TheGreenBow IPSec VPN Client

Configuration Guide

NetGear FVS 318

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

Table of contents

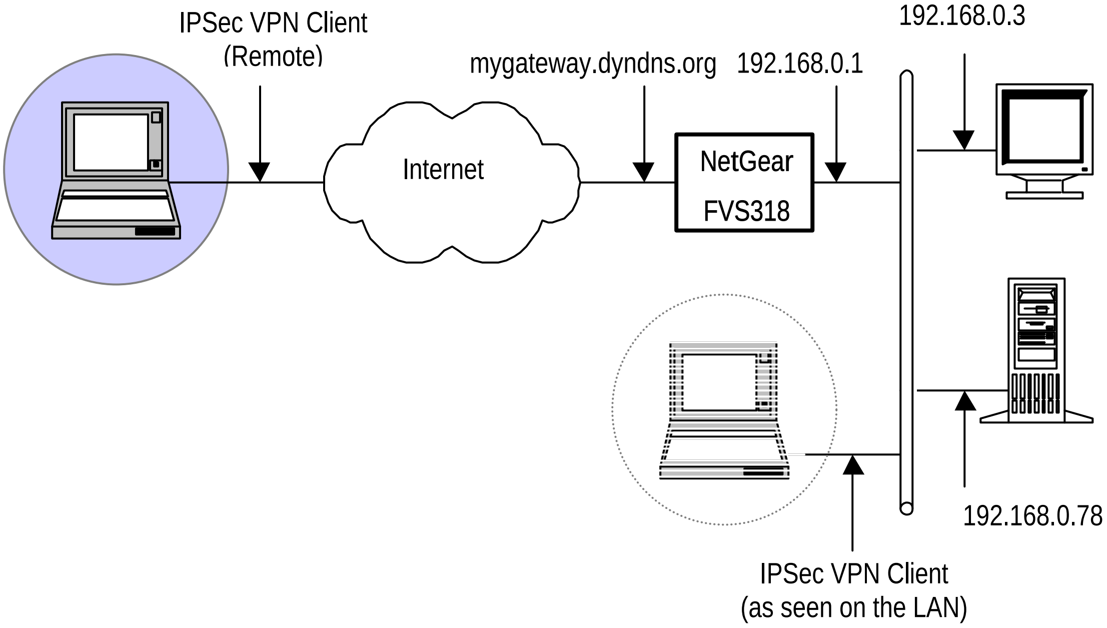
1 Introduction

1.1 Goal of this document

This configuration guide describes how to configure TheGreenBow IPSec VPN Client with a Netgear FVS318 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 Netgear FVS318 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 Netgear FVS318 Restrictions

No known restriction.

2 NetGear FVS 318 VPN Configuration

This section describes how to build an IPSec VPN configuration with your Netgear FVS318 VPN router.

