Quick Note 63

How To Configure IKEv2 VPN between TransPort WR routers using Open SSL Certificates
Contents

1  Introduction .............................................................................................................................................. 3
   1.1  Outline............................................................................................................................................... 3
   1.2  Assumptions........................................................................................................................................ 3
   1.3  Corrections......................................................................................................................................... 3
   1.4  Version............................................................................................................................................... 3

2  Generate Test Certificates ...................................................................................................................... 4
   2.1  Create a Root CA Certificate ............................................................................................................. 4
   2.2  Create a CA-Signed Host Certificate (Responder) .............................................................................. 10
   2.3  Create a CA-Signed Client Certificate (Initiator) ............................................................................. 14
   2.4  Export the certificates and keys in .PEM format.............................................................................. 18
      2.4.1  Export Certificates ...................................................................................................................... 18
      2.4.2  Export Keys ................................................................................................................................. 20

3  Digi Routers Configuration ..................................................................................................................... 22
   3.1  Responder configuration .................................................................................................................. 22
      3.1.1  Upload Certificates and Keys ....................................................................................................... 22
      3.1.2  VPN Configuration ....................................................................................................................... 27
   3.2  Initiator configuration .................................................................................................................... 31
      3.2.1  Upload Certificates and Keys ....................................................................................................... 31
      3.2.2  VPN Configuration ....................................................................................................................... 36

4  Testing ....................................................................................................................................................... 40
   4.1  Check the IPsec tunnel is UP ............................................................................................................. 40
   4.2  Check the Traffic passes through the IPsec tunnel ............................................................................ 42

Configuration Files ........................................................................................................................................ 47
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 using IKEv2.

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 to:

Model: DIGI TransPort WR11/WR21

Firmware versions: 5169 and later

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

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

1.4 Version

<table>
<thead>
<tr>
<th>Version</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Published</td>
</tr>
</tbody>
</table>
2 GENERATE TEST CERTIFICATES

Note: If you already have certificates available, you can skip to section 3

In order to create the certificates that will be used in the IKEv2 VPN, XCA application can be used. The first step is to download and install the latest release of XCA which can be found at: http://sourceforge.net/projects/xca/.

In this section will be explained how to create the Root CA certificate, the CA-Signed Host Certificates for both the Responder and the Initiator, and all the related Keys. Will be also shown how to export those certificates and keys in order to be then uploaded on the Transport routers.

2.1 Create a Root CA Certificate

Open the XCA application, click on File > New Database:
How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

Chose a name for the Database and click “Save”:

Chose a password for the Database and click “OK”:
How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

Under the “Certificates” tab, click on “New Certificate”:

The “Create x509 certificate” window will be shown. In the “Source” tab check the “Template for the new certificate” and ensure that “[default] CA” is selected. Then click on “Apply all”
Go to the “**Subject**” tab, fill in all the information then click the “**Generate a new key**” button:

![Create x509 Certificate](image)

Where:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal name</td>
<td>democa</td>
<td>This is for display purposes in the tool only</td>
</tr>
<tr>
<td>Country Name</td>
<td>DE</td>
<td>The two-letter ISO 3166 abbreviation for your country.</td>
</tr>
<tr>
<td>State or Province Name</td>
<td>somestate</td>
<td>The state or province where your organization is legally located. Do not abbreviate.</td>
</tr>
<tr>
<td>Locality Name</td>
<td>Munich</td>
<td>The city where your organization is legally located. Do not abbreviate.</td>
</tr>
<tr>
<td>Organization Name</td>
<td>Digi</td>
<td>The exact legal name of your organization. Do not abbreviate your organization name.</td>
</tr>
<tr>
<td>Organizational Unit Name</td>
<td>Support</td>
<td>Section of the organization.</td>
</tr>
<tr>
<td>Common Name</td>
<td>DigiCA</td>
<td>In this example DigiCA will be used.</td>
</tr>
<tr>
<td>Email Address</td>
<td><a href="mailto:support@digi.com">support@digi.com</a></td>
<td>Enter your organization general email address.</td>
</tr>
</tbody>
</table>
How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

The “New Key” window will be shown, chose the name and Keysize and click on “Create”:

A pop-up window will show up as a confirmation of the Key creation:

Click “OK” to close this and click again “OK” in the main “Create x509 certificate” window to complete the creation of certificate. Again, a pop-up window will show up as a confirmation of the Certificate creation:
Click “OK” to close this and the certificate should now appear in the XCA main 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.
2.2 Create a CA-Signed Host Certificate (Responder)

Under the “Certificates” tab, click again on “New Certificate” and the “Create x509 certificate” window will be shown.

In the “Source” tab check the “Signing” section and make sure to select “Use this Certificate for signing” and chose the previously created CA.

