TheGreenBow IPSec VPN Client

Configuration Guide

Linksys RV082

WebSite: http://www.thegreenbow.com
Contact: support@thegreenbow.com

Table of contents

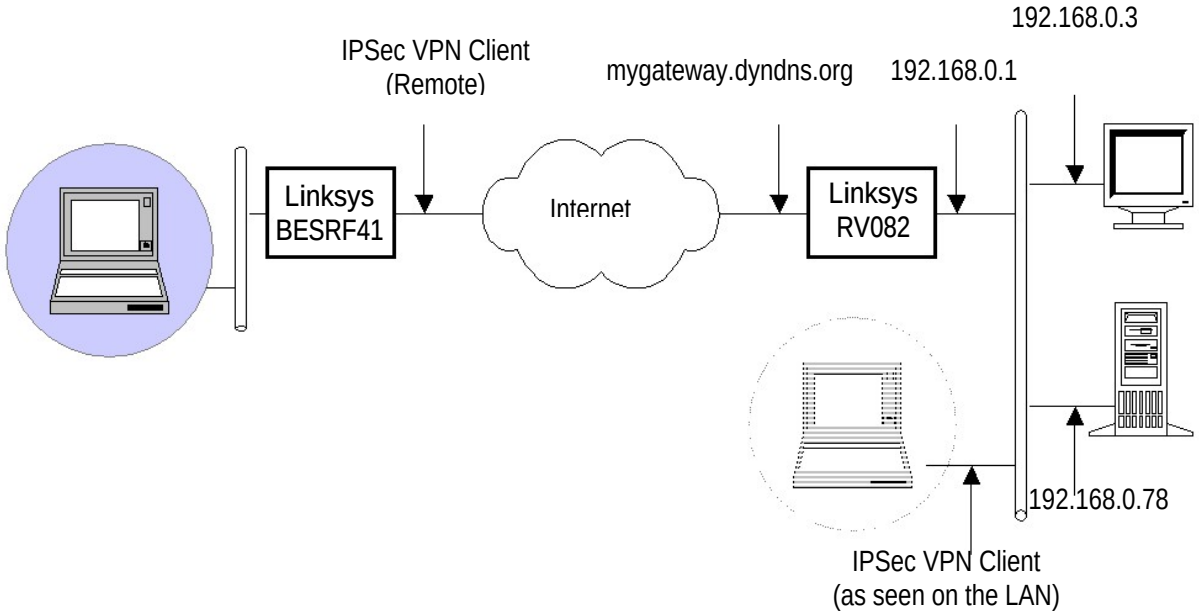
1 Introduction

1.1 Goal of this document

This configuration guide describes how to configure TheGreenBow IPSec VPN Client with Linksys RV082 and Linksys BESRF41 VPN routers.

1.2 VPN Network topology

In our VPN network example (diagram hereafter), we will connect TheGreenBow IPSec VPN Client to the LAN behind the Linksys RV082 router. The VPN client is connected to the Internet through a Linksys BESRF41 VPN router. All the addresses in this document are given for example purpose.



1.3 Linksys RV082 and Linksys BESRF41 Restrictions

No known restrictions.

