TheGreenBow IPSec VPN Client

Configuration Guide

Symantec Firewall/VPN 200

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

Table of contents

1 Introduction

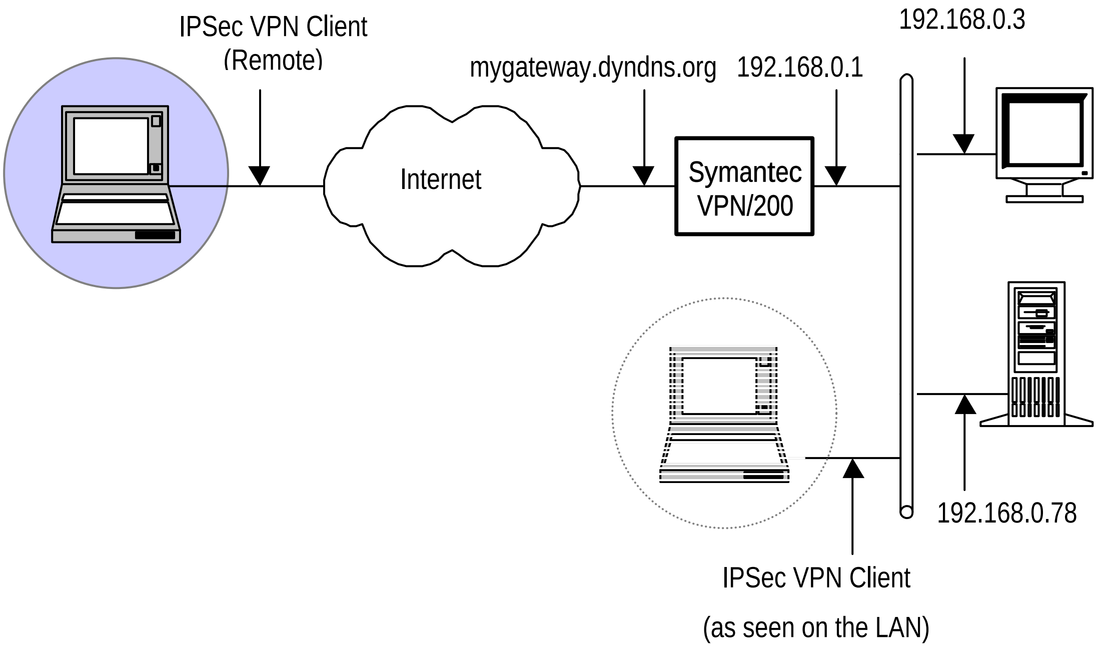
1.1 Goal of this document

This configuration guide describes how to configure TheGreenBow IPSec VPN Client with a Symantec VPN/200 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 Symantec VPN/200 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.

In our example, we will configure an IPSec VPN tunnel between a DSL device and a LAN behind a Symantec. Symantec LAN IP network address will be 192.168.0.1/24



1.3 Symantec VPN/200 Restrictions

No known restrictions.

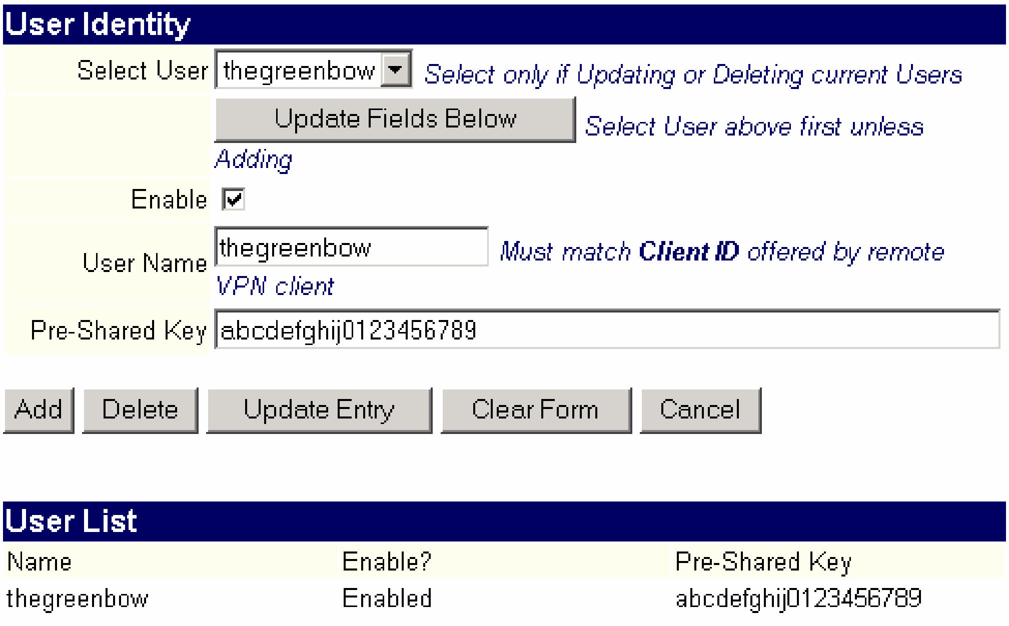
2 Symantec Firewall/VPN 200 VPN Configuration

