

Quick Note 041

TransPort to TransPort VPN Tunnel using OpenSSL certificates.

November 2016

Contents

1	Intro	oduction
	1.1	Outline
	1.2	Corrections
2 3	Vers Con	ion
	lf you a 3.1	already have certificates available, you can skip to section 3.2
	3.1.1	1 Create a Root CA Certificate 4
	3.1.2	2 Create a CA-Signed Host Certificate (Router B, Responder) 6
	3.1.3	3 Create a CA-Signed Client Certificate (Router A, initiator)
	3.1.4	4 Export the certificates and keys in .PEM format10
	3.2	Upload SSL certificates to the router B (responder)13
	3.2.1	1 Upload the certificates via FTP13
	3.2.2	2 Upload the certificates via the Web GUI14
	3.3	Upload SSL certificates to the router A (initiator)15
	3.3.1	1 Upload the certificates via FTP15
	3.3.2	2 Upload the certificates via the Web GUI16
	3.4	Configure the VPN Tunnel settings on router B (responder)
	3.5	Configure the VPN Tunnel settings on router A (Initiator)21
4	Test	ing24
	4.1	Confirm Traffic Traverses the IPSec Tunnels25
5	Con	figuration files

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 <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	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: <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**

Signing request	
Sign this Certificate signing request	
bight the certaincate bighing request	Ŧ
Copy extensions from the request Show reque	est
Modify subject of the request	
ignature algorithm SHA 1	•
Template for the new certificate	
[default] CA	•
Apply extensions Apply sub	ject Apply all

6. 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			
istinguished name							
nternal name	democa		organizatio	organizationName			
countryName	FR		organizatio	organizationalUnitName			
stateOrProvinceName	some-state		commonNa	commonName		DigiCA	
ocalityName	Paris		emailAddre	955	certteam@dig	ji.com	
Type			Conte	ent		Add	

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
	The exact legal name of your
Organization Name	organization. Do not abbreviate
organization Name	your organization name.
	In this example: Digi
	Section of the organization.
Organizational Unit	Examples of sections are
Name	Marketing, Research and
	Development, Human Resources
	or Sales.
Common Name	used.
	Enter your organization general
Empil Address	email address.
Email Address	In this axample
	certteam@digi.com
	<u>oor coouring angiroorni</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.

internal name commonN			
	ame CA	Serial	New Certificate
democa DigiCA	Ves	0	<u>E</u> xport
			Import
			Show Details
			Delete
			Import PKCS#12
			Import PKCS#7
			Plain View
			Jennineeta, Dinkore6 , Zine
111		•	

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**

		Extensions	Key usage	Netscape	Advanced		
Signing	request						
Sign	this Certifica	ite signing <u>r</u> equ	est				-
Cop	y extensions f	from the reques	st		Show	v request	
Mod	ify subject of	the request					
igning	ato a colficion	and contificato w	with the corial	1			
) Use	this Certifica	te for signing	viur uie seridi	democa			•
	1			SHA 1			•
inature	algorithm						
Inature	algorithm						
inature emplat	e for the new	/ certificate					
inature emplat [defaul	aigorithm e for the new t] HTTPS_ser	v certificate					•
inature Templat	algorithm e for the new t] HTTPS_ser	/ certificate		Apply e:	ttensions Ap	ply subject	▼ Apply all
inature emplat [defaul	algorithm e for the new t] HTTPS_ser	v certificate		Apply e	densions Ap	ply 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		organizationalUnitName	digimunich	
stateOrProvinceNam	e somes-state		commonName	wrdigide	
localityName	Munich		emailAddress	digide@digi.com	
Туре			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 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 <u>digide@digi.com</u>

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

ate Keys Certific	cate signing requests	Certificates	Templates	Revocation lists
Internal name	commonName	CA	Serial	New Cartificate
democa	DigiCA	Ves	0	New Certificate
Aug hostcert	wrdigide	No	0	<u>E</u> xport
			(Import
				Show Details
			(Delete
				Import <u>P</u> KCS#12
				Import PKCS#7
				Plain View
				2 Parminecter Time
	1		Þ.	