Under “Template for the new certificate” select “[default] HTTPS_server“ and click “Apply all”:
How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

Go to the “Subject” tab, fill in all the information then click the “Generate a new key” button:

Where:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal name</td>
<td>hostcert</td>
<td>This is for display purposes in the tool, only</td>
</tr>
<tr>
<td>Country Name</td>
<td>DE</td>
<td>The two-letter ISO 3166 abbreviation for your country.</td>
</tr>
<tr>
<td>State or Province Name</td>
<td>somestate</td>
<td>The state or province where your organization is legally located. Do not abbreviate.</td>
</tr>
<tr>
<td>Locality Name</td>
<td>Munich</td>
<td>The city where your organization is legally located. Do not abbreviate.</td>
</tr>
<tr>
<td>Organization Name</td>
<td>Digi</td>
<td>The exact legal name of your organization. Do not abbreviate your organization name.</td>
</tr>
<tr>
<td>Organizational Unit Name</td>
<td>Support2</td>
<td>Section of the organization.</td>
</tr>
<tr>
<td>Common Name</td>
<td>digiwr11</td>
<td>In this example digiwr11 will be used. This will be used as the router Identity for the IPSec tunnel settings on the responder</td>
</tr>
<tr>
<td>Email Address</td>
<td><a href="mailto:support2@digi.com">support2@digi.com</a></td>
<td>Enter your organization general email address.</td>
</tr>
</tbody>
</table>
How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

The “New Key” window will be shown, chose the name and Keysize and click on “Create”:

A pop-up window will show up as a confirmation of the Key creation:

Click “OK” to close this and click again “OK” in the main “Create x509 certificate” window to complete the creation of certificate. Again, a pop-up window will show up as a confirmation of the Certificate creation:
Click “OK” to close this and the certificate should now appear in the window under the CA certificate.

**Please Note:** the value in the Common Name field for this certificate, will be used as Responder ID in the IPsec tunnel settings.
2.3 Create a CA-Signed Client Certificate (Initiator)

Under the “Certificates” tab, click again on “New Certificate” and the “Create x509 certificate” window will be shown.

In the “Source” tab check the “Signing” section and make sure to select “Use this Certificate for signing” and chose the previously created CA.

Under “Template for the new certificate” select “[default] HTTPS_client” and click “Apply all”: 

![Create x509 Certificate window](image)
How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

Go to the “Subject” tab, fill in all the information then click the “Generate a new key” button:

![Create x509 Certificate](image)

Where:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal name</td>
<td>clientcert</td>
<td>This is for display purposes in the tool only</td>
</tr>
<tr>
<td>Country Name</td>
<td>DE</td>
<td>The two-letter ISO 3166 abbreviation for your country.</td>
</tr>
<tr>
<td>State or Province Name</td>
<td>Somestate</td>
<td>The state or province where your organization is legally located. Do not abbreviate.</td>
</tr>
<tr>
<td>Locality Name</td>
<td>Munich</td>
<td>The city where your organization is legally located. Do not abbreviate.</td>
</tr>
<tr>
<td>Organization Name</td>
<td>Digi</td>
<td>The exact legal name of your organization. Do not abbreviate your organization name.</td>
</tr>
<tr>
<td>Organizational Unit Name</td>
<td>Support3</td>
<td>Section of the organization.</td>
</tr>
<tr>
<td>Common Name</td>
<td>digiwr21</td>
<td>In this example <em>digiwr21</em> will be used. This will be used as the router identity for the IPSec tunnel settings on the initiator</td>
</tr>
<tr>
<td>Email Address</td>
<td><a href="mailto:Support3@digi.com">Support3@digi.com</a></td>
<td>Enter your organization general email address.</td>
</tr>
</tbody>
</table>
How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

The “New Key” window will be shown, chose the name and Keysize and click on “Create”:

A pop-up window will show up as a confirmation of the Key creation:

Click “OK” to close this and click again “OK” in the main “Create x509 certificate” window to complete the creation of certificate. Again, a pop-up window will show up as a confirmation of the Certificate creation:
How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

Click “OK” to close this and the certificate should now appear in the window under the CA certificate:

**Please Note:** the value in the Common Name field for this certificate, will be used as Initiator ID in the IPsec tunnel settings.
2.4 Export the certificates and keys in .PEM format

2.4.1 Export Certificates

In the "Certificates" tab, highlight the CA certificate and click on "Export":

In the "Certificate export" window, select PEM (*.crt) as the export format and change the filename to cacert.pem and click "OK":

![Certificate export window](image)
How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

Repeat the previous step for the Client and Host certificate. Rename them certh.pem and certcl.pem:
2.4.2 Export Keys

From the main XCA window, select the “Private Keys” tab, highlight the host certificate key and click the "Export" button:

In the “Export Private Key [RSA]" window, select PEM private (*.pem) as the export format and change the filename to privh.pem and click “OK”:
How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

Repeat the previous step for the Client key and name it `privcl.pem`:

![Image of Certificate and Key management window](image)

After all the above steps are completed, the following files should now be available:

- `cacert.pem`: CA root certificate
- `certh.pem`: Responder certificate
- `certcl.pem`: Initiator certificate
- `privh.pem`: Responder private key
- `privcl.pem`: Initiator private key

**Please note:** It is important that each 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 DIGI ROUTERS CONFIGURATION

3.1 Responder configuration

The Responder configuration consists in uploading the certificates and the keys on the router, and then set up the IKEv2 VPN to use them in the negotiation with the Initiator. All this aspects will be explained in the subsections below.

