TheGreenBow IPSec VPN Client

Configuration Guide

DWnet SAFEcon5

WebSite:	http://www.thegreenbow.com	http://www.dwnet.com.cn
Contact:	support@thegreenbow.com	service@dwnet.com.cn

Table of contents

1 Introduction 3
1.1 Goal of this document 3
1.2 VPN Network topology 3
1.3 DWnet SAFEcon5 VPN Gateway 3
2 DWnet SAFEcon5 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: ethereal 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 ! 9
6 Contacts 11

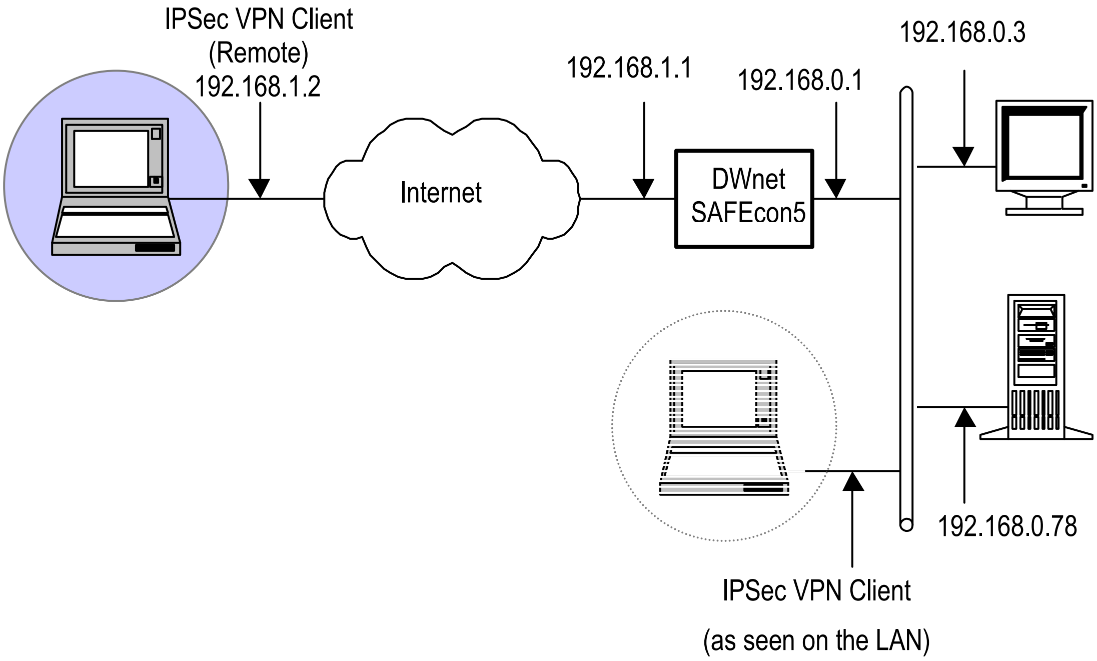
1 Introduction

1.1 Goal of this document

This configuration guide describes how to configure TheGreenBow IPSec VPN Client with a DWnet SAFEcon5 VPN 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 DWnet SAFEcon5 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.