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**

Certific	ate and Ke	y manageme	nt				8
reate	x509 C	Certificate	;			1	a Burlanty 7
Source	Subject	Extensions	Key usage	Netscape	Advanced		
Signing	request						
Sign	this Certifica	ite signing <u>r</u> equ	est				Ŧ
🗸 Сору	extensions f	from the reques	t		Show r	equest	
Mod	ify subject of	the request					
Signature	algorithm			SHA 1			
Template	e for the new	r certificate					
[defaul	t] HTTPS_clie	ent					•
				Apply e	xtensions Apply	v subject A	oply all
						ОК	Cancel

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

	Extensions Rey usage	Netscape Advanced	
istinguished name			
internal name	clientcert	organizationName	DigiUK
countryName	UK	organizationalUnitName	digilondon
stateOrProvinceName	some-state	commonName	wrdigiuk
ocalityName	London	emailAddress	digiuk@digi.com
Туре		Content	Add Delete

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. 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.

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

vate Keys Cert	ificate signing requests	Certificates	Templates	Revocation lists
Internal name	commonName	CA	Serial	New Certificate
Action democa	DigiCA	Ves	0	
Area clientc.	wrdigiuk	No	0	Export
A hostce	rt wrdigide	No	0	Import
				Show Details
				Delete
				Import PKCS#12
				Import P <u>K</u> CS#7
				Plain View
				a Zasminate Con Daringhouse , Zins
	111		•	

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	kate export	
Please en	ter the filename for the certificate.	
Filename	C:/Program Files (x86)/xca	
PEM is a b PKCS#7 is PKCS#12	ase64 encoded Certificate s an official Certificate exchange format is an encrypted official Key-Certificate exchange format	
Export Fo		

- 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

vate keys	Certificate sig	gning requests	Certificates	Templates	Revocation lists
Internal na	ime Ty	/pe Size	Use	Passwo	New Key
clientce	rt RSA	1024	bit 1	Common	New Key
democa	RSA	1024	bit 1	Common	Export
bostcert	RSA	1024	bit 1	Common	
					Import
					Import PFX (PKCS#12)
					Show Details
					<u>S</u> hort becaus
					Delete
		III		4	N N N N N N N N N N N N N N N N N N N
		III			

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**

(ey e>	port	
Please en	er the filename for the key.	
Filename	C:/Program Files (x86)/xca privh.pem	
PKCS#8 is Export Fo When exp	an encrypted official Key-exchange form mat PEM porting the private key it should be encryp	voted.
Expor	t as PKCS#8	
Encry	pt the Key with a password	

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

Host: 192,168,1,104	Username: U	sername	Password		Port	21	Quickconnect	P				
esponse: ommand: esponse: esponse: tatus:	227 Entering Pa LIST 150 Opening da 226 File sent Ok Directory listing	ssive Mode (192 ta connection for successful	,168,1,104,4 r LIST	,3).	Fort		Querconnect					•
ocal site: C:\temp\wr2	1cert\ vr21cert cacerts ps				 ■ ■ ■ ■ 	emote site: } 📜 🖊	1					•
Itename	1,082 Privac 1,082 Privac 1,082 Privac 1,082 Privac 887 Privac 891 Privac	pe Last cy Enh 2/21 cy Enh 2/21 cy Enh 2/21 cy Enh 2/21 cy Enh 2/21	modified //2014 12:0 //2014 12:1 //2014 12:1 //2014 12:1 //2014 12:1			lename user activate ana.txt anaip.cc anappp bgp.cor CAcert.c	.sb ap .cap .f .er	Filesize 33,685 1,000,000 1,000,000 1,000,000 256 1,371	Filetype File folder SB File Text Doc Wireshar Wireshar CONF File Security	Last modifi 2/1/2014 1: 10/2/2013 2/25/2014 2/25/2014 2/25/2014 1/1/2000 1/1/2000	Permissi dr-xr-xr-x -rwxrwxr -r-xr-xr-x -r-xr-xr-x -r-xr-xr-x -rwxrwxr -rwxrwxr	* II
files. Total size: 5,024	l bytes				53 Driorit	files and	1 directory. I	otal size: 1	4,248,584 by	rtes		

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

Upload CA Cert	ificates	
Upload certificate	e authority (CA) certificates. Files may be in ASN.1 [DER or PEM Base64 encoded formats.
	Upload File: C:\Temp\wr21cert\cacert.pem	Browse
Upload		

