

TheGreenBow IPsec VPN Client

Configuration Guide

Cisco RVS4000

Website: www.thegreenbow.com
Contact: support@thegreenbow.com

Table of Contents

1	Introduction	3
1.1	Goal of this document.....	3
1.2	VPN Network topology	3
1.3	CISCO RVS4000 Restrictions.....	3
1.4	CISCO RVS4000 VPN Gateway.....	3
1.5	CISCO RVS4000 VPN Gateway product info.....	3
2	CISCO RVS4000 VPN configuration.....	4
3	TheGreenBow IPsec VPN Client configuration	5
3.1	VPN Client Phase 1 (IKE) Configuration	5
3.2	VPN Client Phase 2 (IPsec) Configuration	6
3.3	Open IPsec VPN tunnels.....	6
4	Tools in case of trouble.....	7
4.1	A good network analyser: Wireshark.....	7
5	VPN IPsec Troubleshooting.....	8
5.1	“PAYLOAD MALFORMED” error (wrong Phase 1 [SA])	8
5.2	“INVALID COOKIE” error	8
5.3	“no keystate” error	8
5.4	“received remote ID other than expected” error	8
5.5	“NO PROPOSAL CHOSEN” error	9
5.6	“INVALID ID INFORMATION” error	9
5.7	I clicked on “Open tunnel”, but nothing happens.	9
5.8	The VPN tunnel is up but I can’t ping !	10
6	Contacts	11

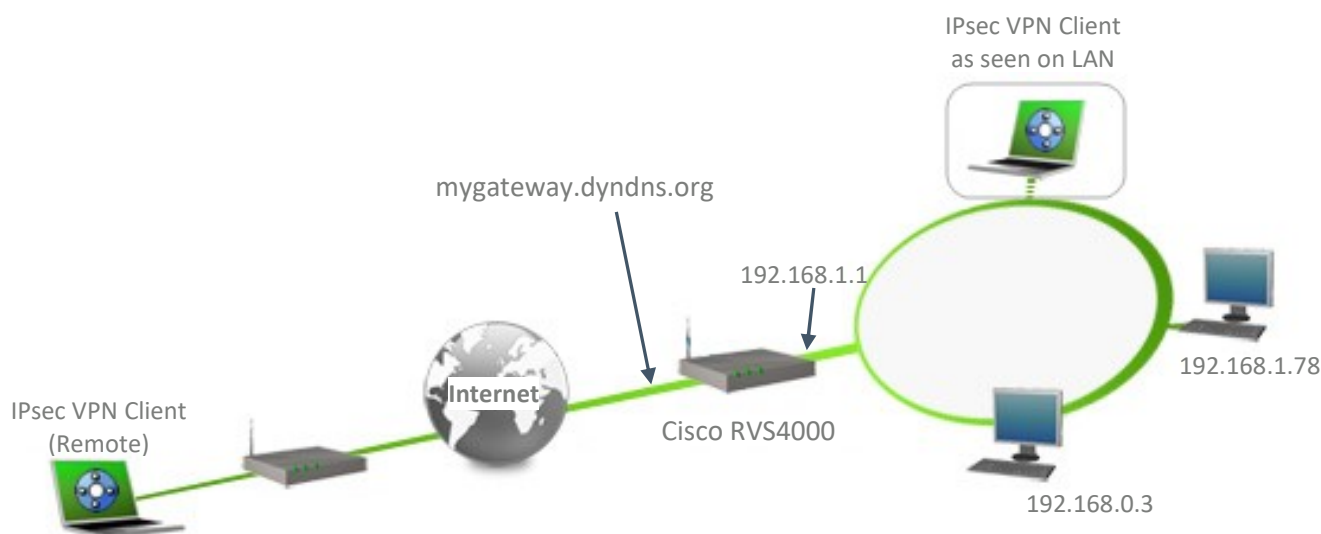
1 Introduction

1.1 Goal of this document

This configuration guide describes how to configure TheGreenBow IPsec VPN Client software with a CISCO RVS4000 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 CISCO RVS4000 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 CISCO RVS4000 Restrictions

No known restrictions.

