Application Note

How to Configure an IKEv2 VPN Tunnel Between Two Digi Transport Routers

14 March 2017
Contents

1 INTRODUCTION .................................................................................................................................... 5
  1.1 Outline .......................................................................................................................................... 5
  1.2 Assumptions ................................................................................................................................... 5
  1.3 Corrections ................................................................................................................................... 6
  1.4 Version .......................................................................................................................................... 6

2 DIGI CONFIGURATION – INITIATOR ...................................................................................................... 7
  2.1 LAN Settings ................................................................................................................................ 7
  2.2 WAN Settings ................................................................................................................................ 8
    2.2.1 ETH 1 configuration .................................................................................................................. 8
    2.2.2 Default Route configuration .................................................................................................. 10
  2.3 IKEv2 Configuration ................................................................................................................... 10
  2.4 IPsec tunnel Configuration ........................................................................................................ 12
  2.5 Preshared Key Configuration ..................................................................................................... 14

3 DIGI CONFIGURATION - RESPONDER ................................................................................................ 16
  3.1 LAN Settings ................................................................................................................................ 16
  3.2 WAN Settings ................................................................................................................................ 17
    3.2.1 Cellular module configuration ............................................................................................... 17
    3.2.2 WAN Interface Configuration (PPP1) ..................................................................................... 19
    3.2.3 Default Route Configuration .................................................................................................. 20
  3.3 IKEv2 Configuration ................................................................................................................... 21
  3.4 IPsec Tunnel Configuration ....................................................................................................... 22
  3.5 Preshared Key Configuration ..................................................................................................... 24

4 TESTING .............................................................................................................................................. 26
  4.1 Analyser Settings ........................................................................................................................ 26
  4.2 Setting the tunnel UP .................................................................................................................. 29
  4.3 Testing Traffic on the tunnel ........................................................................................................ 31

5 CONFIGURATION FILES ...................................................................................................................... 36
How to Configure an IKEv2 VPN Tunnel Between Two Digi Transport Routers

5.1 Initiator Configuration ................................................................. 36
5.2 Responder Configuration............................................................. 39
# Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-1-1</td>
<td>Overview Diagram</td>
<td>5</td>
</tr>
<tr>
<td>2-1</td>
<td>LAN Settings</td>
<td>7</td>
</tr>
<tr>
<td>2-2</td>
<td>ETH 1 Configuration</td>
<td>8</td>
</tr>
<tr>
<td>2-3</td>
<td>ETH 1 Configuration – Advanced</td>
<td>9</td>
</tr>
<tr>
<td>2-4</td>
<td>Default Route</td>
<td>10</td>
</tr>
<tr>
<td>2-5</td>
<td>IKE v2 configuration</td>
<td>11</td>
</tr>
<tr>
<td>2-6</td>
<td>IPsec Tunnel Configuration</td>
<td>12</td>
</tr>
<tr>
<td>2-7</td>
<td>Preshared Key Configuration - Initiator user</td>
<td>14</td>
</tr>
<tr>
<td>2-8</td>
<td>Preshared Key Configuration - Responder user</td>
<td>15</td>
</tr>
<tr>
<td>3-1</td>
<td>LAN Settings</td>
<td>16</td>
</tr>
<tr>
<td>3-2</td>
<td>Mobile settings</td>
<td>17</td>
</tr>
<tr>
<td>3-3</td>
<td>PPP 1 settings</td>
<td>19</td>
</tr>
<tr>
<td>3-4</td>
<td>Default Route</td>
<td>20</td>
</tr>
<tr>
<td>3-5</td>
<td>IKEv2 Configuration</td>
<td>21</td>
</tr>
<tr>
<td>3-6</td>
<td>IPsec Tunnel Configuration</td>
<td>22</td>
</tr>
<tr>
<td>3-7</td>
<td>Preshared Key Configuration - Initiator user</td>
<td>24</td>
</tr>
<tr>
<td>3-8</td>
<td>Preshared Key Configuration - Responder user</td>
<td>25</td>
</tr>
<tr>
<td>4-1</td>
<td>Analyser Settings - Initiator</td>
<td>26</td>
</tr>
<tr>
<td>4-2</td>
<td>Analyser Settings – Responder</td>
<td>27</td>
</tr>
</tbody>
</table>
# INTRODUCTION

## 1.1 Outline

This application note will consider the following scenario:

![Figure 1-1-1: Overview Diagram](image)

Internet Protocol Security (IPsec) is a set of protocols providing cryptographic security services and allows creation of encrypted tunnel between two private networks (VPN). In order to set up and maintain the IPsec VPN, Internet Key Exchange Protocol (IKE) is used. In the last few years, a new version has been designed for IKE protocol (IKEv2), that has the basic outcome as IKEv1 but introduces many improvements as decreased latency (only 4 messages need to be exchanged for set up the VPN) and reliability (all messages are acknowledge and sequenced).

