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 0
2.3 T.D.T. R-Router Series Phase 2 (IPSec) Configuration 6
2.4 T.D.T. R-Router Series IPSec Status Pages 0
3 TheGreenBow IPSec VPN Client configuration 0
3.1 VPN Client Phase 1 (IKE) Configuration 0
3.2 VPN Client Phase 2 (IPSec) Configuration 0
3.3 Open IPSec VPN tunnels 0
4 Tools in case of trouble 0
4.1 A good network analyser: ethereal 0
5 VPN IPSec Troubleshooting 0
5.1 « PAYLOAD MALFORMED » error (wrong Phase 1 [SA]) 0
5.2 « INVALID COOKIE » error 0
5.3 « no keystate » error 0
5.4 « received remote ID other than expected » error 0
5.5 « NO PROPOSAL CHOSEN » error 0
5.6 « INVALID ID INFORMATION » error 0
5.7 I clicked on “Open tunnel”, but nothing happens. 0
5.8 The VPN tunnel is up but I can’t ping ! 0
6 Contacts 15

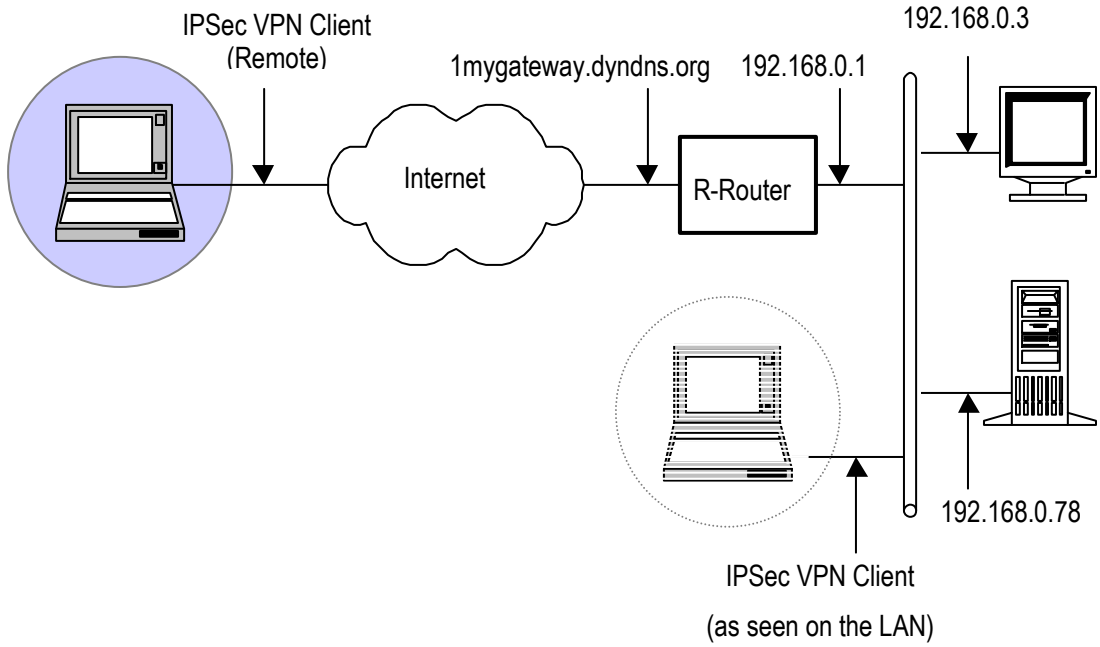
1 Introduction

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.