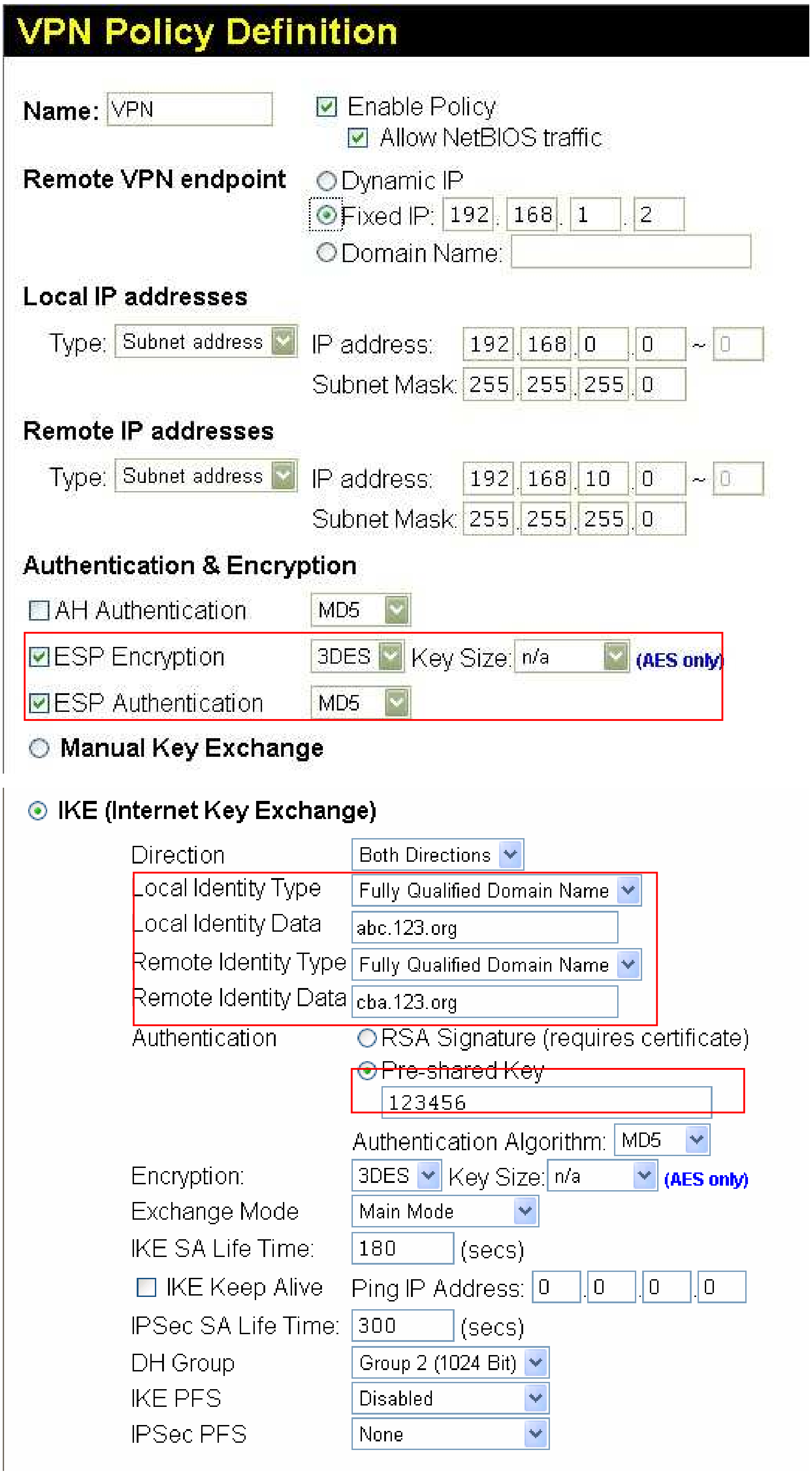
1.3 DWnet SAFEcon5 VPN Gateway

Our tests and VPN configuration have been conducted with DWnet SAFEcon5 firmware release version 100B.

2 DWnet SAFEcon5 VPN configuration

This section describes how to build an IPSec VPN configuration with your DWnet SAFEcon5 VPN router.

Once connected to your VPN gateway, you must select “VPN(IPSec)” tabs and “Add New Policy”



VPN Policy Definition

Name: VPN

☑ Enable Policy

☑ Allow NetBIOS traffic

Remote VPN endpoint

○ Dynamic IP

● Fixed IP: 192 . 168 . 1 . 2

○ Domain Name:

Local IP addresses

Type: Subnet address

IP address: 192 . 168 . 0 . 0 ~ 0

Subnet Mask: 255 . 255 . 255 . 0

Remote IP addresses

Type: Subnet address

IP address: 192 . 168 . 10 . 0 ~ 0

Subnet Mask: 255 . 255 . 255 . 0

Authentication & Encryption

☐ AH Authentication MD5

☑ ESP Encryption 3DES Key Size: n/a (AES only)

☑ ESP Authentication MD5

○ Manual Key Exchange

● IKE (Internet Key Exchange)