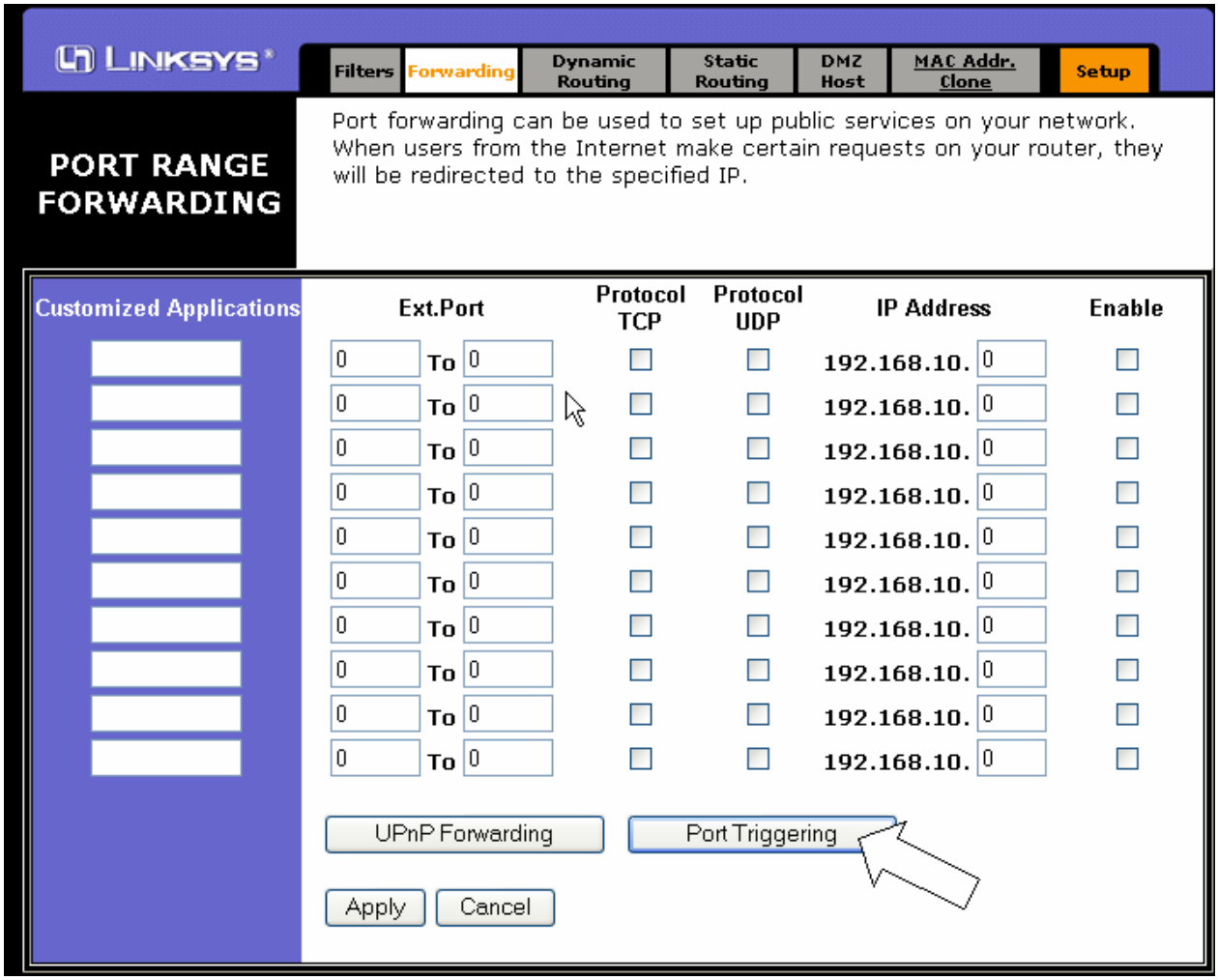
2 Linksys BESRF41 VPN configuration

This section describes how to build an IPSec VPN configuration with your Linksys BESRF41 VPN router.