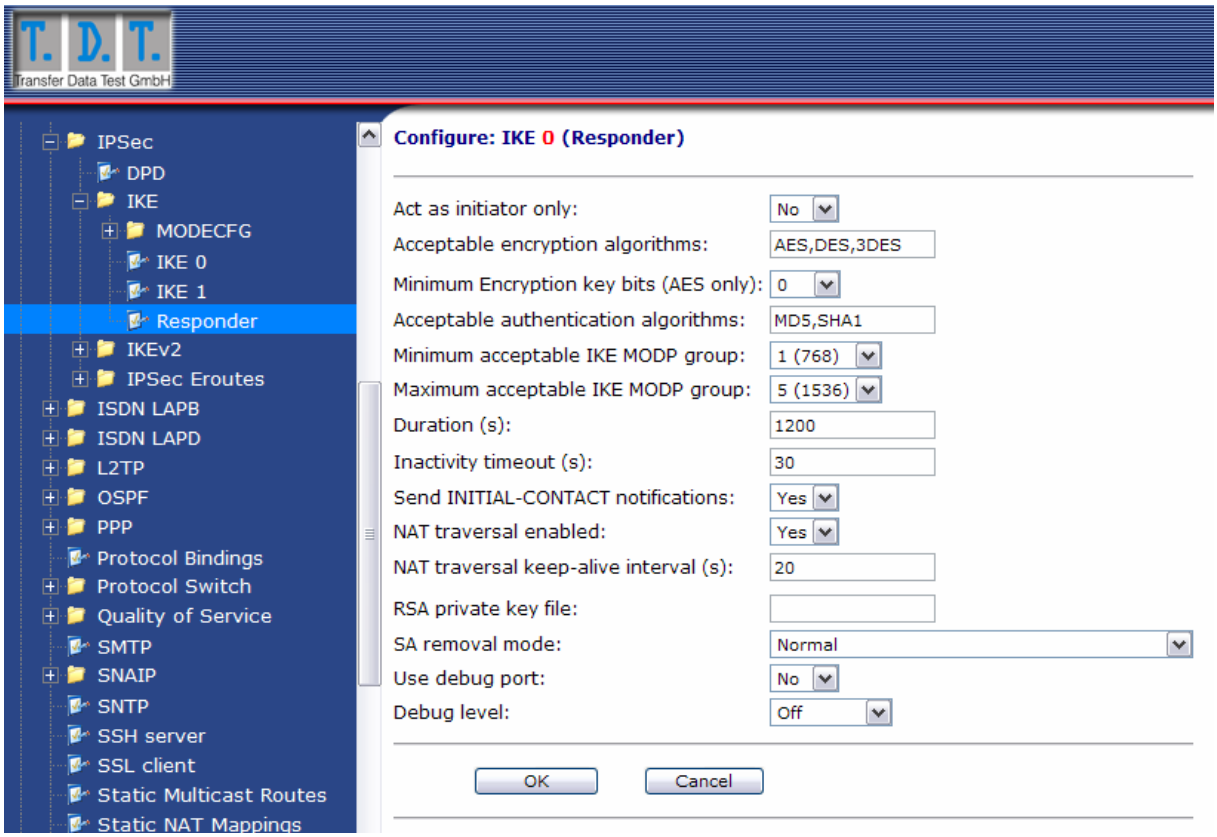
2 T.D.T. R-Router Series VPN configuration

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.

