TheGreenBow IPSec VPN Client

Configuration Guide

Digitel NRX 5122

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

Configuration Guide written by:

Writer: Suport Technical
Company: www.digitel.com.br

Table of contents

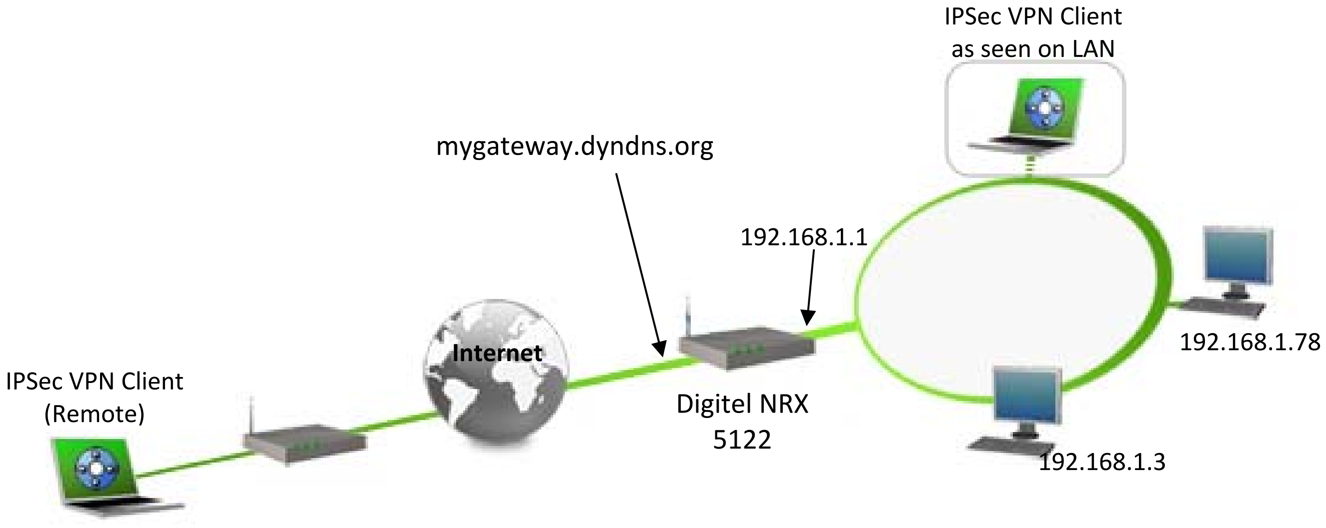
1 Introduction

1.1 Goal of this document

This configuration guide describes how to configure TheGreenBow IPSec VPN Client software with a Digitel NRX 5122 VPN router 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 Digitel NRX 5122 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 Digitel NRX 5122 Restrictions

Depending on the topology to be used may need some changes to the configuration script Digitel NRX 5122. In this case you should contact the Digitel via e-mail suporte@digitel.com.br .

1.4 Digitel NRX 5122 VPN Gateway

Our tests and VPN configuration have been conducted with Digitel NRX 5122 firmware release 79309e.

1.5 Digitel NRX 5122 VPN Gateway product info

It is critical that users find all necessary information about Digitel NRX 5122 VPN Gateway. All product info, User Guide and knowledge base for the Digitel NRX 5122 VPN Gateway can be found on the Digitel NRX 5122 website: www.digitel.com.br/pt/produtos/produto.asp?idLinha=11&idCat=36&Id=38

NRX 5122 Product page	http://www.digitel.com.br/pt/produtos/produto.asp?IdLinha=11&IdCat=36&Id=38
NRX 5122FAQ/Knowledge Base	suporte@digitel.com.br

2 Digitel NRX 5122 VPN configuration

This section describes how to build an IPSec VPN configuration with your Digitel NRX 5122 VPN router.

