 **TheGreenBow IPSec VPN Client**
Configuration Guide
Linksys WRV200

WebSite: <http://www.thegreenbow.com>

Contact: support@thegreenbow.com

Configuration Guide written by:

Writer: TheGreenBow Support Team

Company: www.thegreenbow.com

Table of contents

1	Introduction	3
1.1	Goal of this document	3
1.2	VPN Network topology	3
1.3	Linksys WRV200 Restrictions	3
1.4	Linksys WRV200 VPN Gateway	3
1.5	Linksys WRV200 VPN Gateway product info.....	4
2	Linksys WRV200 VPN configuration.....	5
2.1	Configure Linksys WRV200 to allow IPSEC Pass Through	5
2.2	Create an IPSec VPN tunnel in the Linksys WRV200 router	6
2.3	Advanced settings for IPSec tunnel in Linksys WRV200	7
3	TheGreenBow IPSec VPN Client configuration	8
3.1	VPN Client Phase 1 (IKE) Configuration	8
3.2	VPN Client Phase 2 (IPSec) Configuration	9
3.3	Open IPSec VPN tunnels.....	9
4	Tools in case of trouble.....	10
4.1	A good network analyser: Wireshark	10
5	VPN IPSec Troubleshooting	11
5.1	« PAYLOAD MALFORMED » error (wrong Phase 1 [SA])	11
5.2	« INVALID COOKIE » error.....	11
5.3	« no keystate » error	11
5.4	« received remote ID other than expected » error.....	11
5.5	« NO PROPOSAL CHOSEN » error	12
5.6	« INVALID ID INFORMATION » error	12
5.7	I clicked on "Open tunnel", but nothing happens.....	12
5.8	The VPN tunnel is up but I can't ping !.....	12
6	Contacts.....	14

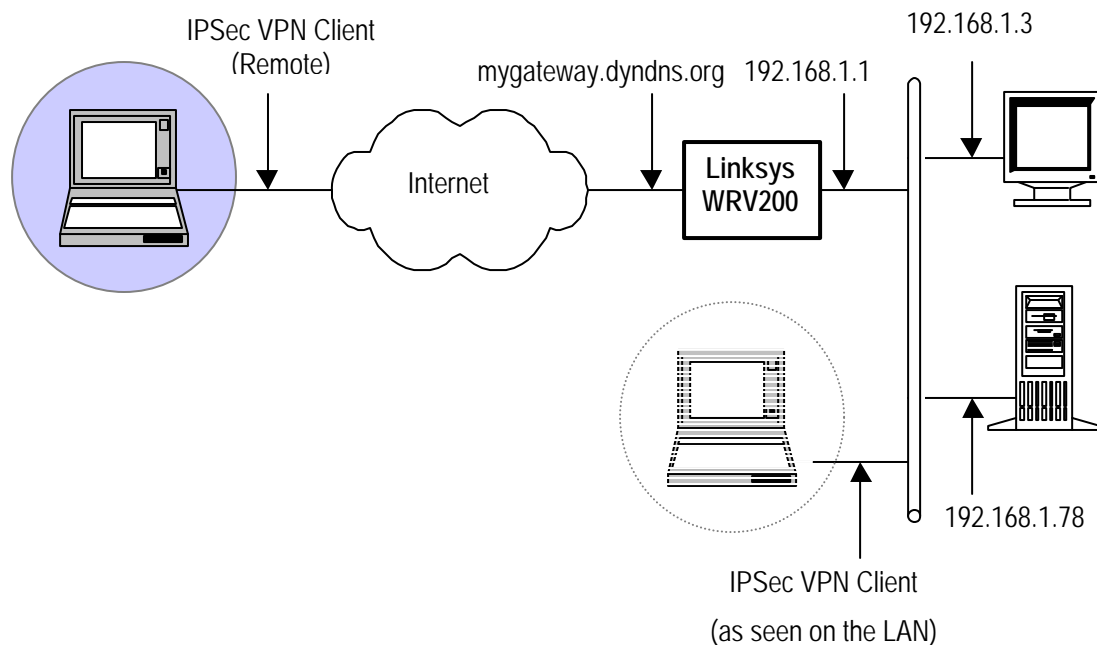
1 Introduction

1.1 Goal of this document

This configuration guide describes how to configure TheGreenBow IPsec VPN Client with a Linksys WRV200 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 Linksys WRV200 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 Linksys WRV200 Restrictions

No known restrictions.

1.4 Linksys WRV200 VPN Gateway

Our tests and VPN configuration have been conducted with Linksys WRV200 firmware release 1.0.21-ETSI.

