



THEGREENBOW



TheGreenBow IPsec VPN Client Configuration Guide

Digi ConnectPort WAN VPN Cellular Gateway

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

Contact: support@thegreenbow.com

Configuration Guide written by:

Company:

Table of contents

1	Introduction	3
1.1	Goal of this document	3
1.2	VPN Network topology	3
1.3	Firmware Restrictions	3
1.4	Digi ConnectPort Wan VPN Cellular Gateway	3
1.5	Digi ConnectPort Wan VPN Cellular Gateway product info	3
2	Digi ConnectPort Wan VPN Cellular Gateway VPN configuration	4
3	TheGreenBow IPSec VPN Client configuration	7
3.1	VPN Client Phase 1 (IKE) Configuration	7
3.2	VPN Client Phase 2 (IPSec) Configuration	9
3.3	Open IPSec VPN tunnels	9
4	Tools in case of trouble	10
4.1	A good network analyser: Wireshark	10
5	VPN IPSec Troubleshooting	11
5.1	« PAYLOAD MALFORMED » error (wrong Phase 1 [SA])	11
5.2	« INVALID COOKIE » error	11
5.3	« no keystate » error	11
5.4	« received remote ID other than expected » error	11
5.5	« NO PROPOSAL CHOSEN » error	12
5.6	« INVALID ID INFORMATION » error	12
5.7	I clicked on "Open tunnel", but nothing happens	12
5.8	The VPN tunnel is up but I can't ping !	12
6	Contacts	14

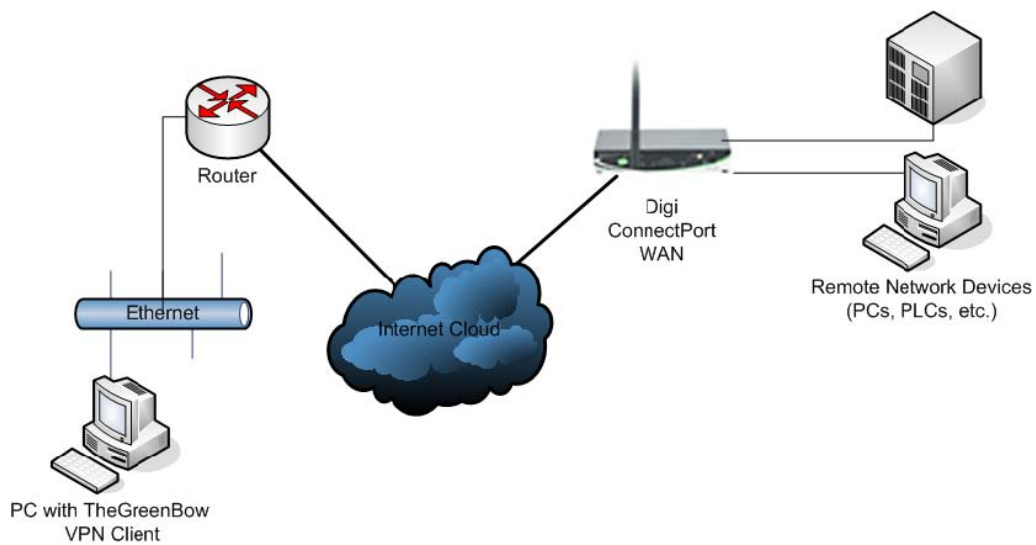
1 Introduction

1.1 Goal of this document

This configuration guide describes how to configure TheGreenBow IPsec VPN Client software with a Digi ConnectPort VPN Cellular Gateway to establish VPN connections for remote access to corporate network

1.2 VPN Network topology

In our VPN network example (diagram hereafter), we will connect TheGreenBow IPsec VPN Client software to the LAN behind the Digi ConnectPort Wan VPN Cellular Gateway. 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 Firmware Restrictions

Digi Firmware required for TheGreenBow IPsec VPN Client: Firmware version must be 2.8 or later. To download the latest firmware, go to <http://www.digi.com/support>.

1.4 Digi ConnectPort Wan VPN Cellular Gateway

Our tests and VPN configuration have been conducted with Digi firmware release 2.8.4.16.