This Application Note gives a guide on configuring an IPsec VPN with IKEv2 between two TransPort routers.

## 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 and configure it with basic routing functions.

This application note applies only to:

**Model:** Digi Transport WR44

**Other Compatible Models:** Digi Transport VC7400 VPN Concentrator, WR, SR or DR.

**Firmware versions:** 5.077 and later

**Configuration:** This Application Note assumes the devices are set to their factory default configurations. Most configuration commands are only shown if they differ from the factory default.
How to Configure an IKEv2 VPN Tunnel Between Two Digi Transport Routers

For the purpose of this application note the following applies:

- Preconditions: This guide assumes that two Digi TransPort are reachable to each other via an Internet connection.

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 Number</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>Draft</td>
</tr>
<tr>
<td>1.0</td>
<td>January 2017 – Updated WEB UI, brand, tests</td>
</tr>
</tbody>
</table>
2 DIGI CONFIGURATION – INITIATOR

2.1 LAN Settings

In this AN the LAN interface of the Transport that acts as Initiator is configured on ETH 0 and left as default (192.168.1.1). The configuration can be checked going to the WEB UI:

CONFIGURATION – NETWORK > INTERFACES > ETHERNET > ETH 0

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>192.168.1.1</td>
<td>This parameter specifies the IP address of this Ethernet port on your LAN</td>
</tr>
<tr>
<td>Mask</td>
<td>255.255.255.0</td>
<td>The subnet mask of the IP subnet to which the router is attached via this Ethernet port</td>
</tr>
</tbody>
</table>
2.2  WAN Settings

First of all, the Digi TransPort acting as Initiator must have an Internet connection, in this Application note we will configure the ETH WAN in the WR44 as follows.

2.2.1  ETH 1 configuration

In this Application note we will configure the ETH 1 as DHCP Client:

CONFIGURATION – NETWORK > INTERFACES > ETHERNET > ETH 1

![Figure 2-2 ETH 1 Configuration](image)

Then, IPsec must be enabled under the interface, going into the advanced section:
How to Configure an IKEv2 VPN Tunnel Between Two Digi Transport Routers

**Figure 2-3 ETH 1 Configuration – Advanced**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get an IP address automatically using DHCP</td>
<td>Ticked</td>
<td>When selected, enable the DHCP client on the ETH interface so it will get an IP address automatically using DHCP</td>
</tr>
<tr>
<td>Enable IPsec on this interface</td>
<td>Enabled</td>
<td>Enable IPsec security features for this interface</td>
</tr>
</tbody>
</table>
2.2.2 Default Route configuration

In the scenario considered in this AN, the default gateway for the TransPort that acts as Initiator is 10.10.1.3, so a default route need to be configured:

**CONFIGURATION - NETWORK > IP ROUTING/FORWARDING > STATIC ROUTES > DEFAULT ROUTE 0:**

![Figure 2-4 Default Route](image)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Ethernet 1</td>
<td>The interface used to route the packets is selected from the drop-down list and its instance number is entered into the adjacent text box.</td>
</tr>
</tbody>
</table>

2.3 IKEv2 Configuration

In order to configure the IKEv2 part for the initiator, set the parameters as indicated below:

**CONFIGURATION – NETWORK > VPN > IPSEC > IKE > IKEV2 > IKEV2 0**
How to Configure an IKEv2 VPN Tunnel Between Two Digi Transport Routers

Figure 2-5 IKE v2 configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption</td>
<td>AES (128 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 for Phase 1</td>
<td>2 (1024)</td>
<td>Sets the key length used in the IKE Diffie-Hellman exchange</td>
</tr>
</tbody>
</table>

Click apply to temporarily save the changes.
2.4 IPsec tunnel Configuration

The following section describes how to configure the Digi TransPort’s IPsec Tunnel settings on the initiator.

Refer to the following picture and table for the settings of parameters:

**CONFIGURATION – NETWORK > VPN > IPSEC > IPSEC TUNNELS > IPSEC 0**

![IPsec Tunnel Configuration](image)

Figure 2-6 IPsec Tunnel Configuration
# How to Configure an IKEv2 VPN Tunnel Between Two Digi Transport Routers