	Doc.Ref	tgbvpn_ug_linksys_wrv200_en
	Doc.version	3.0 – Jul 2008
	VPN version	4.x

1.5 Linksys WRV200 VPN Gateway product info

All product info, User Guide and knowledge base for the Linksys RVS4000 VPN Gateway can be found on the Linksys website: <http://www.linksys.com>

- Linksys RVS4000 Product page:
http://www.linksys.com/servlet/Satellite?c=L_Product_C2&childpagename=US%2FLayout&cid=1147187335899&pagename=Linksys%2FCommon%2FVisitorWrapper
- Linksys RVS4000 User Guide:
[http://www.linksys.com/servlet/Satellite?blobcol=urldata&blobheadername1=Content-
Type&blobheadername2=Content-
Disposition&blobheadervalue1=application%2Fpdf&blobheadervalue2=inline%3B+filename%3Dwrv200-
ug.pdf&blobkey=id&blobtable=MungoBlobs&blobwhere=1193770230560&ssbinary=true&lid=343931191
2B02](http://www.linksys.com/servlet/Satellite?blobcol=urldata&blobheadername1=Content-
Type&blobheadername2=Content-
Disposition&blobheadervalue1=application%2Fpdf&blobheadervalue2=inline%3B+filename%3Dwrv200-
ug.pdf&blobkey=id&blobtable=MungoBlobs&blobwhere=1193770230560&ssbinary=true&lid=343931191
2B02)

2 Linksys WRV200 VPN configuration

This section describes how to build an IPSec VPN configuration with your Linksys WRV200 VPN router. Once connected to your Linksys WRV200 VPN gateway, you must select 'VPN' tabs.

2.1 Configure Linksys WRV200 to allow IPSEC Pass Through

Note: Configure IPSec Pass Through for good measure unless you know better or care to experiment.

Select the tabs 'VPN' and then 'VPN Pass Through'. Enable the 'IPSec Pass Through' and 'Save Settings'.

The screenshot displays the Linksys WRV200 web interface. The top navigation bar includes 'LINKSYS A Division of Cisco Systems, Inc.' and 'Wireless-G VPN Router with RangeBooster WRV200'. The main navigation menu has tabs for 'Setup', 'Wireless', 'Firewall', 'VPN', 'QoS', 'Administration', and 'Status'. Under the 'VPN' tab, there are sub-tabs for 'VPN Client Access', 'VPN Passthrough', 'IPSec VPN', and 'VPN Summary'. The 'VPN Passthrough' sub-tab is selected, showing three options: 'IPSec Passthrough', 'PPTP Passthrough', and 'L2TP Passthrough'. Each option has radio buttons for 'Enabled' and 'Disabled'. The 'IPSec Passthrough' option is highlighted with a green box, and its 'Enabled' radio button is selected. A help box on the right explains that these features allow for establishing VPN tunnels through the router's firewall.

2.2 Create an IPSec VPN tunnel in the Linksys WRV200 router

To configure the IPSec Tunnel in the Linksys WRV200 VPN gateway, you must select 'VPN' and then 'IPSec VPN' tabs. You will obtain a configuration page as shown in the screenshot below.

- 'VPN Tunnel': To create a tunnel, select a 'Tunnel Name' from the 'Tunnel Entry' list. If your VPN Client will be behind a NAT device, enable the NAT-Traversal for the tunnel.
- 'Local Secure Group': select 'Subnet' to access by VPN Client.
- Configure other parameters as mentioned below and 'Save Settings'.

The screenshot displays the Linksys VPN configuration interface. The 'VPN' tab is selected, and the 'IPSec VPN' sub-tab is active. The configuration is divided into several sections:

- VPN Tunnel:** Tunnel Entry is set to 'Tunnel A'. The 'VPN Tunnel' checkbox is checked (Enabled). The Tunnel Name is 'Tunnel1'. The 'NAT-Traversal' checkbox is also checked (Enabled).
- Local Secure Group:** Type is set to 'Subnet'. The IP Address is 192.168.1.0 and the Mask is 255.255.255.0.
- Remote Secure Group:** Type is set to 'Any' with a note: '(This Gateway accepts request from any IP Address!)'.
- Remote Secure Gateway:** Type is set to 'Any' with a note: '(This Gateway accepts request from any IP Address!)'.
- Key Management:** Key Exchange Method is 'Auto (IKE)'. Encryption is 'AES128', Authentication is 'SHA1', and the Pre-Shared Key is '0123456789'. PFS is checked (Enabled). ISAKMP Key Lifetime is 28800 and IPsec Key Lifetime is 3600.
- Tunnel Options:** 'Dead Peer Detection' is checked. Detection Delay is 30s and Detection Timeout is 120s. 'DPD Action' is set to 'Recover Connection'. 'Anti-replay' is checked. A note states: 'If IKE failed more than 5 times, block this unauthorized IP for 60 seconds'.
- Global Options:** 'Global NAT-Traversal' is checked (Enabled).

