Application Note

How to create an IPsec VPN between a Digi TransPort router and TheGreenBow VPN client

14 March 2017
Contents

1 Introduction ......................................................................................................................................... 4
  1.1 Outline .......................................................................................................................................... 4
  1.2 Assumptions ................................................................................................................................. 4
  1.3 Corrections ................................................................................................................................... 5
  1.4 Version .......................................................................................................................................... 5

2 Digi Configuration ................................................................................................................................ 6
  2.1 WAN Setting .................................................................................................................................. 6
    2.1.1 Cellular module configuration ................................................................................................. 6
    2.1.2 WAN Interface Configuration (PPP1) ....................................................................................... 7
  2.2 IPsec Tunnel configuration .......................................................................................................... 9
  2.3 IKE Responder configuration ..................................................................................................... 10
  2.4 Preshared Key ............................................................................................................................ 11

3 TheGreenBow VPN client configuration ............................................................................................ 13
  3.1 Launch TheGreenBow Client ..................................................................................................... 13
  3.2 Phase 1 Configuration: Authentication ..................................................................................... 14
  3.3 Phase 1 Configuration: Advanced ............................................................................................. 17
  3.4 Phase 2 Configuration ................................................................................................................ 18

4 TESTING .............................................................................................................................................. 20
  4.1 Open the tunnel from the client ................................................................................................ 20
  4.2 Check Tunnel on the TransPort ................................................................................................. 22
  4.3 Test traffic through the tunnel .................................................................................................. 23
    4.3.1 Configure the analyser ........................................................................................................... 23
    4.3.2 Test traffic ............................................................................................................................... 24
    4.3.3 Check analyser trace .............................................................................................................. 25

5 CONFIGURATION FILE ........................................................................................................................ 28
  5.1 Configuration file.......................................................................................................................... 28
## Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 1-1</td>
<td>Overview Diagram</td>
<td>4</td>
</tr>
<tr>
<td>Figure 2-1</td>
<td>Mobile settings</td>
<td>7</td>
</tr>
<tr>
<td>Figure 2-2</td>
<td>PPP 1 configuration</td>
<td>8</td>
</tr>
<tr>
<td>Figure 2-3</td>
<td>IPsec Settings</td>
<td>9</td>
</tr>
<tr>
<td>Figure 2-4</td>
<td>IKE Responder</td>
<td>11</td>
</tr>
<tr>
<td>Figure 2-5</td>
<td>PreShared Key</td>
<td>12</td>
</tr>
<tr>
<td>Figure 3-1</td>
<td>Launch TheGreenbow Client</td>
<td>13</td>
</tr>
<tr>
<td>Figure 3-2</td>
<td>TheGreenBow client Configuration Panel</td>
<td>13</td>
</tr>
<tr>
<td>Figure 3-3</td>
<td>TheGreenBow Phase 1 - new</td>
<td>14</td>
</tr>
<tr>
<td>Figure 3-4</td>
<td>TheGreenBow Phase 1</td>
<td>15</td>
</tr>
<tr>
<td>Figure 3-5</td>
<td>TheGreenBow Phase 1 - Authentication</td>
<td>16</td>
</tr>
<tr>
<td>Figure 3-6</td>
<td>TheGreenBow Phase 1 - Advanced</td>
<td>17</td>
</tr>
<tr>
<td>Figure 3-7</td>
<td>TheGreenBow Phase 2_new</td>
<td>18</td>
</tr>
<tr>
<td>Figure 3-8</td>
<td>TheGreenBow Phase 2 settings</td>
<td>19</td>
</tr>
<tr>
<td>Figure 4-1</td>
<td>Opening the tunnel</td>
<td>20</td>
</tr>
<tr>
<td>Figure 4-2</td>
<td>Connection Panel</td>
<td>20</td>
</tr>
<tr>
<td>Figure 4-3</td>
<td>Tunnel Opened_1</td>
<td>21</td>
</tr>
<tr>
<td>Figure 4-4</td>
<td>Tunnel opened_2</td>
<td>21</td>
</tr>
<tr>
<td>Figure 4-5</td>
<td>Tunnel status on the TransPort</td>
<td>22</td>
</tr>
<tr>
<td>Figure 4-6</td>
<td>Analyser Configuration</td>
<td>23</td>
</tr>
<tr>
<td>Figure 4-7</td>
<td>Ping test</td>
<td>24</td>
</tr>
<tr>
<td>Figure 4-8</td>
<td>Refresh trace</td>
<td>25</td>
</tr>
</tbody>
</table>
How to create an IPsec VPN between a Digi TransPort router and TheGreenBow VPN client

