TheGreenBow VPN Client

IPSec Configuration Guide

Router :	**Linksys BEFSX41**
WebSite :	http://www.thegreenbow.com
Contact :	support@thegreenbow.com

1 Linksys Configuration

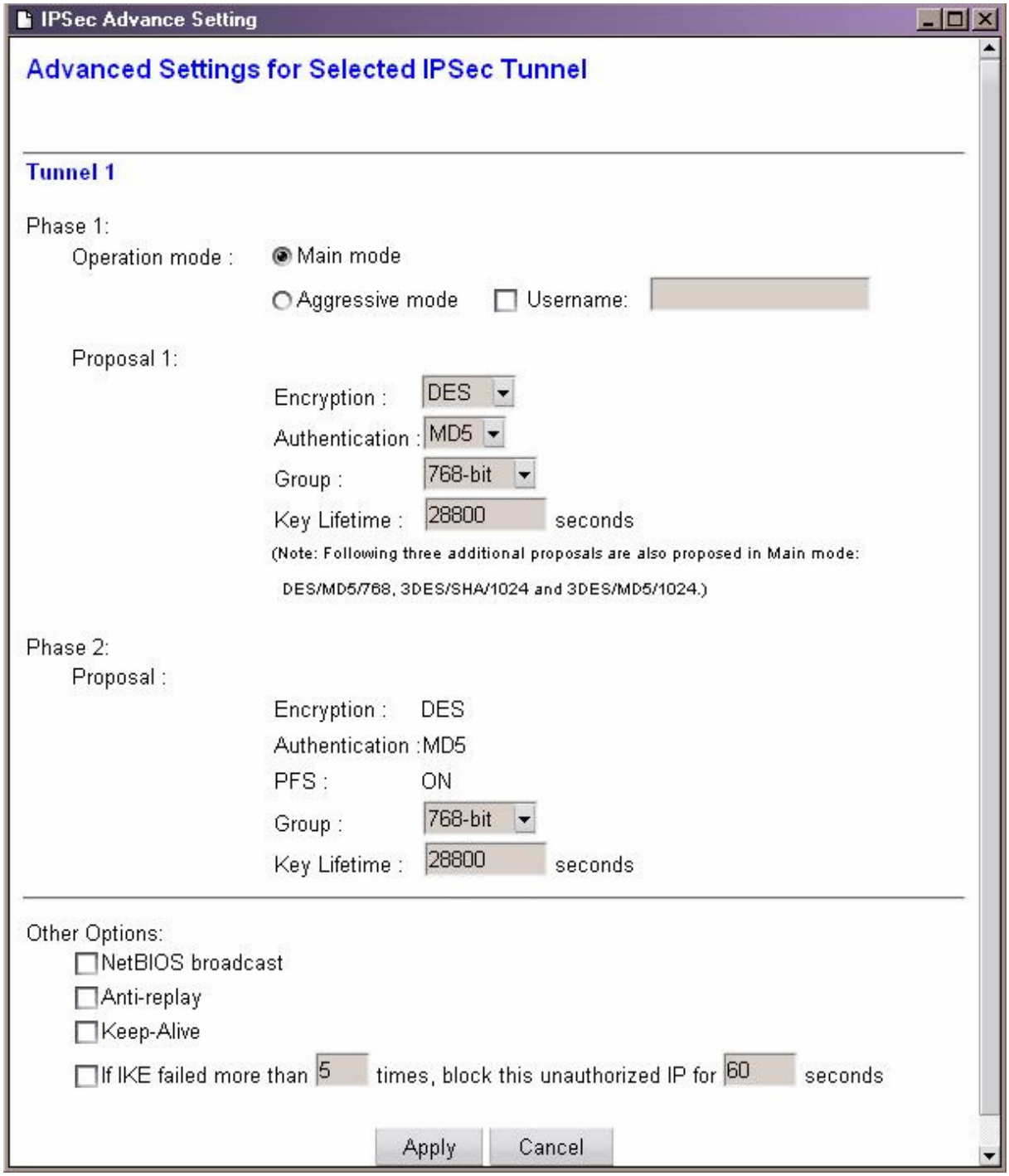
1.1 Configuration interface

Linksys configuration can be achieved with a web browser. Read Linksys documentation for more information.