1.4 CISCO RVS4000 VPN Gateway

Our tests and VPN configuration have been conducted with CISCO RVS4000.

1.5 CISCO RVS4000 VPN Gateway product info

It is critical that users find all necessary information about CISCO RVS4000 VPN Gateway. All product info, User Guide and knowledge base for the CISCO RVS4000 VPN Gateway can be found on the CISCO RVS4000 website: <http://www.cisco.com>

CISCO RVS4000 Product page

<https://www.cisco.com/c/en/us/support/routers/rvs4000-4-port-gigabit-security-router-vpn/model.html>

CISCO RVS4000 User Guide

https://www.cisco.com/c/dam/en/us/td/docs/routers/csbr/rvs4000/administration/Localization/French/rvs4000_ag_OL-23752.pdf

2 CISCO RVS4000 VPN configuration

This section describes how to build an IPsec VPN configuration with your CISCO RVS4000 VPN router. Once connected to your CISCO RVS4000 VPN gateway, you must select “VPN” and “IPSec VPN” tabs.

The screenshot displays the configuration interface for a CISCO RVS4000 VPN router. On the left is a navigation menu with the following items: Setup, Firewall, ProtectedLink, VPN (highlighted), Summary, IPSec VPN (highlighted), VPN Client Accounts, VPN Passthrough, QoS, Administration, IPS, L2 Switch, and Status. The main content area is titled "IPSec VPN" and contains several configuration sections:

- Select Tunnel Entry:** A dropdown menu set to "Tunnel1", with "Delete" and "Summary" buttons.
- IPSec VPN Tunnel:** Radio buttons for "Enable" (selected) and "Disable".
- Tunnel Name:** A text field containing "Tunnel1".
- Local Group Setup:**
 - Local Security Gateway Type:** A dropdown menu set to "IP Only".
 - IP address:** Four empty input boxes.
 - Local Security Group Type:** A dropdown menu set to "Subnet".
 - IP Address:** Four input boxes containing "192", "168", "1", and "0".
 - Subnet Mask:** Four input boxes containing "255", "255", "255", and "0".
- Remote Group Setup:**
 - Remote Security Gateway Type:** A dropdown menu set to "IP Only".
 - IP address:** A dropdown menu and four empty input boxes.
 - Remote Security Group Type:** A dropdown menu set to "IP addr".
 - IP Address:** Four input boxes containing "192", "168", "20", and "1".
- IPSec Setup:**
 - Keying Mode:** A dropdown menu set to "IKE with Preshared Key".
 - Phase 1:**
 - Encryption:** A dropdown menu set to "3DES".
 - Authentication:** A dropdown menu set to "MD5".
 - Group:** A dropdown menu set to "768-bit".
 - Key Lifetime:** An input box containing "28800" followed by "sec".
 - Phase 2:**
 - Encryption:** A dropdown menu set to "3DES".
 - Authentication:** A dropdown menu set to "MD5".
 - Perfect Forward Secrecy:** A dropdown menu set to "Enable".
 - Preshared Key:** A text field containing "0123456789".
 - Group:** A dropdown menu set to "768-bit".
 - Key Lifetime:** An input box containing "3600" followed by "sec".

Click on Advanced + button and enable NAT-Traversal

3 TheGreenBow IPsec VPN Client configuration

This section describes the required configuration to connect to a CISCO RVS4000 VPN router via VPN connections.

