TheGreenBow IPSec VPN Client
Configuration Guide
T.D.T. R-Router Series

WebSite:  http://www.thegreenbow.com
Contact:  support@thegreenbow.com
Table of contents

1 Introduction .................................................................................................................................................... 3
  1.1 Goal of this document .................................................................................................................................. 3
  1.2 VPN Network topology ............................................................................................................................... 3
  1.3 T.D.T. R-Router Series Restrictions ......................................................................................................... 3
  1.4 T.D.T. R-Router Series VPN Gateway ...................................................................................................... 3

2 T.D.T. R-Router Series VPN configuration ..................................................................................................... 4
  2.1 T.D.T. R-Router Series Phase 1 (IKE) Configuration .................................................................................. 4
  2.2 T.D.T. R-Router Series Preshared Key Configuration ............................................................................. 4
  2.3 T.D.T. R-Router Series Phase 2 (IPSec) Configuration .............................................................................. 6
  2.4 T.D.T. R-Router Series IPSec Status Pages ............................................................................................. 6

3 TheGreenBow IPSec VPN Client configuration ............................................................................................. 7
  3.1 VPN Client Phase 1 (IKE) Configuration ................................................................................................... 7
  3.2 VPN Client Phase 2 (IPSec) Configuration .............................................................................................. 7
  3.3 Open IPSec VPN tunnels ......................................................................................................................... 7

4 Tools in case of trouble.................................................................................................................................. 7
  4.1 A good network analyser: ethereal ............................................................................................................ 7

5 VPN IPSec Troubleshooting .......................................................................................................................... 7
  5.1 « PAYLOAD MALFORMED » error (wrong Phase 1 [SA]) ......................................................................... 7
  5.2 « INVALID COOKIE » error ...................................................................................................................... 7
  5.3 « no keystate » error .................................................................................................................................. 7
  5.4 « received remote ID other than expected » error .................................................................................... 7
  5.5 « NO PROPOSAL CHOSEN » error ......................................................................................................... 7
  5.6 « INVALID ID INFORMATION » error ..................................................................................................... 7
  5.7 I clicked on “Open tunnel”, but nothing happens ..................................................................................... 7
  5.8 The VPN tunnel is up but I can’t ping ! .................................................................................................... 7

6 Contacts....................................................................................................................................................... 15
1 Introduction

1.1 Goal of this document

This configuration guide describes how to configure TheGreenBow IPSec VPN Client with a T.D.T. R-Router Series VPN router.

1.2 VPN Network topology

In our VPN network example (diagram hereafter), we will connect TheGreenBow IPSec VPN Client to the LAN behind the T.D.T. R-Router Series router. The VPN client is connected to the Internet with a DSL connection or through a LAN. All the addresses in this document are given for example purpose.

1.3 T.D.T. R-Router Series Restrictions

Depending on the firmware version, T.D.T. R-Router Series may not support NAT-T. The IPSec VPN Client cannot connect if it stands on a LAN.

1.4 T.D.T. R-Router Series VPN Gateway

Our tests and VPN configuration have been conducted with T.D.T. R-Router Series firmware release version Rev4892.
2 T.D.T. R-Router Series VPN configuration

This section describes how to build an IPSec VPN configuration with your T.D.T. R-Router Series VPN router. Once connected to your VPN gateway, you must select “Security” and “VPN” tabs.

2.1 T.D.T. R-Router Series Phase 1 (IKE) Configuration

- Configure • IPSec • IKE • Responder
2.2 T.D.T. R-Router Series Preshared Key Configuration

- Configure • IPSec • IKE • Responder

![Configure: User 10 - 19](image)

- Wildcard: `*`
- `abcdefgh`: Preshared Key
2.3 T.D.T. R-Router Series Phase 2 (IPSec) Configuration

- Configure • IPSec • Eroute 0 - 9 • Eroute 0
2.4 T.D.T. R-Router Series IPSec Status Pages

• Status • Eventlog

11:43:42, 08 Jan 2007, Eroute 0 VPN up peer: 89.51.180.152
11:43:42, 08 Jan 2007, New IPSec SA created by 89.51.180.152
11:43:42, 08 Jan 2007, New Phase 2 IKE Session 89.51.180.152, Responder
11:43:41, 08 Jan 2007, IKE Keys Negotiated. Peer:
11:43:41, 08 Jan 2007, New Phase 1 IKE Session 89.51.180.152, Responder