Once connected to your Digitel NRX 5122 VPN gateway, you must select "Security" and "VPN" tabs.

```
SET LAN LAN0 MODE AUTO
SET LAN LAN0 IP 192.168.1.254 MASK 255.255.255.0
SET LAN LAN0 UP

SET LAN LAN1 MODE AUTO
SET LAN LAN1 IP 192.168.30.15 MASK 255.255.255.0
SET LAN LAN1 UP

SET ROUTES DEFAULT GW1 192.168.30.1 COST1 1
SET ROUTES UP

SET IPSEC FRAGICMP TRUE NATT TRUE MTU 1412 TYPE DEFAULTROUTE
SET IPSEC CHANNEL0 NAME Teste  MODE TUNNEL
SET IPSEC CHANNEL0 AUTO ADD DPDACTION RESTART DPDDELAY 120 DPDTIMEOUT 120
SET IPSEC CHANNEL0 LEFT ADDRESSTYPE DEFAULTROUTE
SET IPSEC CHANNEL0 LEFT SUBNET TRUE NET 192.168.1.0 MASK 255.255.255.0
SET IPSEC CHANNEL0 RIGHT ADDRESSTYPE ANY
SET IPSEC CHANNEL0 RIGHT SUBNET FALSE
SET IPSEC CHANNEL0 KEY AUTH ESP AUTHBY SECRET PASS digitel
SET IPSEC CHANNEL0 KEY ISAKMP 24H RETRIES 0 KEYLIFE 1H
SET IPSEC CHANNEL0 IKE0 ALG 3DES HASH MD5 DH 2
SET IPSEC CHANNEL0 ESP0 ALG 3DES HASH MD5
SET IPSEC UP
```

Where:

```
SET LAN LAN0 MODE AUTO
```

Sets LAN0 for autonegotiation.

```
SET LAN LAN0 IP 192.168.1.254 MASK 255.255.255.0
```

Set IP address of the interface LAN0. In this case is Local Network.

```
SET LAN LAN1 MODE AUTO
```

Set LAN1, that is interface of internet access, for autonegotiation.

```
SET LAN LAN1 IP 192.168.30.15 MASK 255.255.255.0
```

Set interface LAN1 IP address.

```
SET ROUTES DEFAULT GW1 192.168.30.1 COST1 1
```

Set router default route.

3 Digitel NRX 5122 VPN configuration options

● FRAGICMP: This option allows the fragmentation of packets. Accepts TRUE or FALSE.

● HIDETOS: Provides a copy of the TOS field value and forwards it to the packet. Accepts TRUE or FALSE.

● UNIQUEIDS: Enables the replacement of all IDs of former connections with a new one. Accepts TRUE or FALSE.

● NATT: Enables the option of NAT Traversal. Accepts TRUE or FALSE.

● MTU: Sets the value of MTU. Accepts a value between 64 and 16 260.

● TYPE: Sets the type of connection. Accepts INTERFACE or DEFAULTROUTE.

● UP: Enable the settings.

● DOWN: Disable the settings.

● PURGE: Clears the settings.

● CHANNELn: For the channel configuration, the following parameters are available:

- NAME: Sets the name for the channel.
- DPDACTION: Sets what action should be taken after the tunnel is considered dead: NONE, CLEAR, HOLD, and RESTART.
- DPDDELAY: Set a value in seconds for the delay between Dead Peer Detection (RFS 3706) and KEEPALIVES for a given connection, the default is 30 seconds. If DPDTIMEOUT is configured, but the DPDDELAY is not, then the DPDDELAY is configured in its default pattern
- DPDTIMEOUT: Set a value in seconds, that IPSEC will be on hold without any traffic before considering the connection closed. The default is 120 seconds.
- AGGRESSIVE: Enables aggressive way. Accepts TRUE or FALSE.
- LEFT: Sets the local side of the tunnel. To configure this option, the following parameters are available:
  - ADDRESSTYPE: Accepts the following options for configuration: ANY, USER, DEFAULTROUTE, OPPORTUNISTIC, BINDED (this option can only be selected if TYPE is set as INTERFACE).
  - ADDRESS: This option can only be adjusted if ADDRESSTYPE is set as USER. Accepts an IP address for the interface.
  - SUBNET: This option accepts TRUE (true) or FALSE (false).
  - Enables the configuration of a subnet.
  - NET: This option can only be configured if SUBNET is enabled as TRUE. Configures an IP address for the subnet.
  - MASK: This option can only be configured if SUBNET is enabled as TRUE. Sets an IP address for the subnet mask.
  - USEGATEWAY: Enables the configuration of a gateway. This option accepts either TRUE or FALSE.
  - ID: Defines a string for authentication.
  - GATEWAY: For this option to be configured, USEGATEWAY must be enabled as TRUE. Configures the gateway IP address.

