



 TheGreenBow IPSec VPN Client
Configuration Guide
Apliware firewall

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

Contact: support@thegreenbow.com

Table of contents

1	Introduction	0
1.1	Goal of this document	0
1.2	Network topology	0
2	Apliware VPN Configuration	0
2.1	Apliware Firewall create a new IPSec tunnel	0
2.2	Apliware Firewall port redirection	0
3	TheGreenBow IPSec VPN Client configuration	0
3.1	VPN Client Phase 1 (IKE) Configuration	0
3.2	VPN Client Phase 2 (IPSec) Configuration	0
3.3	Open IPSec VPN tunnels	0
4	VPN IPSec Troubleshooting	0
4.1	« PAYLOAD MALFORMED » error	0
4.2	« INVALID COOKIE » error	0
4.3	« no keystate » error	0
4.4	« Received remote ID other than expected » error	0
4.5	« NO PROPOSAL CHOSEN » error	0
4.6	« INVALID ID INFORMATION » error	0
4.7	I clicked on "Open tunnel", but nothing happens.	0
4.8	The VPN tunnel is up but I can't ping !	0
5	Contacts	0

1 Introduction

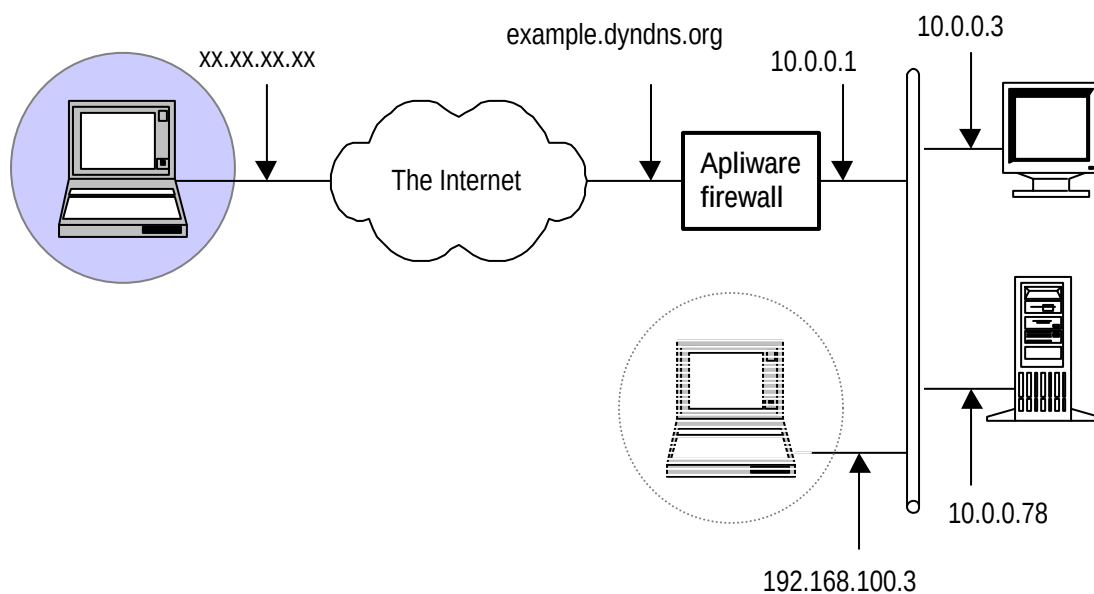
1.1 Goal of this document

This document describes how to configure an Apliware firewall such as Multicom Ethernet II and TheGreenBow VPN Client in order to establish a VPN tunnel between them. Apliware version used in this document is 3.7.

1.2 Network topology

In our example, we will connect TheGreenBow VPN client to the LAN behind the Apliware Firewall Multicom. The VPN client can be connected to the Internet by a dialup connection from an ISP. It supports also NAT-T. A VPN connection can be established also from a LAN.

The client will have a virtual IP address in the remote LAN. All the addresses in this document are given for example purpose.