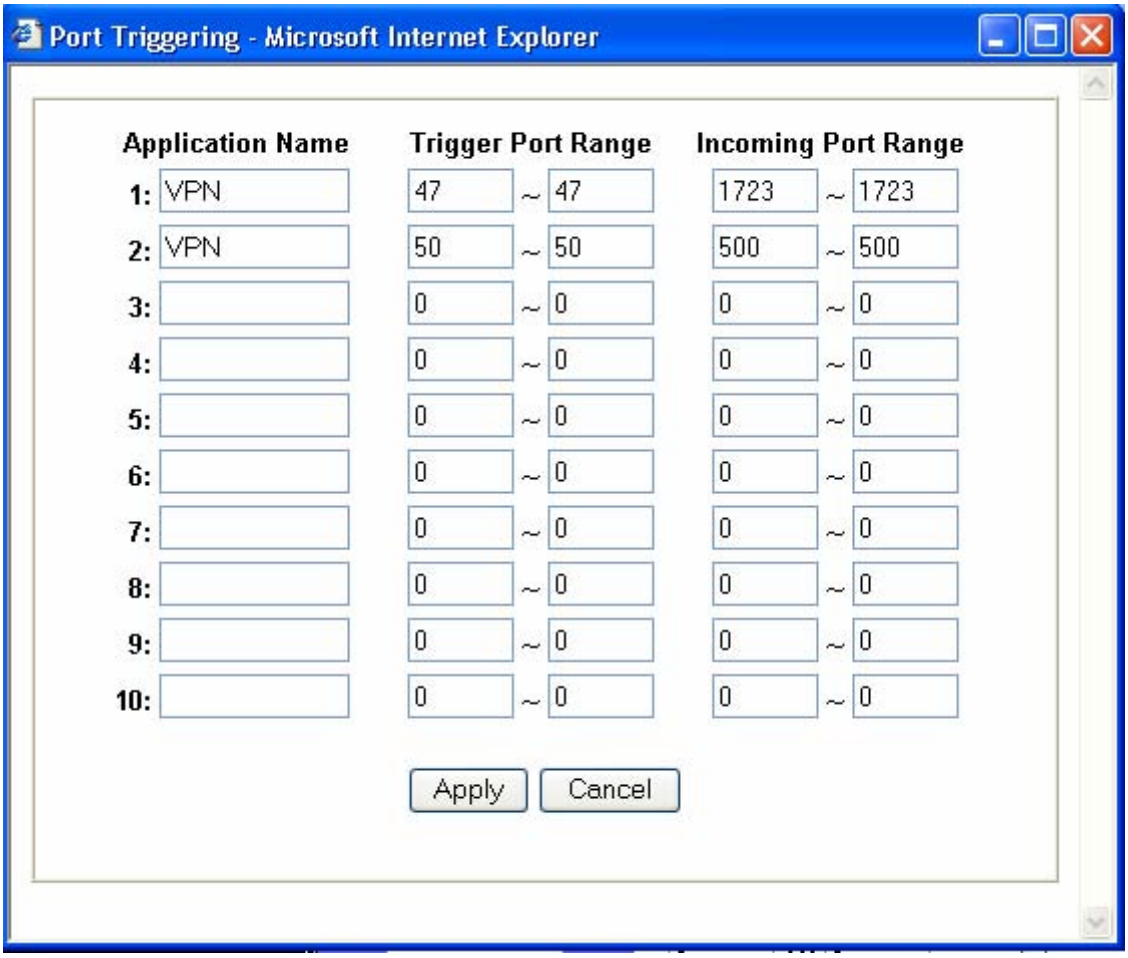
Once connected to your VPN gateway, you must go through the following steps.

2.1 Linksys BESRF41 Configuring Port Triggering

Select on "ADVANCED" tab ➔ "FORWARDING" ➔ "PORT TRIGGERING"