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

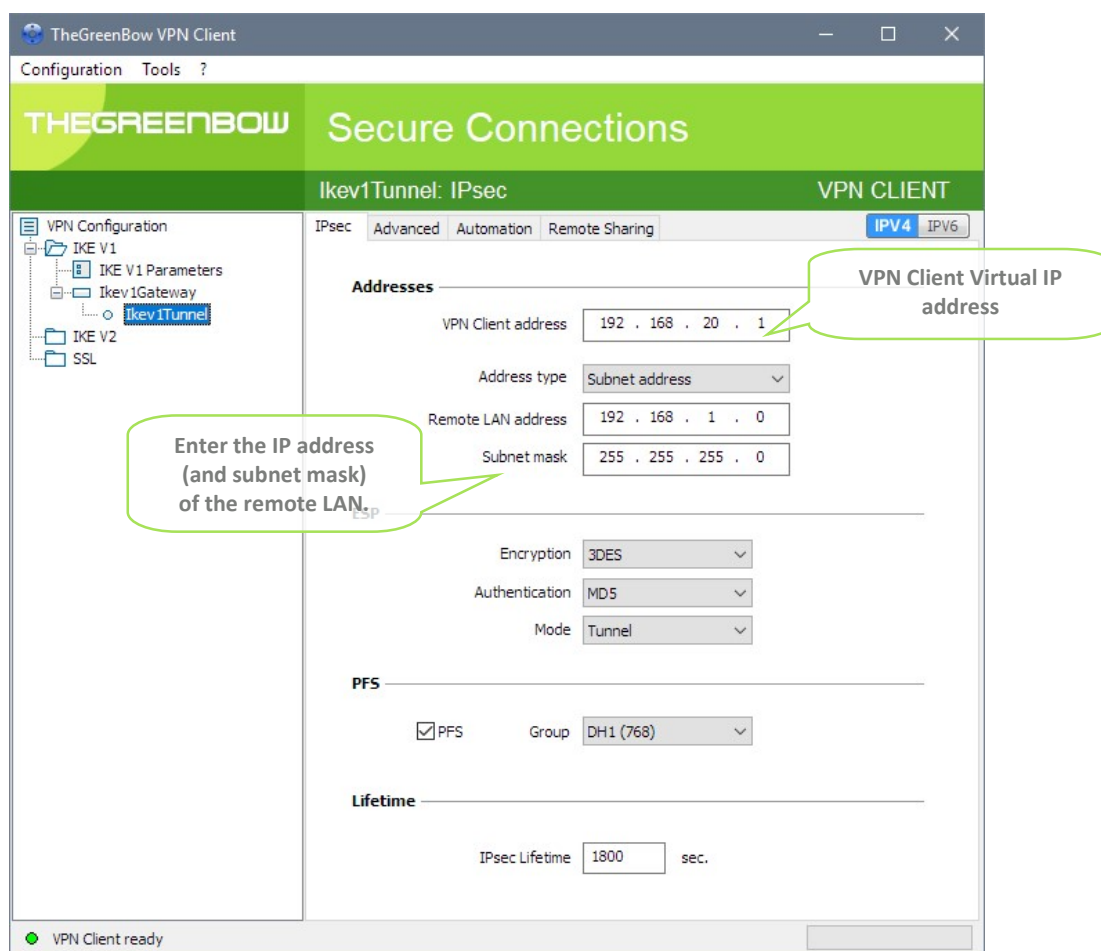
3.1 VPN Client Phase 1 (IKE) Configuration

The screenshot shows the 'TheGreenBow VPN Client' window with the 'Secure Connections' tab selected. The left sidebar shows a tree view of the configuration, with 'IKE V1' expanded and 'Ikev1Gateway' selected. The main area displays the 'Ikev1Gateway: Authentication' configuration. The 'Remote Gateway' section has 'Interface' set to 'Any' and 'Remote Gateway' set to 'mygateway.dyndns.org'. A callout bubble points to the 'Remote Gateway' field with the text: 'The remote VPN Gateway IP address is either an explicit IP address or a DNS Name'. The 'Authentication' section has 'Preshared Key' selected, with a 'Confirm' field showing '0123456789'. A callout bubble points to the 'Confirm' field with the text: '0123456789'. The 'X-Auth' section has 'Enabled' checked, with 'X-Auth Popup' also checked. The 'Cryptography' section has 'Encryption' set to '3DES', 'Authentication' set to 'MD5', and 'Key Group' set to 'DH1 (768)'. At the bottom, a status bar shows 'VPN Client ready'.