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The IP address or hostname of the remote unit</td>
<td>37.80.37.21</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 &gt; Use these settings for the Local LAN</td>
<td>IP address: 192.168.1.0 Mask: 255.255.255.0</td>
<td>The subnet LAN of the local peer</td>
</tr>
<tr>
<td>Remote LAN &gt; Use these settings for the Remote LAN</td>
<td>IP address: 172.16.0.0 Mask: 255.255.255.0</td>
<td>The subnet LAN of the other peer</td>
</tr>
<tr>
<td>Use the following security on this tunnel</td>
<td>Preshared Keys (Selected)</td>
<td>Choose the security type for the connection. In this AN, Preshared Keys are used</td>
</tr>
<tr>
<td>Our ID</td>
<td>initiator</td>
<td>The ID that the initiator will use. This AN will use “transport” as the local ID.</td>
</tr>
<tr>
<td>Our ID type</td>
<td>IKE ID</td>
<td>Choose the type of ID used, IKE ID allows the use of descriptive text strings (friendly names)</td>
</tr>
<tr>
<td>Remote ID</td>
<td>responder</td>
<td>Set the ID that responder will use. In this AN we will use the id “transport2” as the Remote ID for this tunnel.</td>
</tr>
<tr>
<td>Use &lt;&gt; encryption on this tunnel</td>
<td>AES (128 bit keys)</td>
<td>This is the encryption type to use for the tunnel. This AN uses 3DES</td>
</tr>
<tr>
<td>Use &lt;&gt; authentication on this tunnel</td>
<td>SHA1</td>
<td>This is the authentication type to use for the tunnel. This AN uses SHA1.</td>
</tr>
<tr>
<td>Use Diffie Hellman group &lt;&gt;</td>
<td>2</td>
<td>This is the Diffie Hellman (DH) group to use. This AN uses group 2.</td>
</tr>
<tr>
<td>Use IKE &lt;&gt; to negotiate this tunnel</td>
<td>v2</td>
<td>Set The IKE version to use to negotiate this IPsec tunnel, for this AN select “v2”</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 the 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>
### 2.5 Preshared Key Configuration

In IKEv2 for the configuration of Preshared Key, two users need to be configured, one for the local peer and one for the remote. The key for the two users can be different (but each has to match the one configured on the other peer for the same user).

Note that any user can be used as the user for the Preshared Key, but best practice recommends using a user in the upper range of users because these users have the (router management) Access Level already set to ‘None’. If a lower User number is configured, the Access Level should be changed to be ‘None’.

Refer to the following pictures and tables for the configuration of the users:

**CONFIGURATION – SECURITY > USERS > USER 10-14 > USER 10**

![Figure 2-7 Preshared Key Configuration - Initiator user](image)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>initiator</td>
<td>This is the username for the local peer and should match the Local ID configured in the IPsec tunnel</td>
</tr>
<tr>
<td>Password/Confirm</td>
<td>****</td>
<td>Fill this field with the Preshared Key for the Local peer ID in the VPN tunnel</td>
</tr>
<tr>
<td>Access Level</td>
<td>None</td>
<td>This is the access level for the user, in the case of preshared key user, it will not be granted any admin access</td>
</tr>
</tbody>
</table>
How to Configure an IKEv2 VPN Tunnel Between Two Digi Transport Routers

CONFIGURATION – SECURITY > USERS > USER 10-14 > USER 10

Figure 2-8 Preshared Key Configuration - Responder user

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>responder</td>
<td>This is the username for the remote peer and should match the Remote ID configured in the IPsec tunnel</td>
</tr>
<tr>
<td>Password/Confirm</td>
<td>****</td>
<td>Fill this field with the Preshared Key for the Remote peer ID in the VPN tunnel.</td>
</tr>
<tr>
<td>Access Level</td>
<td>None</td>
<td>This is the access level for the user, in the case of preshared key user, it will not be granted any admin access</td>
</tr>
</tbody>
</table>
3 DIGI CONFIGURATION - RESPONDER

As done for the initiator, in order to configure the Digi TransPort, connect a PC to the ETH0 of the TransPort and log into the Web User Interface (WebUI) with a browser at the default address 192.168.1.1. Then follow the sections below.

3.1 LAN Settings

In this AN the LAN interface of the Transport that acts as Responder is configured on ETH 0, so that need to be changed from the default settings, going to the WEB UI at the section CONFIGURATION – NETWORK > INTERFACES > ETHERNET > ETH 0:

![Figure 3-1 LAN Settings](image)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>172.16.0.1</td>
<td>Specifies the IP address of this Ethernet port</td>
</tr>
<tr>
<td>Mask</td>
<td>255.255.255.0</td>
<td>Specifies the subnet mask of the IP subnet to which the unit is attached via this Ethernet port</td>
</tr>
</tbody>
</table>
Please note that having changed the LAN address, you will need to connect again to the router with the browser pointing at the new address 172.16.0.1 (this implies a change also in the IP address of your laptop).

### 3.2 WAN Settings

First of all, the Digi TransPort acting as responder must have an Internet connection, in this Application note we will configure the Cellular WAN in the WR44 as follows.

#### 3.2.1 Cellular module configuration

Refer to the following picture and table for the settings of parameters. Note that the SIM PIN, username and password fields may or may not be required.