GSM GPRS/EDGE APN Type needed: VPN and GRE end-points usually require a static (persistent) IP addresses and must support mobile terminated data connections. If mobile termination is not an option with your current APN, you will need to acquire a new one that supports mobile termination from your cellular provider.

1.5 Digi ConnectPort Wan VPN Cellular Gateway product info

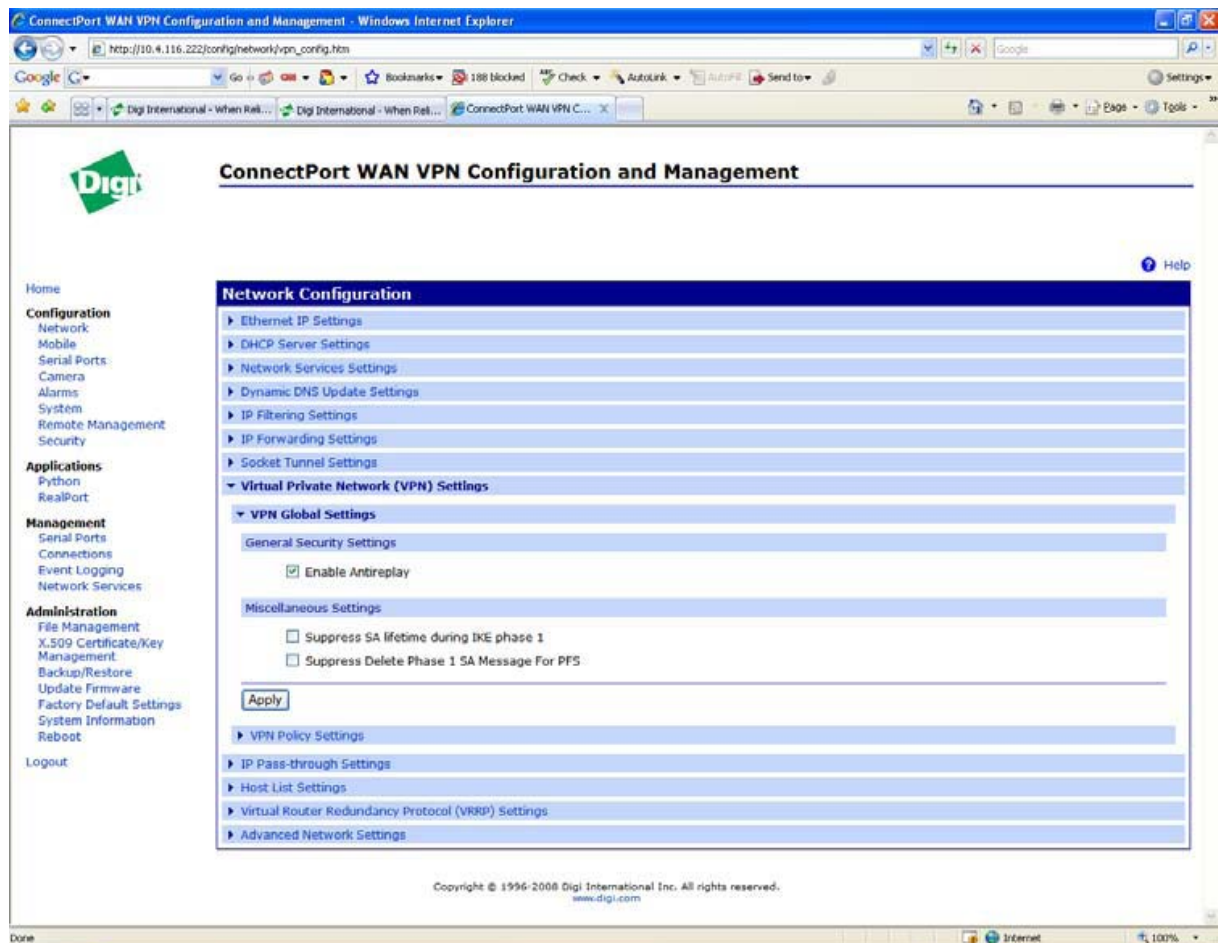
It is critical that users find all necessary information about Digi ConnectPort Wan VPN Cellular Gateway VPN Gateway. All product info, User Guide and knowledge base for the Digi ConnectPort Wan VPN Cellular Gateway VPN Gateway can be found on the Digi ConnectPort Wan VPN Cellular Gateway website <http://www.digi.com/products/cellulargateways/connectportwanvpn.jsp#overview>.