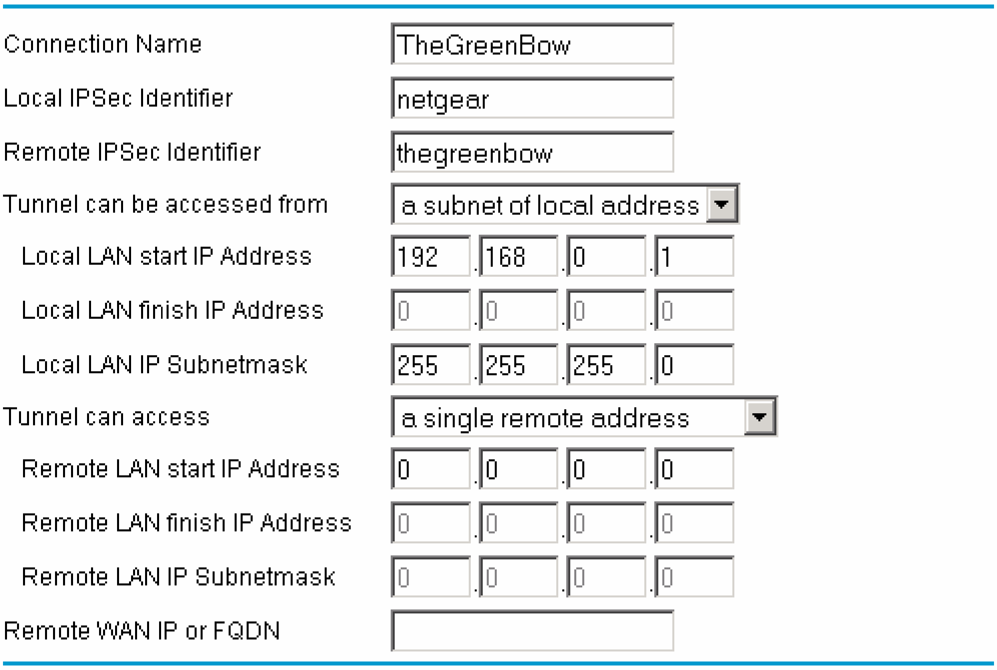
Once connected to your Netgear VPN gateway, you must select "**VPN Setting**" link in order to change NetGear FVS318 VPN configuration.

The first settings show:

- Phase 1 identities (Local and Remote IPsec Identifier)
- Phase 2 identities (LAN IP address and Remote LAN IP address).

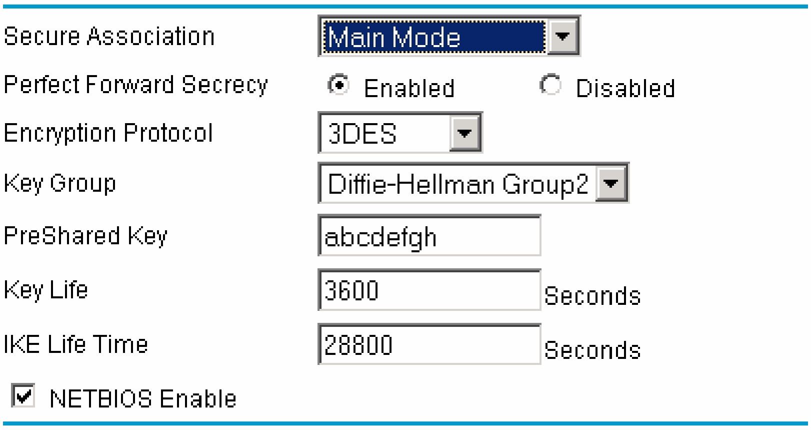
The "**Tunnel can be accessed**" value is local LAN behind the Netgear FVS318. You must select "**a subnet of local address**". This setting is the VPN Client's target.

The "Tunnel can access" value is the VPN Client's address. You must select "**a single remote address**" and "0.0.0.0".



Connection Name	TheGreenBow
Local IPSec Identifier	netgear
Remote IPSec Identifier	thegreenbow
Tunnel can be accessed from	a subnet of local address
Local LAN start IP Address	192 . 168 . 0 . 1
Local LAN finish IP Address	0 . 0 . 0 . 0
Local LAN IP Subnetmask	255 . 255 . 255 . 0
Tunnel can access	a single remote address
Remote LAN start IP Address	0 . 0 . 0 . 0
Remote LAN finish IP Address	0 . 0 . 0 . 0
Remote LAN IP Subnetmask	0 . 0 . 0 . 0
Remote WAN IP or FQDN	

The following screen contains information about algorithms used during IKE and by ESP.