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

Subject	Issuer	Expiration	Filename	
DigiCA	DigiCA	Eab 21 11:00:00 2025 CMT	cacort nom	View

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**

Upload Certificate or Private	Keys		
Upload RSA keys and certificate	s. Certificate and key files may be in	ASN.1 DER or PEM Ba	ase64 encoded formats.
Upload File:	C:\Temp\wr21cert\certh.pem	Browse	
Upload			

The Certificate should now appear under the Installed Certificates

Subject	Issuer	Expiration	Key Size	Filename		
sarian.router		Feb 19 15:33:10 2036 GMT	1024	cert01.pem	View	Delete
wrdigiuk	DigiCA	Feb 21 11:02:00 2015 GMT	1024	certh.pem	View	Delete
ad Certificate or ad RSA keys and c	Private Keys ertificates. Certifi	cate and key files may be in ASN.1	DER or PEM Ba	se64 encoded form	nats.	
Unio	ad File:		Browse			

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**.

pload RSA key. Key files may	be in PEM Base64 encoded format.	
Upload File:	C:\Temp\wr21cert\privh.pem	Browse
Filename:	privh.pem	
Passphrase:		
Confirm Passphrase:		

3.3 Upload SSL certificates to the router A (initiator)

3.3.1 Upload the certificates via FTP

ost: 192.168.1.10	4 <u>U</u> sern	ame: username	Pass <u>w</u> ord:	•••••	Port: 21	Quickconne	ct 💌				_
sponse: mmand:	227 Ente LIST	ering Passive Mod	e (192,168,1,104,4	,3).							1
sponse:	150 Ope	ning data connect	tion for LIST								
sponse. itus:	Director	listing successfu	L								
					- Domoto alto	. (
bear site: C: (temp	wr21cert				Remote site	. 7					_
	xcacerts				a 🔍 🖊						
	Temps				-						
	Cilesies.	Cil et un e	Least an estimat		-						
liename	Filesize	гнетуре	Last modified		_						
cacert nem	1 082	Privacy Enh	2/21/2014 12:0	J	Filename	<u> </u>	Filesize	Filetype	Last modifi	Permissi	1
certcl.pem	1.082	Privacy Enh	2/21/2014 12:1		N						2
gerth.pem	1,082	Filmer Enh	2/21/2014 12:1		👢 user			File folder	2/1/2014 1:	dr-xr-xr-x	: [
🖉 privcl.pem	887	Privacy Enh	2/21/2014		activate	e.sb	33,685	SB File	10/2/2013	-rwxrwxr	•
🏸 privh.pem	891	Privacy Enh	2/21/2014 12:1		ana.txt	•	1,000,000	Text Doc	2/25/2014	-r-xr-xr-x	
					anaeth	.cap	1,000,000	Wireshar	2/25/2014	-r-xr-xr-x	
					anaip.c	ар	1,000,000	Wireshar	2/25/2014	-r-xr-xr-x	
					bon co	nf	1,000,000	CONF File	2/23/2014		
					CAcert	cer	1.371	Security	1/1/2000	-rwxrwxr	١.
					•		111	,	-, -,	•	
files. Total size:	6,024 bytes				53 files and	d 1 director	y. Total size: 1	4,248,584 by	/tes		
Server/Local file	D	irec Remote	file	Size	Priority Statu	s					-

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

Upload CA Cert	ificates	
Upload certificate	e authority (CA) certificates. Files may be in ASN.1 [DER or PEM Base64 encoded formats.
	Upload File: C:\Temp\wr21cert\cacert.pem	Browse
Upload		

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

Subject	Issuer	Expiration	Filename	
DigiCA	DigiCA	Eab 21 11:00:00 2025 CMT	cacert nem	View

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. Certificates	ate and key files may be in	ASN.1 DER or PEM Bas	e64 encoded formats.
Upload File: C:\Temp\v	vr21cert\certcl.pem	Browse	
Upload			

The Certificate should now appear under the Installed Certificates

talled Certificates						
Subject	Tssuer	Expiration	Key Size	Filename	_	_
sarian.router		Feb 19 15:33:10 2036 GMT	1024	cert01.pem	View	Delete
wrdigide	DigiCA	Feb 21 11:04:00 2015 GMT	1024	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**.

