



Configuration Guide

Vyatta Router with Pre-Shared Key

 WebSite:
 http://www.thegreenbow.com

 Contact:
 support@thegreenbow.com



Table of contents

1	Intro	duction	3
	1.1	Goal of this document	3
	1.2	VPN Network topology	3
	1.3	Vyatta Router Restrictions	3
	1.4	Vyatta VPN Gateway	3
	1.5	Vyatta VPN Router product info	3
2	Vva	ta VPN Router configuration	4
-	2.1	Config the Vvatta Router system using CLL	4
	2.2	The very important steps in Vvatta VPN router configuration	6
n	The		-
3	2.1	JreenBow IPSec VPN Client configuration	1
	3.1 2.2	VPN Client Phase 1 (IRE) Configuration	/
	3.Z	Open JDS og VDN tuppele	ŏ 0
	3.3	Open in Sec VPN luilliels	0
4	Too	s in case of trouble	9
4	Tool 4.1	s in case of trouble A good network analyser: Wireshark	9 9
4 5	Tool 4.1 VPN	s in case of trouble A good network analyser: Wireshark IPSec Troubleshooting	9 9 10
4 5	Tool 4.1 VPN 5.1	s in case of trouble A good network analyser: Wireshark IPSec Troubleshooting « PAYLOAD MALFORMED » error (wrong Phase 1 [SA])	9 9 10
4	Tool 4.1 VPN 5.1 5.2	s in case of trouble A good network analyser: Wireshark IPSec Troubleshooting « PAYLOAD MALFORMED » error (wrong Phase 1 [SA]) « INVALID COOKIE » error.	9 9 10 10
4	Tool 4.1 VPN 5.1 5.2 5.3	s in case of trouble A good network analyser: Wireshark IPSec Troubleshooting « PAYLOAD MALFORMED » error (wrong Phase 1 [SA]) « INVALID COOKIE » error « no keystate » error	9 9 10 10 10
4	Tool 4.1 VPN 5.1 5.2 5.3 5.4	s in case of trouble A good network analyser: Wireshark IPSec Troubleshooting « PAYLOAD MALFORMED » error (wrong Phase 1 [SA]) « INVALID COOKIE » error « no keystate » error « received remote ID other than expected » error	9 9 10 10 10
4	Tool 4.1 5.1 5.2 5.3 5.4 5.5	s in case of troubleA good network analyser: Wireshark	9 9 10 10 10 10
4	Tool 4.1 5.1 5.2 5.3 5.4 5.5 5.6	s in case of trouble A good network analyser: Wireshark IPSec Troubleshooting « PAYLOAD MALFORMED » error (wrong Phase 1 [SA]) « INVALID COOKIE » error « no keystate » error « no keystate » error « received remote ID other than expected » error « NO PROPOSAL CHOSEN » error « INVALID ID INFORMATION » error	9 9 10 10 10 10 11
4	Tool 4.1 5.1 5.2 5.3 5.4 5.5 5.6 5.7	s in case of trouble A good network analyser: Wireshark IPSec Troubleshooting « PAYLOAD MALFORMED » error (wrong Phase 1 [SA]) « INVALID COOKIE » error « no keystate » error « received remote ID other than expected » error « NO PROPOSAL CHOSEN » error « INVALID ID INFORMATION » error I clicked on "Open tunnel", but nothing happens	9 9 10 10 10 10 11 11
4	Tool 4.1 5.1 5.2 5.3 5.4 5.5 5.6 5.7 5.8	s in case of troubleA good network analyser: Wireshark	9 9 10 10 10 10 11 11
4 5 6	Tool 4.1 VPN 5.1 5.2 5.3 5.4 5.5 5.6 5.7 5.8 Con	s in case of trouble A good network analyser: Wireshark IPSec Troubleshooting « PAYLOAD MALFORMED » error (wrong Phase 1 [SA]) « INVALID COOKIE » error « no keystate » error « no keystate » error « received remote ID other than expected » error « NO PROPOSAL CHOSEN » error « INVALID ID INFORMATION » error I clicked on "Open tunnel", but nothing happens The VPN tunnel is up but I can't ping !	9 9 10 10 10 10 11 11 11 13