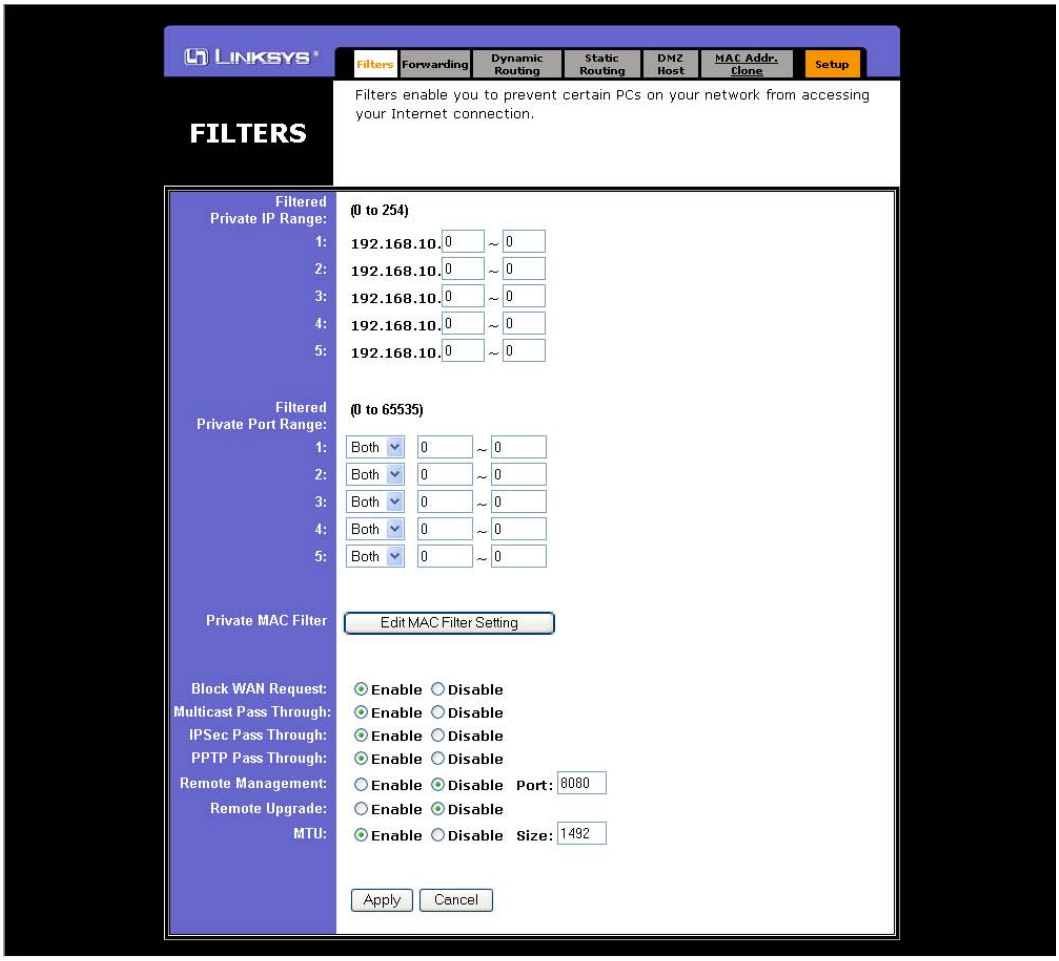
Configure the PORT TRIGGER page as follows:



2.2 Configure Linksys BESRF41 to allow IPSEC Pass Through

Note: This may not be necessary with the configuration of port triggering, but configure IPSec Pass Through for good measure unless you know better or care to experiment.

Select "ADVANCED" ➔ "FILTERS" ➔ "ENABLE IPSEC PASS THROUGH"