Jpload Private Key		
Upload RSA key. Key files may	/ be in PEM Base64 encoded format.	
Upload File:	C:\Temp\wr21cert\privcl.pem	Browse
Filename:	privcl.pem	
Passphrase:		
Confirm Passphrase:		
Upload		

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

Enable IPSec on PPP 1 (mobile interface) :

Configuration – Network > Interfaces > Mobile

 Enable NAT on this interface 	
○IP address ◉IP address a	nd Port
Enable IPsec on this interface	
Keep Security Associations	(SAs) when this Mobile interface is disconnected
Use interface Default 🗸 0	for the source IP address of IPsec packets
Enable the firewall on this integration	erface

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

Presc 1 Description: [cert Tunne] The IP address or hostname of the remote unit use as a backup unit Local LAN e Use these settings for the local LAN IP Address: 192.168.10. Mask: 255.255.255.0 Use interface PPP ● 0 ● Remote Subnet ID: Use the following security on this tunnel Off O Preshared Keys ● RSA Signature ● XAUTH Init RSA RSA Key File: privh.pem ● Our ID: wrdigluk Our ID: wrdigluk Our ID: wrdigluk Our ID: wrdigluk Our ID: wrdiglue Use [AES (256 bit keys) ● encryption on this tunnel Use IKE [D] ● FQDN ● User FQDN ● IPv4 Address Remote ID: Use IKE [VI ♥ to negotiate this tunnel Use IKE [VI ♥ to negotiate this tunnel Use IKE configuration: [♥] Bring this tunnel up All the time Mhenever a route to the destination is available IO endemand If the tunnel is down and a packet is ready to be sent forp the packet Bring this tunnel is down and a packet is ready to be sent forp the packet Bring this tunel down if it is idle for ● hrs ● mins ● secs	configuration - Network > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec 1
Description: Cert Tunnel The IP address or hostname of the remote unit Use The IP address or hostname of the remote unit Use Cocal LAN Penderess: 192.168.1.0 Penderess: 192.168.1.0 Penderess: 192.168.1.0 Penderess: 192.168.1.0 Person of the remote UAN Penderess: 192.168.1.0 Person of the remote UAN Penderess Penderes	▼ IPsec 1
The IP address or hostname of the remote unit Use as a backup unit Local LAN Remote LAN IP Address: 192.168.1.0 Mask: 255.255.255.0 Use interface PPP V 0 • Remote Subnet ID: Use the following security on this tunnel Our ID: Wrdigluk Our ID type IKE ID • FQDN • User FQDN • IPv4 Address Remote ID: Wrdiglde Use EAES (256 bit keys) v encryption on this tunnel Use IKE vi to negotiate this tunnel Use IKE vi to negotiate this tunnel Use IKE configuration: • v Bring this tunnel up • All the time • On demand If the tunnel is down and a packet is ready to be sent for the packet Bring this tunnel down if it is idle for 0 for the solution of secs	Description: Cert Tunnel
Use as a backup unit Local LAN We these settings for the local LAN IP Address: 192.168.10.0 Mask: 255.255.255.0 Use interface PPP 0 Remote Subnet ID: Use the following security on this tunnel Our ID: Wrdigluk Use fAES (256 bit keys) encryption on this tunnel Use KE [v] to negotiate this tunnel Use IKE [v] to negotiate this tunnel Use IKE [vi to negotiate this tunnel Use IKE [vi to negotiate this tunnel Use IKE [vi to negotiate this tunnel It the tunne lis down and a packet is ready to be sent for the packet Fing this tunnel down if it is ide for 0 hrs 0 mins 0 secs	The IP address or hostname of the remote unit
Local LAN Remote LAN Use these settings for the local LAN IP Address: I92.168.10.0 Mask: Z55.255.05.0 Use interface PPP	Use as a backup unit