Buttons for 'Save Settings' and 'Cancel Changes' are located at the bottom right of the configuration area.

2.3 Advanced settings for IPSec tunnel in Linksys WRV200

Once you saved the settings, click 'Advanced Settings' in 'Key Management' to configure phase steps. Configure as shown below and 'Save Settings'.

LINKSYS
A Division of Cisco Systems, Inc.

Auto (IKE) Advanced Settings

Tunnel Entry : Tunnel A

Phase 1

Operation Mode: Main

Encryption Method: AES128

Authentication Method: SHA1

DH Group: Group 2: 1024-bits

ISAKMP Key Lifetime (s): 28800

Phase 2

Encryption Method: AES128

Authentication Method: SHA1

PFS: Enabled Disabled

DH Group: Group 2: 1024-bits

IPsec Key LifeTime (s): 3600

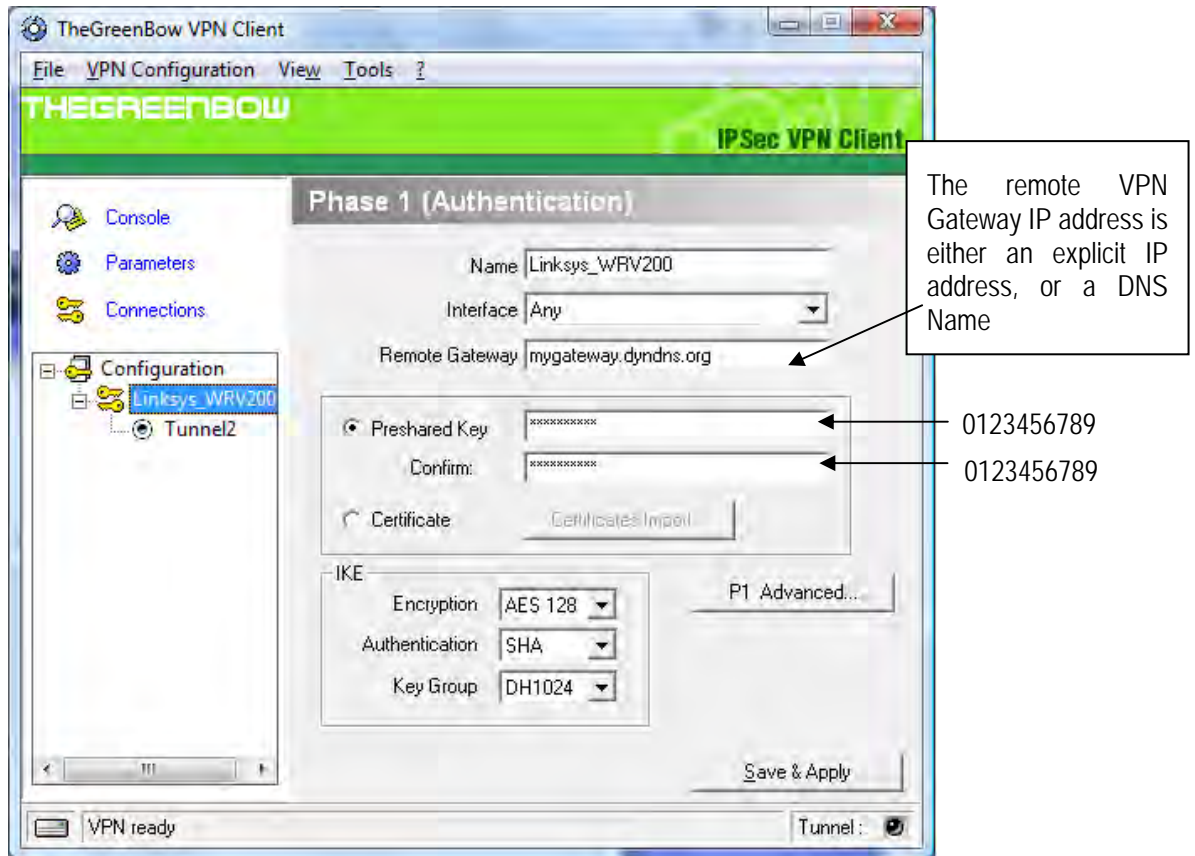
Save Settings Close

3 TheGreenBow IPsec VPN Client configuration

This section describes the required configuration to connect to a Linksys WRV200 VPN router.