**Configuration → Interfaces → Mobile → Mobile Settings**

![Figure 3-2: Mobile settings](image)
How to Configure an IKEv2 VPN Tunnel Between Two Digi Transport Routers

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIM</td>
<td>1</td>
<td>Select SIM 1 for the PPP 1 interface</td>
</tr>
<tr>
<td>Service Plan/APN</td>
<td>internet.t-d1.de</td>
<td>The Access Point Name for the network</td>
</tr>
<tr>
<td>SIM PIN / Confirm SIM PIN</td>
<td>&lt;PIN&gt; (optional)</td>
<td>Insert/Confirm the SIM PIN if required by the SIM</td>
</tr>
<tr>
<td>Username</td>
<td>W-WAN username</td>
<td>Enter the username given by your wireless operator (If required)</td>
</tr>
<tr>
<td>Password/Confirm Password</td>
<td>W-WAN Password</td>
<td>Enter the password given by your wireless operator (If required)</td>
</tr>
</tbody>
</table>

Click Apply.

Note: The APN is dependent on the mobile operator, check with the service provider to obtain the correct APN.
3.2.2 WAN Interface Configuration (PPP1)

The following section configures the Digi TransPort to use PPP 1 for the cellular interface. Leave all the default settings, except for what is indicated in the following. The username and password fields may or may not be required by the SIM.

**CONFIGURATION → INTERFACES → ADVANCED → PPP1**

![Figure 3-3 PPP 1 settings](image)
How to Configure an IKEv2 VPN Tunnel Between Two Digi Transport Routers

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>&lt;Username&gt;</td>
<td>The username to use when authenticating with the mobile operator</td>
</tr>
<tr>
<td>Password / Confirm Password</td>
<td>&lt;Password&gt;</td>
<td>The password to use when authenticating with the mobile operator</td>
</tr>
<tr>
<td>Enable IPsec on this interface</td>
<td>Ticked</td>
<td>Enables IPsec on PPP 1 interface.</td>
</tr>
</tbody>
</table>

Click apply, then go to **ADMINISTRATION → SAVE CONFIGURATION** and save.

### 3.2.3 Default Route Configuration

In the scenario considered in this AN the default gateway for the TransPort that acts as Responder is 10.10.2.3, so a default route need to be configured:

**CONFIGURATION - NETWORK > IP ROUTING/FORWARDING > STATIC ROUTES > DEFAULT ROUTE 0:**

![Figure 3-4 Default Route](image.png)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>PPP 1</td>
<td>Set the interface used to default route the packets, is selected from the drop-down list and the interface instance number is entered into the adjacent text box</td>
</tr>
</tbody>
</table>
3.3 IKEv2 Configuration

In order to configure the IKEv2 part for the responder, set the parameters as indicated below.

In order to have the TransPort to be able to respond to IKE request for every authentication/encryption/PRF/group algorithm, check all the options as shown below (by default may not be all already selected). Leave the rest of the settings as default.

CONFIGURATION – NETWORK > VPN > IPSEC > IKE > IKEV2 > IKEV2 RESPONDER

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption</td>
<td>ALL selected</td>
<td>Set the acceptable encryption algorithms and minimum AES key length</td>
</tr>
<tr>
<td>Authentication</td>
<td>ALL selected</td>
<td>Set the acceptable authentication algorithms.</td>
</tr>
<tr>
<td>PRF Algorithm</td>
<td>ALL selected</td>
<td>Set the acceptable PRF (Pseudo Random Function) algorithms</td>
</tr>
</tbody>
</table>
3.4 IPsec Tunnel Configuration

The following section describes how to configure the Digi TransPort's IPsec Tunnel settings on the responder.

Refer to the following picture and table for the settings of parameters:

**CONFIGURATION – NETWORK > VPN > IPSEC > IPSEC TUNNELS > IPSEC 0**

![IPsec Tunnel Configuration](image)

*Figure 3-6 IPsec Tunnel Configuration*
How to Configure an IKEv2 VPN Tunnel Between Two Digi Transport Routers

