TheGreenBow IPSec VPN Client

Configuration Guide

D-Link DFL 700

WebSite: http://www.thegreenbow.com

Contact: support@thegreenbow.com

Table of contents

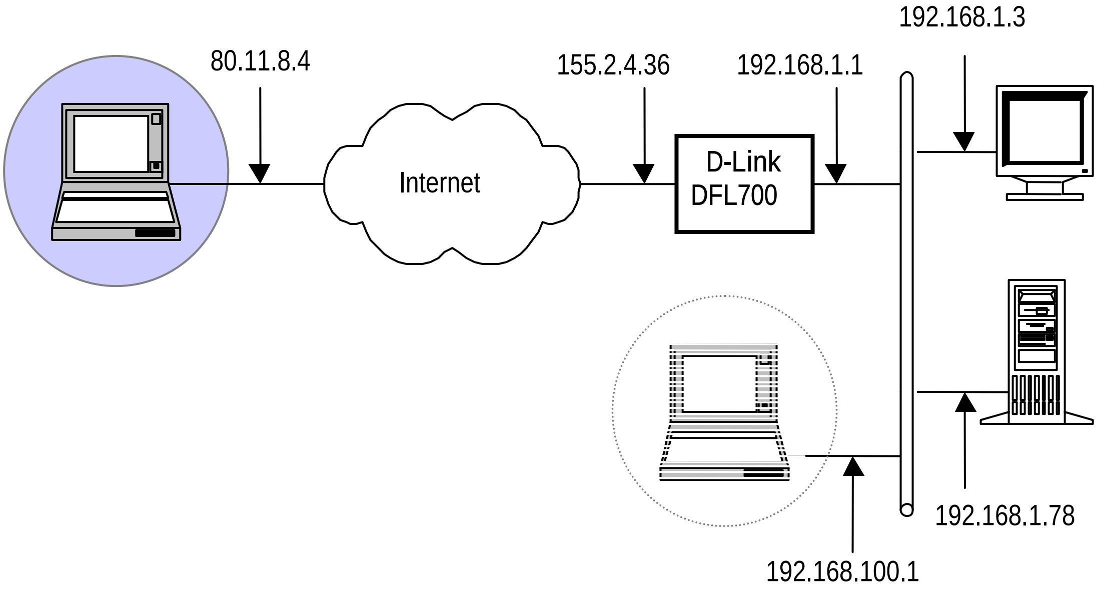
1 Introduction

1.1 Goal of this document

This VPN configuration guide describes how to configure TheGreenBow IPSec VPN Client with a D-Link DFL 700 router.

1.2 Network topology

In our example, we will connect TheGreenBow VPN client to the LAN behind the D-Link DFL700 Router. The VPN Client is connected to the Internet by a dialup/DSL connection from an ISP. The client will have a virtual IP address in the remote LAN. All the addresses in this document are given for example purpose.