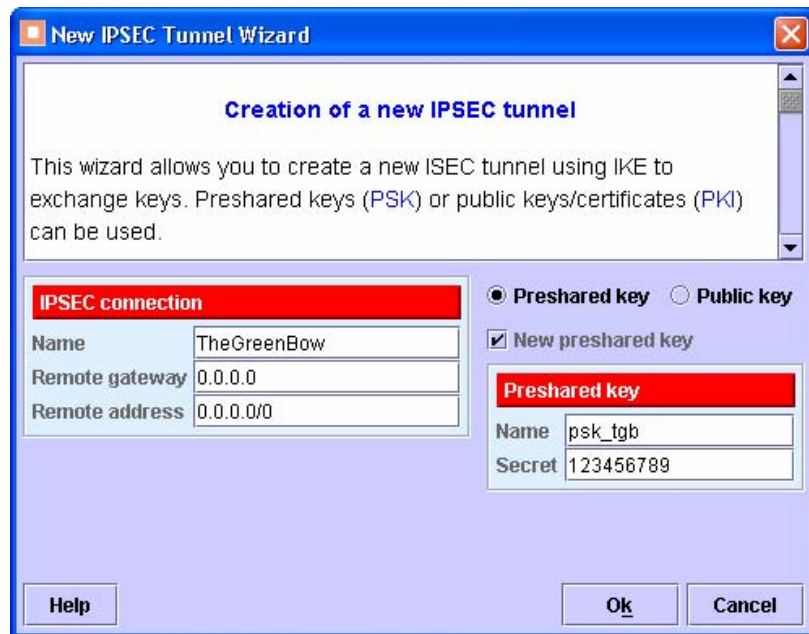


2 Apliware VPN Configuration

This section describes how to build an IPSec VPN configuration with your Apliware Firewall Multicom VPN router.

2.1 Apliware Firewall create a new IPSec tunnel

Once connected to your VPN gateway, you must create a new IPSEC tunnel. In Apliware Firewall configurator, select menu “Wizard” and “New IPsec Tunnel...”. The following values are given as example:



New IPSEC Tunnel Wizard

Creation of a new IPSEC tunnel

This wizard allows you to create a new ISEC tunnel using IKE to exchange keys. Preshared keys (PSK) or public keys/certificates (PKI) can be used.