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local LAN &gt; Use these settings for the Local LAN</td>
<td>IP address: 172.16.1.0 Mask: 255.255.255.0</td>
<td>The subnet LAN of the local peer</td>
</tr>
<tr>
<td>Remote LAN &gt; Use these settings for the Remote LAN</td>
<td>IP address: 192.168.1.0 Mask: 255.255.255.0</td>
<td>The subnet LAN of the other peer</td>
</tr>
<tr>
<td>Use the following security on this tunnel</td>
<td>Preshared Keys (Selected)</td>
<td>Choose the security type for the connection. In this AN, Preshared Keys are used</td>
</tr>
<tr>
<td>Our ID</td>
<td>Transport2</td>
<td>The ID that the responder will use. This AN will use “transport2” as the local ID.</td>
</tr>
<tr>
<td>Our ID type</td>
<td>IKE ID</td>
<td>Choose the type of ID used, IKE ID allows the use of descriptive text strings (friendly names)</td>
</tr>
<tr>
<td>Remote ID</td>
<td>transport</td>
<td>Set the ID that initiator will use. In this AN we will use the id “transport” as the Remote ID for this tunnel.</td>
</tr>
<tr>
<td>Use &lt;&gt; encryption on this tunnel</td>
<td>3DES</td>
<td>This is the encryption type to use for the tunnel. This AN uses 3DES</td>
</tr>
<tr>
<td>Use &lt;&gt; authentication on this tunnel</td>
<td>SHA1</td>
<td>This is the authentication type to use for the tunnel. This AN uses SHA1.</td>
</tr>
<tr>
<td>Use Diffie Hellman group &lt;&gt;</td>
<td>2</td>
<td>This is the Diffie Hellman (DH) group to use. This AN uses group 2.</td>
</tr>
<tr>
<td>Use IKE &lt;&gt; to negotiate this tunnel</td>
<td>v2</td>
<td>Set The IKE version to use to negotiate this IPsec tunnel, for this AN select “v2”</td>
</tr>
<tr>
<td>Bring this tunnel up</td>
<td>On demand</td>
<td>This controls how the IPsec tunnel is brought up, for the responder “On demand” option is chosen</td>
</tr>
<tr>
<td>If the 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. For the responder is chosen “drop packet” option</td>
</tr>
</tbody>
</table>

Local LAN > Use these settings for the Local LAN | IP address: 172.16.1.0 Mask: 255.255.255.0 | The subnet LAN of the local peer |
Remote LAN > Use these settings for the Remote LAN | IP address: 192.168.1.0 Mask: 255.255.255.0 | The subnet LAN of the other peer |
Use the following security on this tunnel | Preshared Keys (Selected) | Choose the security type for the connection. In this AN, Preshared Keys are used |
3.5 Preshared Key Configuration

As done for the initiator, also in the responder two users need to be configured for the two peers. Refer to the following pictures and tables for the configuration of the users:

**CONFIGURATION – SECURITY > USERS > USER 10-14 > USER 10**

![Figure 3-7 Preshared Key Configuration - Initiator user](image)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>initiator</td>
<td>This is the username for the local peer and should match the Local ID configured in the IPsec tunnel</td>
</tr>
<tr>
<td>Password/Confirm</td>
<td>****</td>
<td>Fill this field with the Preshared Key for the Local peer ID in the VPN tunnel</td>
</tr>
<tr>
<td>Access Level</td>
<td>None</td>
<td>This is the access level for the user, in the case of preshared key user, it will not be granted any admin access</td>
</tr>
</tbody>
</table>
How to Configure an IKEv2 VPN Tunnel Between Two Digi Transport Routers

**CONFIGURATION – SECURITY > USERS > USER 10-14 > USER 11**

![Figure 3-8 Preshared Key Configuration - Responder user](image)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>responder</td>
<td>This is the username for the remote peer and should match the Remote ID configured in the IPsec tunnel</td>
</tr>
<tr>
<td>Password/Confirm</td>
<td>****</td>
<td>Fill this field with the Preshared Key for the Remote peer ID in the VPN tunnel.</td>
</tr>
<tr>
<td>Access Level</td>
<td>None</td>
<td>This is the access level for the user, in the case of preshared key user, it will not be granted any admin access</td>
</tr>
</tbody>
</table>
4 TESTING

4.1 Analyser Settings

In many cases is very useful configure the analyser in order to have a debug trace for the IKE negotiation in case of issues of setting up the VPN and for check that the traffic is correctly tunnelled.

On both initiator and responder change the settings of the Analyser as shown below (uncheck everything else):

**MANAGEMENT - ANALYSER > SETTINGS**

**Initiator (WR44):**

![Figure 4-1 Analyser Settings - Initiator](image)
Responder (WR21):
### How to Configure an IKEv2 VPN Tunnel Between Two Digi Transport Routers

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Analyser</td>
<td>Selected</td>
<td>This checkbox is used to enable or disable the analyser.</td>
</tr>
<tr>
<td>Maximum packet capture size</td>
<td>1500</td>
<td>The number of bytes that are captured and stored for each packet. If the packet is bigger than the configured size, the packet is truncated. Common practice is to set it to 1500.</td>
</tr>
<tr>
<td>Log Size</td>
<td>180</td>
<td>The maximum size of the pseudo file “ana.txt” that is used to store the captured data packets. Common practice is to set at this maximum (180). Notice that the data is compressed so more than 180Kb of trace data will be captured.</td>
</tr>
<tr>
<td>Protocol layers</td>
<td>Layer 3 (Network)</td>
<td>Specify which protocol layers are captured and included in the analyser trace. For the purpose of this AN the Network Layer (Layer 3) is chosen.</td>
</tr>
<tr>
<td>Enable IKE debug</td>
<td>Selected</td>
<td>Used to enable/disable the inclusion of IKE packets in the analyser trace when using IPsec.</td>
</tr>
<tr>
<td>IP Sources</td>
<td>ETH 0 &amp; ETH 1, ETH 0 &amp; PPP 1</td>
<td>Select the IP sources over which packets will be captured and included in the analyser trace.</td>
</tr>
</tbody>
</table>
4.2 Setting the tunnel UP