This section describes the configuration of a Symantec Firewall/VPN 200 gateway in order to open a Client-To-Gateway tunnel with the TheGreenBow IPSec VPN Client. Read Symantec documentation for more details about this VPN gateway.

2.1 Symantec User identity

In the main web configuration page of the Symantec VPN gateway, click on "*Client Identity*". You have to set:

- the user name : thegreenbow
- a preshared key associated with this user: abcdefghij0123456789. This value must be at least 20 bytes long.



User Identity

Select User: thegreenbow *Select only if Updating or Deleting current Users*

Select User above first unless Adding

Enable ☑

User Name: thegreenbow *Must match **Client ID** offered by remote VPN client*

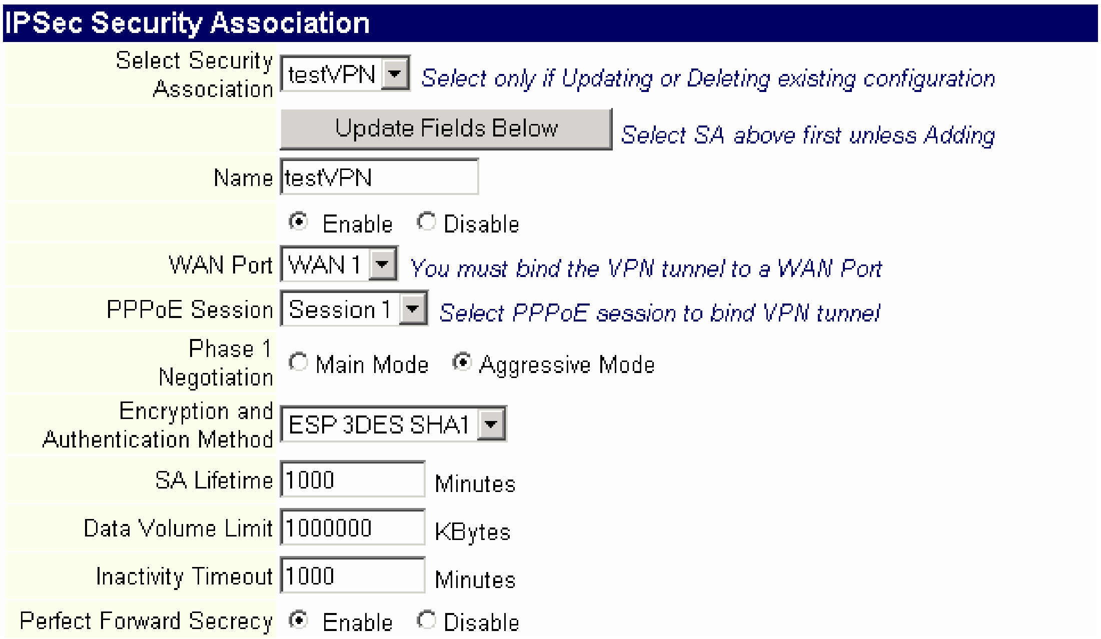
Pre-Shared Key: abcdefghij0123456789

User List

Name	Enable?	Pre-Shared Key
thegreenbow	Enabled	abcdefghij0123456789

2.2 Symantec Dynamic key

In order to enable a VPN client to get connected with the VPN gateway, a dynamic key must be configured. The following picture shows settings that can be used:



IPSec Security Association

Select Security Association: testVPN ▾ *Select only if Updating or Deleting existing configuration*