3.1.1 Upload Certificates and Keys

The upload of Certificates and Keys can be performed using an FTP client like Filezilla or using the TransPort WEB User Interface.

In this example, in order to upload the files, the connection to the Transport is done on the local LAN (so using the ETH o IP address of the router).

FTP:

Open an FTP connection (In this example, using FileZilla) to the TransPort router that acts as responder and Transfer the certificates and Key files to the root directory:
How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

Where:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>192.168.1.1</td>
<td>IP Address of the TransPort router</td>
</tr>
<tr>
<td>Username</td>
<td>username</td>
<td>Username with Access Level: Super to log in to the TransPort router (default: username)</td>
</tr>
<tr>
<td>Password</td>
<td>password</td>
<td>Password for the user with Access Level: Super to log in to the TransPort router (default: password)</td>
</tr>
<tr>
<td>cacert.pem</td>
<td>-</td>
<td>CA Root certificate</td>
</tr>
<tr>
<td>certh.pem</td>
<td>-</td>
<td>Host Certificate</td>
</tr>
<tr>
<td>privh.pem</td>
<td>-</td>
<td>Host Private Key</td>
</tr>
</tbody>
</table>
How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

Web GUI:

Open a web browser to the IP address of the TransPort router that acts as responder and do the following steps to upload each file:

ADMINISTRATION > X.509 CERTIFICATE MANAGEMENT > CERTIFICATE AUTHORITIES (CAs)

In the “Upload CA Certificates” section, click the “Browse” button, go to the file location where cacert.pem is located, select the file, click “Open” and then click Upload:

The CA Certificate should now appear under the Installed Certificate Authority Certificates
In the “Upload Certificates or Private Keys” section, click the “Browse” button, go to the file location where `certh.pem` is located, select the file, click “Open” and then click “Upload”:

The Certificate should now appear under the Installed Certificates:
How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

ADMINISTRATION > X.509 CERTIFICATE MANAGEMENT > KEY FILES

In the “Upload Private Key” section, click the “Browse” button, go to the file location where `privh.pem` is located, select the file, click “Open”.

Type the file name “`privh.pem`” in the Filename field and click on “Upload”.

Before leaving the page, wait for the message “Key file saved” to be displayed to be sure that the upload is successful:
3.1.2 VPN Configuration

In this example the WAN Interface of the responder is the Mobile one, so on the PPP 1 interface the IPsec must be enabled:

**CONFIGURATION – NETWORK > INTERFACES > MOBILE**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Plan/APN</td>
<td>internet</td>
<td>Enter the APN of your mobile provider</td>
</tr>
<tr>
<td>Enable IPSec on this interface</td>
<td>✓</td>
<td>Enable IPSec on PPP 1 interface</td>
</tr>
</tbody>
</table>
How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

Then, the IPsec tunnel must be configured with the following settings:

**CONFIGURATION – NETWORK > VIRTUAL PRIVATE NETWORKING (VPN) > IPSEC > IPSEC TUNNELS > IPSEC 0-9 > IPSEC 0**

![IPsec Tunnel Configuration Screen](image-url)