As soon as the initiator is configured to set up a VPN, it will try to connect to the responder. For a successful negotiation we should see the following logs in the eventlog of the devices:

**MANAGEMENT - EVENT LOG**

**Initiator:**

10:55:41, 03 Jan 2017, (69) IKEv2 Negotiation completed pe, Initiator
10:55:41, 03 Jan 2017, Eroute 0 VPN up peer: responder
10:55:41, 03 Jan 2017, New IPSec SA created by responder
10:55:41, 03 Jan 2017, (69) New IKEv2 Negotiation peer 37.80.102.65, Initiator (Create Child)
10:55:41, 03 Jan 2017, IKE Request Received From Eroute 0
10:55:41, 03 Jan 2017, Par change by username, eroute 0 autosa to 2
10:55:38, 03 Jan 2017, (69) IKEv2 Negotiation completed pe, Initiator
10:55:38, 03 Jan 2017, PPP 1 down, LL disconnect
10:55:37, 03 Jan 2017, (69) New IKEv2 Negotiation peer 37.80.102.65, Initiator (Info)

**Responder:**

10:50:51, 03 Jan 2017, (154) IKEv2 Negotiation completed pe, Responder
10:50:51, 03 Jan 2017, Eroute 0 VPN up peer: initiator
10:50:51, 03 Jan 2017, New IPSec SA created by initiator
10:50:49, 03 Jan 2017, Telnet session closed
10:50:48, 03 Jan 2017, (154) IKEv2 Negotiation completed pe, Responder

The status of the IPsec and IKEv2 SAs can also be seen in the WEB UI:

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

**Initiator:**

![IPSec Status Table](image-url)
Responder:
4.3 Testing Traffic on the tunnel

Once the VPN is UP, in order to test if LAN to LAN traffic is tunnelled as configured, do a ping from a host on initiator LAN to a host in responder LAN. In this AN the two hosts have 192.168.1.100 and 172.16.1.100 as ip addresses.

Looking at the trace on the initiator (MANAGEMENT - ANALYSER > TRACE):

1) An ICMP ECHO REQUEST arrives on ETH 0 form 192.168.1.100, with destination address the host at Responder LAN side (172.16.0.100):

```
-------- 3-1-2017 13:06:43.230 --------
45 00 00 3C 11 8B 00 00 80 01 BA B5 C0 A8 01 64     E............d
AC 10 00 64 08 00 4D 4C 00 01 00 00 61 62 63 64     ...d..ML....abcd
65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74     efgijklmnopqrstuvwxyz
75 76 77 61 62 63 64 65 66 67 68 69                  uvwabcdefghi

IP (In) From REM TO LOC IFACE: ETH 0
45             IP Ver:        4
00            Hdr Len:       20
00              TOS:           Routine
00              Delay:         Normal
00              Throughput:    Normal
00              Reliability:   Normal
00 3C          Length:        60
11 8B          ID:            4491
00 00          Frag Offset:   0
00              Congestion:    Normal
80              TTL:           128
01              Proto:         ICMP
BA B5          Checksum:      47797
C0 A8 01 64    Src IP:        192.168.1.100
AC 10 00 64    Dst IP:        172.16.0.100
ICMP:
08              Type:          ECHO REQ
00              Code:          0
4D 4C          Checksum:      19533
--------
```
2) The packet matches the eroute 0 and is encrypted and sent through the tunnel with source 10.104.1.121 (initiator WAN address) and destination 37.80.102.65 (responder WAN address)

```
-----   3-1-2017  13:06:43.230   -------
45 00 00 3C 11 8B 00 00 7F 01 BB B5 C0 A8 01 64 E..<...........d
AC 10 00 64 08 00 4D 4C 00 01 00 0F 61 62 63 64 ...d..ML....abcd
65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 efgijklmnopqrstuvwxyz
75 76 77 61 62 63 64 65 66 67 68 69 uvwbcdefghi

ER 0-responder From LOC TO REMIFACE: ETH 1
45             IP Ver:        4
00             Hdr Len:       20
AC 10 00 64    Dst IP:        172.16.0.100
4D 4C          Checksum:      19533
IP (Final) From LOC TO REM    IFACE: ETH 1
45             IP Ver:        4
00             Hdr Len:       20
AC 10 00 64    Dst IP:        172.16.0.100
```