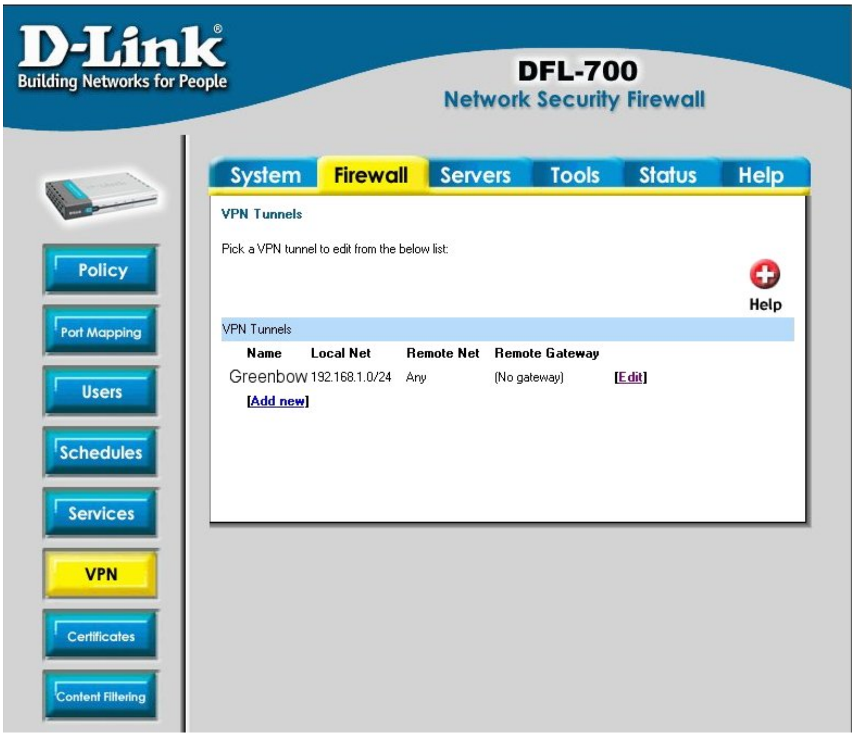
2 D-Link DFL700 VPN Configuration

This section describes how to build an IPSec VPN configuration with your D-Link DFL700 VPN router. Read D-Link DFL700 documentation for more information.

D-Link VPN configuration can be achieved with a web browser, so once connected to your VPN gateway, you must first select, "**Firewall**" and click on "“**VPN**” link in the DFL-700 VPN configuration interface.

2.1 D-Link DFL700 create a VPN tunnel

Select a connection and click on "**Edit**", or “**Add new**”.



VPN Tunnels

Pick a VPN tunnel to edit from the below list:

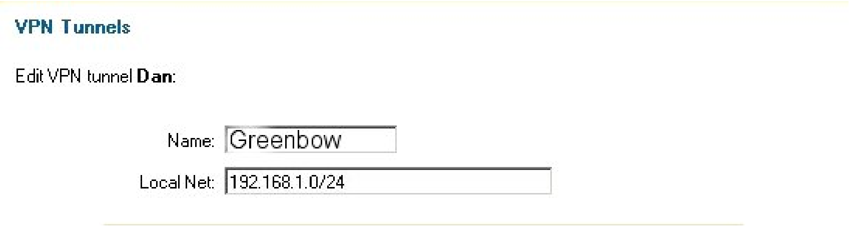
VPN Tunnels

Name	Local Net	Remote Net	Remote Gateway	
Greenbow	192.168.1.0/24	Any	(No gateway)	[Edit]

[Add new]

Enter a "**Name**" for the tunnel in the name field.

Specify your local network. This is the network which TheGreenBow VPN clients should be allowed to connect to.



VPN Tunnels

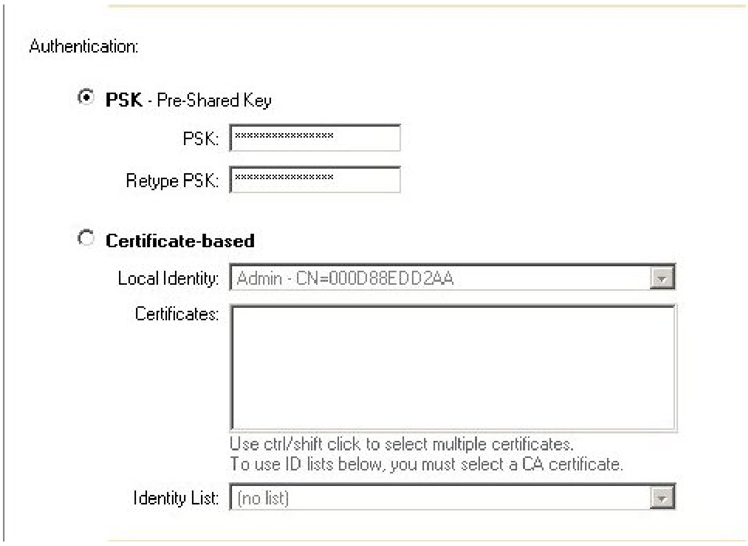
Edit VPN tunnel **Dan**:

Name: Greenbow

Local Net: 192.168.1.0/24

2.2 D-Link DFL700 choose pre shared keys

Choose PSK-Pre-Shared Key for Authentication type.