- **Description:** IKEv2 with Certs
- **Local LAN**
  - IP Address: 192.168.1.0
  - Mask: 255.255.255.0
- **Remote LAN**
  - IP Address: 192.168.10.0
  - Mask: 255.255.255.0
  - Use interface PPP
- **Use AES (256 bit keys)**
- **Use SHA1**
- **Use Diffie Hellman group 2**
- **Use IKE v2**
- **RSA Key File:** privh.pem
- **Our ID:** digiwr11
- **Remote ID:** digiwr21
- **Authentication on this tunnel**
- **RSA Signatures**
- **XAUTH Init RSA**
- **XAUTH Init Preghost Keys**
- **Preghost Keys**
- **User FQDN**
- **IPv4 Address**
- **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 hours 0 minutes 0 seconds
- **Renew the tunnel after:** 0 hours 0 minutes 0 seconds
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Ikev2 with Certs</td>
<td>Description of the IPsec tunnel</td>
</tr>
<tr>
<td>Local LAN IP Address</td>
<td>192.168.1.0</td>
<td>Use this IP address for the local LAN subnet. This is usually the IP address of the router’s Ethernet interface or that of a specific device on the local subnet</td>
</tr>
<tr>
<td>Local LAN Mask</td>
<td>255.255.255.0</td>
<td>Use this IP mask for the local LAN subnet. The mask sets the range of IP addresses that will be allowed to use the IPsec tunnel.</td>
</tr>
<tr>
<td>Remote LAN IP Address</td>
<td>192.168.10.0</td>
<td>Use this IP address for the remote LAN subnet. This is usually the IP address of the peer’s Ethernet interface or that of a specific device on the local subnet</td>
</tr>
<tr>
<td>Remote LAN Mask</td>
<td>255.255.255.0</td>
<td>Use this IP mask for the remote LAN subnet. The mask sets the range of IP addresses that will be allowed to use the IPsec tunnel.</td>
</tr>
<tr>
<td>Use the following security on this tunnel</td>
<td>RSA Signatures</td>
<td>Select RSA signature security for this tunnel to use the uploaded certificates</td>
</tr>
<tr>
<td>RSA Key File</td>
<td>privh.pem</td>
<td>Private key file used for the responder</td>
</tr>
<tr>
<td>Our ID</td>
<td>digiwr11</td>
<td>ID that is matching the CN of the certificate in the first router (<strong>responder</strong>))</td>
</tr>
<tr>
<td>Our ID type</td>
<td>IKE ID</td>
<td>Defines how the remote peer is to process the Our ID configuration. Set to IKE ID to match the information used in the certificate</td>
</tr>
<tr>
<td>Remote ID</td>
<td>digiwr21</td>
<td>Remote ID that is matching the CN in the second router certificate (<strong>initiator</strong>)</td>
</tr>
<tr>
<td>Use () encryption on this tunnel</td>
<td>AES (256 bit keys)</td>
<td>The ESP encryption protocol to use with this IPsec tunnel</td>
</tr>
<tr>
<td>Use () Authentication on this tunnel</td>
<td>SHA1</td>
<td>The ESP authentication algorithm to use with this IPsec tunnel</td>
</tr>
<tr>
<td>Use Diffie Hellman group ()</td>
<td>2</td>
<td>The Diffie Hellman (DH) group to use when negotiating new IPsec SAs.</td>
</tr>
<tr>
<td>Use IKE n to negotiate this tunnel</td>
<td>v2</td>
<td>The IKE version to use to negotiate this IPsec tunnel</td>
</tr>
<tr>
<td>Use IKE configuration</td>
<td>0</td>
<td>The IKE configuration instance to use with this Eroute when the router is configured as an Initiator (so left as default in this case, it makes no difference as this router will no act as initiator)</td>
</tr>
<tr>
<td>Bring this tunnel up</td>
<td>On Demand</td>
<td>Controls how the IPsec tunnel is brought up.</td>
</tr>
<tr>
<td>If this tunnel is down and a packet is ready to be sent</td>
<td>Drop the packet</td>
<td>Defines the action that is performed when the IPsec tunnel is down and a packet needs to be sent</td>
</tr>
</tbody>
</table>
How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

Then, the IKEv2 responder section must be configured with the following settings:

CONFIGURATION - NETWORK > VIRTUAL PRIVATE NETWORKING (VPN) > IPSEC > IKEv2 > IKEv2 RESPONDER and > ADVANCED

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption</td>
<td>AES (256 bit)</td>
<td>Defines the encryption algorithm used</td>
</tr>
<tr>
<td>Authentication</td>
<td>SHA1</td>
<td>Defines the authentication algorithm used</td>
</tr>
<tr>
<td>PRF Algorithm</td>
<td>SHA1</td>
<td>Defines the PRF (Pseudo Random Function) algorithm used</td>
</tr>
<tr>
<td>MODP Group between x and y</td>
<td>1(778) and 2(1024)</td>
<td>The acceptable range for MODP group.</td>
</tr>
<tr>
<td>Advanced &gt; RSA private key file</td>
<td>privh.pem</td>
<td>The name of a X.509 certificate file holding the router's private part of the public/private key pair used in certificate exchanges. In this case is the Private key file used for the responder</td>
</tr>
</tbody>
</table>
3.2 Initiator configuration

The Initiator configuration consists in uploading the certificates and the keys on the router, and then set up the IKEv2 VPN to use them in the negotiation with the Responder. All these aspects will be explained in the subsections below.

3.2.1 Upload Certificates and Keys

The upload of Certificates and Keys can be performed using an FTP client like Filezilla or using the TransPort WEB User Interface.

In this example, in order to upload the files, the connection to the Transport is done on the local LAN (so using the ETH or IP address of the router).

FTP:

Open an FTP connection (In this example, using FileZilla) to the TransPort router that acts as initiator and transfer the certificates and Key files to the root directory:
How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

Where:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>192.168.10.1</td>
<td>IP Address of the TransPort router</td>
</tr>
<tr>
<td>Username</td>
<td>username</td>
<td>Username with Access Level : Super to log in to the TransPort router (default : username)</td>
</tr>
<tr>
<td>Password</td>
<td>password</td>
<td>Password for the user with Access Level : Super to log in to the TransPort router (default : password)</td>
</tr>
<tr>
<td>cacert.pem</td>
<td>-</td>
<td>CA Root certificate</td>
</tr>
<tr>
<td>certcl.pem</td>
<td>-</td>
<td>Host Certificate</td>
</tr>
<tr>
<td>privcl.pem</td>
<td>-</td>
<td>Host Private Key</td>
</tr>
</tbody>
</table>
How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

Web GUI:

Open a web browser to the IP address of the TransPort router that acts as initiator and do the following steps to upload each file:

**ADMINISTRATION > X.509 CERTIFICATE MANAGEMENT > CERTIFICATE AUTHORITIES (CAs)**

In the “Upload CA Certificates” section, click the “Browse” button, go to the file location where `cacert.pem` is located, select the file, click “Open” and then click **Upload**:

The **CA Certificate** should now appear under the **Installed Certificate Authority Certificates**.
How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

ADMINISTRATION > X.509 CERTIFICATE MANAGEMENT > IPSEC/SSH/HTTPS CERTIFICATES

In the “Upload Certificates or Private Keys” section, click the “Browse” button, go to the file location where certcl.pem is located, select the file, click “Open” and then click “Upload”:

The Certificate should now appear under the Installed Certificates:
How To Configure IKEv2 VPN between TransPort routers using OpenSSL Certificates

ADMINISTRATION > X.509 CERTIFICATE MANAGEMENT > KEY FILES

In the “Upload Private Key” section, click the “Browse” button, go to the file location where privcl.pem is located, select the file, click “Open”.

Type the file name “privcl.pem” in the Filename field and click on “Upload”.

Before leaving the page, wait for the message “Key file saved” to be displayed to be sure that the upload is successful:
3.2.2 VPN Configuration

In this example the WAN Interface of the responder is the Mobile one, so on the PPP 1 interface the IPSec must be enabled:

**CONFIGURATION – NETWORK > INTERFACES > MOBILE**

![VPN Configuration Configuration - Network - Interfaces - Mobile](image)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Plan/APN</td>
<td>internet</td>
<td>Enter the APN of your mobile provider</td>
</tr>
<tr>
<td>Enable IPSec on this interface</td>
<td>✔️️</td>
<td>Enable IPSec on PPP 1 interface</td>
</tr>
</tbody>
</table>
How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

Then, the IPsec tunnel must be configured with the following settings:

**CONFIGURATION – NETWORK > VIRTUAL PRIVATE NETWORKING (VPN) > IPSEC > IPSEC TUNNELS > IPSEC 0-9 > IPSEC 0**
How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

Where:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Ikev2 with Certs</td>
<td>Description of the IPsec tunnel</td>
</tr>
<tr>
<td>The IP address or hostname of the remote unit</td>
<td>37.85.24.187</td>
<td>The IP address or hostname of the remote IPsec peer that a VPN will be initiated to.</td>
</tr>
<tr>
<td>Local LAN IP Address</td>
<td>192.168.10.0</td>
<td>Use this IP address for the local LAN subnet. This is usually the IP address of the router’s Ethernet interface or that of a specific device on the local subnet</td>
</tr>
<tr>
<td>Local LAN Mask</td>
<td>255.255.255.0</td>
<td>Use this IP mask for the local LAN subnet. The mask sets the range of IP addresses that will be allowed to use the IPsec tunnel.</td>
</tr>
<tr>
<td>Remote LAN IP Address</td>
<td>192.168.1.0</td>
<td>Use this IP address for the remote LAN subnet. This is usually the IP address of the peer’s Ethernet interface or that of a specific device on the local subnet</td>
</tr>
<tr>
<td>Remote LAN Mask</td>
<td>255.255.255.0</td>
<td>Use this IP mask for the remote LAN subnet. The mask sets the range of IP addresses that will be allowed to use the IPsec tunnel.</td>
</tr>
<tr>
<td>Use the following security on this tunnel</td>
<td>RSA Signatures</td>
<td>Select RSA signature security for this tunnel to use the uploaded certificates</td>
</tr>
<tr>
<td>RSA Key File</td>
<td>privcl.pem</td>
<td>Private key file used for the responder</td>
</tr>
<tr>
<td>Our ID</td>
<td>digiwr21</td>
<td>ID that is matching the CN of the certificate in the first router (initiator)</td>
</tr>
<tr>
<td>Our ID type</td>
<td>IKE ID</td>
<td>Defines how the remote peer is to process the Our ID configuration. Set to IKE ID to match the information used in the certificate</td>
</tr>
<tr>
<td>Remote ID</td>
<td>digiwr11</td>
<td>Remote ID that is matching the CN in the second router certificate (responder)</td>
</tr>
<tr>
<td>Use ( ) encryption on this tunnel</td>
<td>AES (256 bit keys)</td>
<td>The ESP encryption protocol to use with this IPsec tunnel</td>
</tr>
<tr>
<td>Use ( ) Authentication on this tunnel</td>
<td>SHA1</td>
<td>The ESP authentication algorithm to use with this IPsec tunnel</td>
</tr>
<tr>
<td>Use Diffie Hellman group ( )</td>
<td>2</td>
<td>The Diffie Hellman (DH) group to use when negotiating new IPsec SAs.</td>
</tr>
<tr>
<td>Use IKE n to negotiate this tunnel</td>
<td>v2</td>
<td>The IKE version to use to negotiate this IPsec tunnel.</td>
</tr>
<tr>
<td>Use IKE configuration</td>
<td>0</td>
<td>The IKE configuration instance to use with this Eroute when the router is configured as an Initiator</td>
</tr>
<tr>
<td>Bring this tunnel up</td>
<td>All the time</td>
<td>This controls how the IPsec tunnel is brought up, for the initiator “All the time” option is chosen</td>
</tr>
<tr>
<td>If this tunnel is down and a packet is ready to be sent</td>
<td>Bring the tunnel up</td>
<td>Defines the action that is performed when the IPsec tunnel is down and a packet needs to be sent. For the initiator in this AN the “bring the tunnel up” option is chosen</td>
</tr>
</tbody>
</table>
How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