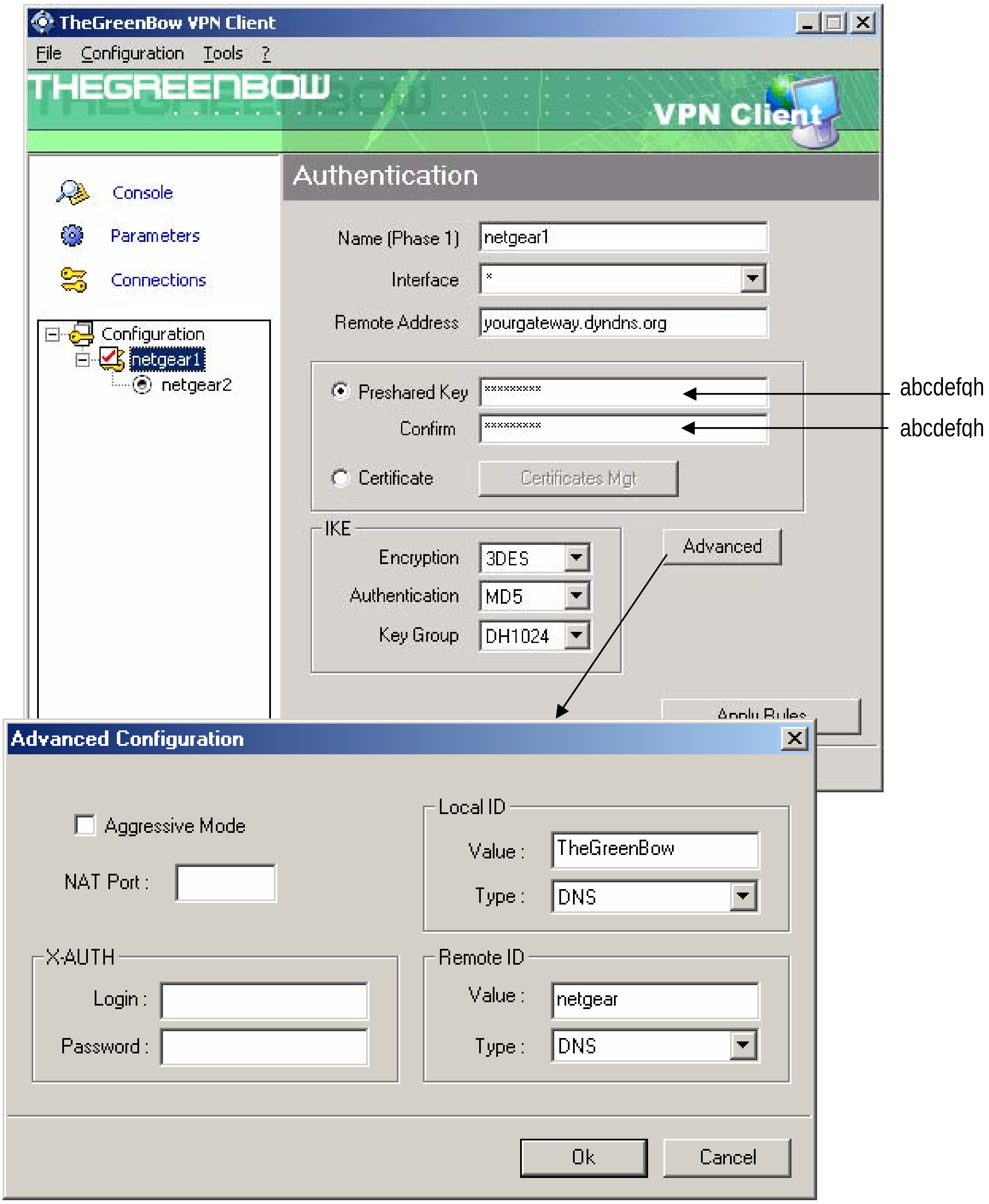
Secure Association	Main Mode
Perfect Forward Secrecy	● Enabled ○ Disabled
Encryption Protocol	3DES
Key Group	Diffie-Hellman Group2
PreShared Key	abcdefgh
Key Life	3600 Seconds
IKE Life Time	28800 Seconds

☑ NETBIOS Enable

Note: Diffie-Hellman Group2 is also known as Diffie-Hellman 1024 (DH 1024) and Diffie-Hellman Group1 as Diffie-Hellman 768.