IPSEC connection

Name: TheGreenBow
 Remote gateway: 0.0.0.0
 Remote address: 0.0.0.0/0

☒ Preshared key ☐ Public key

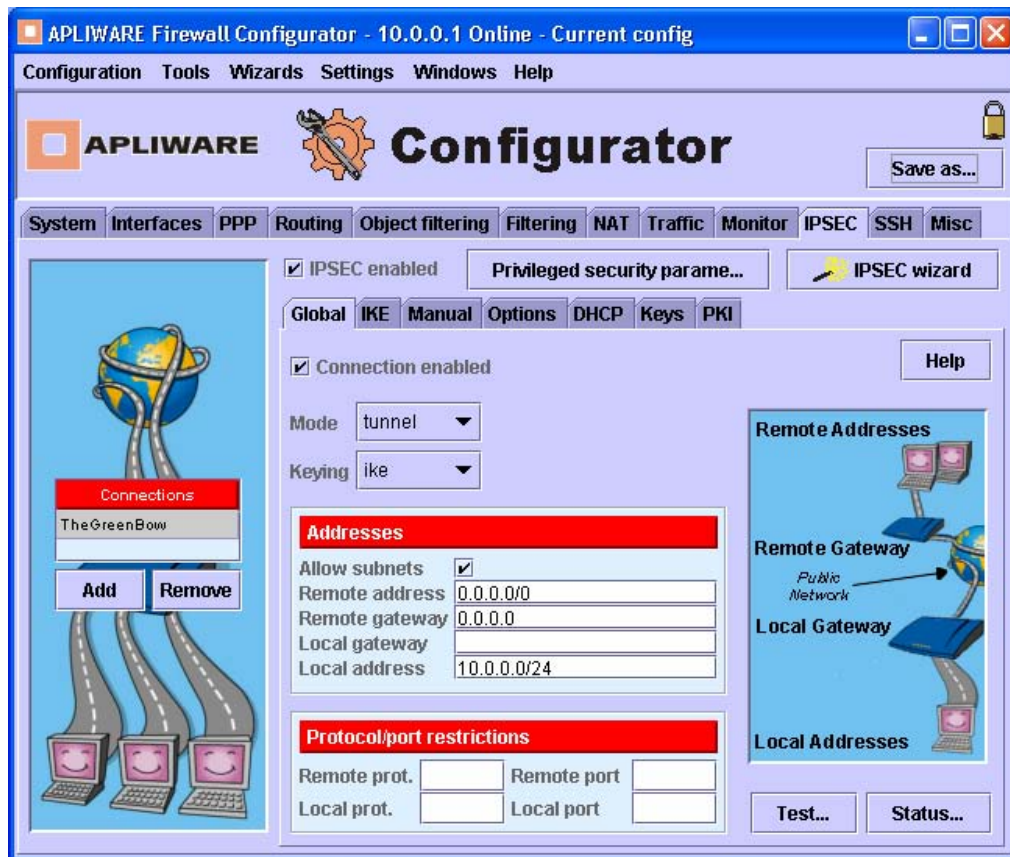
☒ New preshared key

Preshared key

Name: psk_tgb
 Secret: 123456789

Help Ok Cancel

Once finished, you can find these settings in “IPSEC” Tabs. You must check “Allow subnets” if you want to allow multiple users to use your new IPsec connection.

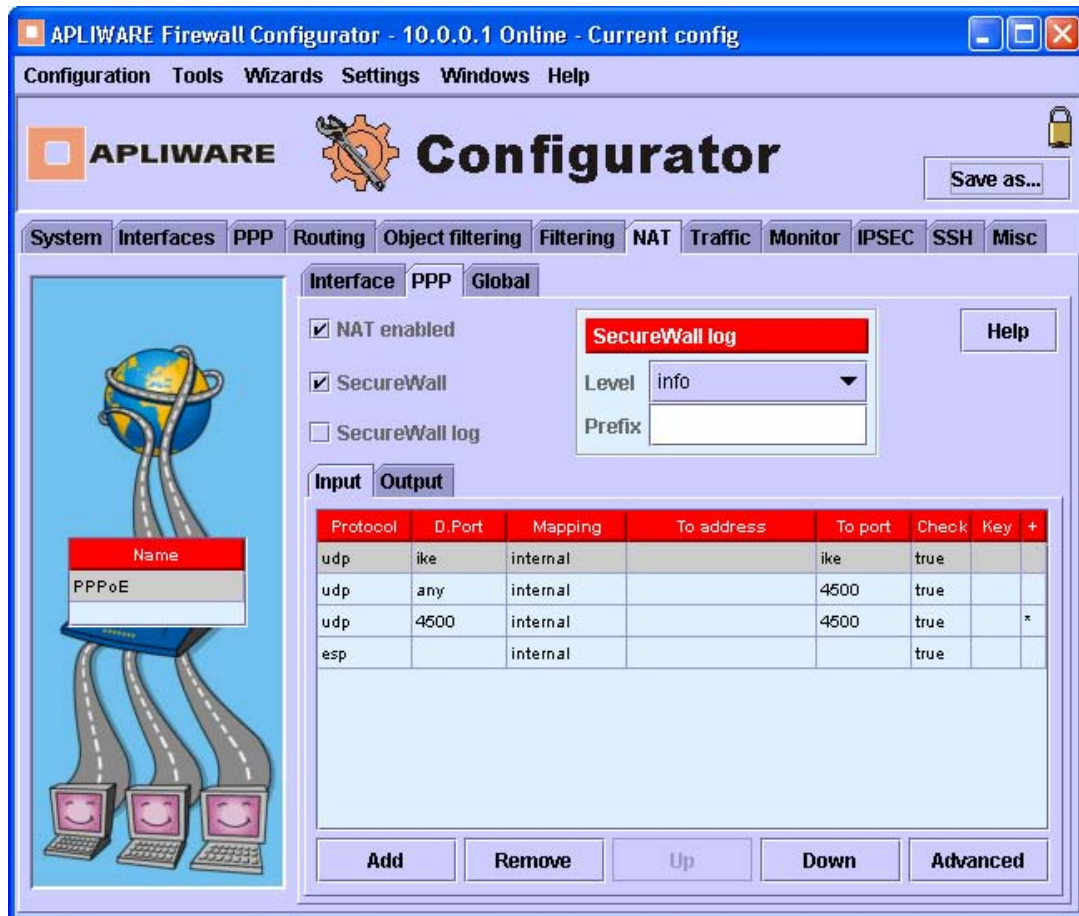


2.2 Apliware Firewall port redirection

Once the tunnel is created, you must configure port redirection. The VPN Client uses UDP port 500 and 4500. It uses also ESP protocol for encrypted packets.