• Status • IPSec • IPSec Peers

**IPSec Peers**

<table>
<thead>
<tr>
<th>Peer IP</th>
<th>Peer ID</th>
<th>DPD</th>
<th>NATT local port</th>
<th>NATT remote port</th>
</tr>
</thead>
<tbody>
<tr>
<td>89.51.180.152</td>
<td>89.51.180.152</td>
<td>Active (60)</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

- Remove all unused

• Status • IPSec • IKE SAs

**IKE Status**

**V1 SAs**

<table>
<thead>
<tr>
<th>Peer ID</th>
<th>Peer IP</th>
<th>Our IP</th>
<th>Session ID</th>
<th>Time Left</th>
</tr>
</thead>
<tbody>
<tr>
<td>89.51.180.152</td>
<td>89.51.180.152</td>
<td>87.230.126.17</td>
<td>0x0</td>
<td>1335</td>
</tr>
</tbody>
</table>

- Remove All V1 SAs

• Status • IPSec • IPSec SAs • Eroute 0 – 9 • Eroute 0

**IPSec Status: Eroutes 0 – 9**

**Outbound V1 SAs**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>86612</td>
<td>0</td>
<td>89.51.180.152</td>
<td>10.3.2.130</td>
<td></td>
<td>255.255.255.0</td>
<td>192.168.0.0</td>
<td>255.255.255.0</td>
<td>N/A</td>
<td>MD5</td>
<td>DES</td>
<td>N/A</td>
<td>65</td>
<td>32899</td>
<td>712</td>
<td>712</td>
<td>PPP S</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Remove All

**Inbound V1 SAs**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>86612</td>
<td>0</td>
<td>89.51.180.152</td>
<td>10.3.2.130</td>
<td></td>
<td>255.255.255.0</td>
<td>192.168.0.0</td>
<td>255.255.255.0</td>
<td>N/A</td>
<td>MD5</td>
<td>DES</td>
<td>N/A</td>
<td>215</td>
<td>32551</td>
<td>712</td>
<td>712</td>
<td>PPP S</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Remove All
3 TheGreenBow IPSec VPN Client configuration

3.1 VPN Client Phase 1 (IKE) Configuration

![Phase 1 configuration](image)

The remote VPN Gateway IP address is either an explicit IP address, or a DNS Name.
3.2 VPN Client Phase 2 (IPSec) Configuration

You may notice that we have selected SHA as authentication algorithm despite that fact MD5 algorithm is used for phase 2 in R-Router Series advanced settings. The real authentication algorithm used is defined in main configuration page (Eroute n) of the R-Router Series router settings.

3.3 Open IPSec VPN tunnels

Once both R-Router Series router and TheGreenBow IPSec VPN Client have been configured accordingly, you are ready to open VPN tunnels. First make sure you enable your firewall with IPSec traffic.

1. Click on "Save & Apply" to take into account all modifications we’ve made on your VPN Client configuration

2. Click on "Open Tunnel", or generate traffic that will automatically open a secure IPSec VPN Tunnel (e.g. ping, IE browser)