1 INTRODUCTION

1.1 Outline

In this application note we will consider the following scenario:

![Overview Diagram](image)

**Figure 1-1: Overview Diagram**

It is often required to configure a Digi TransPort router as a VPN Server, in order to allow a remote user, using a VPN client, to connect securely to a private LAN passing through Internet.

This application note explains the procedure of creating an IPsec VPN between a Digi TransPort router (as the VPN Server) and the TheGreenBow VPN client, installed on remote user PC.

With the VPN creation, the ip address 172.16.1.100 will be assigned to the GreenBow client and the remote user will be able to communicate securely with the corporate LAN through the VPN.

Note that although in this example the WR21 model is used, the same settings can be applied to all other Digi TransPort models with IPsec enabled (certain models may not have the IPsec encryption option enabled, if this is the case, please contact Digi Support for details on how to enable this option).

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
How to create an IPsec VPN between a Digi TransPort router and TheGreenBow VPN client

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 WR21

**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.

For the purpose of this application note the following applies:

- This guide assumes that the Digi has an active connection from a cellular provider that is mobile terminated, and that TheGreenBow VPN client is installed and activated on a PC that will be used to connect to the TransPort through the 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>1.0</td>
<td>First version - Published</td>
</tr>
<tr>
<td>2.0</td>
<td>New version – Rebranded and new WEB UI</td>
</tr>
</tbody>
</table>
2 DIGI CONFIGURATION

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.

2.1 WAN Setting

First of all, the Digi TransPort must have an Internet connection, in this Application note we will configure the Cellular WAN in the WR21 as follows.

2.1.1 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**

<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>
How to create an IPsec VPN between a Digi TransPort router and TheGreenBow VPN client

Click Apply.

Note: The APN is dependent on the mobile operator, check with the service provider to obtain the correct APN.

2.1.2 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.
How to create an IPsec VPN between a Digi TransPort router and TheGreenBow VPN client

**CONFIGURATION → INTERFACES → ADVANCED → PPP1**

![PPP 1 configuration](image)

*Figure 2-2: PPP 1 configuration*
How to create an IPsec VPN between a Digi TransPort router and TheGreenBow VPN client

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>&lt;Username&gt; (optional)</td>
<td>The username to use when authenticating with the mobile operator</td>
</tr>
<tr>
<td>Password / Confirm Password</td>
<td>&lt;Password&gt; (optional)</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.

### 2.2 IPsec Tunnel configuration

The following section describes how to configure the Digi TransPort’s VPN settings.

**CONFIGURATION – NETWORK ➔ VIRTUAL PRIVATE NETWORKING (VPN) ➔ IPSEC ➔ IPSEC TUNNELS ➔ IPSEC 0**

![Figure 2-3: IPsec Settings](image-url)
How to create an IPsec VPN between a Digi TransPort router and TheGreenBow VPN client

<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: 192.168.1.0&lt;br&gt;Mask: 255.255.255.0</td>
<td>The LAN or IP subnet that the remote VPN client will have access to</td>
</tr>
<tr>
<td>Remote LAN &gt; Use these settings for the Remote LAN</td>
<td>IP address: 172.16.1.0&lt;br&gt;Mask: 255.255.255.0</td>
<td>The subnet that TheGreenBow client will use to connect to the TransPort</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>WR21</td>
<td>The ID that the TransPort will use. This AN will use “WR21” 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>Client</td>
<td>Set the ID that TheGreenBow client will use. In this AN we will use the id “Client” 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 AES 128-bit</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>
</tbody>
</table>

Click Apply to temporarily save the changes.