To download the latest release of TheGreenBow IPsec VPN Client software, please go to http://www.thegreenbow.com/vpn_down.html.

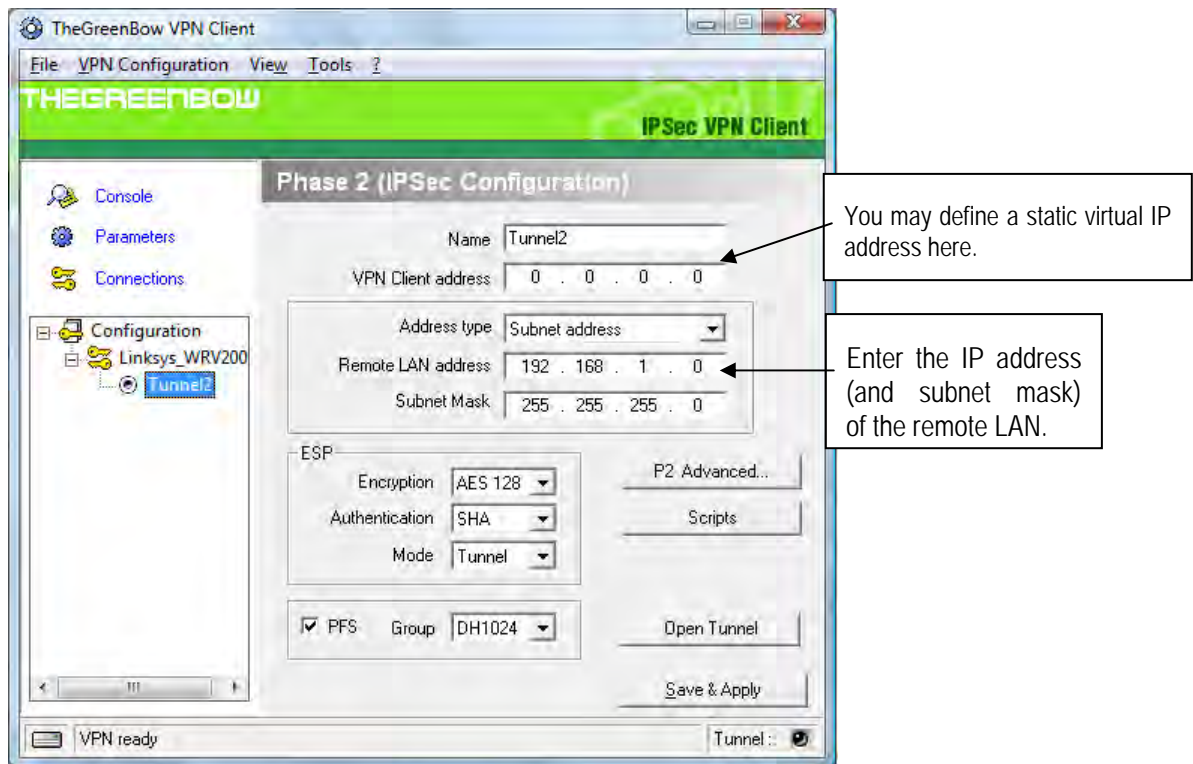
3.1 VPN Client Phase 1 (IKE) Configuration



Phase 1 configuration

This configuration is one example of can be accomplished in term of Pre Shared Key. You may want to refer to either the Linksys WRV200 router user guide or TheGreenBow IPsec VPN Client User Guide for more details on other options.