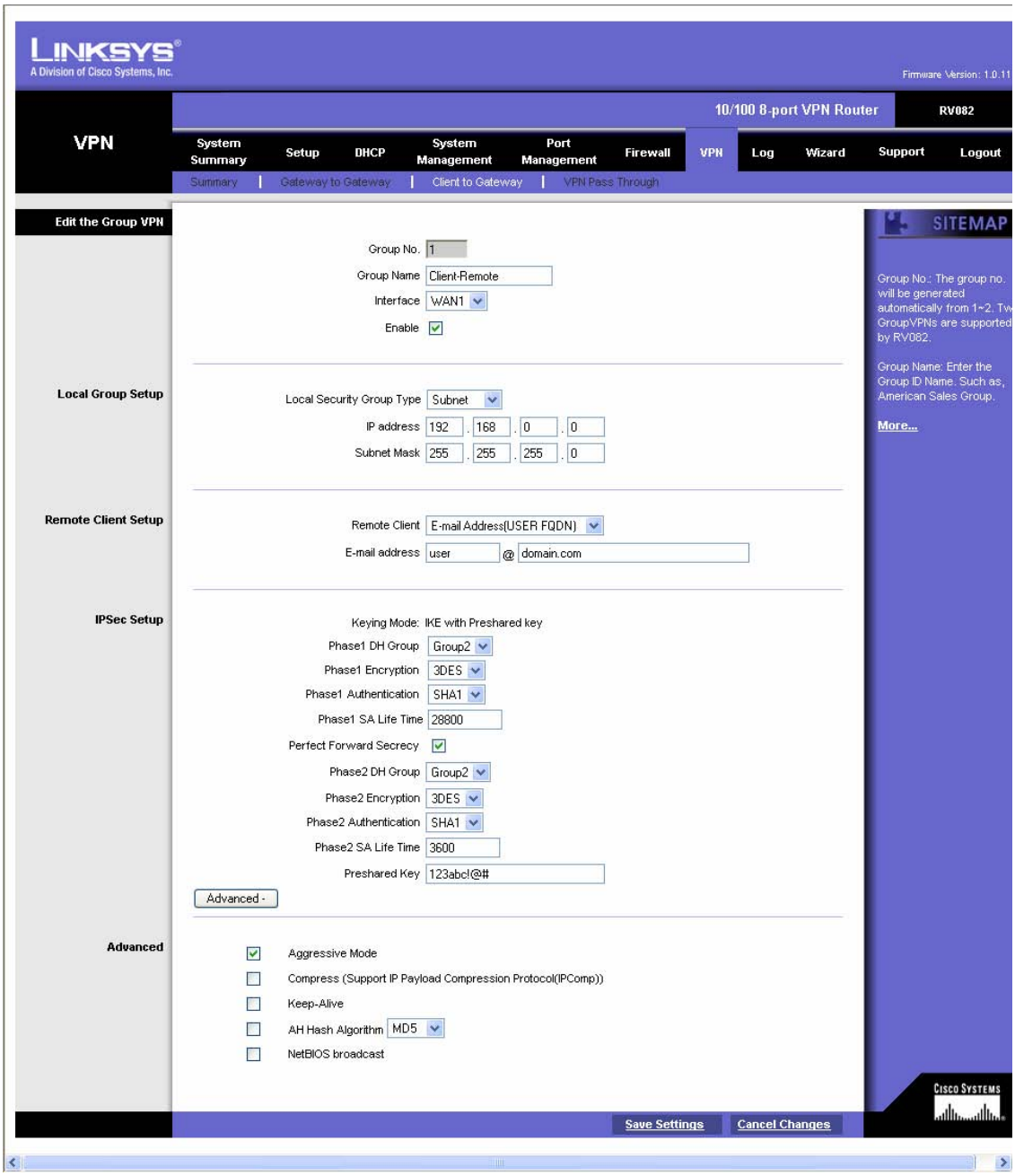
3 Linksys RV082 VPN configuration

This section describes how to build an IPSec VPN configuration with your Linksys RV082 VPN router (end point in our diagram). Once connected to your VPN gateway, you must go through the following steps. Note these IPSec values. Make sure you remember IPSec / IKE Phase1 and Phase 2 attributes as you'll need them to configure TheGreenBow IPSec VPN Client side.

Note: Our experience has been that the Greenbow IPSEC VPN client will work only with the Linksys RV082 when the RV082 is configured to accept the incoming VPN request through a CLIENT-TO-GATEWAY connection of the type *GROUP (not TUNNEL).*

3.1 Configuring Port Triggering

Select "VPN" ➔ "CLIENT-to-GATEWAY" ➔ "GROUP" (Note: If you select GROUP you will see the following page with “Group No.”).



3.2 Remote Client Setup

We have tested EMAIL ADDRESS (USER FQDN) successfully, under REMOTE CLIENT SETUP.

Note: This email address can be any email address, and the domain name DOES NOT need to resolve to an actual IP address on your network (i.e. you can use your @hotmail.com or @yahoo.com email address).

3.3 IPSec Setup

Under IPSEC SETUP it is necessary that all the GROUP, ENCRYPTION and AUTHENTICATION settings match those configured on TheGreenbow IPSec VPN Client (respective to Phase1 (auth) and Phase2 (ipsec). The PRESHARED KEY must match on TheGreenbow IPSec VPN Client too. It is not necessary to change the Phase 1 SA Lifetimes or Phase 2 SA Lifetimes on the Linksys RV082 (or TheGreenbow either for that matter); the defaults will work well. I suggest selecting PERFECT FORWARD SECRECY for added protection against compromised keys.

