

TheGreenBow IPSec VPN Client Configuration Guide Linksys RV082

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

IPSec VPN Router Configuration

0/16

Doc.Ref	tgbvpn_ug_LinksysRV082_en
Doc.version	2.0 – Feb.2005
VPN version	2.5x

Table of contents

1	Introduction	0 0
	.2 VPN Network topology	0
	.3 Linksys RV082 and Linksys BESRF41 Restrictions	0
2	Linksys BESRF41 VPN configuration	0
	Linksys BESRF41 Configuring Port Triggering	0
		0
3	Linksys RV082 VPN configuration	0
	1 Configuring Port Triggering	0
	3 IPSec Setun	0
	A Advanced options	0
	5 Group VPN	0
4	TheGreenBow IPSec VPN Client configuration	0
	.1 VPN Client Phase 1 (IKE) Configuration	0
	.2 VPN Client Phase 2 (IPSec) Configuration	0
	.3 Global parameters	0
_		0
5	VPN IPSec Troubleshooting	0
	2 « INVALID COOKIE » error	0
	a.3 « no keystate » error	0
	.4 « received remote ID other than expected » error	0
	.5 « NO PROPOSAL CHOSEN » error	0
	.6 « INVALID ID INFORMATION » error	0
	7 I Clicked on "Open lunnel", but notning nappens	U 0
,		0
6	Contacts	U

THECOECOECOECIA	Doc.Ref	tgbvpn_ug_LinksysRV082_en
	Doc.version	2.0 – Feb.2005
	VPN version	2.5x

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.

THECOECOECOECOHIa 10 10 10 10 10 10 10 10 10 10 10 10 10	Doc.Ref	tgbvpn_ug_LinksysRV082_en
	Doc.version	2.0 – Feb.2005
	VPN version	1 2.5x

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"

Linksys*	Filters Fo	rwarding	Dynamic	Static	DMZ	MAC Addr.	Setup
PORT RANGE FORWARDING	Port forw When us will be re	varding ca ers from t directed t	n be used he Interne o the spe	to set up pu et make certa cified IP.	ublic serv ain reque	ices on your n ists on your ro	etwork. uter, they
Customized Applications	Ext	t.Port	Proto TC	col Protoco P UDP	¹ II	^o Address	Enable
	0 -	To 0			192.1	68.10 . 0	
	0 -	To 0] ଢ ⊏		192.1	68.10. O	
	0 -	To 0			192.1	68.10. 0	
	0 -	To 0			192.1	68.10 . 0	
	0 -	To 0			192.1	68.10 . 0	
	0 -	To 0			192.1	68.10 . 0	
	0 -	To 0			192.1	68.10 . 0	
	0 -	To 0			192.1	68.10 . 0	
	0 -	To 0			192.1	68.10 . 0	
	0 -	To 0			192.1	68.10. 0	
	UPnF Apply	> Forwardin	9	Port Trigge	ering V	*	

TH	E	6	R	100.00	E	-	M	011110
				1				

Doc.Ref	tgbvpn_ug_LinksysRV082_en
Doc.version	2.0 – Feb.2005
VPN version	2.5x

Configure the **PORT TRIGGER** page as follows:

Ap	plication Name	Trigg	er Po	rt Range	Incomin	g Po	ort Range
1:	VPN	47	~	47	1723	~	1723
2:	VPN	50	~	50	500	~	500
3:		0	~	0	0	~	0
4:		0	~	0	0	~	0
5:	-	0	~	0	0	~	0
6:		0	~	0	0	_~	0
7:		0	~	0	0	~	0
8:		0	~	0	0	~	0
9:		0	~	0	0	~	0
10:		0	~	0	0	~	0
		Abt	ly (Cancel]		

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.