How to Configure an IKEv2 VPN Tunnel Between Two Digi Transport Routers
How to Configure an IKEv2 VPN Tunnel Between Two Digi Transport Routers

00 0C          ID:            12
00 00          Frag Offset:   0
  Congestion: Normal
       May Fragment
       Last Fragment
FA          TTL:           250
11          Proto:         UDP
28 EF        Checksum:      10479
0A 68 01 79  Src IP:        10.104.1.121
25 50 66 41  Dst IP:        37.80.102.65
UDP:
11 94        SRC Port:      IKE FLOAT (4500)
11 94        DST Port:      IKE FLOAT (4500)
00 6C        Length:        108
00 00        Checksum:      0

----------

3) The reply arrives on ETH1 through the tunnel:

-----   3-1-2017  13:06:44.480   -----
45 00 00 80 00 0B 00 00 E9 11 39 F0 25 50 66 41   E.......9.%PfA
0A 68 01 79 11 94 11 94 00 6C 00 00 76 41 2D C2    .h.y.....l..vA-.n
00 00 00 07 6A DA 9C E0 8A E4 81 8F 07 BB 76    .........V
46 A1 2A EB D1 52 98 6F 42 89 83 83 13 AE 0F 6E    .F.*R.oB.....n
77 3F 2E 7C BC 94 D7 15 88 57 BE B3 8F 8C 55 37    w?.|.....W....U7
67 41 5A 11 5F 62 E8 AF 51 8C BF 2B A5 C1     gA.\..^b..Q楼上
CD 48 5A BE E4 90 74 7E 2B 9D 68 86 10 C5 CA 63   .HZ...t+-h....c
57 FD 33 1C 7E 86 E5 1D 1B 4E EE 98 1F 98 AA DF    W.3~....@......

IP (In) From REM TO LOC       IFACE: ETH 1
45          IP Ver:        4
 Hdr Len:    20
00          TOS:           Routine
Delay:      Normal
Throughput: Normal
Reliability: Normal
00 80       Length:        128
00 0B       ID:            11
00 00       Frag Offset:   0
  Congestion: Normal
       May Fragment
       Last Fragment
E9          TTL:           233
11          Proto:         UDP
39 F0        Checksum:      14832
25 50 66 41  Src IP:        37.80.102.65
0A 68 01 79  Dst IP:        10.104.1.121
UDP:
11 94        SRC Port:      IKE FLOAT (4500)
11 94        DST Port:      IKE FLOAT (4500)
00 6C        Length:        108
4) The packet is decrypted and the ICMP ECHO REPLY is revealed and sent to the destination host via ETH 0:

```
----- 3-1-2017 13:06:44.480       -------
45 00 00 3C 54 BC 00 00 7F 01 78 84 AC 10 00 64       E..<T......x.....d
C0 A8 01 64 00 00 55 4C 00 01 00 0F 61 62 63 64       ...d..UL....abcd
65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74       efgijklmnopqrstuvwxyz
75 76 77 61 62 63 64 65 66 67 68 69       uvwbcdefghi
IP (Cont) From REM TO LOC  IFACE: ETH 1
45             IP Ver:        4
Hdr Len:       20
00             TOS:           Routine
Delay:         Normal
Throughput:    Normal
Reliability:   Normal
00 3C          Length:        60
54 BC          ID:            21692
00 00          Frag Offset:   0
Congestion:    Normal
May Fragment
Last Fragment
7F             TTL:           127
01             Proto:         ICMP
78 84          Checksum:      30852
AC 10 00 64    Src IP:        172.16.0.100
C0 A8 01 64    Dst IP:        192.168.1.100
ICMP:
00             Type:          ECHO REPLY
00             Code:          0
55 4C          Checksum:      19541
-------
----- 3-1-2017 13:06:44.480       -------
45 00 00 3C 54 BC 00 00 7E 01 79 84 AC 10 00 64       E..<T......y.....d
C0 A8 01 64 00 00 55 4C 00 01 00 0F 61 62 63 64       ...d..UL....abcd
65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74       efgijklmnopqrstuvwxyz
75 76 77 61 62 63 64 65 66 67 68 69       uvwbcdefghi
IP (Final) From LOC TO REM    IFACE: ETH 0
45             IP Ver:        4
Hdr Len:       20
00             TOS:           Routine
Delay:         Normal
Throughput:    Normal
Reliability:   Normal
00 3C          Length:        60
54 BC          ID:            21692
```
How to Configure an IKEv2 VPN Tunnel Between Two Digi Transport Routers

00 00     Frag Offset:   0
           Congestion: Normal
                      May Fragment
                      Last Fragment
7E         TTL:         126
01         Proto:       ICMP
79 84      Checksum:    31108
AC 10 00 64 Src IP:     172.16.0.100
C0 A8 01 64 Dst IP:     192.168.1.100
ICMP:
00         Type:       ECHO REPLY
00         Code:       0
55 4C      Checksum:   19541
----------
5 CONFIGURATION FILES