3.4 Advanced options

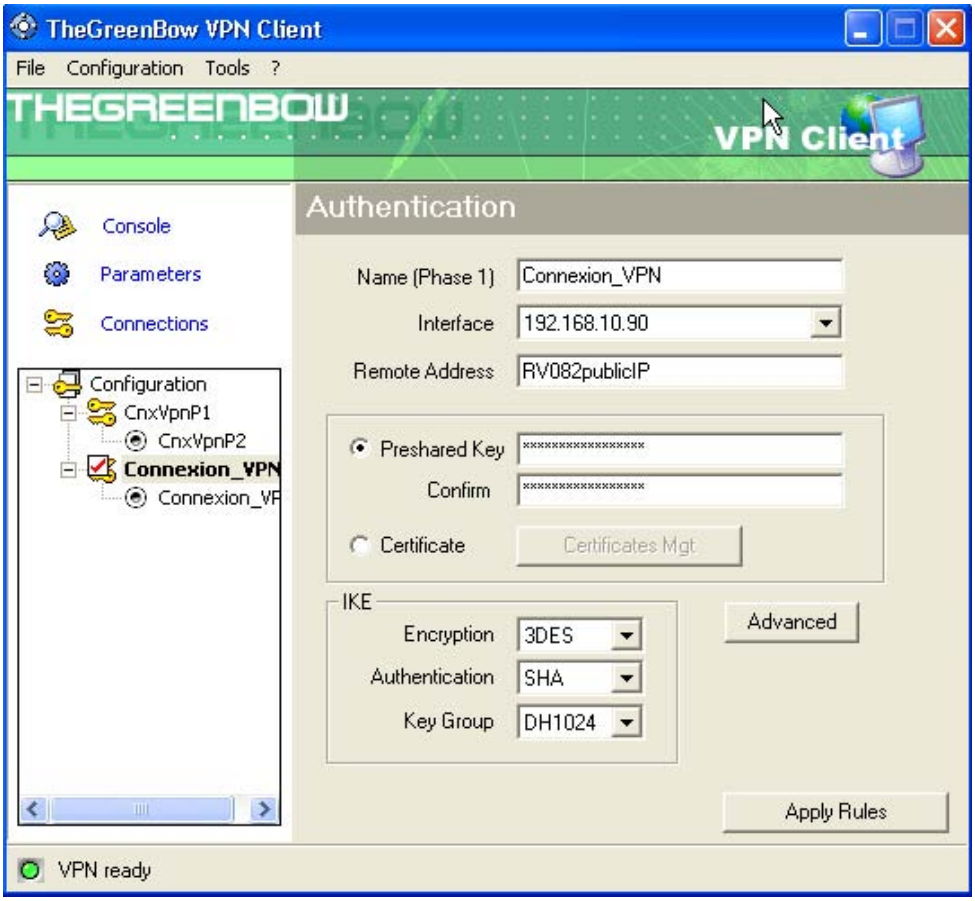
We recommend selecting only AGGRESSIVE mode (if any) on the RV082. Make sure to select AGGRESSIVE mode on TheGreenbow IPSec VPN Client ADVANCED options too (see TheGreenbow setup).

3.5 Group VPN

Don't forget to ENABLE the GROUP VPN.

4 TheGreenBow IPSec VPN Client configuration

4.1 VPN Client Phase 1 (IKE) Configuration



Phase 1 configuration

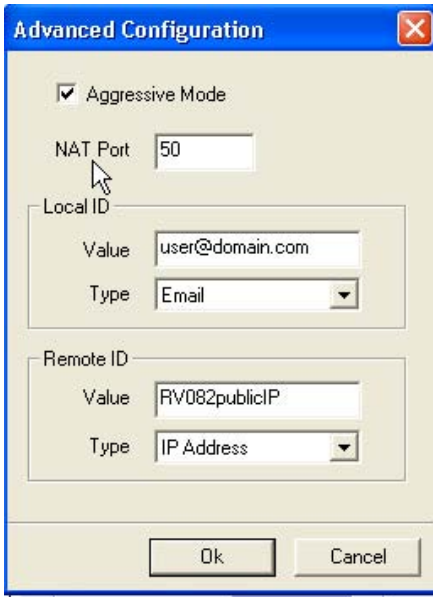
a. The INTERFACE address is the actual IP address of your network card (on your private LAN is the assumption).

b. The REMOTE ADDRESS is the public IP address of your Linksys RV082 VPN router.

c. PRESHARE KEY is the same as on your Linksys RV082.