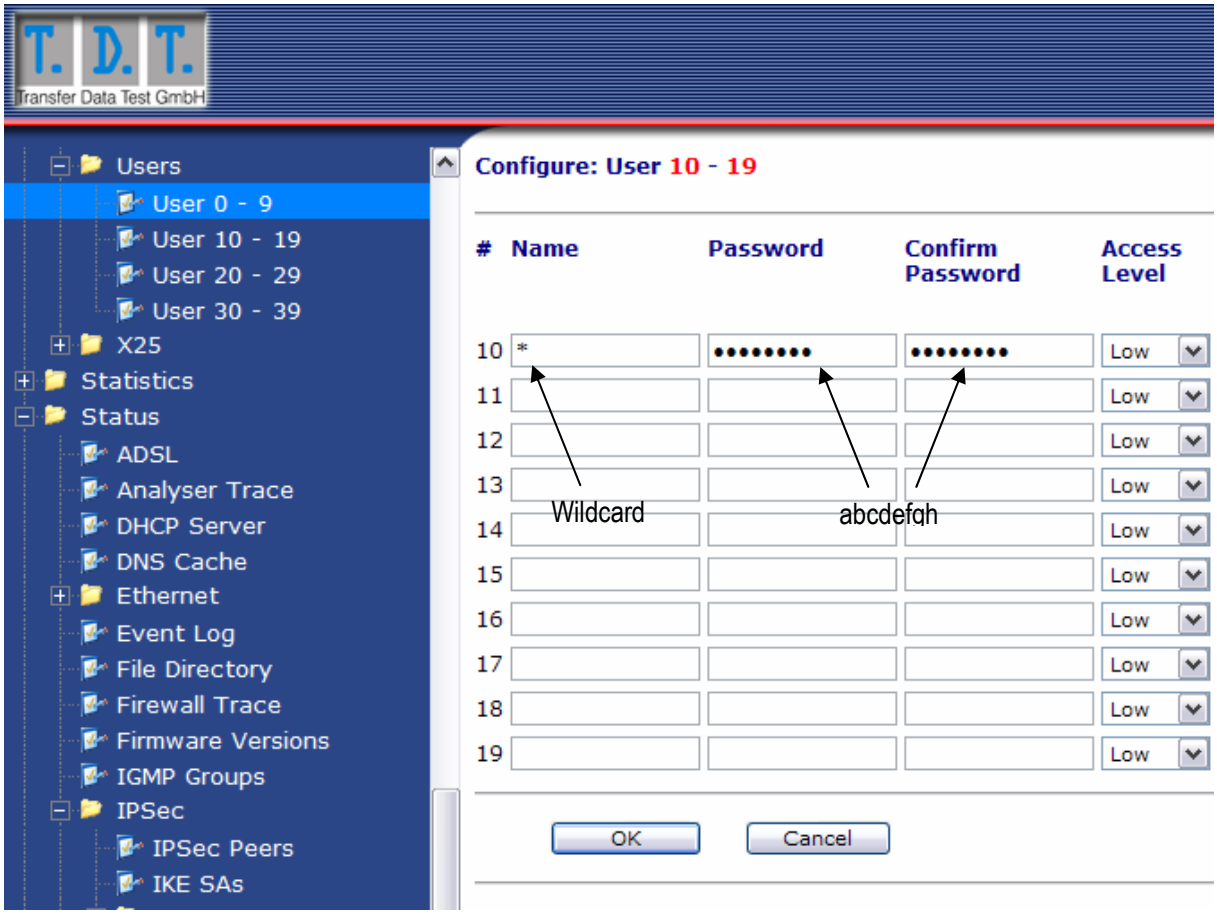
2.1 T.D.T. R-Router Series Phase 1 (IKE) Configuration