 Use these settings for the local LAN IP Address: 192.168.10.0 Mask: 255.255.255.0 Use interface PPP Remote Subnet ID: Use the following security on this tunnel Off Preshared Keys XAUTH Init Preshared Keys RSA Signatures XAUTH Init RSA RSA Key File: privh.pem Our ID: Wrdigluk Our ID: Wrdigluk Our ID: Wrdigluk Our ID: Wrdigluk Use fES (255 bit keys) encryption on this tunnel Use IKE (1) to negotiate this tunnel Use IKE configuration: 0 If the tunnel is down and a packet is ready to be sent for the packet Bring this tunnel is to make this ready to be sent for the packet Bring this tunnel is down and a packet is ready to be sent for the packet Bring this tunnel is down and a packet is ready to be sent for the packet 	Local LAN Remote LAN
Use the following security on this tunnel Off Preshared Keys XAUTH Init Preshared Keys RSA Signatures XAUTH Init RSA RSA Key File: privh.pem V Our ID: Wrdigluk Our ID type IKE ID FQDN User FQDN IPv4 Address Remote ID: Wrdiglde Use AES (256 bit keys) V encryption on this tunnel Use MD5 V authentication on this tunnel Use IMD5 V authentication on this tunnel Use IKE v1 V to negotiate this tunnel Use IKE v1 V to negotiate this tunnel Use IKE configuration: 0 V Bring this tunnel up All the time Whenever a route to the destination is available © on demand If the tunnel is down and a packet is ready to be sent drop the packet Bring this tunnel down if it is idle for 0 hrs 0 mins 0 secs	 ♥ Use these settings for the local LAN ♥ Use these settings for the remote LAN IP Address: 192.168.10.0 Mask: 255.255.255.0 ♥ Use these settings for the remote LAN IP Address: 192.168.1.0 Mask: 255.255.255.0 ♥ No ♥ Remote Subnet ID:
Our ID: wrdigluk Our ID type IKE ID FQDN User FQDN IPv4 Address Remote ID: wrdigide Use AES (256 bit keys) I encryption on this tunnel Use MD5 I authentication on this tunnel Use Diffie Hellman group 2 Use IKE vi I to negotiate this tunnel Use IKE configuration: 0 Bring this tunnel up All the time Wenever a route to the destination is available If the tunnel is down and a packet is ready to be sent drop the packet Bring this tunnel down if it is idle for 0	Use the following security on this tunnel Off OPreshared Keys XAUTH Init Preshared Keys RSA Signatures XAUTH Init RSA RSA Key File: privh.pem
Use Diffie Hellman group 2 V Use IKE v1 v to negotiate this tunnel Use IKE configuration: 0 V Bring this tunnel up All the time Whenever a route to the destination is available @On demand If the tunnel is down and a packet is ready to be sent drop the packet V Bring this tunnel down if it is idle for 0 hrs 0 mins 0 secs	Our ID: wrdigiuk Our ID type IKE ID OFQDN OUser FQDN OIPv4 Address Remote ID: wrdigide Use AES (256 bit keys) V encryption on this tunnel Use MDS V authentication on this tunnel
Bring this tunnel up All the time Whenever a route to the destination is available On demand If the tunnel is down and a packet is ready to be sent drop the packet Bring this tunnel down if it is idle for hrs mins markets	Use Diffie Hellman group $\boxed{2 \checkmark}$ Use IKE $\boxed{v1 \lor}$ to negotiate this tunnel Use IKE configuration: $\boxed{0 \lor}$
If the tunnel is down and a packet is ready to be sent drop the packet Bring this tunnel down if it is idle for 0 hrs 0 mins 0 secs	Bring this tunnel up All the time Whenever a route to the destination is available On demand
Bring this tunnel down if it is idle for 0 hrs 0 mins 0 secs	If the tunnel is down and a packet is ready to be sent drop the packet
	Bring this tunnel down if it is idle for 0 hrs 0 mins 0 secs

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.

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

IKE Debug	
IKE U	
Use the fo	lowing settings for negotiation
	Encryption: ONone ODES O3DES OAES (128 bit) OAES (192 bit) AES (256 bit)
	Authentication: O None O MD5 O SHA1
	Mode: Main OAggressive
MODP	Group for Phase 1: 1 (768) 💙
MODP	Group for Phase 2: 2 (1024) 🗸
Renegotiat	e after 8 hrs 0 mins 0 secs
Advance	ed in the second se
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



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.