[Update Fields Below] *Select SA above first unless Adding*

Name: testVPN

● Enable ○ Disable

WAN Port: WAN 1 ▾ *You must bind the VPN tunnel to a WAN Port*

PPPoE Session: Session 1 ▾ *Select PPPoE session to bind VPN tunnel*

Phase 1 Negotiation: ○ Main Mode ● Aggressive Mode

Encryption and Authentication Method: ESP 3DES SHA1 ▾

SA Lifetime: 1000 Minutes

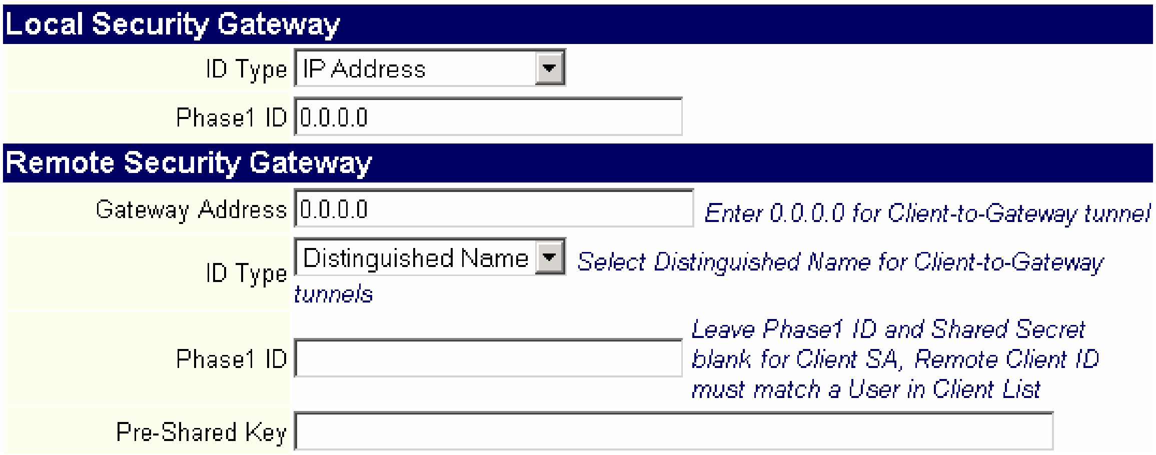
Data Volume Limit: 1000000 KBytes

Inactivity Timeout: 1000 Minutes

Perfect Forward Secrecy: ● Enable ○ Disable

Aggressive mode setting is mandatory. These settings will be reported in the IPSec VPN Client configuration interface.

Phase 1 IDs are configured in "*Local Security Gateway*" and "*Remote Security Gateway*".



Local Security Gateway

ID Type: IP Address ▾

Phase1 ID: 0.0.0.0

Remote Security Gateway

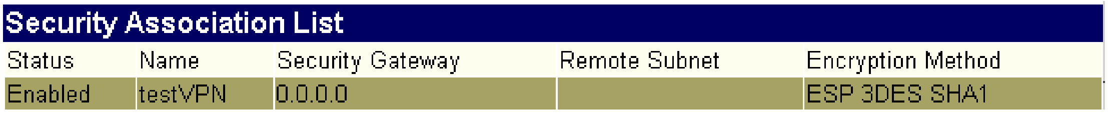
Gateway Address: 0.0.0.0 *Enter 0.0.0.0 for Client-to-Gateway tunnel*

ID Type: Distinguished Name ▾ *Select Distinguished Name for Client-to-Gateway tunnels*

Phase1 ID: *Leave Phase1 ID and Shared Secret blank for Client SA, Remote Client ID must match a User in Client List*

Pre-Shared Key:

When finished, click on "*Add*". A new line will appear in the "*Security Association List*".