### 2.3 IKE Responder configuration

The default settings should allow the TransPort to be a “Responder” to the VPN connection already. So it is enough to check that the settings are as default:
How to create an IPsec VPN between a Digi TransPort router and TheGreenBow VPN client

**CONFIGURATION – NETWORK ➔ VIRTUAL PRIVATE NETWORKING (VPN) ➔ IPSEC ➔ IKE ➔ IKE 0**

![Configuration - Network > Virtual Private Networking (VPN) > IPsec > IKE > IKE 0](image)

**Figure 2-4: IKE Responder**

### 2.4 Preshared Key

For the Preshared Key of the VPN tunnel a user will be configured.

Note that any user can be used for the Preshared Key, but best practice recommends using one in the upper range of users because these have the (router management) Access Level already set to a non-admin value. If a lower User number is configured, the Access Level should be changed to be ‘None’.
How to create an IPsec VPN between a Digi TransPort router and TheGreenBow VPN client

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

![Configuration - Security > Users > User 10 - 14 > User 10](image)

**Figure 2-5: PreShared Key**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Client</td>
<td>This is the username and should match the Remote ID configured in the IPsec tunnel 0</td>
</tr>
<tr>
<td>Password</td>
<td>****</td>
<td>Fill this field with the Preshared Key for 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 THEGREENBOW VPN CLIENT CONFIGURATION

The following section describes how to configure TheGreenBow VPN client settings. Download and install TheGreenBow VPN client, this can be obtained from https://www.thegreenbow.com/.

3.1 Launch TheGreenBow Client

Launch TheGreenBow VPN client on the PC that needs to build a VPN into the TransPort. An icon is shown in the Windows system tray as shown is the screenshot below:

![Launch TheGreenbow Client](image1)

Figure 3-1: Launch TheGreenbow Client

Right click on the icon and select “Configuration Panel”, the following windows will open:

![TheGreenBow client Configuration Panel](image2)

Figure 3-2: TheGreenBow client Configuration Panel
3.2 Phase 1 Configuration: Authentication

Right-click on “IKE V1” under VPN Configuration, and select New Phase 1, as shown below:

![Figure 3-3: TheGreenBow Phase 1 - new](image)

The “Ikev1Gateway” is added below in the tree as shown in the following picture:
How to create an IPsec VPN between a Digi TransPort router and TheGreenBow VPN client

Figure 3-4: TheGreenBow Phase 1

Click on “Ikev1Gateway” and refer to the following picture for the setting of parameters:
How to create an IPsec VPN between a Digi TransPort router and TheGreenBow VPN client

Figure 3-5: TheGreenBow Phase 1 - Authentication

Please note:

- **Addresses:** Let the “Interface” as any and set the Remote Gateway with the Mobile IP address of the TransPort.
- **Authentication:** Set the Preshared Key that matches what was used on the TransPort.
- **IKE:** **Encryption/Authentication/Key Group** have to match the parameters that were configured on the TransPort’s IKE 0 page. This AN uses AES 128-bit, SHA1, and DH2.
3.3 Phase 1 Configuration: Advanced

Click the Advanced tab and set the parameters as follows:

![TheGreenBow Phase 1 - Advanced](image)

Please note:

- **Advanced features**: Check the box for Aggressive Mode.
- Choose the type of **Local ID** that will be used, and fill in the value. This AN uses an IKE ID (Also known as KEY ID) as the type, and matches the value that was used on the TransPort for the Remote ID field.
- Choose the type of **Remote ID** that will be used, and fill in the value. This AN uses an IKE ID (Also known as KEY ID) as the type, and matches the value that was used on the TransPort for the Local ID field.
How to create an IPsec VPN between a Digi TransPort router and TheGreenBow VPN client

3.4 Phase 2 Configuration

Right click on the name of the Phase 1 settings (“Ikev1Gateway” in this example) and click on New Phase 2, as shown in the screenshot below:

![Figure 3-7: TheGreenBow Phase 2_new](image)

An “Ikev1Tunnel” will show up under “Ikev1Gateway”, click on it and refer to the following window for the settings:
How to create an IPsec VPN between a Digi TransPort router and TheGreenBow VPN client