3.2 VPN Client Phase 2 (IPSec) Configuration



Phase 2 Configuration

3.3 Open IPSec VPN tunnels

Once both Linksys WRV200 router and TheGreenBow IPSec VPN Client software 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 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 Linksys WRV200 VPN router.

```

20080701 121924 Default [SA Linksys_wRV200-P1] SEND phase 1 Main Mode [SA] [VID] [VID] [VID] [VID] [VID]
20080701 121934 Default [SA Linksys_wRV200-P1] RECV phase 1 Main Mode [SA] [VID] [VID] [VID]
20080701 121934 Default [SA Linksys_wRV200-P1] SEND phase 1 Main Mode [KEY_EXCH] [NONCE] [NAT_D] [NAT_D]
20080701 121934 Default [SA Linksys_wRV200-P1] RECV phase 1 Main Mode [KEY_EXCH] [NONCE] [NAT_D] [NAT_D]
20080701 121934 Default [SA Linksys_wRV200-P1] SEND phase 1 Main Mode [HASH] [ID] [NOTIFY]
20080701 121934 Default [SA Linksys_wRV200-P1] RECV phase 1 Main Mode [HASH] [ID]
20080701 121934 Default phase 1 done: initiator id 192.168.205.152, responder id 88.162.180.74
20080701 121934 Default [SA Linksys_wRV200-Tunnel2-P2] SEND phase 2 Quick Mode [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [ID]
20080701 121935 Default [SA Linksys_wRV200-Tunnel2-P2] RECV phase 2 Quick Mode [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [ID]
20080701 121935 Default [SA Linksys_wRV200-Tunnel2-P2] SEND phase 2 Quick Mode [HASH]
20080701 122008 Default [SA Linksys_wRV200-P1] RECV Informational [HASH] [NOTIFY] type DPD_R_U_THERE
20080701 122008 Default [SA Linksys_wRV200-P1] SEND Informational [HASH] [NOTIFY] type DPD_R_U_THERE_ACK
    
```

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: Wireshark

Wireshark 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 tool is available on website <http://www.wireshark.org>. It can be used to follow protocol exchange between two devices. For installation and use details, read its specific documentation (<http://www.wireshark.org/docs/>).

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

5 VPN IPSec Troubleshooting

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

```

114920 Default (SA Linksys_WRV200-P1) SEND phase 1 Main Mode [SA][VID]
114920 Default (SA Linksys_WRV200-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 Linksys_WRV200-P1) SEND phase 1 Main Mode [SA][VID]
115317 Default (SA Linksys_WRV200-P1) RECV phase 1 Main Mode [SA][VID]
115317 Default (SA Linksys_WRV200-P1) SEND phase 1 Main Mode [KEY][NONCE]
115319 Default (SA Linksys_WRV200-P1) RECV phase 1 Main Mode [KEY][NONCE]
115319 Default (SA Linksys_WRV200-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 Linksys_WRV200-P1) SEND phase 1 Main Mode [SA][VID]
120349 Default (SA Linksys_WRV200-P1) RECV phase 1 Main Mode [SA][VID]
120349 Default (SA Linksys_WRV200-P1) SEND phase 1 Main Mode [KEY][NONCE]
120351 Default (SA Linksys_WRV200-P1) RECV phase 1 Main Mode [KEY][NONCE]
120351 Default (SA Linksys_WRV200-P1) SEND phase 1 Main Mode [ID][HASH][NOTIFY]
120351 Default (SA Linksys_WRV200-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 Linksys_WRV200-P1) SEND phase 1 Main Mode [SA][VID]
115913 Default (SA Linksys_WRV200-P1) RECV phase 1 Main Mode [SA][VID]
115913 Default (SA Linksys_WRV200-P1) SEND phase 1 Main Mode [KEY][NONCE]
115915 Default (SA Linksys_WRV200-P1) RECV phase 1 Main Mode [KEY][NONCE]
115915 Default (SA Linksys_WRV200-P1) SEND phase 1 Main Mode [ID][HASH][NOTIFY]
115915 Default (SA Linksys_WRV200-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 Linksys_WRV200-Tunnel2-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 Linksys_WRV200-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 Linksys_WRV200-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 Linksys_WRV200-P1) SEND phase 1 Main Mode [SA][VID]
122625 Default (SA Linksys_WRV200-P1) RECV phase 1 Main Mode [SA][VID]
122625 Default (SA Linksys_WRV200-P1) SEND phase 1 Main Mode [KEY][NONCE]
122626 Default (SA Linksys_WRV200-P1) RECV phase 1 Main Mode [KEY][NONCE]
122626 Default (SA Linksys_WRV200-P1) SEND phase 1 Main Mode [ID][HASH][NOTIFY]
122626 Default (SA Linksys_WRV200-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 Linksys_WRV200-Tunnel2-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 Linksys_WRV200-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

Doc.Ref	tgbvpn_ug_linksys_wrv200_en
Doc.version	3.0 – Jul 2008
VPN version	4.x

- If you still cannot ping, follow ICMP traffic on VPN server LAN interface and on LAN computer interface (with Wireshark 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 Wireshark (<http://www.wireshark.org>) on one of your target computer. You can check that your pings arrive inside the LAN.

	Doc.Ref	tgbvpn_ug_linksys_wrv200_en
	Doc.version	3.0 – Jul 2008
	VPN version	4.x

6 Contacts

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

Technical support by email at support@thegreenbow.com

Sales contacts by email at sales@thegreenbow.com