THECOMON DIGITION	Doc.Ref	tgbvpn_cg-vyatta-router-psk-en
	Doc.version	Jul 2012
	VPN version	5.x

1 Introduction

1.1 Goal of this document

This configuration guide describes how to configure TheGreenBow IPSec VPN Client software with a Vyatta VPN Router to establish VPN connections for remote access to corporate network

1.2 VPN Network topology

In our VPN network example (diagram hereafter), we will connect TheGreenBow IPSec VPN Client software to the LAN behind the Vyatta VPN 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 Vyatta Router Restrictions

Depending on the firmware version, Vyatta Router may not support NAT-T and as a consequence the IPSec VPN Client software could not connect if standing on a LAN behind (e.g. router at home, ..).

1.4 Vyatta VPN Gateway

ur tests and VPN configuration have been conducted with Vyatta Router firmware release VC6.4.

1.5 Vyatta VPN Router product info

It is critical that users find all necessary information about Vyatta VPN Router Gateway. All product info, User Guide and knowledge base for the Vyatta VPN Router can be found on the Vyatta Router website: www.vyatta.org.

Vyatta Router Product page	http://www.vyatta.org/downloads
Vyatta Router User Guide	http://www.vyatta.org/documentation
Vyatta Router FAQ/Knowledge Base	http://www.vyatta.org/forum

THECOECOEMII (1011101)	Doc.Ref	tgbvpn_cg-vyatta-router-psk-en
	Doc.version	Jul 2012
	VPN version	5.x

2 Vyatta VPN Router configuration

This section describes how to build an IPSec VPN configuration with your Vyatta VPN Router.

Once connected to your Vyatta VPN gateway, you must select "Security" and "VPN" tabs.

This DOCUMENT does not include how to install the Vyatta system. For more this information, please visit Vyatta website.

2.1 Config the Vyatta Router system using CLI

login:vyatta

password:vyatta

vyatta@vyatta:~\$ configure

vyatta@vyatta# set system gateway-address 192.168.252.XXX

vyatta@vyatta# set interfaces ethernet eth0 address 192.168.252.23/24

vyatta@vyatta# set interfaces ethernet eth1 address 192.168.253.23/24

vyatta@vyatta# set protocols static route 0.0.0.0/0 next-hop 192.168.252.XXX(not necessary, and you also could set up the firewall policy using "set firewall" CLI which is important but not relative with ipsec setup, so if you care about your security, I recommend you read Vyatta document for this.)

vyatta@vyatta# set vpn ipsec

[edit]

vyatta@vyatta# edit vpn ipsec

[edit vpn ipsec]

vyatta@vyatta# set esp-group esp-d

[edit vpn ipsec]

vyatta@vyatta# edit esp-group esp-d

[edit vpn ipsec esp-group esp-d]

vyatta@vyatta# set compression disable

[edit vpn ipsec esp-group esp-d]

vyatta@vyatta# set lifetime 3600

[edit vpn ipsec esp-group esp-d]

vyatta@vyatta# set mode tunnel

[edit vpn ipsec esp-group esp-d]

vyatta@vyatta# set pfs dh-group2

[edit vpn ipsec esp-group esp-d]

vyatta@vyatta# set proposal 1 encryption aes256

[edit vpn ipsec esp-group esp-d]

vyatta@vyatta# set proposal 1 hash sha1

[edit vpn ipsec esp-group esp-d]

vyatta@vyatta# top

[edit]