• Configure • IPSec • IKE • Responder



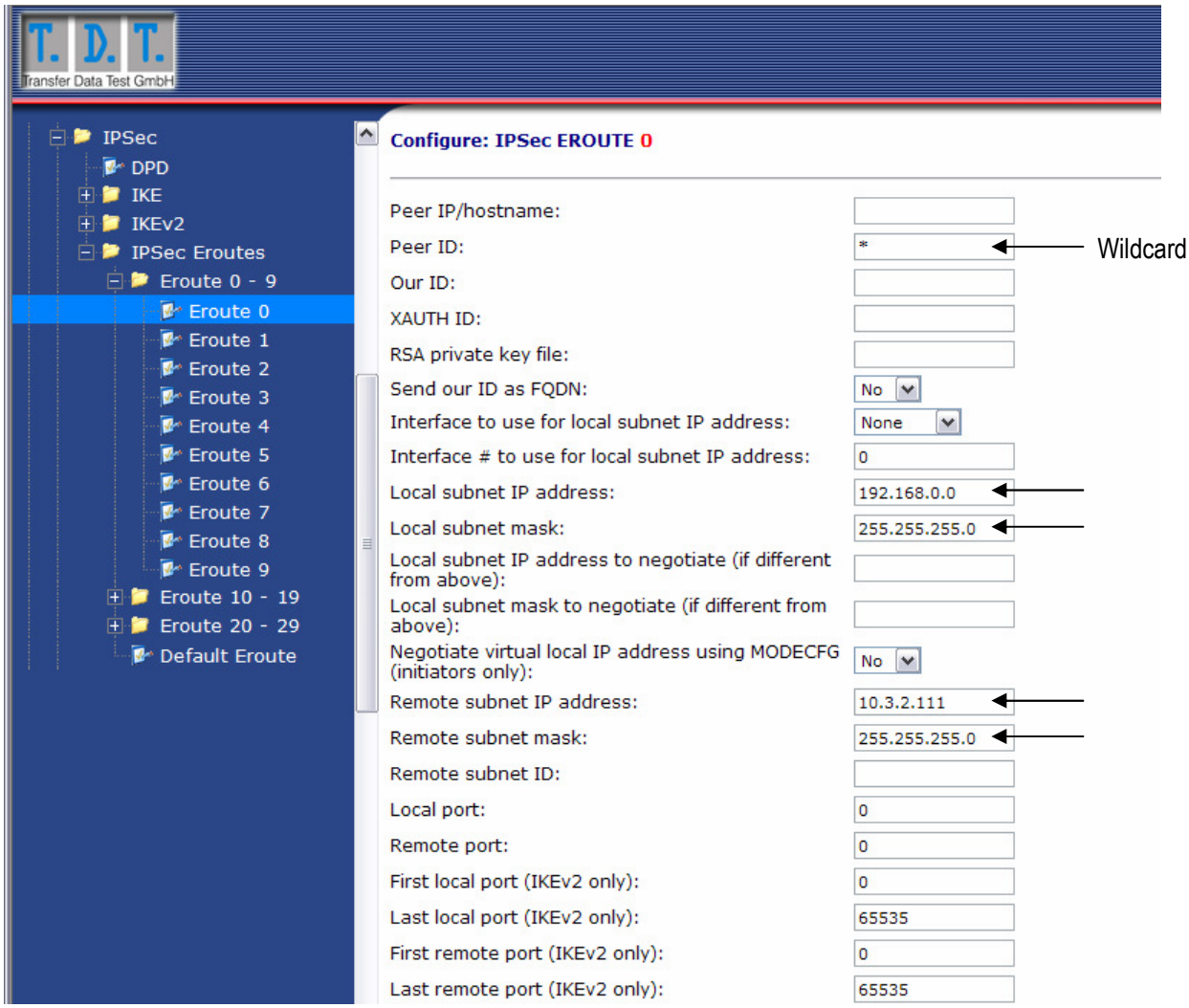
2.2 T.D.T. R-Router Series Preshared Key Configuration