Authentication:

● **PSK** - Pre-Shared Key

PSK: ****************

Retype PSK: ****************

○ **Certificate-based**

Local Identity: Admin - CN=000D88EDD2AA

Certificates:

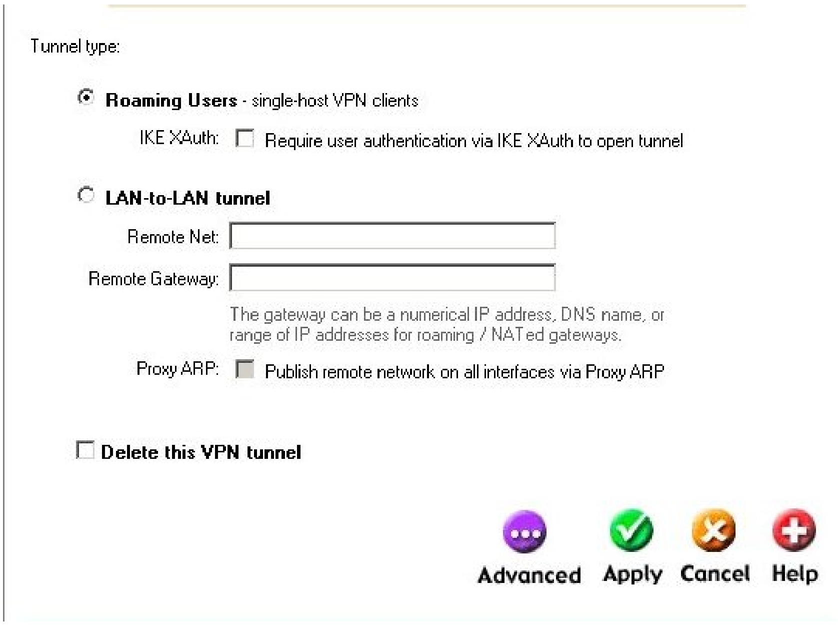
Use ctrl/shift click to select multiple certificates.
To use ID lists below, you must select a CA certificate.

Identity List: (no list)

2.3 D-Link DFL700 enable VPN users

In the page "Tunnel Type" choose "Roaming User".

Don’t forget to disable IKE X-Auth if necessary.



Tunnel type:

● **Roaming Users** - single-host VPN clients

IKE XAuth: □ Require user authentication via IKE XAuth to open tunnel

○ **LAN-to-LAN tunnel**

Remote Net:

Remote Gateway:

The gateway can be a numerical IP address, DNS name, or range of IP addresses for roaming / NATed gateways.

Proxy ARP: □ Publish remote network on all interfaces via Proxy ARP

□ **Delete this VPN tunnel**

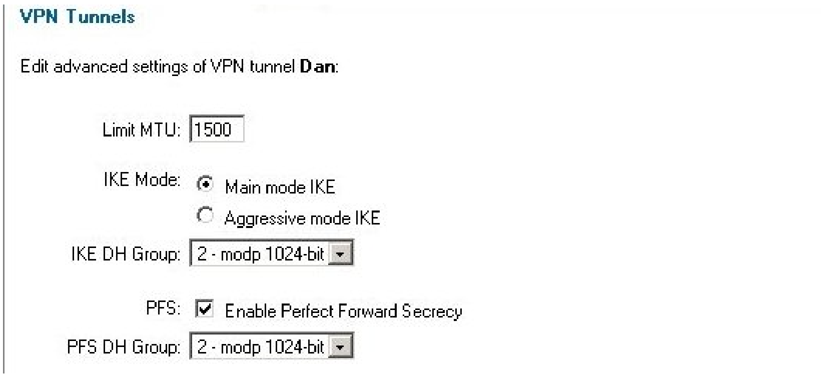
Click the Advanced button.