In Apliware Firewall Configurator, select "NAT" tab, then "PPP" tab and "input" tab. You need to add four internal mappings:

- UDP port 500 to UDP port 500
- Any UDP to UDP 4500
- UDP 4500 to UDP 4500
- ESP



3 TheGreenBow IPsec VPN Client configuration

3.1 VPN Client Phase 1 (IKE) Configuration

Settings used in the Apliware Firewall Configurator, such as preshared key, must be copied in TheGreenBow VPN client settings.

TheGreenBow VPN Client

File VPN Configuration Tools ?

THEGREENBOW VPN Client

Phase 1 (Authentication)

Name: multicom

Interface: *

Remote Gateway: example.dyndns.org

☒ Preshared Key: 123456789

Confirm: 123456789

☐ Certificate: Certificates Import...

IKE

Encryption: 3DES

Authentication: SHA

Key Group: DH1024

Advanced...

Save & Apply

VPN Tunnel active

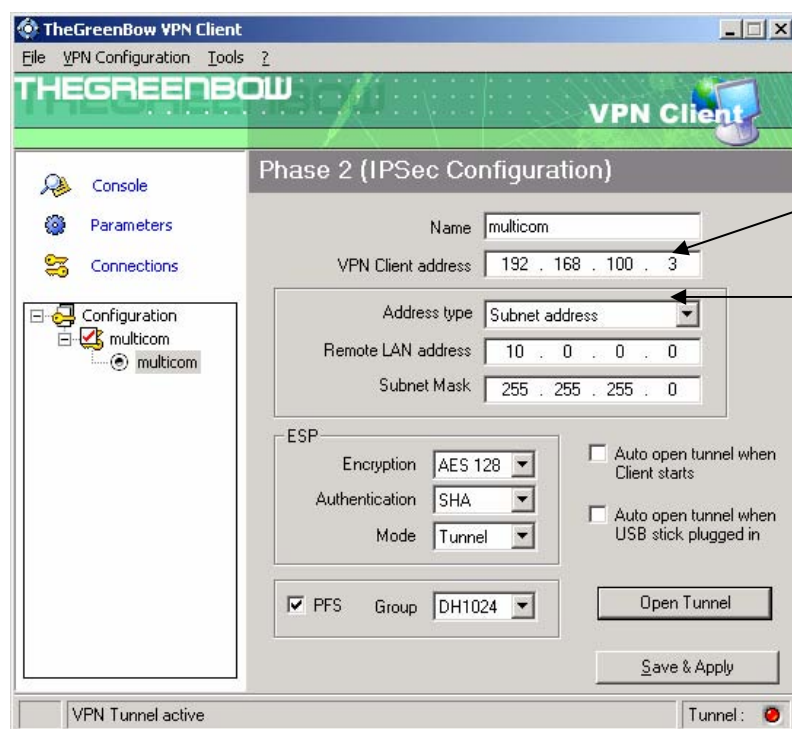
Tunnel: [Red Light]

The remote firewall IP address is either an explicit IP address, or a DNS Name

Phase 1 configuration

3.2 VPN Client Phase 2 (IPSec) Configuration

In phase 2 settings, you can use a virtual IP address or let 0.0.0.0 in VPN client address field. In that case the client will use network adapter IP address as virtual IP.



Set up here a virtual IP address.