3. Select "Connections" to see opened VPN Tunnels

4. Select "Console" if you want to access to the IPSec VPN logs and adjust filters to display less IPSec messaging. The following example shows a successful connection between TheGreenBow IPSec VPN Client and a Microsoft Windows 2000 Server.
<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>0.153567</td>
<td>192.168.1.3</td>
<td>102.168.1.3</td>
<td>ISAKMP</td>
<td>ISAKMP Identity Protection (Main Mode)</td>
</tr>
<tr>
<td>4</td>
<td>0.297585</td>
<td>192.168.1.3</td>
<td>102.168.1.3</td>
<td>ISAKMP</td>
<td>ISAKMP Identity Protection (Main Mode)</td>
</tr>
<tr>
<td>5</td>
<td>0.500892</td>
<td>192.168.1.3</td>
<td>102.168.1.3</td>
<td>ISAKMP</td>
<td>ISAKMP Identity Protection (Main Mode)</td>
</tr>
<tr>
<td>6</td>
<td>0.310386</td>
<td>192.168.1.3</td>
<td>102.168.1.3</td>
<td>ISAKMP</td>
<td>ISAKMP Identity Protection (Main Mode)</td>
</tr>
<tr>
<td>7</td>
<td>0.339742</td>
<td>192.168.1.3</td>
<td>102.168.1.2</td>
<td>ISAKMP</td>
<td>ISAKMP Quick Mode</td>
</tr>
<tr>
<td>8</td>
<td>0.332913</td>
<td>192.168.1.2</td>
<td>102.168.1.3</td>
<td>ISAKMP</td>
<td>ISAKMP Quick Mode</td>
</tr>
<tr>
<td>9</td>
<td>0.332741</td>
<td>192.168.1.3</td>
<td>102.168.1.2</td>
<td>ISAKMP</td>
<td>ISAKMP Quick Mode</td>
</tr>
<tr>
<td>10</td>
<td>0.334980</td>
<td>192.168.1.2</td>
<td>102.168.1.3</td>
<td>ISAKMP</td>
<td>ISAKMP Quick Mode</td>
</tr>
<tr>
<td>11</td>
<td>0.692100</td>
<td>192.168.1.2</td>
<td>102.168.1.2</td>
<td>ESP</td>
<td>ESP (SPI=0x9290f2bc)</td>
</tr>
<tr>
<td>12</td>
<td>1.692108</td>
<td>192.168.1.3</td>
<td>102.168.1.2</td>
<td>ESP</td>
<td>ESP (SPI=0x9290f2bc)</td>
</tr>
<tr>
<td>13</td>
<td>1.693104</td>
<td>192.168.1.2</td>
<td>102.168.1.3</td>
<td>ESP</td>
<td>ESP (SPI=0x9290f2bc)</td>
</tr>
<tr>
<td>14</td>
<td>2.693800</td>
<td>192.168.1.3</td>
<td>102.168.1.2</td>
<td>ESP</td>
<td>ESP (SPI=0x9290f2bc)</td>
</tr>
<tr>
<td>15</td>
<td>2.694026</td>
<td>192.168.1.2</td>
<td>102.168.1.2</td>
<td>ESP</td>
<td>ESP (SPI=0x9290f2bc)</td>
</tr>
</tbody>
</table>

**Ethernet II, src: 06:10:19:4c:bf:127, dst: 00:10:19:4c:bf:ff**
4 Tools in case of trouble

Configuring an IPSec VPN tunnel can be a hard task. One missing parameter can prevent a VPN connection from being established. Some tools are available to find source of troubles during a VPN establishment.

4.1 A good network analyser: ethereal

Ethereal is a free software that can be used for packet and traffic analysis. It shows IP or TCP packets received on a network card. This tools is available on website http://www.ethereal.com/. It can be used to follow protocol exchange between two devices. For installation and use details, read its specific documentation.
5 VPN IPSec Troubleshooting

5.1 « PAYLOAD MALFORMED » error (wrong Phase 1 [SA])

If you have an « PAYLOAD MALFORMED » error you might have a wrong Phase 1 [SA], check if the encryption algorithms are the same on each side of the VPN tunnel.

5.2 « INVALID COOKIE » error

If you have an « INVALID COOKIE » error, it means that one of the endpoint is using a SA that is no more in use. Reset the VPN connection on each side.

5.3 « no keystate » error

Check if the preshared key is correct or if the local ID is correct (see « Advanced » button). You should have more information in the remote endpoint logs.

5.4 « received remote ID other than expected » error

The « Remote ID » value (see « Advanced » Button) does not match what the remote endpoint is expected.
### 5.5 « NO PROPOSAL CHOSEN » error

If you have an « NO PROPOSAL CHOSEN » error, check that the « Phase 2 » encryption algorithms are the same on each side of the VPN Tunnel.

Check « Phase 1 » algorithms if you have this:

<table>
<thead>
<tr>
<th>Line</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>115911</td>
<td>Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [SA][VID]</td>
</tr>
<tr>
<td>115913</td>
<td>Default (SA CNXVPN1-P1) RECEV phase 1 Main Mode [SA][VID]</td>
</tr>
<tr>
<td>115913</td>
<td>Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [KEY][NONCE]</td>
</tr>
<tr>
<td>115915</td>
<td>Default (SA CNXVPN1-P1) RECEV phase 1 Main Mode [KEY][NONCE]</td>
</tr>
<tr>
<td>115915</td>
<td>Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [ID][HASH][NOTIFY]</td>
</tr>
<tr>
<td>115915</td>
<td>Default (SA CNXVPN1-P1) RECEV phase 1 Main Mode [ID][HASH][NOTIFY]</td>
</tr>
<tr>
<td>115915</td>
<td>Default phase 1 done: initiator id c364cd70: 195.100.205.112, responder id c364cd72: 195.100.205.114, src: 195.100.205.112 dst: 195.100.205.114</td>
</tr>
<tr>
<td>115915</td>
<td>Default (SA CNXVPN1-CNXXVPN1-P2) SEND phase 2 Quick Mode [SA][KEY][ID][HASH][NONCE]</td>
</tr>
<tr>
<td>115915</td>
<td>Default RECEV Informational [HASH][NOTIFY] with NO_PROPOSAL_CHOSEN error</td>
</tr>
<tr>
<td>115915</td>
<td>Default CNXVPN1-P1 deleted</td>
</tr>
</tbody>
</table>

### 5.6 « INVALID ID INFORMATION » error

If you have an « INVALID ID INFORMATION » error, check if « Phase 2 » ID (local address and network address) is correct and match what is expected by the remote endpoint.

Check also ID type ("Subnet address" and "Single address"). If network mask is not check, you are using a IPV4_ADDR type (and not a IPV4_SUBNET type).

<table>
<thead>
<tr>
<th>Line</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>122623</td>
<td>Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [SA][VID]</td>
</tr>
<tr>
<td>122625</td>
<td>Default (SA CNXVPN1-P1) RECEV phase 1 Main Mode [SA][VID]</td>
</tr>
<tr>
<td>122626</td>
<td>Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [KEY][NONCE]</td>
</tr>
<tr>
<td>122626</td>
<td>Default (SA CNXVPN1-P1) RECEV phase 1 Main Mode [KEY][NONCE]</td>
</tr>
<tr>
<td>122626</td>
<td>Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [ID][HASH][NOTIFY]</td>
</tr>
<tr>
<td>122626</td>
<td>Default (SA CNXVPN1-P1) RECEV phase 1 Main Mode [ID][HASH][NOTIFY]</td>
</tr>
<tr>
<td>122626</td>
<td>Default phase 1 done: initiator id c364cd70: 195.100.205.112, responder id c364cd72: 195.100.205.114, src: 195.100.205.112 dst: 195.100.205.114</td>
</tr>
<tr>
<td>122626</td>
<td>Default (SA CNXVPN1-CNXXVPN1-P2) SEND phase 2 Quick Mode [SA][KEY][ID][HASH][NONCE]</td>
</tr>
<tr>
<td>122626</td>
<td>Default RECEV Informational [HASH][NOTIFY] with INVALID_ID_INFORMATION error</td>
</tr>
<tr>
<td>122626</td>
<td>Default CNXVPN1-P1 deleted</td>
</tr>
</tbody>
</table>

### 5.7 I clicked on “Open tunnel”, but nothing happens.

Read logs of each VPN tunnel endpoint. IKE requests can be dropped by firewalls. An IPSec Client uses UDP port 500 and protocol ESP (protocol 50).

### 5.8 The VPN tunnel is up but I can’t ping !

If the VPN tunnel is up, but you still cannot ping the remote LAN, here are a few guidelines:

- Check Phase 2 settings: VPN Client address and Remote LAN address. Usually, VPN Client IP address should not belong to the remote LAN subnet
- Once VPN tunnel is up, packets are sent with ESP protocol. This protocol can be blocked by firewall. Check that every device between the client and the VPN server does accept ESP
- Check your VPN server logs. Packets can be dropped by one of its firewall rules.
- Check your ISP support ESP
• If you still cannot ping, follow ICMP traffic on VPN server LAN interface and on LAN computer interface (with Ethereal for example). You will have an indication that encryption works.
• Check the “default gateway” value in VPN Server LAN. A target on your remote LAN can receive pings but does not answer because there is a no “Default gateway” setting.
• You cannot access to the computers in the LAN by their name. You must specify their IP address inside the LAN.
• We recommend you to install ethereal (http://www.ethereal.com) on one of your target computer. You can check that your pings arrive inside the LAN.
6 Contacts

News and updates on TheGreenBow web site: http://www.thegreenbow.com

Technical support by email at support@thegreenbow.com

Sales contacts at +33 1 43 12 39 37 or by email at info@thegreenbow.com