vyatta@vyatta# edit vpn ipsec

 Doc.Ref
 tgbvpn_cg-vyatta-router-psk-en

 Doc.version
 Jul 2012

 VPN version
 5.x

[edit vpn ipsec] vyatta@vyatta# set ike-group ike-d [edit vpn ipsec] vyatta@vyatta# edit ike-group ike-d [edit vpn ipsec ike-group ike-d] vyatta@vyatta# set lifetime 3600 [edit vpn ipsec ike-group ike-d] vyatta@vyatta# set proposal 1 dh-group 2 [edit vpn ipsec ike-group ike-d] vyatta@vyatta# set proposal 1 encryption aes256 [edit vpn ipsec ike-group ike-d] vyatta@vyatta# set proposal 1 hash sha1 [edit vpn ipsec ike-group ike-d] vyatta@vyatta# top [edit] vyatta@vyatta# set vpn ipsec nat-traversal enable [edit] vyatta@vyatta# set vpn ipsec ipsec-interfaces interface eth0 [edit] vyatta@vyatta# commit [vpn] VPN Warning: IPSec configured but no site-to-site peers or l2tp remote-users configured [edit] vyatta@vyatta# set vpn ipsec site-to-site peer 0.0.0.0 [edit] vyatta@vyatta# edit vpn ipsec site-to-site peer 0.0.0.0 [edit vpn ipsec site-to-site peer 0.0.0.0] vyatta@vyatta# set authentication mode pre-shared-secret [edit vpn ipsec site-to-site peer 0.0.0.0] vyatta@vyatta# set authentication pre-shared-secret 123456 [edit vpn ipsec site-to-site peer 0.0.0.0] vyatta@vyatta# set default-esp-group esp-d [edit vpn ipsec site-to-site peer 0.0.0.0] vyatta@vyatta# set ike-group ike-d [edit vpn ipsec site-to-site peer 0.0.0.0] vyatta@vyatta# set local-ip 192.168.252.23 [edit vpn ipsec site-to-site peer 0.0.0.0] vyatta@vyatta# set tunnel 1 local subnet 192.168.253.0/24 [edit vpn ipsec site-to-site peer 0.0.0.0] vyatta@vyatta# set tunnel 1 remote subnet 0.0.0.0/0 [edit vpn ipsec site-to-site peer 0.0.0.0] vyatta@vyatta# top



[edit] vyatta@vyatta# commit vyatta@vyatta# save

2.2 The very important steps in Vyatta VPN router configuration

Vyatta Open-source Router using StrangSwan as its IPSec solution, but in VC6.4, there is bug making user can not connect their road-warrior client. The bug in its VPN-config perl script, which did not include some necessary configuration using in StrongSwan.

The solution is below: vyatta@vyatta# exit exit vyatta@vyatta:~\$ sudo vi /etc/ipsec.conf Then open and edit the conf file and add below configuration into the "conn peer-0.0.0.0-tunnel-1" section leftsourceip=192.168.253.23 rightsubnetwithin=0.0.0.0/0 save & quit the conf file, then at the CLI restart vpn damon

The Router Ready!

vyatta@vyatta:~\$ restart vpn

THECOEDOM	Doc.Ref	tgbvpn_cg-vyatta-router-psk-en
	Doc.version	Jul 2012
	VPN version	5.x

3 TheGreenBow IPSec VPN Client configuration

This section describes the required configuration to connect to a Vyatta VPN Router via VPN connections.

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

3.1 VPN Client Phase 1 (IKE) Configuration

😳 TheGreenBow VPN	N Client
<u>C</u> onfiguration <u>T</u> ools <u>?</u>	
THEGREENBOW	IPSec VPN Client
Save Apply	Vyatta: Authentication Authentication Advanced Certificate The remote VPN Addresses Gateway IP address is either an explicit IP address or a DNS Name Interface 192.168.252.101 address or a DNS Name Remote Gateway 192.168.252.23 address or a DNS Name Authentication • • • © Preshared Key • • • Confirm • • • Confirm • • • KE Encryption AE5256 • Authentication • • • Key Group DH2 (1024) • •
• VPN Client ready	

Phase 1 configuration

You may use either Preshared key, Certificates, USB Tokens, OTP Token (One Time Password) or X-Auth combined with RADIUS Server for User Authentication with the Vyatta Router. This configuration is one example of what can be accomplished in term of User Authentication. You may want to refer to either the Vyatta Router user guide or TheGreenBow IPSec VPN Client software User Guide for more details on User Authentication options.

THECDEED CON 104011010	Doc.Ref	tgbvpn_cg-vyatta-router-psk-en
	Doc.version	Jul 2012
	VPN version	5.x

3.2 VPN Client Phase 2 (IPSec) Configuration

TheGreenBow VP	N Client	_	
<u>Configuration</u> <u>Loois ?</u>			
THEGREENBOW			
		IPSec VPN	Client
Save Apply	Tunnell: IPSec		
VPN Configuration	IPSec Advanced Scripts		VPN Client Virtual IP
Global Parameters	Addresses		address
Tunnel	VPN Client address	10 . 0 . 0 . 1	
in o tobtest	Address type	Subnet address	
	Remote LAN address	192 . 168 . 253 . 0	
	Subnet mask	255 . 255 . 255 . 0	
	FCD		Enter the IP address
	L3r		(and subnet mask)
	Encryption	AES256	of the remote LAN.
	Authentication	SHA-1	
	Mode	Tunnel	
	PFS		_
	PFS Group	DH2 (1024)	
• VPN Client ready	<u> </u>		