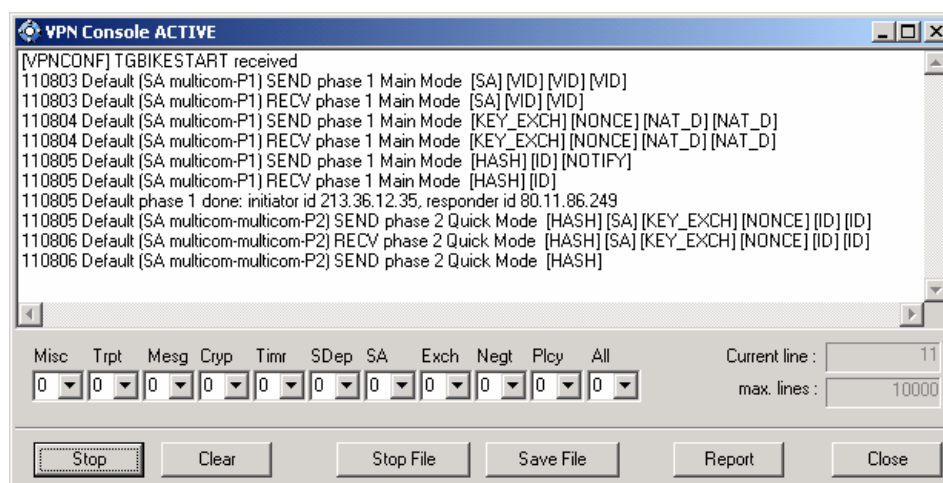
Enter the IP address (and subnet mask) of the remote LAN.

Phase 2 Configuration

3.3 Open IPSec VPN tunnels

Once both Apliware Firewall 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 MUTICOM-P1) SEND phase 1 Main Mode [SA][VID]
114920 Default (SA MUTICOM-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 MUTICOM-P1) SEND phase 1 Main Mode [SA][VID]
115317 Default (SA MUTICOM-P1) RECV phase 1 Main Mode [SA][VID]
115317 Default (SA MUTICOM-P1) SEND phase 1 Main Mode [KEY][NONCE]
115319 Default (SA MUTICOM-P1) RECV phase 1 Main Mode [KEY][NONCE]
115319 Default (SA MUTICOM-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. Concerning Apliware firewall, use a syslog client.

4.4 « Received remote ID other than expected » error

```

120348 Default (SA MUTICOM-P1) SEND phase 1 Main Mode [SA][VID]
120349 Default (SA MUTICOM-P1) RECV phase 1 Main Mode [SA][VID]
120349 Default (SA MUTICOM-P1) SEND phase 1 Main Mode [KEY][NONCE]
120351 Default (SA MUTICOM-P1) RECV phase 1 Main Mode [KEY][NONCE]
120351 Default (SA MUTICOM-P1) SEND phase 1 Main Mode [ID][HASH][NOTIFY]
120351 Default (SA MUTICOM-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) do not match what the remote endpoint is expected.

4.5 « NO PROPOSAL CHOSEN » error

```

115911 Default (SA MUTICOM-P1) SEND phase 1 Main Mode [SA][VID]
115913 Default (SA MUTICOM-P1) RECV phase 1 Main Mode [SA][VID]
115913 Default (SA MUTICOM-P1) SEND phase 1 Main Mode [KEY][NONCE]
115915 Default (SA MUTICOM-P1) RECV phase 1 Main Mode [KEY][NONCE]
115915 Default (SA MUTICOM-P1) SEND phase 1 Main Mode [ID][HASH][NOTIFY]
115915 Default (SA MUTICOM-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 MUTICOM-MUTICOM-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 MUTICOM-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 MUTICOM-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 MUTICOM-P1) SEND phase 1 Main Mode [SA][VID]
122625 Default (SA MUTICOM-P1) RECV phase 1 Main Mode [SA][VID]
122625 Default (SA MUTICOM-P1) SEND phase 1 Main Mode [KEY][NONCE]
122626 Default (SA MUTICOM-P1) RECV phase 1 Main Mode [KEY][NONCE]
122626 Default (SA MUTICOM-P1) SEND phase 1 Main Mode [ID][HASH][NOTIFY]
122626 Default (SA MUTICOM-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 MUTICOM-MUTICOM-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 MUTICOM-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").

4.7 I clicked on "Open tunnel", but nothing happens.

Read logs of each 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.

	Doc.Ref	tgbvpn_Aplware_en
	Doc.version	1.0 – Dec.2004
	VPN version	2.5x

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