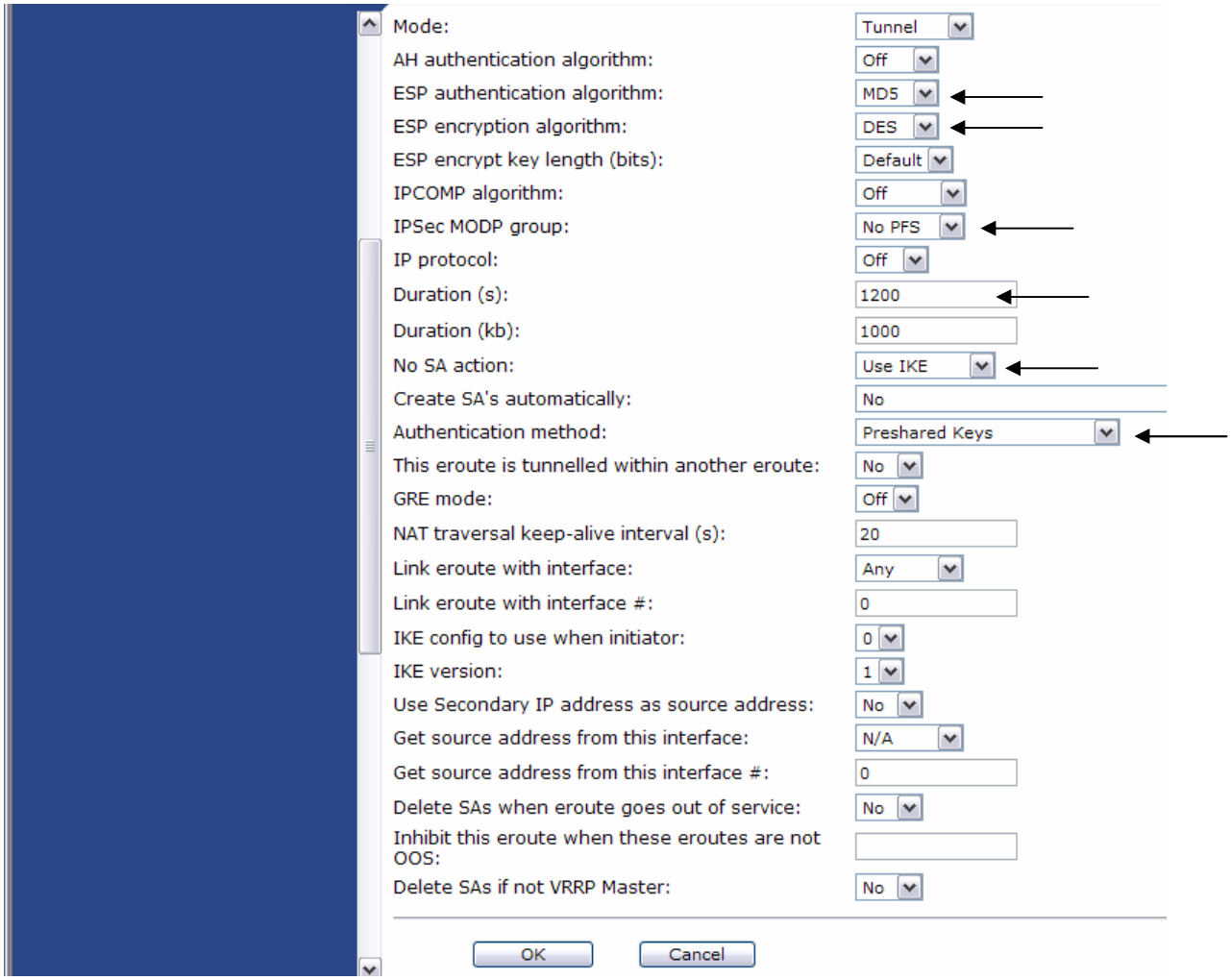
• Configure • IPSec • IKE • Responder



2.3 T.D.T. R-Router Series Phase 2 (IPSec) Configuration

• Configure • IPSec • Eroute 0 - 9 • Eroute 0




Mode: Tunnel
AH authentication algorithm: Off
ESP authentication algorithm: MD5
ESP encryption algorithm: DES
ESP encrypt key length (bits): Default
IPCOMP algorithm: Off
IPSec MODP group: No PFS
IP protocol: Off
Duration (s): 1200
Duration (kb): 1000
No SA action: Use IKE
Create SA's automatically: No
Authentication method: Preshared Keys
This eroute is tunnelled within another eroute: No
GRE mode: Off
NAT traversal keep-alive interval (s): 20
Link eroute with interface: Any
Link eroute with interface #: 0
IKE config to use when initiator: 0
IKE version: 1
Use Secondary IP address as source address: No
Get source address from this interface: N/A
Get source address from this interface #: 0
Delete SAs when eroute goes out of service: No
Inhibit this eroute when these eroutes are not OOS:
Delete SAs if not VRRP Master: No
OK
Cancel