Digi ConnectPort Product page	http://www.digi.com/pdf/prd_rwc_connectportwanvpn.pdf
Digi ConnectPort User Guide	http://ftp1.digi.com/support/documentation/90000857-88_B.pdf
Digi ConnectPort FAQ/Knowledge Base	http://www.digi.com/support/kbase/?pid=2990&osvid=0

2 Digi ConnectPort Wan VPN Cellular Gateway VPN configuration

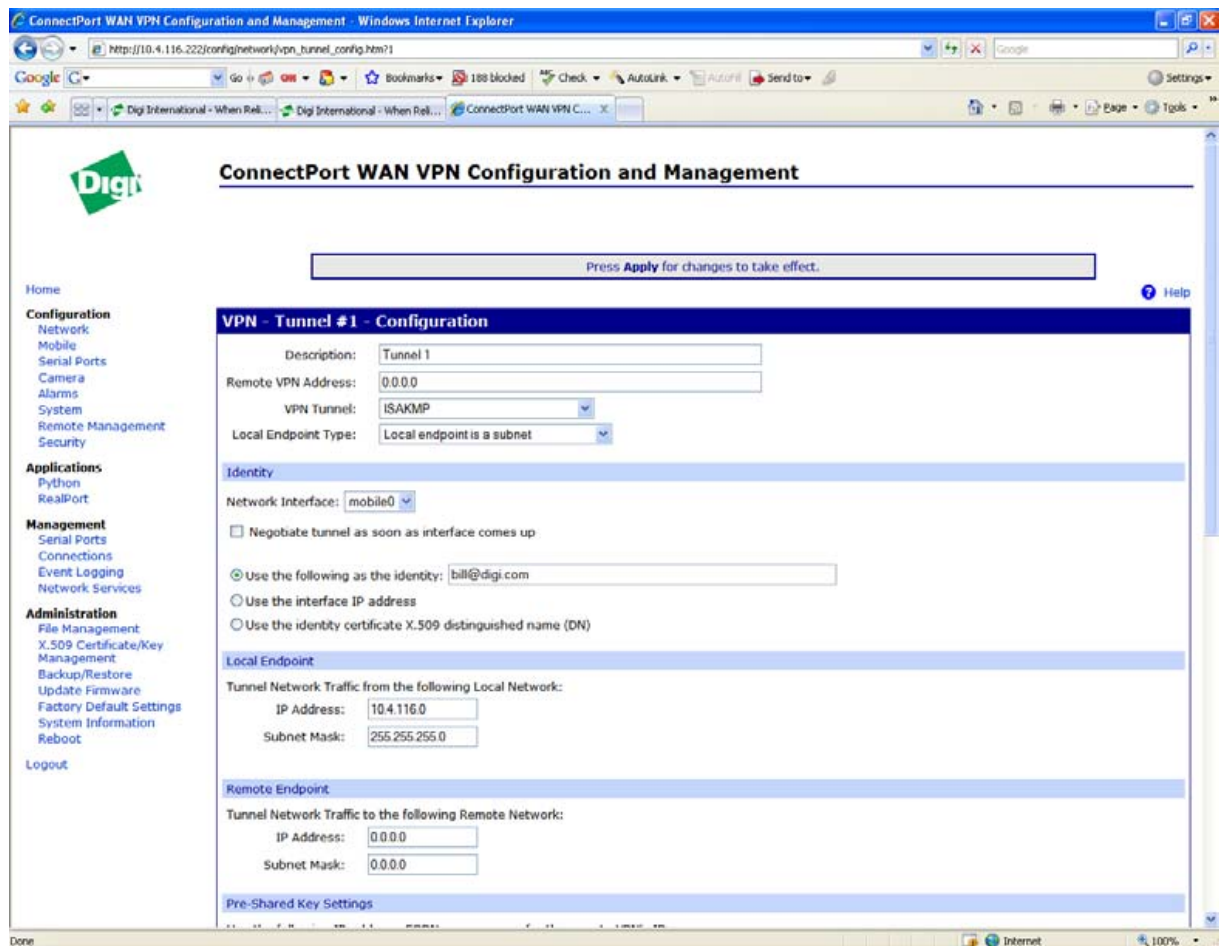
This section describes how to build an IPSec VPN configuration with your Digi ConnectPort Wan VPN Cellular Gateway.