THEODEEDECIII MONTON	Doc.Ref	tgbvpn_ug_LinksysRV082_en
	Doc.version	2.0 – Feb.2005
	VPN version	2.5x

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

Linksys'	Filters Forwarding Dynamic Static DNZ <u>MAC.Addr.</u> Setup
FILTERS	Filters enable you to prevent certain PCs on your network from accessing your Internet connection.
Filtered Private IP Range:	(0 to 254)
1:	192.168.10.0 ~ 0
2:	192.168.10.0 ~ 0
3:	192.168.10.0 ~ 0
4:	192.168.10.0 ~ 0
5:	192.168.10.0 ~ 0
Filtered Private Port Range:	(0 to 65535)
1:	Both 🔽 0 ~ 0
2:	Both 🕜 0 ~ 0
3:	Both 🕑 0 ~ 0
4:	Both 🔽 0 ~ 0
5:	Both 🔽 0 ~ 0
Private MAC Filter	Edit MAC Filter Setting
Block WAN Request:	
Multicast Pass Through:	Enable Disable
IPSec Pass Through:	● Enable ○ Disable
PPTP Pass Through:	Enable Obisable
Remote Management:	C Enable O Disable Port: 8080
Remote Upgrade:	Chable Disable
	Apply Cancel

Doc.Ref	tgbvpn ug LinksysRV082 en
Doc.version	2.0 – Feb.2005
VPN version	2.5x

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" \rightarrow "CLIENT-to-GATEWAY" \rightarrow "GROUP" (Note: If you select GROUP you will see the following page with "Group No.").

	1						10	/100 8-po	rt VPN Rou	ter	RV0
VPN	System Summary Summary	Setup Gateway to Ga	DHCP	System Management Client to Gatev	Port Management vay VPN Pas	Firewall	VPN	Log	Wizard	Support	
Edit the Group VPN			Group No Group Name Interface Enable	- 1 2 Client-Remote ≥ WAN1 ▼ = ♥						Group No will be ge automatic GroupVPI by RV082	SITE .: The g nerated ally fror vs are s .:
Local Group Setup		Local Security	/ Group Type IP address Subnet Masł	Subnet 192 . 168 255 . 255	. 0 . 0 . 255 . 0					Group Na Group ID I American <u>More</u>	me:Ent Name.S Sales (
Remote Client Setup		F E-	Remote Clien mail address	t E-mail Address	USER FQDN) 💌 @ domain.com						
IPSec Setup	Advanced -	H Phase Phase1 A Phase1 A Phase1 Phase1 Phase Phase2 Phase2 Phase2 Phase2	Keying Mode ef DH Group 1 Encryption uthentication SA Life Tim ard Secrecy e2 DH Group 2 Encryption uthentication SA Life Time eshared Key	IKE with Presha Group2 3DES SHA1 28800 Group2 3DES SHA1 Group2 3DES SHA1 3DES SHA1 3DES SHA1 3DES 3DES 3DES	red key						
Advanced		Aggressive M Compress (Si Keep-Alive AH Hash Algo NetBIOS broa	lode upport IP Pay orithm MD5 dcast	rload Compressio	n Pratocol((PComp))						Cisco

TH	EC	R	-		B	N I	0111101	
			1					

Doc.Ref	tgbvpn_ug_LinksysRV082_en
Doc.version	2.0 – Feb.2005
VPN version	2.5x

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**.

THECOECOECOE (10101010101010101010101010101010101010	Doc.Ref tgbvpn_ug_LinksysRV082_en
	Doc.version 2.0 – Feb.2005
	VPN version 2.5x

4 TheGreenBow IPSec VPN Client configuration

4.1 VPN Client Phase 1 (IKE) Configuration

TheGreenBow VPN Clie	int		
File Configuration Tools ?			
THEGREENBO			
🔎 Console	Authentication	ו	
🙀 Parameters	Name (Phase 1)	Connexion_VPN	
S Connections	Interface	192.168.10.90	•
Configuration	Remote Address	RV082publicIP	
CnxVpnP2	Preshared Key	*****	
Connexion_VF	Confirm	*****	
	C Certificate	Certificates Mgt	
	-IKE		
	Encryption	3DES 💌	Advanced
	Authentication	SHA 💌	
	Key Group	DH1024 -	
< >			Apply Rules
O VPN ready			

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.

THECDEEDE®N 104040404	Doc.Ref	tgbvpn_ug_LinksysRV082_en
	Doc.version	2.0 – Feb.2005
	VPN version	2.5x

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.