Direction: Both Directions

Local Identity Type: Fully Qualified Domain Name

Local Identity Data: abc.123.org

Remote Identity Type: Fully Qualified Domain Name

Remote Identity Data: cba.123.org

Authentication:

○ RSA Signature (requires certificate)

● Pre-shared Key

123456

Authentication Algorithm: MD5

Encryption: 3DES Key Size: n/a (AES only)

Exchange Mode: Main Mode

IKE SA Life Time: 180 (secs)

☐ IKE Keep Alive Ping IP Address: 0 . 0 . 0 . 0

IPSec SA Life Time: 300 (secs)

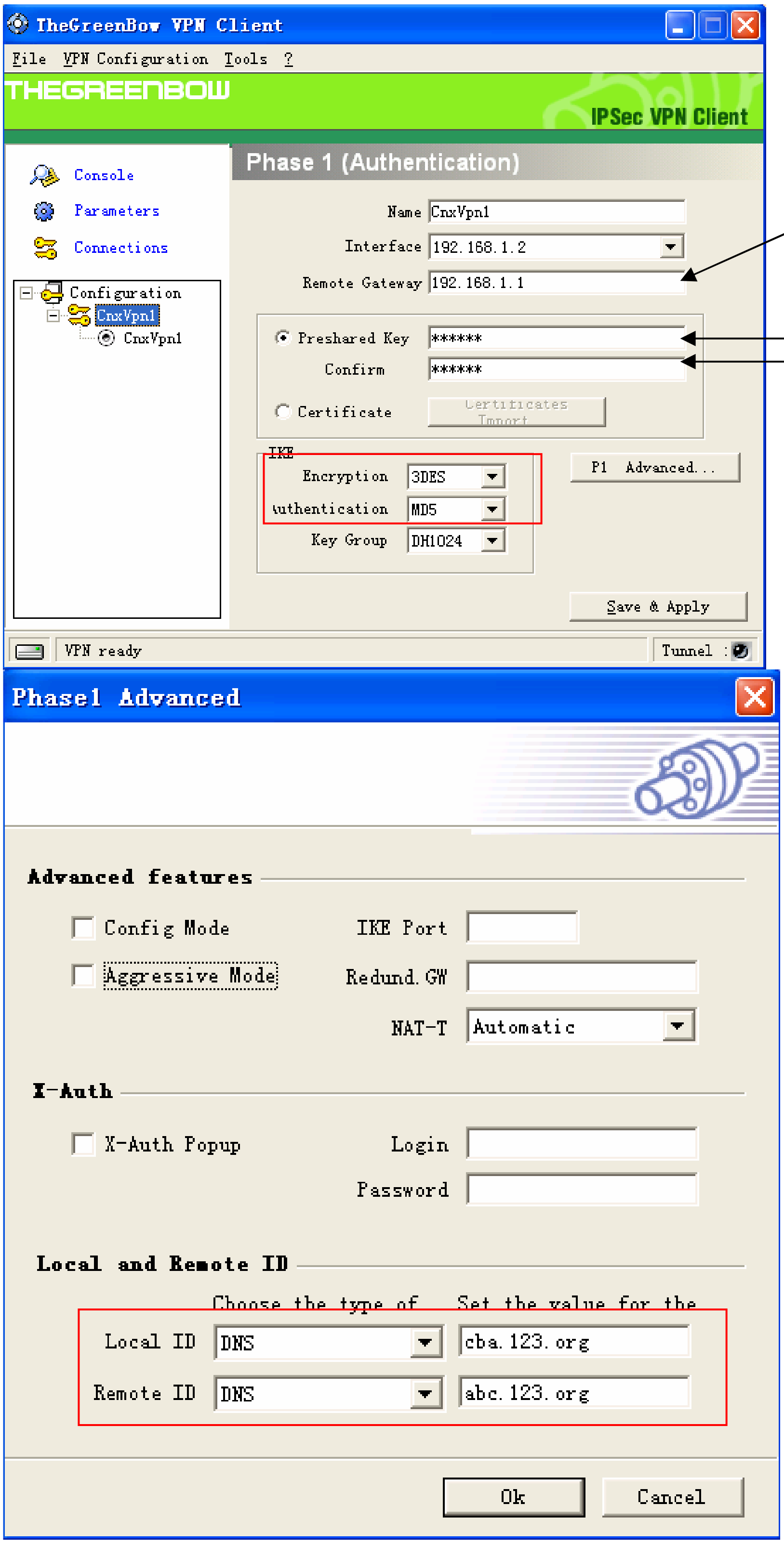
DH Group: Group 2 (1024 Bit)