2.4 D-Link DFL700 Advanced menu

In the "**Advanced Menu**", don't modify "Limit MTU"and select "Main Mode IKE".

For IKE DH Group, you can choose the Diffie-Hellman Group 1 (modp 728 bits) or 2 (modp 1024).

Enable PFS if you want and select PFS DH Group 1 or 2.



VPN Tunnels

Edit advanced settings of VPN tunnel **Dan**:

Limit MTU: 1500

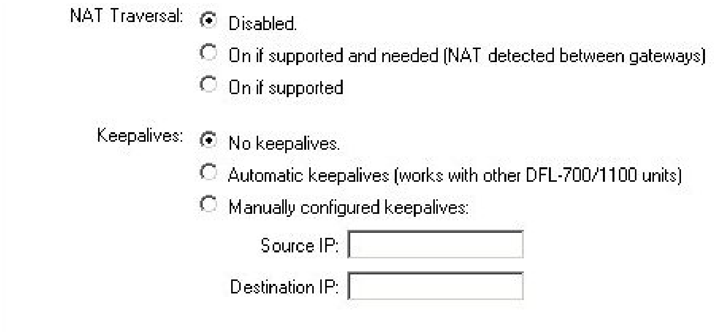
IKE Mode: ● Main mode IKE ○ Aggressive mode IKE

IKE DH Group: 2 - modp 1024-bit

PFS: ☑ Enable Perfect Forward Secrecy

PFS DH Group: 2 - modp 1024-bit

Disable Nat Traversal and Keepalives.



NAT Traversal: ● Disabled. ○ On if supported and needed (NAT detected between gateways) ○ On if supported

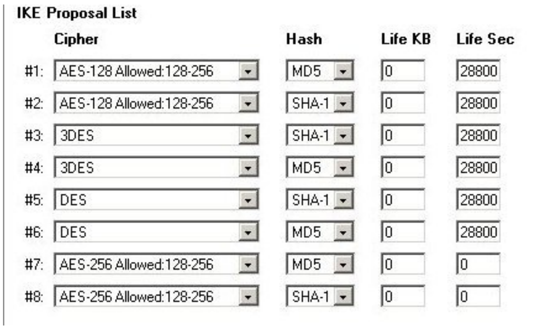
Keepalives: ● No keepalives. ○ Automatic keepalives (works with other DFL-700/1100 units) ○ Manually configured keepalives:

Source IP:

Destination IP:

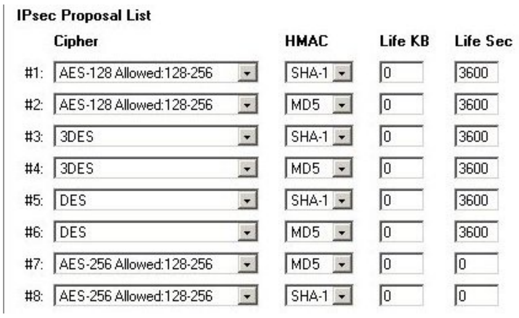
2.5 D-Link DFL700 IPSec and IKE Proposals

Select the Proposal List for IKE and IPSec with algorithms you want. TheGreenBow VPN Client (release 2.03 and above) supports DES, 3DES, AES (128, 192 or 256 bits) and MD5 or SHA.



IKE Proposal List

	Cipher	Hash	Life KB	Life Sec
#1:	AES-128 Allowed:128-256	MD5	0	28800
#2:	AES-128 Allowed:128-256	SHA-1	0	28800
#3:	3DES	SHA-1	0	28800
#4:	3DES	MD5	0	28800
#5:	DES	SHA-1	0	28800
#6:	DES	MD5	0	28800
#7:	AES-256 Allowed:128-256	MD5	0	0
#8:	AES-256 Allowed:128-256	SHA-1	0	0



IPsec Proposal List

	Cipher	HMAC	Life KB	Life Sec
#1:	AES-128 Allowed:128-256	SHA-1	0	3600
#2:	AES-128 Allowed:128-256	MD5	0	3600
#3:	3DES	SHA-1	0	3600
#4:	3DES	MD5	0	3600
#5:	DES	SHA-1	0	3600
#6:	DES	MD5	0	3600
#7:	AES-256 Allowed:128-256	MD5	0	0
#8:	AES-256 Allowed:128-256	SHA-1	0	0

Click the "**Apply**" button at bottom to apply the changes.