Phase 2 Configuration

3.3 Open IPSec VPN tunnels

Once both Vyatta 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 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 Vyatta VPN Router.

```
2012-05-15 18:01:15 Default (SA Vyatta-P1) SEND phase 1 Main Mode [SA] [VID] [VID] [VID] [VID] [VID]
2012-05-15 18:01:15 Default (SA Vyatta-P1) RECV phase 1 Main Mode [SA] [VID] [VID] [VID] [VID] [VID]
2012-05-15 18:01:15 Default (SA Vyatta-P1) SEND phase 1 Main Mode [KEY_EXCH] [NONCE] [NAT_D] [NAT_D]
2012-05-15 18:01:15 Default (SA Vyatta-P1) RECV phase 1 Main Mode [KEY_EXCH] [NONCE] [NAT_D] [NAT_D]
2012-05-15 18:01:15 Default (SA Vyatta-P1) SEND phase 1 Main Mode [KEY_EXCH] [NONCE] [NAT_D] [NAT_D]
2012-05-15 18:01:15 Default (SA Vyatta-P1) SEND phase 1 Main Mode [HASH] [ID]
2012-05-15 18:01:15 Default (SA Vyatta-P1) RECV phase 1 Main Mode [HASH] [ID]
2012-05-15 18:01:15 Default (SA Vyatta-P1) RECV phase 2 Quick Mode [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [ID]
2012-05-15 18:01:15 Default (SA Vyatta-Tunnel1-P2) SEND phase 2 Quick Mode [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [ID]
2012-05-15 18:01:15 Default (SA Vyatta-Tunnel1-P2) SEND phase 2 Quick Mode [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [ID]
```

Doc.Ref	tgbvpn_cg-vyatta-router-psk-en
Doc.version	Jul 2012
VPN version	5.x

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

	- —						
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)		
I							
🖽 Fr an	ne 1 (142 k	ovtes on wire.	142 bytes captur		2		
🖽 Ethe	Ethernet II, Src: 00:50:04;ad:f2:73, Dst: 00:10:b5:07:2f:ff						

Doc.Ref	tgbvpn_cg-vyatta-router-psk-en
Doc.version	Jul 2012
VPN version	5.x

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

115315Default (SA CNXVPN1-P1) SEND phase 1 Main Mode[SA][VID]115317Default (SA CNXVPN1-P1) RECV phase 1 Main Mode[SA][VID]115317Default (SA CNXVPN1-P1) SEND phase 1 Main Mode[KEY][NONCE]115319Default (SA CNXVPN1-P1) RECV phase 1 Main Mode[KEY][NONCE]115319Default (SA CNXVPN1-P1) SEND phase 1 Main Mode[ID][HASH][NOTIFY]115319Default (SA CNXVPN1-P1) SEND phase 1 Main Mode[ID][HASH][NOTIFY]115319Default 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 (SA CNXVPN1-P1) RECV 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.

THECOMPONIA 13014010	Doc.Ref	tgbvpn_cg-vyatta-router-psk-en
	Doc.version	Jul 2012
	VPN version	5.x

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][NON [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 CNXVPN1-CNXVPN1-P2) 115915 Default (SA 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 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
                                   CNXVPN1-CNXVPN1-P2)
                                                                           phase
122626
            Default
                          (SA
                                                                 SEND
                                                                                             Ouick
                                                                                                        Mode
                                                                                       2
[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

THEGREEDBOU	Doc.Ref	tgbvpn_cg-vyatta-router-psk-en
	Doc.version	Jul 2012
	VPN version	5.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.

THEGREEDBOU	Doc.Ref	tgbvpn_cg-vyatta-router-psk-en
	Doc.version	Jul 2012
	VPN version	5.x

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 by email at <u>sales@thegreenbow.com</u>

Secure, Strong, Simple.

TheGreenBow Security Software