IKE PFS: Disabled

IPSec PFS: None

3 TheGreenBow IPSec VPN Client configuration

3.1 VPN Client Phase 1 (IKE) Configuration



Phase 1 (Authentication)

Name CnxVpn1

Interface 192.168.1.2

Remote Gateway 192.168.1.1

● Preshared Key ******

Confirm ******

○ Certificate — Certificates Import

IKE

Encryption 3DES

uthentication MD5

Key Group DH1024

P1 Advanced...

Save & Apply

VPN ready — Tunnel :

Advanced features

□ Config Mode — IKE Port

□ Aggressive Mode — Redund. GW

NAT-T Automatic

X-Auth

□ X-Auth Popup — Login — Password

Local and Remote ID

	Choose the type of	Set the value for the
Local ID	DNS	cba.123.org
Remote ID	DNS	abc.123.org

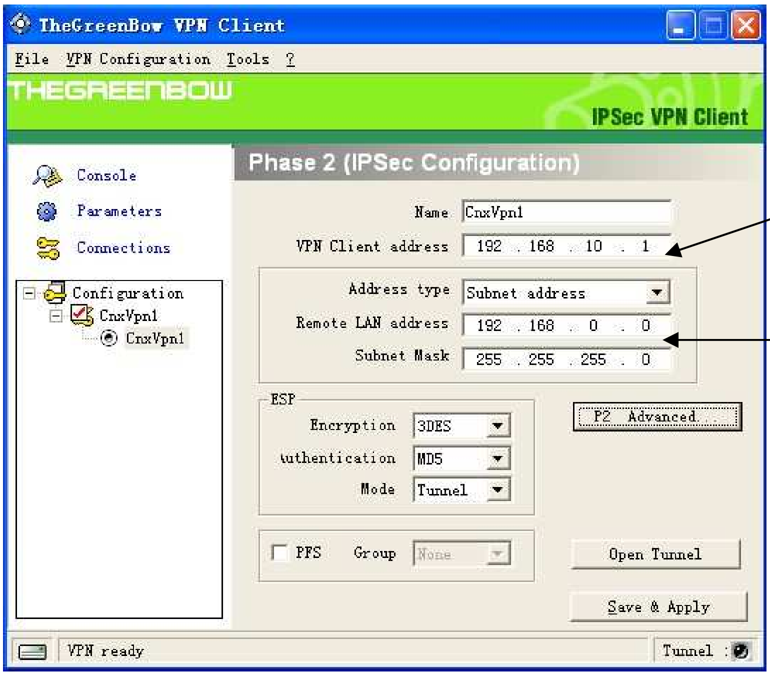
The remote VPN Gateway IP address is either an explicit IP address, or a DNS Name

123456

123456

Phase 1 configuration

3.2 VPN Client Phase 2 (IPSec) Configuration



Phase 2 (IPSec Configuration)

Name: CnxVpn1

VPN Client address: 192 . 168 . 10 . 1

Address type: Subnet address

Remote LAN address: 192 . 168 . 0 . 0

Subnet Mask: 255 . 255 . 255 . 0

ESP

Encryption: 3DES

uthentication: MD5

Mode: Tunnel

□ PFS Group: None

You may define a static virtual IP address here.