![TheGreenBow VPN Client](image)

**Figure 3-8: TheGreenBow Phase 2 settings**

Please note:

- **VPN Client address**: Fill this field with the IP address that matches what was setup as the Remote LAN on the TransPort IPsec tunnel configuration. Here is used 172.16.1.100 as the IP the PC will use to make the VPN connection. So that the PC will use this IP address as its IP address for the VPN connection, also responding on it on the tunnel.
- **Address Type**: choose Subnet Address.
- **Remote LAN address**: The remote LAN subnet that will be accessed via the VPN. This AN uses 192.168.1.0 as the TransPort router’s LAN subnet
- **Subnet mask**: fill in the mask for the Remote LAN Subnet Address. This AN uses 255.255.255.0.
- **ESP-Encryption/Authentication/Mode**: those parameters have to match the parameters that were configured on the TransPort’s IPsec Tunnel 0 page. This AN uses AES 128-bit, SHA1, and Tunnel as the mode.
- **PFS**: Diffie Hellman group 2 was configured on the TransPort router. The same should be configured here.
4 TESTING

4.1 Open the tunnel from the client

Click on the TheGreenBow icon shown in the Windows system tray:

![Figure 4-1: Opening the tunnel](image)

The connection Panel will be shown:

![Figure 4-2: Connection Panel](image)

Click on “Open” for the Tunnel just created, the Tunnel will be negotiated and you will see it as green on the connection panel:
How to create an IPsec VPN between a Digi TransPort router and TheGreenBow VPN client

![VPN Connections](image1)

Figure 4-3: Tunnel Opened_1

Also the icon in the Windows system tray will become green:

![VPN Tunnel opened](image2)

Figure 4-4: Tunnel opened_2
4.2 Check Tunnel on the TransPort

In the eventlog section of the TransPort, the VPN will be shown coming up:

**MANAGEMENT-EVENTLOG:**

```
15:04:38, 18 Nov 2016,Eroute 0 VPN up peer: client
15:04:38, 18 Nov 2016,New IP Sec SA created by client
15:04:18, 18 Nov 2016,(692) New Phase 2 IKE Session 217.151.242.13,Responder
15:04:18, 18 Nov 2016,(691) New Phase 1 IKE Session 217.151.242.13,Responder
```

The status of the VPN tunnel can also be checked under connections status:

**MANAGEMENT-CONENCTIONS → VPN → IPSEC → IPSEC TUNNELS**

![Figure 4-5: Tunnel status on the TransPort](image-url)
4.3 Test traffic through the tunnel

4.3.1 Configure the analyser

In order to test that the Tunnel is working as expected, it is better to configure the analyser on the TransPort so that it will give a significant trace during the test.

**MANAGEMENT-ANALYSER → SETTINGS**

![Analyser Configuration](image)

**Figure 4-6: Analyser Configuration**
4.3.2 Test traffic

A simple way to test if the Tunnel is working as expected, is try to make a ping from the TransPort LAN address to the VPN client address:

ADMINISTRATION-EXECUTE A COMMAND:

```
Command: ping 172.16.1.100 -e0
```

The ping should be successful.

Please note that the command `ping <ipaddress> -<e0>` is used to send the ping having as the source address the one configured on ETH0 (so it will match the tunnel descriptors as if it comes from a host on the ETH 0 LAN).
How to create an IPsec VPN between a Digi TransPort router and TheGreenBow VPN client

4.3.3 Check analyser trace

MANAGEMENT-ANALYSER → TRACE

![Analyser Trace](image)

Click on “Refresh” the packet trace will be displayed:

- The Echo Request packet coming from the TransPort to the PPP interface is processed by Eroute 0

```
-----  18-11-2016  13:51:19.550  -----  
45 00 00 26 00 0A 00 00 F9 01 52 AF C0 A8 01 01   E..&......R.....
AC 10 01 64 08 00 58 F2 78 22 00 0A 01 78 00 00    ...d..X.x"...x..
00 03 9F 68 85 FD

ER 0-client From LOC TO REM   IFACE: PPP 1
45             IP Ver:        4
00             Hdr Len:       20
00             TOS:           Routine
00             Delay:         Normal
00             Throughput:    Normal
00             Reliability:   Normal
00 26          Length:        38
00 0A          ID:            10
00 00          Frag Offset:   0
00 00          Congestion:    Normal
00 00          May Fragment
00 00          Last Fragment
F9             TTL:           249
01             Proto:         ICMP
S2 AF          Checksum:      21167
C0 A8 01 01    Src IP:        192.168.1.1
```
How to create an IPsec VPN between a Digi TransPort router and TheGreenBow VPN client

The encrypted packet exiting from the PPP 1 interface with NAT applied and directed to the Public IP address of the remote PC:

- Inbound IKE float encapsulation is removed and the resulting ESP packet is shown:
How to create an IPsec VPN between a Digi TransPort router and TheGreenBow VPN client

```
| 08 56 1B 12 B0 2B 43 39 0D 40 12 E1 6E 46 22 9D | .V...+C9.@..nF". |
| 0A 2D 63 56 9C 9C 92 68 73 EC 59 DA B7 72 59 09 | .-cV...hs.Y...rY. |
| C8 41 30 13 67 DC A4 | .A0.Qg.. |

IP (In) From REM TO LOC      IFACE: PPP 1
45                           IP Ver:  4
   IPHdr Len:     20
00                          TOS:    Routine
   Delay:         Normal
   Throughput:   Normal
   Reliability:  Normal
00 68                        Length: 104
38 D3                        ID:    14547
00 00                        Frag Offset: 0
    Congestion: Normal
                   May Fragment
                   Last Fragment
6E                           TTL:  110
32                           Proto: ESP
49 A7                        Checksum: 18855
D9 97 F2 0D                  Src IP: 217.151.242.13
25 55 D8 EF                  Dst IP: 37.85.216.239

----------

- Decrypted ESP packet reveals the Echo reply with the real source and destination:

```
| 45 00 00 26 38 D3 00 00 80 01 92 E6 AC 10 01 64 | E..&8.........d |
| C0 A8 01 01 00 00 60 F2 72 22 00 0A 01 78 00 00 | ......`x"....X.. |
| 00 03 9F 68 85 FD | ...h..

IP (Cont) From REM TO LOC      IFACE: PPP 1
45                           IP Ver:  4
   IPHdr Len:     20
00                          TOS:    Routine
   Delay:         Normal
   Throughput:   Normal
   Reliability:  Normal
00 26                        Length: 38
38 D3                        ID:    14547
00 00                        Frag Offset: 0
    Congestion: Normal
                   May Fragment
                   Last Fragment
80                           TTL:  128
01                           Proto: ICMP
92 E6                        Checksum: 37606
AC 10 01 64                  Src IP: 172.16.1.100
C0 A8 01 01                  Dst IP: 192.168.1.1
ICMP:
00                           Type: ECHO REPLY
00                           Code: 0
60 F2                        Checksum: 62048
```

----------
5  CONFIGURATION FILE

5.1  Configuration file

This is the config.da0 file used for the purpose of this Application Note

```plaintext
eth 0 IPaddr "192.168.1.1"
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 "The GreenBow VPN"
eroute 0 peerid "client"
eroute 0 ourid "wr21"
eroute 0 locip "192.168.1.0"
eroute 0 locmsk "255.255.255.0"
eroute 0 remip "172.16.1.0"
eroute 0 remmsk "255.255.255.0"
eroute 0 ESPauth "SHA1"
eroute 0 ESPenc "AES"
eroute 0 authmeth "PRESHARED"
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 (LTE)"
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
web 0 showgswiz ON
```
How to create an IPsec VPN between a Digi TransPort router and TheGreenBow VPN client

```plaintext
modemcc 0 info_asy_add 4
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 ipprotfilt "~1"
ana 0 maxdata 1500
ana 0 logsize 180
cmd 0 unitid "ss%>
   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 "KD51SVJDVg="
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 "client"
user 10 epassword "PDZxU0FFQFU="
user 10 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 mo_autooff ON
cloud 0 ssl ON
```