2.4 T.D.T. R-Router Series IPSec Status Pages

• Status • Eventlog

```
11:43:44, 08 Jan 2007,IKE SA Removed. Peer: 89.51.180.152,Successful
Negotiation
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

Peer IP	Peer ID	DPD	NATT local port	NATT remote port
89.51.180.152	89.51.180.152	Active (60). Next REQ in 122 secs	N/A	N/A

Remove all unused

• Status • IPSec • IKE SAs

IKE Status

V1 SAs

Peer ID	Peer IP	Our IP	Session ID	Time Left	
89.51.180.152	89.51.180.152	87.230.126.17	0x0	1335	Remove

Remove All V1 SAs

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

IPSec Status: Eroutes 0 -> 0

Outbound V1 SAs

SPI	Eroute	Peer IP	Rem. IP	Rem. Mask	Loc. IP	Loc. Mask	AH	ESP Auth	ESP Enc	IPCOMP	KBytes Delivered	KBytes Left	Time Left	Interface	
a6dd1aa4	0	89.51.180.152	10.3.2.111	255.255.255.255	192.168.0.0	255.255.255.0	N/A	MD5	DES	N/A	68	32699	712	PPP 3	Remove

Remove All

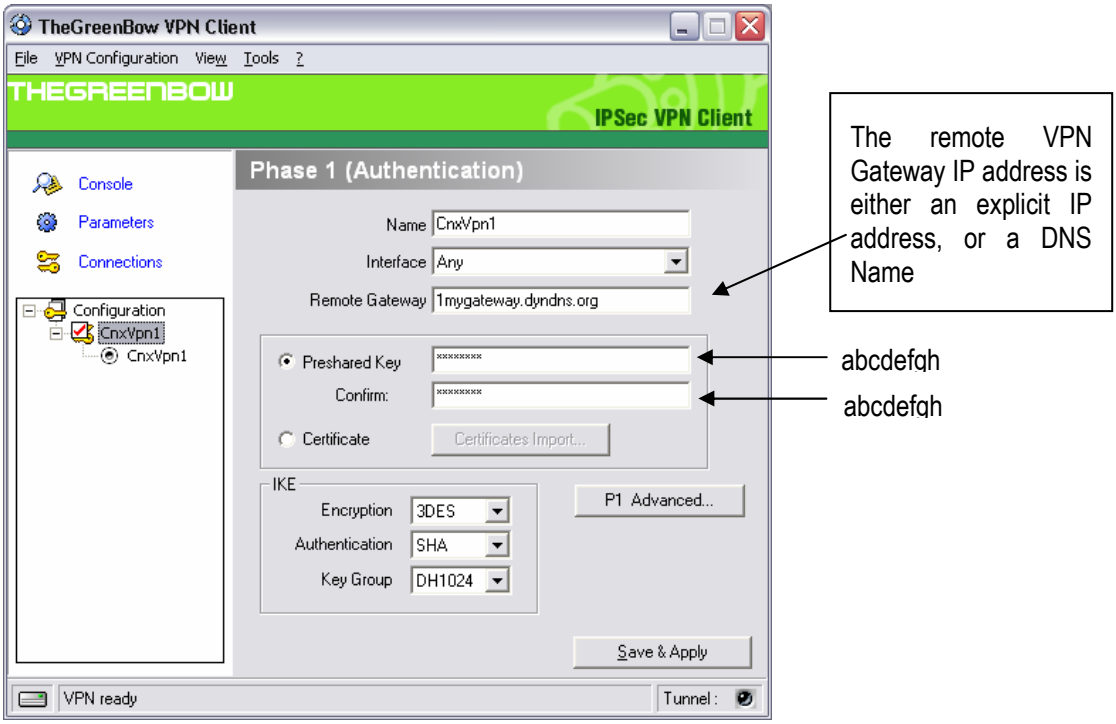
Inbound V1 SAs

SPI	Eroute	Peer IP	Rem. IP	Rem. Mask	Loc. IP	Loc. Mask	AH	ESP Auth	ESP Enc	IPCOMP	KBytes Delivered	KBytes Left	Time Left	Interface	
4d1a9e23	0	89.51.180.152	10.3.2.111	255.255.255.255	192.168.0.0	255.255.255.0	N/A	MD5	DES	N/A	216	32551	712	PPP 3	Remove

Remove All

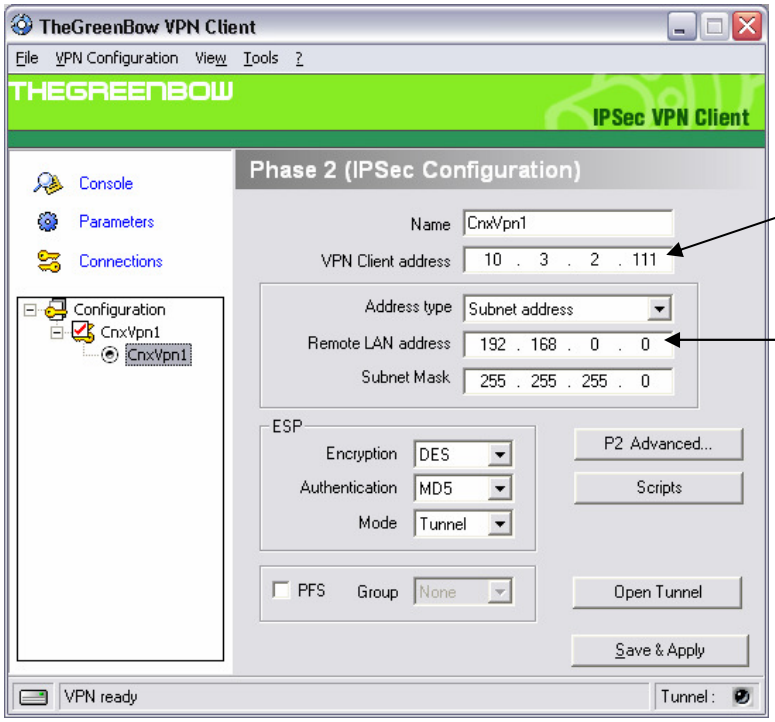
3 TheGreenBow IPSec VPN Client configuration

3.1 VPN Client Phase 1 (IKE) Configuration



Phase 1 configuration

3.2 VPN Client Phase 2 (IPSec) Configuration



You may define a static virtual IP address here.

If you use 0.0.0.0, you will have error "Local-ID" is missing. It does not prevent you from establishing a tunnel