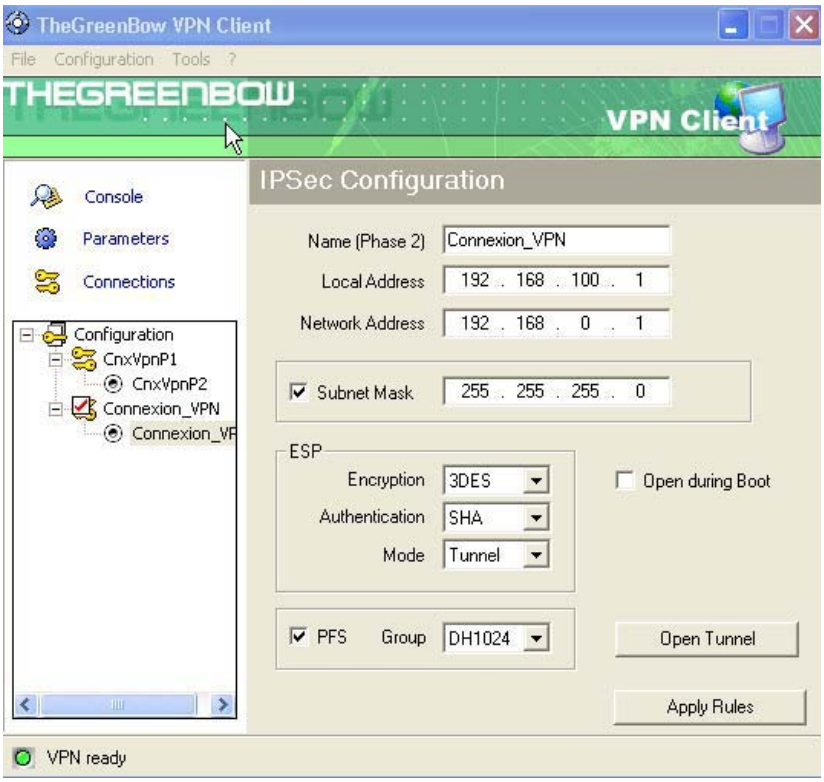
d. IKE settings are the same as the Phase1 GROUP, ENCRYPTION and AUTHENTICATION settings on the Linksys RV082 GROUP VPN page.

e. Click ADVANCED and configure your options to mirror those on the Linksys RV082. Enter the value 50 for the NAT PORT. If you chose Aggressive mode on the Linksys RV082 you must select the same option here too.



f. Click OK and on the Phase1 (Authentication) page click "Save & Apply" to take into account latest modifications on your VPN configuration

4.2 VPN Client Phase 2 (IPSec) Configuration



Phase 2 Configuration

a. The Local Address is a virtual IP address that must be on a different subnet than the IP address on your network card and also NOT on the same subnet as the private LAN behind the Linksys RV082.

   i.e. Your NIC address: 192.168.10.90/24
   Local address: 192.168.100.1/24 (cannot be 192.168.10.xxx/24).

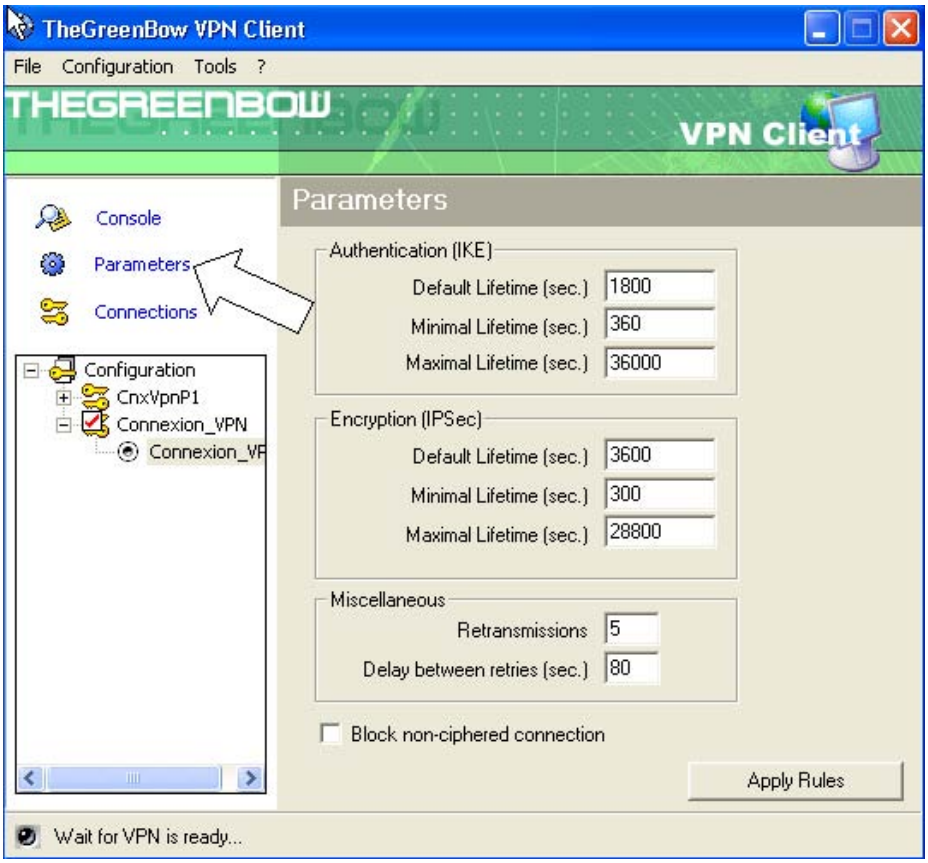
b. The Network Address is the private IP address of the LAN port on the Linksys RV082. Checking SUBNET MASK allows access to all systems on the subnet of the Linksys RV082's LAN.