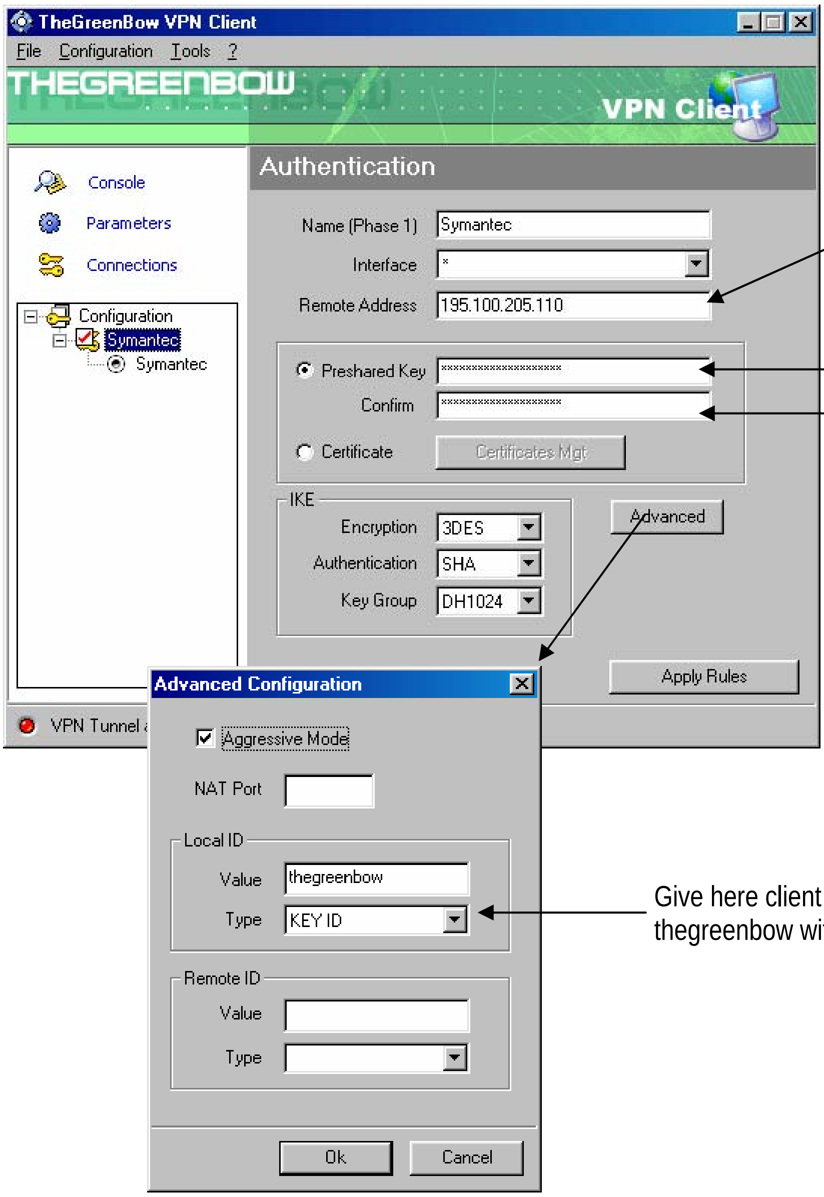
Security Association List

Status	Name	Security Gateway	Remote Subnet	Encryption Method
Enabled	testVPN	0.0.0.0		ESP 3DES SHA1

3 TheGreenBow VPN client configuration

3.1 Client Phase 1 (IKE) Configuration

Note: If the IP address of the VPN Client is automatically assigned, select Interface = " * "



Authentication

Name (Phase 1): Symantec

Interface: *

Remote Address: 195.100.205.110

● Preshared Key: ********************

Confirm: ********************

○ Certificate [Certificates Mgt]

IKE

Encryption: 3DES

Authentication: SHA

Key Group: DH1024

Advanced Configuration

☑ Aggressive Mode

NAT Port:

Local ID

Value: thegreenbow

Type: KEY ID

Remote ID

Value:

Type:

[Ok] [Cancel]

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

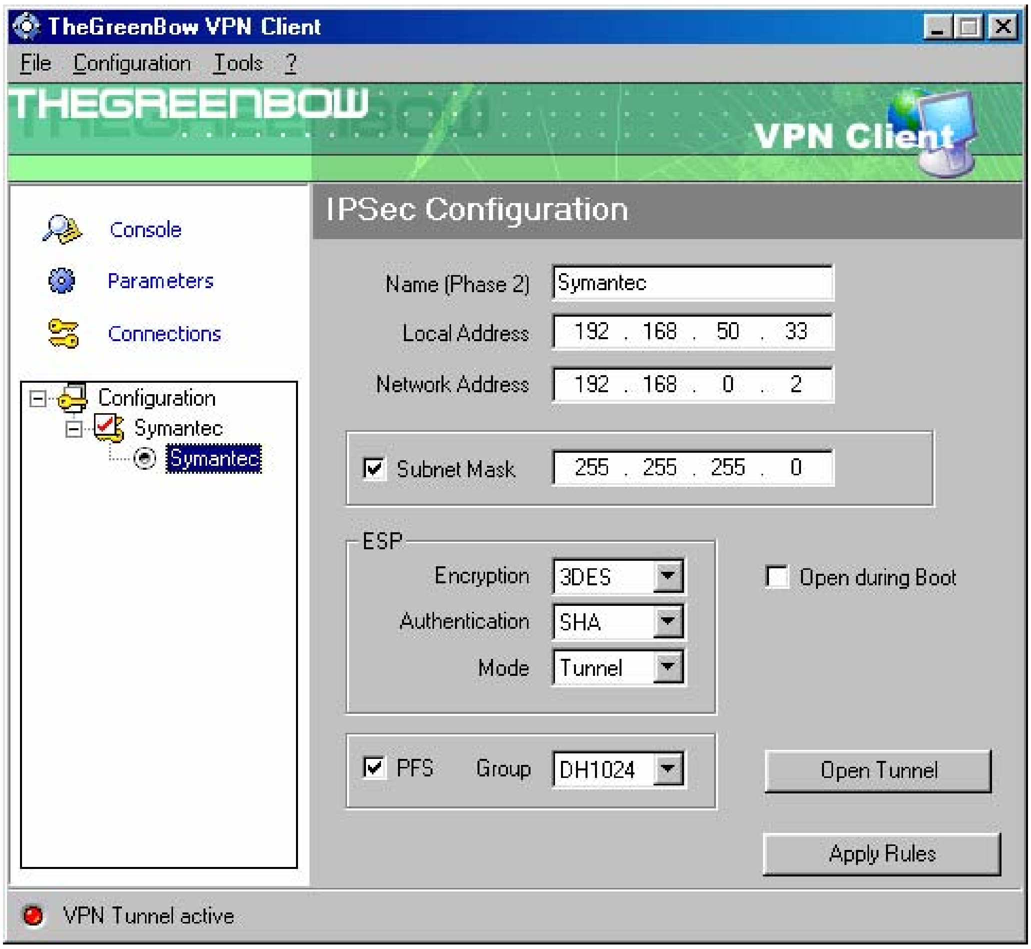
" abcdefghij0123456789"