Enable IKE Responder					
Accept IKE Requests wit	h				
Encry	otion: DES (256 bit)	3DES 🗌 A	ES (128 bit)	□ AES (192 bit)	AES
Authentic	ation: 🗹 MD5 🗌	SHA1			
MODP Group bet	veen: 1 (768) 🗸	and 2 (1024	ŧ) ✔		
Renegotiate after 8	hrs 0 mins 0) secs			
Advanced					

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

	2
RSA private key file: privh.pem	
SA Removal Mode: Both	▼

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

Enable IPSec on PPP 1 (mobile interface) :

Configuration – Network > Interfaces > Mobile

Mobile Network Settings	
☑ Enable NAT on this interface ○ IP address ● IP address and	d Port
✓ 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
Enable the firewall on this inter	face

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

<u>guration - Network > Virtual Private Net</u>	working (VPN) > IPsec > IPsec Tunnels > IPsec 1
▼ IPsec 1	
Description: Cert Tunnel	
The IP address or hostname of the remo	ote unit
Use	as a backup unit
Local LAN	Remote LAN
Use these settings for the local L	LAN
IP Address: 192.168.1.0	IP Address: 192.168.10.0
Mask: 255.255.255.0	Mask: 255.255.0
	Remote Subnet ID:
Use the following security on this tunnel	
Off OPreshared Keys OXAUTH	Init Preshared Keys • RSA Signatures • XAUTH Init RSA
RSA Key File: privel per	2m 🖌
Our ID: wrdigide	
Our ID type IRE ID	OFQDN OUSer FQDN OIPV4 Address
Remote ID: Wraigiuk	·
Use AES (256 bit keys) 🗸 encryption or	on this tunnel
Use MDE M authentication on this turn	
Use Diffie Hellman group 2	
Use IKE v1 V to pagetiste this tupped	
Use IKE configuration: $0 \vee$	
Bring this tunnel up	
All the time Whenever a route to the destination	
O On demand	
If the tunnel is down and a packet is rea	ady to be sent bring the tunnel up
Bring this tunnel down if it is idle for 0	hrs 0 mins 0 secs

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					

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

KE	
IKE Debug	
IKE 0	
Use the following s	settings for negotiation
	Encryption: ONONE ODES O3DES OAES (128 bit) OAES (192 bit) AES (256 bit)
Aut	hentication: O None O MD5 O SHA1
	Mode: Main O Aggressive
MODP Group f	or Phase 1: 1 (768) 🗸
MODP Group f	or Phase 2: 2 (1024) 🗸
Renegotiate after	8 hrs 0 mins 0 secs
Advanced	
Apply	
· + F · 7	

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



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.

IPsec	rivate N	etwor	King (VPN)											
• IPse	ec Tunnel	ls												
Out	bound V	1 SAs												
# P	Peer IP A	ddr	Local Network	Remote Network	АН	ESP Auth	ESP Enc	IP Comp	KBytes Delivered	KBytes Left	Time Left (secs)	Interface	VIP	
0 82	2.82.182.	182 19	2.168.1.0/24	192.168.10.	0/24	N/A	MD5	N/A	0	0	25574	PPP 1	N/A	Remove
Rer	move All	1												
Inbo	ound V1	SAS												
# P	Peer IP A	ddr	Local Network	Remote Network	АН	ESP Auth	ESP Enc	IP Comp	KBytes Delivered	KBytes Left	Time Left (secs)	Interface	VIP	
0 8	2.82.182.	182 19	2.168.1.0/24	192.168.10	0/24	N/A	MDS	N/A	0	0	25574	PPP 1	N/A	Remove
Ren	move All													
Outt	bound V2	SAS												
No T	Funnels													
Inbo	ound V2	SAs												
No T	Tunnels													
Def	Frach													

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:

```
Administrator: Command Prompt

C:\Users\Administrator>ping 192.168.1.104

Pinging 192.168.1.104 with 32 bytes of data:

Reply from 192.168.1.104: bytes=32 time=128ms TTL=249

Reply from 192.168.1.104: bytes=32 time=180ms TTL=249

Reply from 192.168.1.104: bytes=32 time=122ms TTL=249

Ping statistics for 192.168.1.104:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approxinate round trip times in milli-seconds:

Minimum = 122ms, Maximum = 180ms, Average = 147ms

C:\Users\Administrator>_
```

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
```