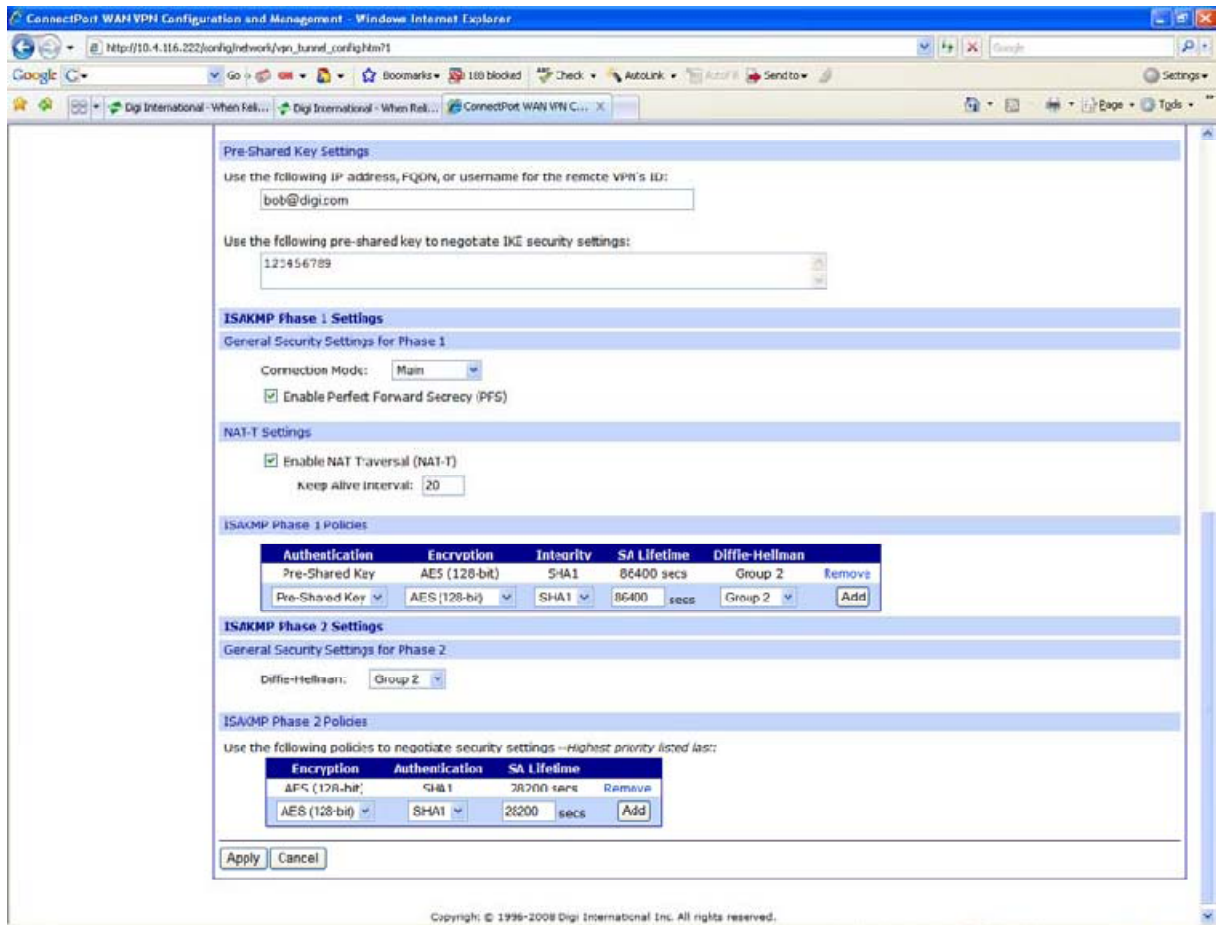
1. Configure the Digi Connect router settings:
 - a. VPN Global Settings
 - i. Navigate to **Configuration > Network > VPN Settings** in the web interface of the unit.
 - ii. Click on **VPN Global Settings**.
 - iii. Click the check box for **Enable Antireplay**.
 - iv. Click **Apply** to save the changes.