**CONFIGURATION – NETWORK > VIRTUAL PRIVATE NETWORKING (VPN) > IPSEC > IKEv2 > IKEv2 0 and > ADVANCED**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption</td>
<td>AES (256 bit)</td>
<td>The encryption algorithm used</td>
</tr>
<tr>
<td>Authentication</td>
<td>SHA1</td>
<td>The authentication algorithm used</td>
</tr>
<tr>
<td>PRF Algorithm</td>
<td>SHA1</td>
<td>The PRF (Pseudo Random Function) algorithm used</td>
</tr>
<tr>
<td>MODP Group for Phase 1</td>
<td>2 (1024)</td>
<td>Sets the key length used in the IKE Diffie-Hellman exchange to 768 bits (group 1) or 1024 bits (group 2). In this example group 2 is chosen to enable a 1024 bit key length</td>
</tr>
<tr>
<td>Advanced &gt; RSA private key file</td>
<td>privcl.pem</td>
<td>The name of a X.509 certificate file holding the router’s private part of the public/private key pair used in certificate exchanges. In this case is the Private key file used for the initiator.</td>
</tr>
</tbody>
</table>
4 TESTING

4.1 Check the IPsec tunnel is UP

This section will show that the IPSec tunnel has been established between the Initiator and the Responder.

The Event log will show the IKEv2 negotiation start and ends successfully in both routers:

MANAGEMENT – EVENT LOG

Initiator:

![Management - Event Log](image)

Responder:

![Management - Event Log](image)
How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

After that, in the connections status section IPsec and IKE v2 SAs will be displayed:

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

**Initiator:**

**Responder:**

**MANAGEMENT - CONNECTIONS > VIRTUAL PRIVATE NETWORKING (VPN) > IPSEC > IKE SAS**

**Initiator:**

**Responder:**
How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

In case of issues in the negotiation, take an IKE/IPsec trace following this guide: http://ftp1.digi.com/support/documentation/QN_045_How_To_setup_analyser_To_Get_IKE_IPsec_trace.pdf.

Please note that debug settings section for IKE, even if using IKEv2, is under general IKE configuration, as there is not a specific one for v2.

4.2 Check the Traffic passes through the IPsec tunnel

This section will show traffic passing across the tunnel. An easy way to test it, is to make a PING from a laptop connected to the ETH of the Initiator to one connected behind the responder. Before do that, to check how this traffic is handled by the router, the analyser section in the initator router (but the same can be done on the responder) must be configured as follows:

MANAGEMENT - ANALYSER > SETTINGS
How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

Once the analyser is configured, do the ping from the laptop on initiator side:

```
C:\windows\system32>ping 192.168.1.101 -n 1
Pinging 192.168.1.101 with 32 bytes of data: Reply from 192.168.1.101: bytes=32 time=924ms TTL=126
Ping statistics for 192.168.1.101:
   Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
   Approximate round trip times in milli-seconds:
      Minimum = 924ms, Maximum = 924ms, Average = 924ms
C:\windows\system32>
```

Then, check the trace, it will show that the ICMP request/reply packets will be sent through the tunnel 0:

**MANAGEMENT - ANALYSER > TRACE**

<table>
<thead>
<tr>
<th>Time</th>
<th>Source IP</th>
<th>Destination IP</th>
<th>Type</th>
<th>Code</th>
<th>Checksum</th>
<th>Length</th>
<th>ID</th>
<th>Frag Offset</th>
<th>TTL</th>
<th>Protocol</th>
<th>Checksum</th>
<th>Src IP</th>
<th>Dst IP</th>
<th>Type</th>
<th>Code</th>
<th>Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>24-3-2017</td>
<td>192.168.1.100</td>
<td>192.168.1.101</td>
<td>ECHO_REQ</td>
<td>0</td>
<td>14476</td>
<td>60</td>
<td>29979</td>
<td>0</td>
<td>128</td>
<td>ICMP</td>
<td>192.168.10.100</td>
<td>192.168.1.101</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24-3-2017</td>
<td>192.168.1.100</td>
<td>192.168.1.101</td>
<td>ECHO_REQ</td>
<td>0</td>
<td>17934</td>
<td>60</td>
<td></td>
<td>0</td>
<td></td>
<td>ICMP</td>
<td>192.168.10.100</td>
<td>192.168.1.101</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---
How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