NAT Port	50	
Local ID —		
Value	user@domain.com	
Туре	Email	•
Remote ID -		
Value	RV082publicIP	
Туре	IP Address	-

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

IEGREENB	PW acy/i		
h			C
Console	IPSec Configu	ration	
Parameters	Name (Phase 2)	Connexion_VPN	
Connections	Local Address	192 . 168 . 100) 1
🛃 Configuration	Network Address	192 . 168 . 0	. 1
CnxVpnP1	🔽 Subnet Mask	255 . 255 . 255	5.0
Connexion_VF	ESP		
	Encryption	3DES 💌	🔲 Open during Boo
	Authentication	SHA 💌	
	Mode	Tunnel 💌	
	PFS Group	DH1024 -	Open Tunnel
			Apply Dules

Phase 2 Configuration

Doc.Ref	tgbvpn_ug_LinksysRV082_en
Doc.version	2.0 – Feb.2005
VPN version	2.5x

- 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.

TheGreenBow VPN Client		
ile Configuration Tools ?		
HEGREENBOU		
Q Console	rameters	
Barameters 7	Authentication (IKE)	
	Default Lifetime (sec.) 1800	
S Connections V	Minimal Lifetime (sec.) 360	
	Maximal Lifetime (sec.) 36000	
CnxVpnP1 CnxVpnP1	Encryption (IPSec)	
Connexion_VF	Default Lifetime (sec.) 3600	
	Minimal Lifetime (sec.) 300	
	Maximal Lifetime (sec.) 28800	
	Miscellaneous	
	Retransmissions 5	
	Delay between retries (sec.) 80	
ſ	Block non-ciphered connection	
		Apply Rules
Wait for VPN is ready		

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)



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.

TH	EG	R	-		B	M	011111	91
			1					

Doc.Ref	tgbvpn_ug_LinksysRV082_en
Doc.version	2.0 – Feb.2005
VPN version	2.5x

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 Mc	ode [SA][VID]	
115317	Default	(SA RV082-P1)	RECV phase 1 Main Mc	ode [SA][VID]	
115317	Default	(SA RV082-P1)	SEND phase 1 Main Mc	ode [KEY][NONCE]	
115319	Default	(SA RV082-P1)	RECV phase 1 Main Mc	ode [KEY][NONCE]	
115319	Default	(SA RV082-P1)	SEND phase 1 Main Mc	ode [ID][HASH][NOTIFY]	
115319	Default	ipsec_get_key	state: no keystate in	n 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	e	[SA]	[VID]			
120349	Default	(SA	RV082-P1)	RECV	phase	1	Main	Mode	е	[SA]	[VID]			
120349	Default	(SA	RV082-P1)	SEND	phase	1	Main	Mode	е	[KEY]] [NON	ICE]		
120351	Default	(SA	RV082-P1)	RECV	phase	1	Main	Mode	е	[KEY]] [NON	ICE]		
120351	Default	(SA	RV082-P1)	SEND	phase	1	Main	Mode	е	[ID]	[HASH	[][NOTIF	[צי	
120351	Default	(SA	RV082-P1)	RECV	phase	1	Main	Mode	e	[ID]	[HASH	[][NOTIF	[צי	
120351	Default	: i	ke_phase_1	_recv	_ID:	re	eceive	ed 1	rem	ote	ID	other	than	expected
support@thegreenbow.fr														

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

THECOCCOCIONI		Doc.Ref	tgbvpn_ug_LinksysRV082_en
		Doc.version	2.0 – Feb.2005
		VPN version	2.5x

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 Ouick 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
                                                                            Ouick
                                                                                      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

THECOECODOL 1040140104	Doc.R	ef tgbvpn_ug_Links	sysRV082_en
	Doc.ve	ersion 2.0 – Feb.2005	
	VPN v	ersion 2.5x	

- 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.



Doc.Ref	tgbvpn_ug_LinksysRV082_en					
Doc.version	2.0 – Feb.2005					
VPN version	2.5x					

6 Contacts

News and updates on TheGreenBow web site : <u>http://www.thegreenbow.com</u> Technical support by email at <u>support@thegreenbow.com</u> Sales contacts at +33 1 43 12 39 37 ou by email at <u>info@thegreenbow.com</u>