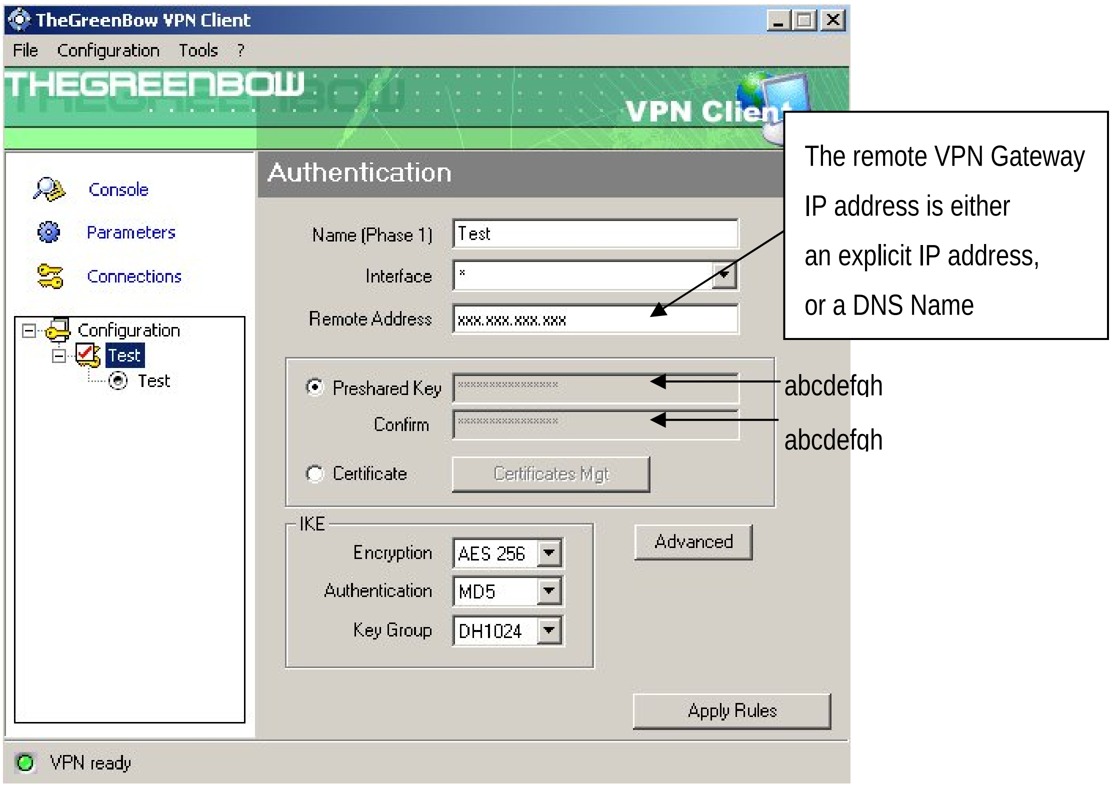
3 TheGreenBow IPSec VPN Client configuration

3.1 VPN Client Phase 1 (IKE) Configuration

In the "**Interface**" field, you can select a star ("*"), if the VPN Client host receive a dynamic IP Address from an ISP for example.

"**Remote Address**" field value is the D-Link DFL700 router public IP address or DNS address.

By clicking in "**Advanced**" button, you can setup Phase 1 IDs and Aggressive Mode.