IP (In) From REM TO LOC IFACE: PPP 1
45
  IP Ver: 4
  Hdr Len: 20
00
  TOS: Routine
  Delay: Normal
  Throughput: Normal
  Reliability: Normal
 78
  Length: 120
15
  ID: 21
00
  Frag Offset: 0
  Congestion: Normal
  May Fragment
  Last Fragment
F4
  TTL: 244
32
  Proto: ESP
26
  Checksum: 9822
25
  Src IP: 37.85.24.187
  Dst IP: 37.81.60.128
----------
24-3-2017 08:28:11.040 -------
45
  IP Ver: 4
  Hdr Len: 20
00
  TOS: Routine
  Delay: Normal
  Throughput: Normal
  Reliability: Normal
  3C
  Length: 60
54
  ID: 21524
00
  Frag Offset: 0
  Congestion: Normal
  May Fragment
  Last Fragment
7F
  TTL: 127
01
  Proto: ICMP
5A
  Checksum: 23187
C0
  Src IP: 192.168.1.101
  Dst IP: 192.168.10.100
ICMP:
  00
  Type: ECHO REPLY
  Code: 0
16
  Checksum: 17942
----------
24-3-2017 08:28:11.040 -------
45
  IP Ver: 4
  Hdr Len: 20
00
  TOS: Routine
  Delay: Normal
  Throughput: Normal
  Reliability: Normal
  3C
  Length: 60

How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

```
54 14    ID:        21524
00 00    Frag Offset: 0
          Congestion: Normal
          May Fragment
          Last Fragment
7E       TTL:       126
01       Proto:     ICMP
5B 93    Checksum:  23443
C0 A8 01 65  Src IP:   192.168.1.101
C0 A8 0A 64  Dst IP:   192.168.10.100
ICMP:
00       Type:      ECHO REPLY
00       Code:      0
16 46    Checksum:  17942
----------
```
How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

CONFIGURATION FILES

This is the config.da0 file used for the purpose of this Application Note on the Responder side:

```
Command: config c show
Command result

eth 0 IPaddr "192.168.1.1"
eth 0 ipanon ON
lapb 0 ans OFF
lapb 0 tinc 120
lapb 1 tinc 120
lapb 3 dtemode 0
lapb 4 dtemode 0
lapb 5 dtemode 0
lapb 6 dtemode 0
ip 0 cird ON
def_route 0 ll_ent "ppp"
def_route 0 ll_add 1
eroute 0 descr "IKEv2 with Certs"
eroute 0 peerid "digiwr21"
eroute 0 ourid "digiwr11"
eroute 0 locip "192.168.1.0"
eroute 0 locmsk "255.255.255.0"
eroute 0 remip "192.168.10.0"
eroute 0 remmsk "255.255.255.0"
eroute 0 ESPauth "SHA1"
eroute 0 ESPenc "AES"
eroute 0 authmeth "RSA"
eroute 0 ikever 2
eroute 0 dhgroup 2
eroute 0 enc_keybits 256
eroute 0 privkey "privh.pem"
dhcp 0 IPmin "192.168.1.100"
dhcp 0 respdelms 500
dhcp 0 mask "255.255.255.0"
dhcp 0 gateway "192.168.1.1"
dhcp 0 DNS "192.168.1.1"
sntp 0 server "time.devicecloud.com"
dyndns 0 ifent "default"
ppp 0 timeout 300
ppp 1 name "W-WAN (HSPA 3G)"
ppp 1 phonenum "*98*1#"
ppp 1 IPaddr "0.0.0.0"
ppp 1 timeout 0
ppp 1 ipsec 1
ppp 1 use_modem 1
ppp 1 aodion 1
ppp 1 autoassert 1
ppp 1 ipanon ON
ppp 1 r_chap OFF
ppp 3 defpak 16
ppp 4 defpak 16
web 0 prelogin_info ON
ftpc1 0 hostname "ftp1.digi.com"
ftpc1 0 directory "support/firmware/transport/radio_module_firmware/he910d"
ike2 0 rencalegs "AES"
ike2 0 renckeybits 256
ike2 0 rauthalgs "SHA1"
```
How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

ike2 0 rprfalgs "SHA1"
ike2 0 rdhmaxgroup 2
ike2 0 privrsakey "privh.pem"
modemcc 0 info_asy_add 3
modemcc 0 init_str "+CGQREQ=1"
modemcc 0 init_str1 "+CGQMIN=1"
modemcc 0 apn "Internet.t-d1.de"
modemcc 0 link_retries 10
modemcc 0 stat_retries 30
modemcc 0 sms_interval 1
modemcc 0 sms_access 1
modemcc 0 sms_concat 0
modemcc 0 init_str_2 "+CGQREQ=1"
modemcc 0 init_str1_2 "+CGQMIN=1"
modemcc 0 apn_2 "Your.APN.goes.here"
modemcc 0 link_retries_2 10
modemcc 0 stat_retries_2 30
modemcc 0 sms_access_2 1
modemcc 0 sms_concat_2 0
ana 0 anon ON
ana 0 l2on OFF
ana 0 xoton OFF
ana 0 lapdon 0
ana 0 lapbon 0
ana 0 maxdata 1500
ana 0 logsize 180
cmd 0 unitid "ss%s>"
cmd 0 cmdnua "99"
cmd 0 hostname "digi.router"
cmd 0 tremto 1200
cmd 0 rcihttp ON
user 0 access 0
user 1 name "username"
user 1 epassword "KD5lSVJDVVg="
user 1 access 0
user 2 access 0
user 3 access 0
user 4 access 0
user 5 access 0
user 6 access 0
user 7 access 0
user 8 access 0
user 9 access 0
local 0 transaccess 2
sslcli 0 verify 10
sslsvr 0 certfile "cert01.pem"
sslsvr 0 keyfile "privrsa.pem"
ssh 0 hostkey1 "privSSH.pem"
ssh 0 nb_listen 5
ssh 0 v1 OFF
cloud 0 ssl ON