b. VPN Policy Settings

- v. Click on **VPN Policy Settings**.
- vi. Click on the **Add** button to setup the individual tunnel.
- vii. Fill in the appropriate information, shown in the following screenshots:





ADDITIONAL NOTES

1. This configuration will work with Dynamic IP addresses, using hostnames established with DynDNS.org, or using the DDNS update feature of Digi Connectware® Manager. When using a Dynamic IP address, you will need to set the VPN tunnel to use **Aggressive Mode** to make the connection work.
2. This configuration will work with other VPN parameters than what is listed in the screenshots. i.e. – DES, 3DES, AES 192-bit, AES 256-bit, etc.
3. This configuration will work with other Digi Cellular products, such as the Connect WAN, Connect WAN 3G, and ConnectPort WAN VPN series of products that support VPN connections.

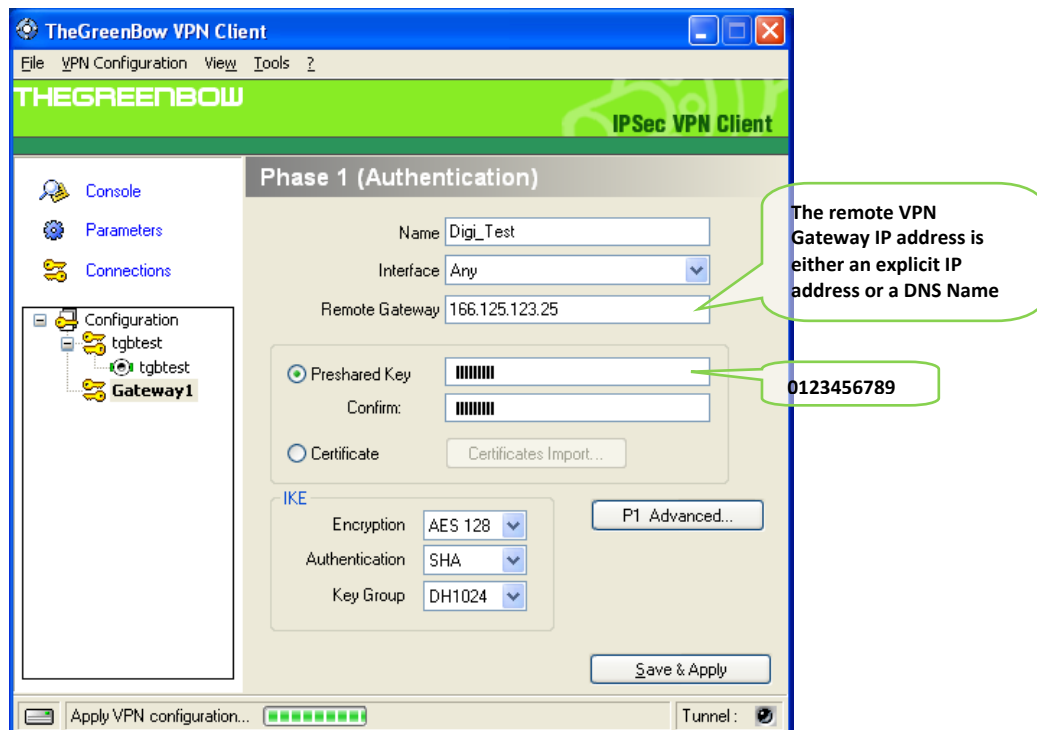
3 TheGreenBow IPSec VPN Client configuration

This section describes the required configuration to connect to a Digi ConnectPort Wan VPN Cellular Gateway via VPN connections.