If you use 0.0.0.0, you will have error “Local-ID” is missing. It does not prevent you from establishing a tunnel

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

Phase 2 Configuration

3.3 Open IPSec VPN tunnels

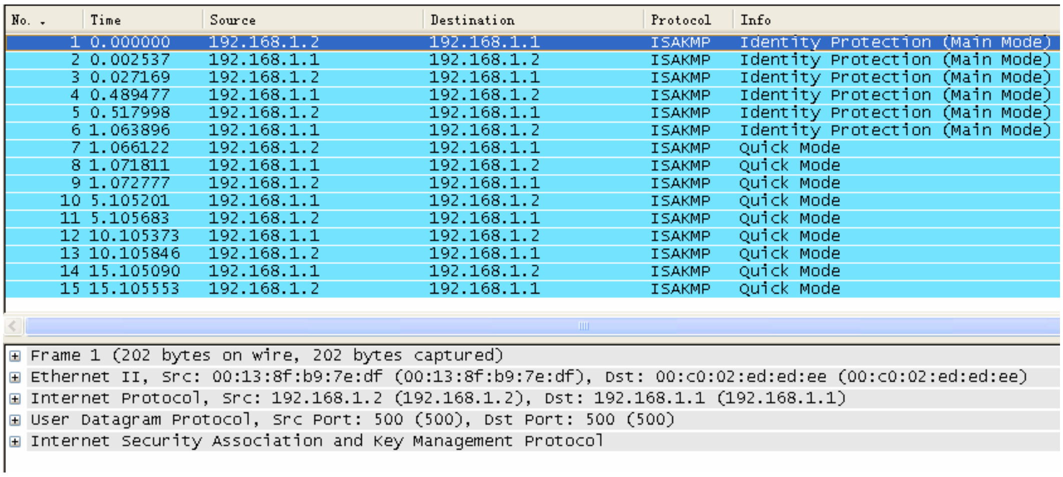
Once both DWnet SAFEcon5 router and TheGreenBow IPSec VPN Client have been configured accordingly, you are ready to open VPN tunnels. First make sure you enable your firewall with IPSec traffic.

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. The following example shows a successful connection between TheGreenBow IPSec VPN Client and a DWnet SAFEcon5 VPN router.



```
No. .   Time        Source         Destination    Protocol  Info
      1 0.000000    192.168.1.2    192.168.1.1    ISAKMP    Identity Protection (Main Mode)
      2 0.002537    192.168.1.1    192.168.1.2    ISAKMP    Identity Protection (Main Mode)
      3 0.027169    192.168.1.2    192.168.1.1    ISAKMP    Identity Protection (Main Mode)
      4 0.489477    192.168.1.1    192.168.1.2    ISAKMP    Identity Protection (Main Mode)
      5 0.517998    192.168.1.2    192.168.1.1    ISAKMP    Identity Protection (Main Mode)
      6 1.063896    192.168.1.1    192.168.1.2    ISAKMP    Identity Protection (Main Mode)
      7 1.066122    192.168.1.2    192.168.1.1    ISAKMP    Quick Mode
      8 1.071811    192.168.1.1    192.168.1.2    ISAKMP    Quick Mode
      9 1.072777    192.168.1.2    192.168.1.1    ISAKMP    Quick Mode
     10 5.105201    192.168.1.1    192.168.1.2    ISAKMP    Quick Mode
     11 5.105683    192.168.1.2    192.168.1.1    ISAKMP    Quick Mode
     12 10.105373   192.168.1.1    192.168.1.2    ISAKMP    Quick Mode
     13 10.105846   192.168.1.2    192.168.1.1    ISAKMP    Quick Mode
     14 15.105090   192.168.1.1    192.168.1.2    ISAKMP    Quick Mode
     15 15.105553   192.168.1.2    192.168.1.1    ISAKMP    Quick Mode

⊞ Frame 1 (202 bytes on wire, 202 bytes captured)
⊞ Ethernet II, Src: 00:13:8f:b9:7e:df (00:13:8f:b9:7e:df), Dst: 00:c0:02:ed:ed:ee (00:c0:02:ed:ed:ee)
⊞ Internet Protocol, Src: 192.168.1.2 (192.168.1.2), Dst: 192.168.1.1 (192.168.1.1)
⊞ User Datagram Protocol, Src Port: 500 (500), Dst Port: 500 (500)
⊞ Internet Security Association and Key Management Protocol
```

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: ethereal

Ethereal 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 tools is available on website http://www.ethereal.com/. It can be used to follow protocol exchange between two devices. For installation and use details, read its specific documentation.

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 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.

6 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

The DWnet web site: http://www.dwnet.com.cn

Technical support by email at service@dwnet.com.cn

Sales contacts at +86 0512 67615551