c. The ESP settings and PFS option must be the same as the Phase2 GROUP, ENCRYPTION and AUTHENTICATION and PFS settings on the Linksys RV082 Group VPN page.

d. Click "Save & Apply" to take into account latest modifications on your VPN configuration.

4.3 Global parameters

It is not necessary to change any of the PARAMETERS options. However, it is recommended that you uncheck the option BLOCK NON-CIPHERED CONNECTIONS, in order to allow HTTP (web) traffic to be routed out to your ISP rather than through the IPSec VPN tunnels (unless you want that). If checked you might not be able to surf the Internet.



4.4 Open the IPSec VPN tunnels

Once both routers Linksys RV082, Linksys BESRF41 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)

No IPSec VPN Tunnel opened:

At least one IPSec VPN Tunnel opened:

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.

5 VPN IPSec Troubleshooting

5.1 « PAYLOAD MALFORMED » error

```
114920 Default (SA RV082-P1) SEND phase 1 Main Mode  [SA][VID]
114920 Default (SA RV082-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 RV082-P1) SEND phase 1 Main Mode  [SA][VID]
115317 Default (SA RV082-P1) RECV phase 1 Main Mode  [SA][VID]
115317 Default (SA RV082-P1) SEND phase 1 Main Mode  [KEY][NONCE]
115319 Default (SA RV082-P1) RECV phase 1 Main Mode  [KEY][NONCE]
115319 Default (SA RV082-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 RV082-P1) SEND phase 1 Main Mode  [SA][VID]
120349 Default (SA RV082-P1) RECV phase 1 Main Mode  [SA][VID]
120349 Default (SA RV082-P1) SEND phase 1 Main Mode  [KEY][NONCE]
120351 Default (SA RV082-P1) RECV phase 1 Main Mode  [KEY][NONCE]
120351 Default (SA RV082-P1) SEND phase 1 Main Mode  [ID][HASH][NOTIFY]
120351 Default (SA RV082-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 RV082-P1) SEND phase 1 Main Mode  [SA][VID]
115913 Default (SA RV082-P1) RECV phase 1 Main Mode  [SA][VID]
115913 Default (SA RV082-P1) SEND phase 1 Main Mode  [KEY][NONCE]
115915 Default (SA RV082-P1) RECV phase 1 Main Mode  [KEY][NONCE]
115915 Default (SA RV082-P1) SEND phase 1 Main Mode  [ID][HASH][NOTIFY]
115915 Default (SA RV082-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    RV082-RV082-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 RV082-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 RV082-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 RV082-P1) SEND phase 1 Main Mode  [SA][VID]
122625 Default (SA RV082-P1) RECV phase 1 Main Mode  [SA][VID]
122625 Default (SA RV082-P1) SEND phase 1 Main Mode  [KEY][NONCE]
122626 Default (SA RV082-P1) RECV phase 1 Main Mode  [KEY][NONCE]
122626 Default (SA RV082-P1) SEND phase 1 Main Mode  [ID][HASH][NOTIFY]
122626 Default (SA RV082-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    RV082-RV082-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 RV082-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