3 TheGreenBow IPSec VPN Client configuration

3.1 VPN Client Phase 1 (IKE) Configuration



Authentication

Name (Phase 1) netgear1

Interface *

Remote Address yourgateway.dyndns.org

● Preshared Key ********* abcdefgh

Confirm ********* abcdefgh

○ Certificate

IKE

Encryption 3DES

Authentication MD5

Key Group DH1024

Advanced Configuration

□ Aggressive Mode

NAT Port :

X-AUTH

Login :

Password :

Local ID

Value : TheGreenBow

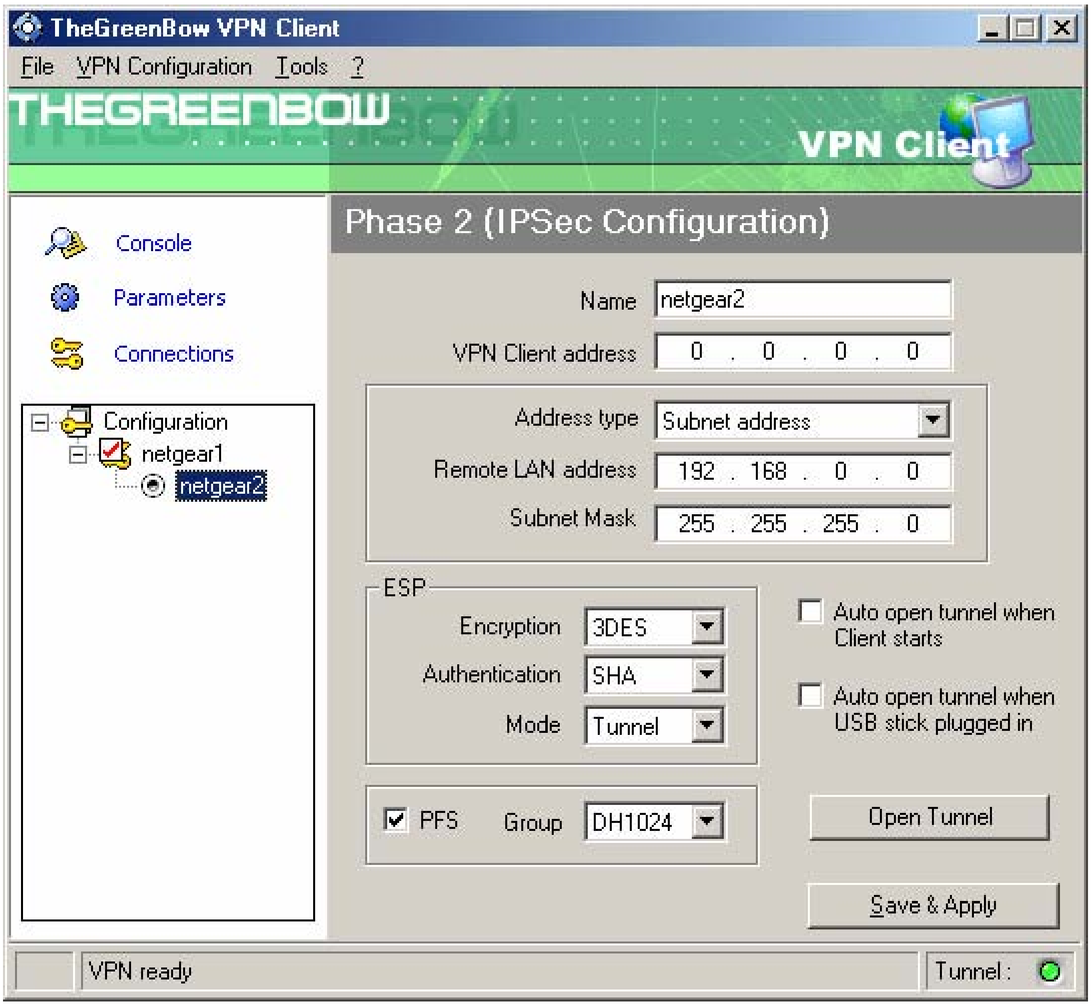
Type : DNS

Remote ID

Value : netgear

Type : DNS

3.2 VPN Client Phase 2 (IPSec) Configuration



Phase 2 (IPSec Configuration)