Name (Phase 1): Test

Interface: *

Remote Address: xxx.xxx.xxx.xxx

● Preshared Key: ******************

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

○ Certificate

IKE

Encryption: AES 256

Authentication: MD5

Key Group: DH1024

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

abcdefgh

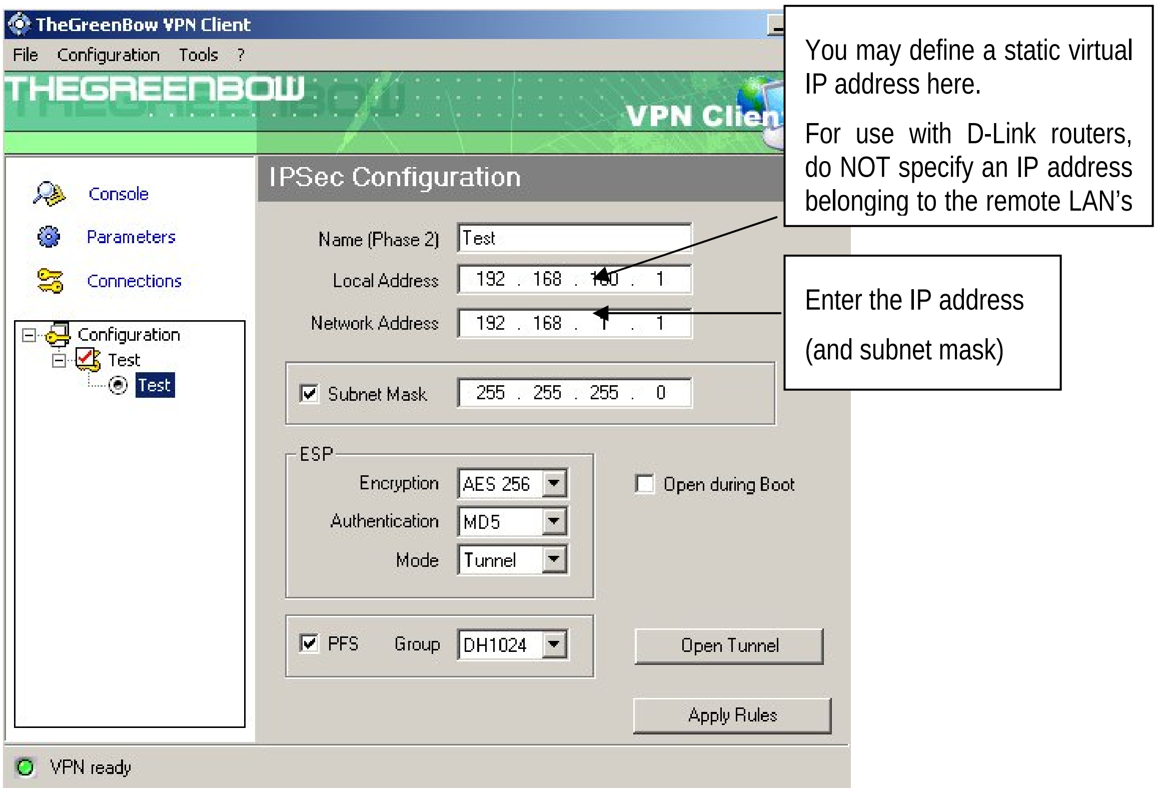
abcdefgh

Phase 1 configuration

3.2 VPN Client Phase 2 (IPSec) Configuration

In this window, you define IPSec Policy.

"**Local Address**" is the virtual IP address of the VPN Client inside the LAN. This address must not belong to the remote LAN.



Name (Phase 2): Test

Local Address: 192 . 168 . 100 . 1

Network Address: 192 . 168 . 1 . 1

☑ Subnet Mask: 255 . 255 . 255 . 0

ESP

Encryption: AES 256

Authentication: MD5

Mode: Tunnel

☐ Open during Boot

☑ PFS Group: DH1024

You may define a static virtual IP address here.

For use with D-Link routers, do NOT specify an IP address belonging to the remote LAN's

Enter the IP address

(and subnet mask)

Phase2 Configuration

3.3 Open IPSec VPN tunnels

Once both D-Link DFL700 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 are exactly the same with a D-Link DFL700 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”). 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