Enter the IP address (and subnet mask) of the remote LAN.

Phase 2 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

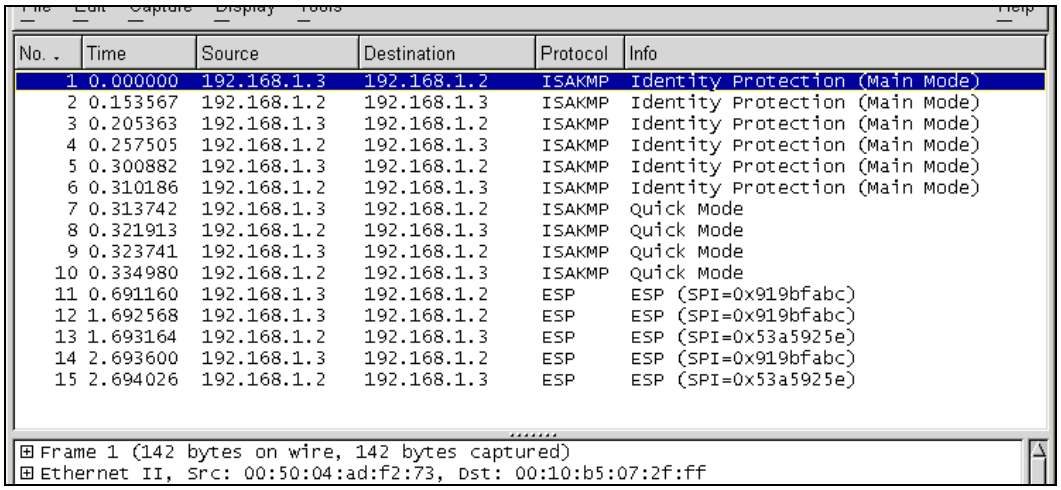
Once both R-Router Series router and TheGreenBow IPSec VPN Client have been configured accordingly, you are ready to open VPN tunnels. First make sure you enable your firewall with IPSec traffic.

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.



No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.3	192.168.1.2	ISAKMP	Identity Protection (Main Mode)
2	0.153567	192.168.1.2	192.168.1.3	ISAKMP	Identity Protection (Main Mode)
3	0.205363	192.168.1.3	192.168.1.2	ISAKMP	Identity Protection (Main Mode)
4	0.257505	192.168.1.2	192.168.1.3	ISAKMP	Identity Protection (Main Mode)
5	0.300882	192.168.1.3	192.168.1.2	ISAKMP	Identity Protection (Main Mode)
6	0.310186	192.168.1.2	192.168.1.3	ISAKMP	Identity Protection (Main Mode)
7	0.313742	192.168.1.3	192.168.1.2	ISAKMP	Quick Mode
8	0.321913	192.168.1.2	192.168.1.3	ISAKMP	Quick Mode
9	0.323741	192.168.1.3	192.168.1.2	ISAKMP	Quick Mode
10	0.334980	192.168.1.2	192.168.1.3	ISAKMP	Quick Mode
11	0.691160	192.168.1.3	192.168.1.2	ESP	ESP (SPI=0x919bfabc)
12	1.692568	192.168.1.3	192.168.1.2	ESP	ESP (SPI=0x919bfabc)
13	1.693164	192.168.1.2	192.168.1.3	ESP	ESP (SPI=0x53a5925e)
14	2.693600	192.168.1.3	192.168.1.2	ESP	ESP (SPI=0x919bfabc)
15	2.694026	192.168.1.2	192.168.1.3	ESP	ESP (SPI=0x53a5925e)

⊞ Frame 1 (142 bytes on wire, 142 bytes captured)
⊞ Ethernet II, Src: 00:50:04:ad:f2:73, Dst: 00:10:b5:07:2f: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])