First, click on "VPN" link in the Linksys configuration interface and select the appropriate tunnel.

In our example, Linksys LAN subnet is 192.168.1.0/255.255.255.0.

If you click on « Advanced settings », you will find

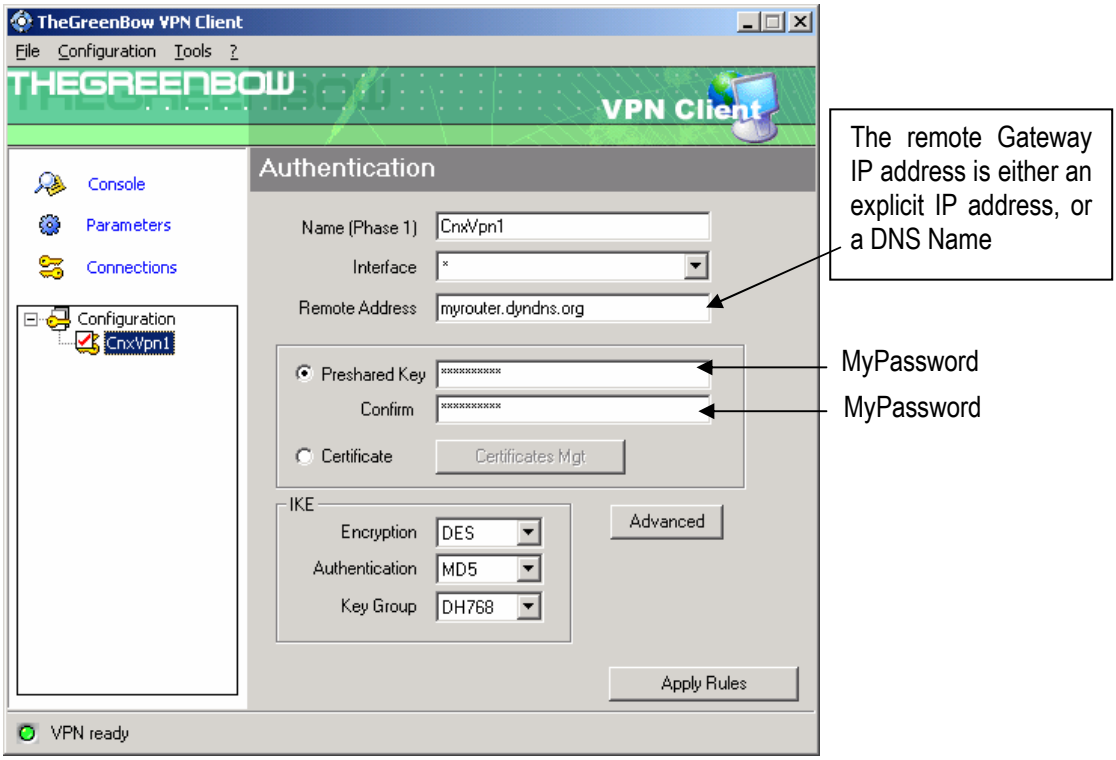


2 TheGreenBow VPN Client Phase 1 (IKE) Configuration

In the « Interface » field, you can select a star (« * »), if the client host receive a dynamic IP Address from an ISP for example.

« Remote Address » field value is the Linksys router public IP address or DNS address.

By clicking in « Advanced » button, you can setup Phase 1 IDs and Aggressive Mode.