" abcdefghij0123456789 "

Give here client identity for phase 1: thegreenbow with KEY_ID type

3.2 Phase 2 (IPSec) Configuration

IP address given in “Local Address” will not be used because Symantec Firewall/VPN 200 gateway does not support virtual IP addresses.



Name (Phase 2): Symantec

Local Address: 192 . 168 . 50 . 33

Network Address: 192 . 168 . 0 . 2

☑ Subnet Mask: 255 . 255 . 255 . 0

ESP

Encryption: 3DES

Authentication: SHA

Mode: Tunnel

□ Open during Boot

☑ PFS Group: DH1024

● VPN Tunnel active

Phase 2 Configuration

3.3 Open the IPSec VPN tunnels

Once both Symantec Firewall/VPN 200 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 "Apply Rules" 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

Those error samples have been voluntarily produced with a Linksys WRV54G, but logs and messaging shall be exactly the same with a Symantec Firewall/VPN200 VPN Gateway.

4.1 « PAYLOAD MALFORMED » error

```
114920 Default (SA WRV54G-P1) SEND phase 1 Main Mode  [SA][VID]
114920 Default (SA WRV54G-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 WRV54G-P1) SEND phase 1 Main Mode  [SA][VID]
115317 Default (SA WRV54G-P1) RECV phase 1 Main Mode  [SA][VID]
115317 Default (SA WRV54G-P1) SEND phase 1 Main Mode  [KEY][NONCE]
115319 Default (SA WRV54G-P1) RECV phase 1 Main Mode  [KEY][NONCE]
115319 Default (SA WRV54G-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 WRV54G-P1) SEND phase 1 Main Mode  [SA][VID]
120349 Default (SA WRV54G-P1) RECV phase 1 Main Mode  [SA][VID]
120349 Default (SA WRV54G-P1) SEND phase 1 Main Mode  [KEY][NONCE]
120351 Default (SA WRV54G-P1) RECV phase 1 Main Mode  [KEY][NONCE]
120351 Default (SA WRV54G-P1) SEND phase 1 Main Mode  [ID][HASH][NOTIFY]
120351 Default (SA WRV54G-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 WRV54G-P1) SEND phase 1 Main Mode  [SA][VID]
115913 Default (SA WRV54G-P1) RECV phase 1 Main Mode  [SA][VID]
115913 Default (SA WRV54G-P1) SEND phase 1 Main Mode  [KEY][NONCE]
115915 Default (SA WRV54G-P1) RECV phase 1 Main Mode  [KEY][NONCE]
115915 Default (SA WRV54G-P1) SEND phase 1 Main Mode  [ID][HASH][NOTIFY]
115915 Default (SA WRV54G-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 WRV54G-WRV54G-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 WRV54G-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 WRV54G-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 WRV54G-P1) SEND phase 1 Main Mode  [SA][VID]
122625 Default (SA WRV54G-P1) RECV phase 1 Main Mode  [SA][VID]
122625 Default (SA WRV54G-P1) SEND phase 1 Main Mode  [KEY][NONCE]
122626 Default (SA WRV54G-P1) RECV phase 1 Main Mode  [KEY][NONCE]
122626 Default (SA WRV54G-P1) SEND phase 1 Main Mode  [ID][HASH][NOTIFY]
122626 Default (SA WRV54G-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 WRV54G-WRV54G-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 WRV54G-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 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