Name: netgear2

VPN Client address: 0 . 0 . 0 . 0

Address type: Subnet address

Remote LAN address: 192 . 168 . 0 . 0

Subnet Mask: 255 . 255 . 255 . 0

ESP

Encryption: 3DES

Authentication: SHA

Mode: Tunnel

☑ PFS Group: DH1024

□ Auto open tunnel when Client starts

□ Auto open tunnel when USB stick plugged in

VPN ready

3.3 Open IPSec VPN tunnels

Once both Netgear FVS318 router 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)

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.

4 VPN IPSec Troubleshooting

4.1 « PAYLOAD MALFORMED » error

```
114920 Default (SA FVS318-P1) SEND phase 1 Main Mode  [SA][VID]
114920 Default (SA FVS318-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.

4.2 « 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.

4.3 « no keystate » error

```
115315 Default (SA FVS318-P1) SEND phase 1 Main Mode  [SA][VID]
115317 Default (SA FVS318-P1) RECV phase 1 Main Mode  [SA][VID]
115317 Default (SA FVS318-P1) SEND phase 1 Main Mode  [KEY][NONCE]
115319 Default (SA FVS318-P1) RECV phase 1 Main Mode  [KEY][NONCE]
115319 Default (SA FVS318-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.

4.4 « received remote ID other than expected » error

```
120348 Default (SA FVS318-P1) SEND phase 1 Main Mode  [SA][VID]
120349 Default (SA FVS318-P1) RECV phase 1 Main Mode  [SA][VID]
120349 Default (SA FVS318-P1) SEND phase 1 Main Mode  [KEY][NONCE]
120351 Default (SA FVS318-P1) RECV phase 1 Main Mode  [KEY][NONCE]
120351 Default (SA FVS318-P1) SEND phase 1 Main Mode  [ID][HASH][NOTIFY]
120351 Default (SA FVS318-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.

4.5 « NO PROPOSAL CHOSEN » error

```
115911 Default (SA FVS318-P1) SEND phase 1 Main Mode  [SA][VID]
115913 Default (SA FVS318-P1) RECV phase 1 Main Mode  [SA][VID]
115913 Default (SA FVS318-P1) SEND phase 1 Main Mode  [KEY][NONCE]
115915 Default (SA FVS318-P1) RECV phase 1 Main Mode  [KEY][NONCE]
115915 Default (SA FVS318-P1) SEND phase 1 Main Mode  [ID][HASH][NOTIFY]
115915 Default (SA FVS318-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    FVS318-FVS318-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 FVS318-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 FVS318-P1) SEND phase 1 Main Mode  [SA][VID]
115911 Default RECV Informational  [NOTIFY] with NO_PROPOSAL_CHOSEN error
```

4.6 « INVALID ID INFORMATION » error

```
122623 Default (SA FVS318-P1) SEND phase 1 Main Mode  [SA][VID]
122625 Default (SA FVS318-P1) RECV phase 1 Main Mode  [SA][VID]
122625 Default (SA FVS318-P1) SEND phase 1 Main Mode  [KEY][NONCE]
122626 Default (SA FVS318-P1) RECV phase 1 Main Mode  [KEY][NONCE]
122626 Default (SA FVS318-P1) SEND phase 1 Main Mode  [ID][HASH][NOTIFY]
122626 Default (SA FVS318-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    FVS318-FVS318-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 FVS318-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).

4.7 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).

4.8 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.

5 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