Phase 1 configuration

This configuration is one example of what can be accomplished in term of User Authentication. You may want to refer to either the CISCO RVS4000v1 router user guide or TheGreenBow IPsec VPN Client software User Guide for more details on User Authentication options.

3.2 VPN Client Phase 2 (IPsec) Configuration



Phase 2 Configuration

3.3 Open IPsec VPN tunnels

Once both CISCO RVS4000 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/ Double click on your Phase2 tunnel name or Click "Open" button in Connection panel to open tunnel.
- 3/ 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 CISCO RVS4000 VPN router.

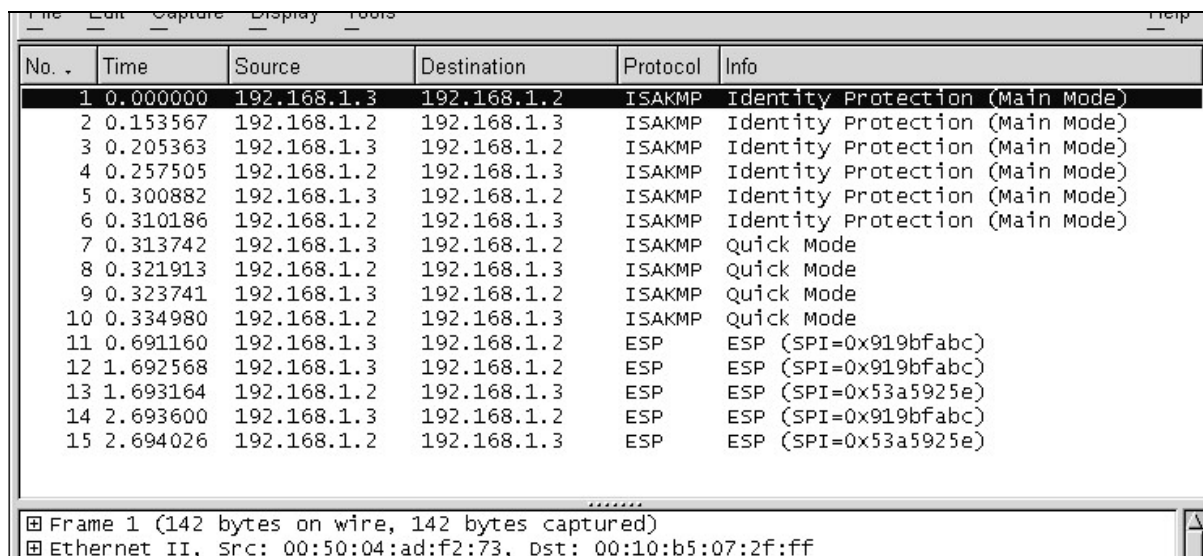
```
20110215 141513 Default phase 1 done: initiator id /C=fr/ST=idf/L=paris/O=bloodzonard/OU=series
20110215 141513 Default (SA gateway1-tunnel1-P2) SEND phase 2 Quick Mode [HASH] [SA] [N
20110215 141514 Default (SA gateway1-tunnel1-P2) RECV phase 2 Quick Mode [HASH] [SA] [N
20110215 141514 Default (SA gateway1-tunnel1-P2) SEND phase 2 Quick Mode [HASH]
20110215 141524 Default (SA gateway1-P1) RECV Informational [HASH] [NOTIFY] type DPD_R_
20110215 141524 Default (SA gateway1-P1) SEND Informational [HASH] [NOTIFY] type DPD_R_
20110215 141534 Default (SA gateway1-P1) SEND Informational [HASH] [DELETE]
20110215 141534 Default <gateway1-tunnel1-P2> deleted
20110215 141534 Default (SA gateway1-P1) SEND Informational [HASH] [DELETE]
```

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 www.wireshark.org. It can be used to follow protocol exchange between two devices. For installation and use details, read its specific documentation (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 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

```
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 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 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 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
```

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
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
```

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 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 (www.wireshark.org) 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: www.thegreenbow.com

Technical support by email at: support@thegreenbow.com

Sales contacts by email at: sales@thegreenbow.com

Secure, Strong, Simple

TheGreenBow Security Software