To download the latest release of TheGreenBow IPSec VPN Client software, please go to http://www.thegreenbow.com/vpn_down.html for a free trial version.

3.1 VPN Client Phase 1 (IKE) Configuration

1. Create a Phase1:
 - a. Right click 'Configuration' in the left hand panel, and click New Phase 1.
 - b. Fill in the appropriate fields shown in the screenshot below:



Phase 1 configuration

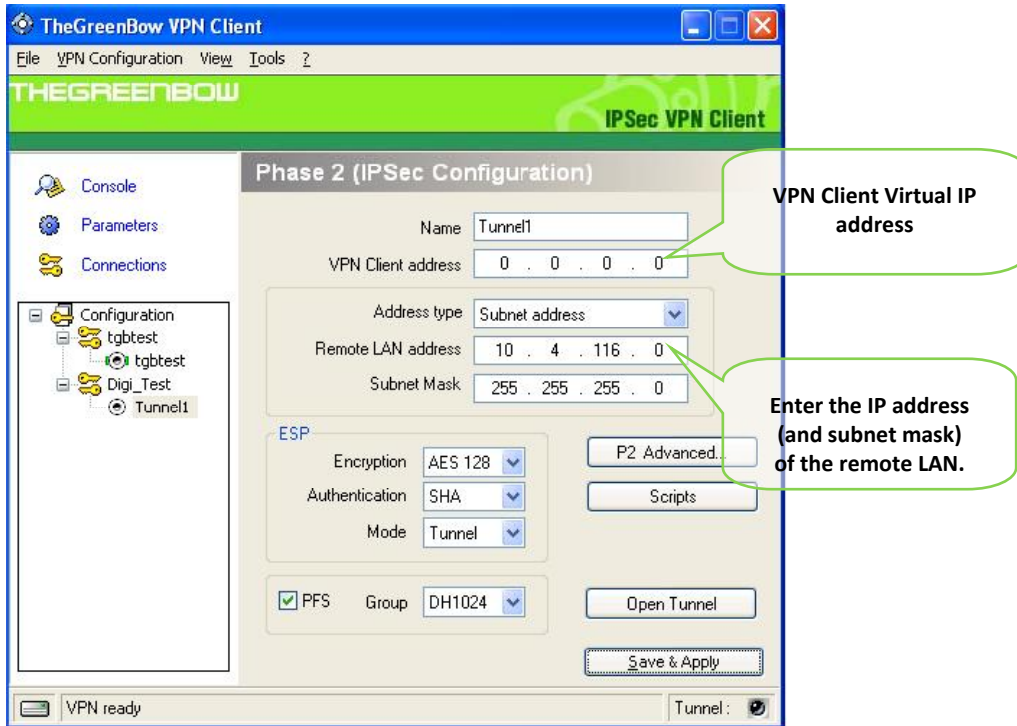
This configuration is one example of what can be accomplished in term of User Authentication. You may want to refer to either the Digi ConnectPort Wan VPN Cellular Gateway User Guide or TheGreenBow IPSec VPN Client software User Guide for more details on User Authentication options.

c. Click the P1 Advanced button. Fill in the appropriate fields shown in the following screenshot:

d. Click 'Save & Apply' to save the settings.

3.2 VPN Client Phase 2 (IPSec) Configuration

2. Create a Phase2:
 - a. Right click the Phase 1 policy that was added in the left hand panel, and click 'Add Phase 2'.
 - b. Fill in the appropriate fields for the Phase 2 settings, shown in the following screenshot:



Phase 2 Configuration

3.3 Open IPsec VPN tunnels

Once both Digi ConnectPort Wan VPN Cellular Gateway and TheGreenBow IPsec VPN Client software 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 Digi ConnectPort Wan VPN Cellular Gateway.

```

20090630 104525 Default [SA Gateway2-P1] SEND phase 1 Main Mode [SA] [VID] [VID] [VID] [VID] [VID]
20090630 104525 Default [SA Gateway2-P1] RECV phase 1 Main Mode [SA] [VID] [VID]
20090630 104526 Default [SA Gateway2-P1] SEND phase 1 Main Mode [KEY_EXCH] [NONCE] [NAT_D] [NAT_D]
20090630 104526 Default [SA Gateway2-P1] RECV phase 1 Main Mode [KEY_EXCH] [NONCE] [NAT_D] [NAT_D]
20090630 104526 Default [SA Gateway2-P1] SEND phase 1 Main Mode [HASH] [ID] [NOTIFY]
20090630 104526 Default [SA Gateway2-P1] RECV phase 1 Main Mode [HASH] [ID]
20090630 104526 Default phase 1 done: initiator id 192.168.205.151, responder id mygateway.dyndns.org
20090630 104526 Default [SA Gateway2-Tunnel3-P2] SEND phase 2 Quick Mode [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [ID]
20090630 104527 Default [SA Gateway2-Tunnel3-P2] RECV phase 2 Quick Mode [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [ID]
20090630 104527 Default [SA Gateway2-Tunnel3-P2] SEND phase 2 Quick Mode [HASH]
20090630 104555 Default [SA Gateway2-P1] SEND Informational [HASH] [NOTIFY] type DPD_R_U_THERE
20090630 104555 Default [SA Gateway2-P1] RECV Informational [HASH] [NOTIFY] type DPD_R_U_THERE_ACK
    
```

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: Wireshark

Wireshark 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 tool is available on website <http://www.wireshark.org>. It can be used to follow protocol exchange between two devices. For installation and use details, read its specific documentation (<http://www.wireshark.org/docs/>).

No. .	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.3	192.168.1.2	ISAKMP	Identity Protection (Main Mode)
2	0.153567	192.168.1.2	192.168.1.3	ISAKMP	Identity Protection (Main Mode)
3	0.205363	192.168.1.3	192.168.1.2	ISAKMP	Identity Protection (Main Mode)
4	0.257505	192.168.1.2	192.168.1.3	ISAKMP	Identity Protection (Main Mode)
5	0.300882	192.168.1.3	192.168.1.2	ISAKMP	Identity Protection (Main Mode)
6	0.310186	192.168.1.2	192.168.1.3	ISAKMP	Identity Protection (Main Mode)
7	0.313742	192.168.1.3	192.168.1.2	ISAKMP	Quick Mode
8	0.321913	192.168.1.2	192.168.1.3	ISAKMP	Quick Mode
9	0.323741	192.168.1.3	192.168.1.2	ISAKMP	Quick Mode
10	0.334980	192.168.1.2	192.168.1.3	ISAKMP	Quick Mode
11	0.691160	192.168.1.3	192.168.1.2	ESP	ESP (SPI=0x919bfabc)
12	1.692568	192.168.1.2	192.168.1.2	ESP	ESP (SPI=0x919bfabc)
13	1.693164	192.168.1.2	192.168.1.3	ESP	ESP (SPI=0x53a5925e)
14	2.693600	192.168.1.3	192.168.1.2	ESP	ESP (SPI=0x919bfabc)
15	2.694026	192.168.1.2	192.168.1.3	ESP	ESP (SPI=0x53a5925e)

Frame 1 (142 bytes on wire, 142 bytes captured)
 Ethernet II, Src: 00:50:04:ad:f2:73, Dst: 00:10:b5:07:2f:ff

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_rcv: 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_rcv_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

Doc.Ref	tgbvpn_cg_digi_connect_port_wan.pdf
Doc.version	1.0 – Oct 2009
VPN version	4.x

- If you still cannot ping, follow ICMP traffic on VPN server LAN interface and on LAN computer interface (with Wireshark 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 Wireshark (<http://www.wireshark.org>) on one of your target computer. You can check that your pings arrive inside the LAN.

	Doc.Ref	tgbvpn_cg_digi_connect_port_wan.pdf
	Doc.version	1.0 – Oct 2009
	VPN version	4.x

6 Contacts

News and updates on TheGreenBow web site: <http://www.thegreenbow.com>

Technical support by email at support@thegreenbow.com

Sales contacts by email at sales@thegreenbow.com