```
114920 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [SA][VID]
114920 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [NOTIFY]
114920 Default exchange_run: exchange_validate failed
114920 Default dropped message from 195.100.205.114 port 500 due to notification
type PAYLOAD_MALFORMED
114920 Default SEND Informational  [NOTIFY] with PAYLOAD_MALFORMED error
```

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

```
115933 Default message_recv: invalid cookie(s) 5918ca0c2634288f 7364e3e486e49105
115933 Default dropped message from 195.100.205.114 port 500 due to notification
type INVALID_COOKIE
115933 Default SEND Informational  [NOTIFY] with 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

```
115315 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [SA][VID]
115317 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [SA][VID]
115317 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [KEY][NONCE]
115319 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [KEY][NONCE]
115319 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [ID][HASH][NOTIFY]
115319 Default ipsec_get_keystate: no keystate in ISAKMP SA 00B57C50
```

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

```
120348 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [SA][VID]
120349 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [SA][VID]
120349 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [KEY][NONCE]
120351 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [KEY][NONCE]
120351 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [ID][HASH][NOTIFY]
120351 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [ID][HASH][NOTIFY]
120351 Default ike_phase_1_recv_ID: received remote ID other than expected
support@thegreenbow.fr
```

The « Remote ID » value (see « Advanced » Button) does not match what the remote endpoint is expected.

5.5 « NO PROPOSAL CHOSEN » error

```
115911 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [SA][VID]
115913 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [SA][VID]
115913 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [KEY][NONCE]
115915 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [KEY][NONCE]
115915 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [ID][HASH][NOTIFY]
115915 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [ID][HASH][NOTIFY]
115915 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
115915   Default   (SA   CNXVPN1-CNXVPN1-P2)   SEND   phase   2   Quick   Mode
[SA][KEY][ID][HASH][NONCE]
115915 Default RECV Informational  [HASH][NOTIFY] with NO_PROPOSAL_CHOSEN error
115915 Default RECV Informational  [HASH][DEL]
115915 Default CNXVPN1-P1 deleted
```

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:

```
115911 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [SA][VID]
115911 Default RECV Informational  [NOTIFY] with NO_PROPOSAL_CHOSEN error
```

5.6 « INVALID ID INFORMATION » error

```
122623 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [SA][VID]
122625 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [SA][VID]
122625 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [KEY][NONCE]
122626 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [KEY][NONCE]
122626 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [ID][HASH][NOTIFY]
122626 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [ID][HASH][NOTIFY]
122626 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
122626   Default   (SA   CNXVPN1-CNXVPN1-P2)   SEND   phase   2   Quick   Mode
[SA][KEY][ID][HASH][NONCE]
122626 Default RECV Informational  [HASH][NOTIFY] with INVALID_ID_INFORMATION error
122626 Default RECV Informational  [HASH][DEL]
122626 Default CNXVPN1-P1 deleted
```

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).

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 ou by email at info@thegreenbow.com