IP address of IPsec packets

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

escription: Cert Tunnel	
be IP address or hostname of the remote unit	
1.2.3.4	
Use	as a backup unit
Local LAN	Remote LAN
Use these settings for the local LAN	Use these settings for the remote LAN
IP Address: 192.168.1.0	IP Address: 192.168.10.0
Mask: 255.255.255.0	Mask: 255.255.255.0
O Use interface PPP → 0	O Remote Subnet ID:
Our ID: wrdigide Our ID type OIKE ID OF0 Bemote ID: wrdigiuk	QDN OIPv4 Address
Our ID: wrdigide Our ID type OKE ID OF Remote ID: wrdigiuk Ise AES (256 bit keys) ♥ encryption on this tu Ise SHA256 ♥ authentication on this tunnel	QDN OUser FQDN IPv4 Address
Our ID: wrdigide Our ID type OIKE ID OFG Remote ID: wrdigidk Ise AES (256 bit keys) ♥) encryption on this to Ise SHA256 ♥ authentication on this tunnel Ise Diffie Hellman group 2 ♥ se IKE VI♥ to negotiate this tunnel Use IKE configuration: 1 ♥	2DN OIPv4 Address
Our ID: wrdigide Our ID: wrdigide Our ID type IKE ID FR Remote ID: wrdigiuk Ise AES (256 bit keys) ▼ encryption on this tunnel Ise SHA256 ▼ authentication on this tunnel Ise Diffie Hellman group 2 ▼ se IKE VI▼ to negotiate this tunnel Use IKE configuration: 1 ▼ wing this tunnel up All the time ® Whenever a route to the destination is av On demand	2DN O User FQDN IPv4 Address
Our ID: wrdigide Our ID type OKE ID OF Remote ID: wrdigiuk Ise <u>AES (256 bit keys)</u> → encryption on this tunnel Ise <u>GHA256</u> → authentication on this tunnel Ise Diffie Hellman group 2 → se IKE <u>v1 v</u> to negotiate this tunnel Use IKE configuration: 1 v	QDN OUser FQDN IPv4 Address

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

figuration - Network > <u>Virtual Private Networking (VPN)</u> > <u>IPsec</u> > <u>IKE</u> > <u>IKE 1</u>
▼ IKE 1
Use the following settings for negotiation Encryption: None ODES OBDES OAES (128 bit) OAES (192 bit) @AES (256 bit)
Authentication: ONONE OMD5 OSHA1
Mode: 🔿 Main 🛛 🖲 Aggressive
MODP Group for Phase 1: 2 (1024) 🗸
MODP Group for Phase 2: 2 (1024) 🗸
Renegotiate after 8 hrs 0 mins 0 secs
> Advanced

```
Apply
```

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

RSA private key file: privcl.pem	
CA Demonstral Medeo (P. 11	
CA Demonstration in the	

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

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, XXXXXXXXXXXXXXXX
----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 SA	5						
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	0×0	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

	see runners o	,											
0	utbound 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
з	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
R	emove All												
In	bound 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	
2		100 100 10/24	100 100 10 0/01	61/6	CHA256	AEC(256)	N/A	0	4608000	2200	000 1	N/A	Remove
12	37.85.19.178	192.168.1.0/24	192.168.10.0/24	IN/ A	511/250	ME3(230)	1970	0	1000000	3300	FEE 1	100	
3	37.85.19.178 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
3 R	37.85.19.178 37.85.19.178 emove All	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
3 R Ou	37.85.19.178 37.85.19.178 emove All stbound V2 SAs	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
3 R Ou No	37.85.19.178 37.85.19.178 temove All utbound V2 SAs o Tunnels	192.168.1.0/24 192.168.1.0/24	192.168.10.0/24	N/A	SHA256	AES(256)	N/A	0	4608000	272	PPP 1	N/A	Remove
3 R Ou No In	37.85.19.178 37.85.19.178 temove All tbound V2 SAs to Tunnels tbound V2 SAs	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

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
1
hostname cisco
1
boot-start-marker
boot-end-marker
1
1
enable password cisco
!
!
!
!
!
!
!
!
1
multilink bundle-name authenticated
1
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
1
!
Т
crypto pki certificate map digitest 10
 subject-name co o = digi
 subject-name co ou = support
subject-name co cn = wrdigiuk
1
crypto pki certificate chain digiroot
 certificate ca 01
 XXXXX
        quit
crypto pki certificate chain digitest
certificate 02
XXXX
        quit
certificate ca 01
XXX
        quit
!
!
!
!
!
!
!
1
1
1
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
1
crypto call admission limit ike sa 6000
1
crypto call admission limit ike in-negotiation-sa 3000
1
crypto dynamic-map mydynmap 1
set security-association lifetime seconds 86400
set security-association idle-time 28200
set transform-set myset
set pfs group2
Т
Т
!
crypto map mymap1 10 ipsec-isakmp dynamic mydynmap
!
!
!
```

```
!
1
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
1
interface FastEthernet0/1
 ip address 192.168.10.0 255.255.258.248
 speed auto
 duplex auto
crypto map mymap1
1
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
!
!
!
!
!
!
1
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
```