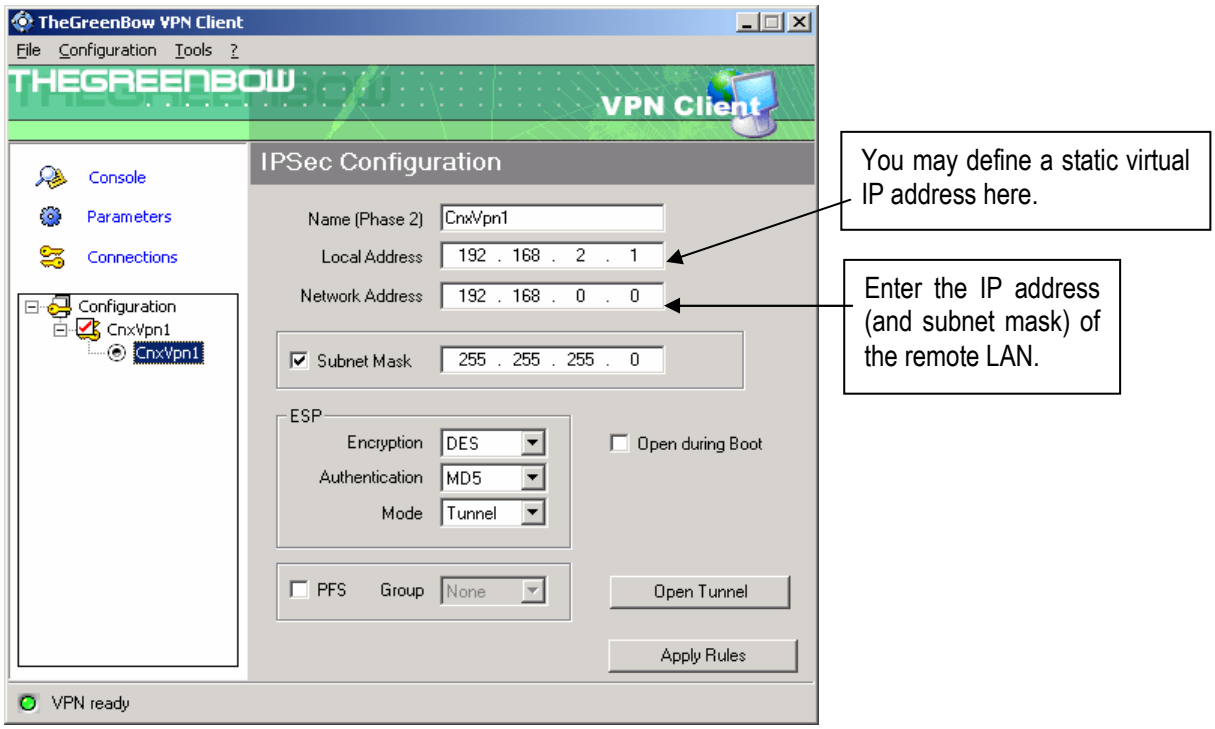
Phase 1 configuration

3 TheGreenBow VPN Client Phase 2 (IPSec) Configuration

In this window, you can configure IPSec Policy.

« Local Address » is the virtual IP address of the client inside the LAN. This address must belong to the remote LAN if you use a Linksys BEFV41. It must not belong to the remote LAN if you use a Linksys RV082

You can also use “0.0.0.0” as value. In that case, IP address from ISP will be used.



Phase2 Configuration

4 Open the tunnel

1. Clic on "Apply Rules"
2. Clic on "Open Tunnel", or open a connexion (e.g. ping)
3. Click on "Console" if you want to access to the VPN logs.

5 Troubleshooting

5.1 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
```

Check if phase 1 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 pre-shared 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 with 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
```

Check if the « Phase 2 » 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
```

Check if « Phase 2 » IDs (local address and network address) are correct and match what is expected by the remote endpoint.

Check also ID type. If network mask is not check, you are using an IPV4_ADDR type (and not a IPV4_SUBNET type). TheGreenBow IPsec client does not support IPV4_RANGE ID type

Check if a previous SA is still alive in Linksys configuration.

5.7 The VPN 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 with ethereal (http://www.ethereal.com) that your pings arrive inside the LAN.
- You cannot access to the computers in the LAN by their name. You must specify their IP address inside the LAN. You can also use HOSTS file for name resolving.
- If you are using Windows XP, check that you have enable NETBIOS over TCPIP.
- Check in the Linksys logs if the packets are blocked
- With **BEFVP41** model, you must give an IP address that belongs to the LAN in field "Local Address".
- With **RV082** model, you must not give an IP address that belongs to the LAN in field "Local Address

6 Contacts

- news and update on web site : http://www.thegreenbow.com
- Technical support by email at support@thegreenbow.com
- Sales contacts at +33 (0)1 43 12 39 37 ou by email at info@thegreenbow.com