5.1 Initiator Configuration

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

```
eth 0 IPaddr "192.168.1.1"
eth 0 ipanon ON
eth 1 dhcpcli ON
eth 1 ipsec 1
eth 1 ipanon ON
lapb 0 ans OFF
lapb 0 tinact 120
lapb 1 tinact 120
lapb 3 dtmode 0
lapb 4 dtmode 0
lapb 5 dtmode 0
lapb 6 dtmode 0
ip 0 cidr ON
def_route 0 ll_ent "ETH"
def_route 0 ll_add 1
eroute 0 descr "IKEv2 IPsec Tunnel"
eroute 0 peerip "37.80.102.65"
eroute 0 peerid "responder"
eroute 0 ourid "initiator"
eroute 0 locip "192.168.1.0"
eroute 0 locmsk "255.255.255.0"
eroute 0 remip "172.16.0.0"
eroute 0 remmsk "255.255.255.0"
eroute 0 ESPauth "SHA1"
eroute 0 ESPenc "AES"
eroute 0 authmeth "PRESHARED"
eroute 0 nosa "TRY"
eroute 0 autosa 2
eroute 0 ikever 2
eroute 0 dhgroup 2
eroute 0 enckeybits 128
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 use_modem 1
ppp 1 aodion 1
ppp 1 autoassert 1
```
How to Configure an IKEv2 VPN Tunnel Between Two Digi Transport Routers

```
ppp 1 r_chap OFF
ppp 3 name "DSL"
ppp 3 l1iface "AAL"
ppp 3 username "Enter ADSL Username"
ppp 3 r_addr OFF
ppp 3 IPaddr "0.0.0.0"
ppp 3 l_addr ON
ppp 3 timeout 0
ppp 3 do_nat 2
ppp 3 aodion 1
ppp 3 autoassert 1
ppp 3 immoos ON
ppp 3 echo 10
ppp 3 echodropcnt 5
ppp 3 l_pap OFF
ppp 3 l_chap OFF
ppp 3 defpak 16
ppp 4 defpak 16
web 0 prelogin_info ON
ftpcli 0 hostname "ftp1.digi.com"
ftpcli 0 directory "support/firmware/transport/radio_module_firmware/he910d"
ike2 0 iencalg "AES"
ike2 0 ienckeybits 128
ike2 0 idhgroup 2
modemcc 0 info_asy_add 6
modemcc 0 init_str "+CGQREQ=1"
modemcc 0 init_str1 "+CGQM=1"
modemcc 0 apn "Your.APN.goes.here"
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 "+CGQM=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 ikeon ON
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 anonftp ON
cmd 0 tremto 1200
```
How to Configure an IKEv2 VPN Tunnel Between Two Digi Transport Routers

```plaintext
cmd 0 rcihttp ON
cmd 4 cmd_processor OFF
user 0 access 0
user 1 name "username"
user 1 epassword "KD51SVJDWVg="
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
user 10 name "initiator"
user 10 epassword "PDZxU0FFQFU="
user 10 access 4
user 11 name "responder"
user 11 epassword "PDZxU0FFQFU="
user 11 access 4
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
templog 0 mb_autooff ON
templog 0 mo_autooff ON
cloud 0 ssl ON
```
5.2 Responder Configuration

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

```
eth 0 IPaddr "172.16.0.1"
eth 0 ipanon ON
addp 0 enable 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 IPsec Tunnel"
eroute 0 peerid "initiator"
eroute 0 ourid "responder"
eroute 0 locip "172.16.0.0"
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 "PRESHARED"
eroute 0 ikever 2
eroute 0 dgroup 2
eroute 0 enckeybits 128
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.etherios.com"
snmpuser 0 eCommunity "KCp0VkxP"
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
ike 0 deblevel 4
ike2 0 rencacls "DES,3DES,AES"
ike2 0 renckeybits 128
```
ike2 @ rauthalgs "MD5,SHA1"
ike2 @ rprfalgs "MD5,SHA1"
modemcc 0 asy_add 4
modemcc 0 info_asy_add 2
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 ikeon ON
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 "KD5lSVJDVg="
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
user 10 name "initiator"
user 10 epassword "PDZxU0FFQFU="
user 10 access 4
user 11 name "responder"
user 11 epassword "PDZxU0FFQFU="
user 11 access 4
local 0 transaccess 2
sslsvr 0 certfile "cert01.pem"
sslsvr 0 keyfile "privrsa.pem"
ssh Ø hostkey1 "privSSH.pem"
ssh Ø nb_listen 5
ssh Ø v1 OFF
templog Ø mo_autooff ON
cloud Ø ssl ON