Power Up Profile: 0
OK
How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

This is the config.da0 file used for the purpose of this Application Note on the Initiator side:

```bash
Command: config c show
Command result

eth 0 IPaddr "192.168.10.1"
eth 0 ipanon ON
lapb 0 ans OFF
lapb 0 tinact 120
lapb 1 tinact 120
lapb 3 dtemode 0
lapb 4 dtemode 0
lapb 5 dtemode 0
lapb 6 dtemode 0
ip 0 cidr ON
def_route 0 ll_ent "ppp"
def_route 0 ll_add 1
eroute 0 descr "IKEv2 with Certs"
eroute 0 peerip "37.85.24.187"
eroute 0 peerid "digiwr11"
eroute 0 ourid "digiwr21"
eroute 0 locip "192.168.10.0"
eroute 0 locmsk "255.255.255.0"
eroute 0 remip "192.168.1.0"
eroute 0 remmsk "255.255.255.0"
eroute 0 ESPauth "SHA1"
eroute 0 ESPenc "AES"
eroute 0 authmeth "RSA"
eroute 0 nosa "TRY"
eroute 0 autosa 2
eroute 0 ikever 2
eroute 0 dhgroup 2
eroute 0 enckeybits 256
eroute 0 privkey "privcl.pem"
dhcp 0 IPmin "192.168.1.100"
dhcp 0 respdelms 500
dhcp 0 mask "255.255.255.0"
dhcp 0 gateway "192.168.1.1"
dhcp 0 DNS "192.168.1.1"
sntp 0 server "time.devicecloud.com"
dyndns 0 ifent "default"
ppp 0 timeout 300
ppp 1 name "W-WAN"
ppp 1 phonenum "*98*1#"
ppp 1 IPaddr "0.0.0.0"
ppp 1 timeout 0
ppp 1 ipsec 1
ppp 1 use_modem 1
ppp 1 aodion 1
ppp 1 autoassert 1
ppp 1 ipanon ON
ppp 1 r_chap OFF
ppp 3 defpak 16
ppp 4 defpak 16
web 0 prelogin_info ON
ike2 0 iencalg "AES"
ike2 0 ienckeybits 256
ike2 0 dhgroup 2
ike2 0 privrsakey "privcl.pem"
modemcc 0 asy_add 4
modemcc 0 info_asy_add 2
```
How To Configure IKEv2 VPN between TransPort routers using Open SSL Certificates

```plaintext
modemcc 0 init_str "+CGREQ=1"
modemcc 0 init_str1 "+CGQMIN=1"
modemcc 0 apn "Internet.t-d1.de"
modemcc 0 link_retries 10
modemcc 0 stat_retries 30
modemcc 0 sms_interval 1
modemcc 0 sms_access 1
modemcc 0 sms_concat 0
modemcc 0 init_str_2 "+CGREQ=1"
modemcc 0 init_str1_2 "+CGQMIN=1"
modemcc 0 apn_2 "Your.APN.goes.here"
modemcc 0 link_retries_2 10
modemcc 0 stat_retries_2 30
modemcc 0 sms_access_2 1
modemcc 0 sms_concat_2 0
ana 0 anon ON
ana 0 l2on OFF
ana 0 xoton OFF
ana 0 lapdon 0
ana 0 lapbon 0
ana 0 maxdata 1500
ana 0 logsize 180
cmd 0 unitid "ss%s>
cmd 0 cmdnua "99"
cmd 0 hostname "digi.router"
cmd 0 asyled_mode 2
cmd 0 tremto 1200
cmd 0 rcihttp ON
user 0 access 0
user 1 name "username"
user 1 epassword "KD5lSVJDVVg=
user 1 access 0
user 2 access 0
user 3 access 0
user 4 access 0
user 5 access 0
user 6 access 0
user 7 access 0
user 8 access 0
user 9 access 0
local 0 transaccess 2
sslcli 0 verify 10
sslsvr 0 certfile "cert01.pem"
sslsvr 0 keyfile "privrsa.pem"
ssh 0 hostkey1 "privSSH.pem"
ssh 0 nb_listen 5
ssh 0 v1 OFF
creq 0 digest "MD5"
scep 0 cafile "cadc.pem"
scep 0 keybits 1024
templog 0 mo_autooff ON
cloud 0 ssl ON
Power Up Profile: 0
OK
```