- SOURCEIP: Set an IP address, which will be used when transmitting a packet to the other side of the tunnel.

Example:

```
NRX> SET IPSEC CHANNEL0 LEFT ADDRESSTYPE USER ADDRESS 172.16.1.2
SUBNET TRUE NET 192.168.10.0 MASK 255.255.255.0 USEGATEWAY TRUE
ID user@fqdn.com GATEWAY 10.10.10.5 SOURCEIP 192.168.255.0
```

- RIGHT: Defines the network from the remote side. To accomplish the setting of this option, the same parameters of the option LEFT are available.
- KEY: Sets the key exchange. To achieve this configuration, the following configuration parameters are available:
  - AUTH: Select the type of authentication, ESP or AH.
  - AUTHBY: Select the authentication method, SECRET or RSB.
  - PASS: This option can only be adjusted if AUTHBY is configured as SECRET. Set the password for authentication.
  - BITS: This option can only be adjusted if AUTHBY is configured as RSA. BITS number for the key.
  - PEERPUBLICKEY: This option can only be adjusted if AUTHBY is configured as RSA. Accepts a set of characters referring to remote public key.
  - GENERATEKEY: This option can only be adjusted if AUTHBY is configured as RSA. Sets key generation.
  - LOCALSIDE: This option can only be set if AUTHBY is configured as RSA. Determines which side will be local in the tunnel, if LEFT or RIGHT.
  - NEGRESTART: Sets the times for restart of connection attempt. To accomplish the setting of this option, the following parameters are available:
    - TIME: Sets the time. Accepts an integer value.
    - MARGIN: Sets the margin. Accepts an integer value between 0 and 100.
  - KEYLIFE: Sets the lifetime of the key. Accepts the following syntax: <integer value> <unity>, being H hours, M minutes and S seconds.
  - ISAKMP: Sets the lifetime of the channel before the renegotiation. Accepts the following syntax: <integer value> <unity>, being H hours, M minutes and S seconds.
  - RETRIES: Sets the number of retries for authentication. Accepts an integer value.
  - PERFECTFORWARD: Enables the use of PFS protocol (Perfect Forward Secrecy). This option accepts either TRUE or FALSE.
- AUTO: Sets which operation should be done automatically by ISPEC. To accomplish the setting of this option, the following parameters are available: START, ADD or ROUTE.
- COMPRESS: Accepts TRUE (true) or false (false).
- MODE: Sets the type of connection TUNNEL or TRANSPORT.
- PURGE: Clears the settings for the option CHANNELn.
- IKEn: (Internet Key Exchange) encryption and authentication algorithm that is used in the connection. To configure this option, the following configuration parameters are available:
  - ALG: Sets the encryption algorithm to be used. Accepted one of the options: DES, 3DES, AES, AES256 or NULL.

- HASH: Sets the hash algorithm to be used. Accepts one of the options: MD5, SHA1 or SHA256.
- DH: Configure DiffieHellman group. Accept values: 2, 5, 14, 15, 16, 17 or 18.
- PURGE: Clears the settings that were adjusted in IKEn.

• ESPn: Configuration of authentication and encryption algorithm that will be used in the connection. To accomplish the setting of this option, the following parameters are available:

- ALG: Sets the encryption algorithm to be used. Accepted one of the options DES, 3DES, AES, AES256 or NULL.
- HASH: Sets the hash algorithm MD5, SHA1 or SHA256.
- PURGE: Clears the settings for the ESP option.

● IPSECn: This option can only be adjusted if TYPE is set as INTERFACE. To accomplish the setting of this option, the following parameters are available:

• INTERFACE: Defines which interface will be used by IPSEC.

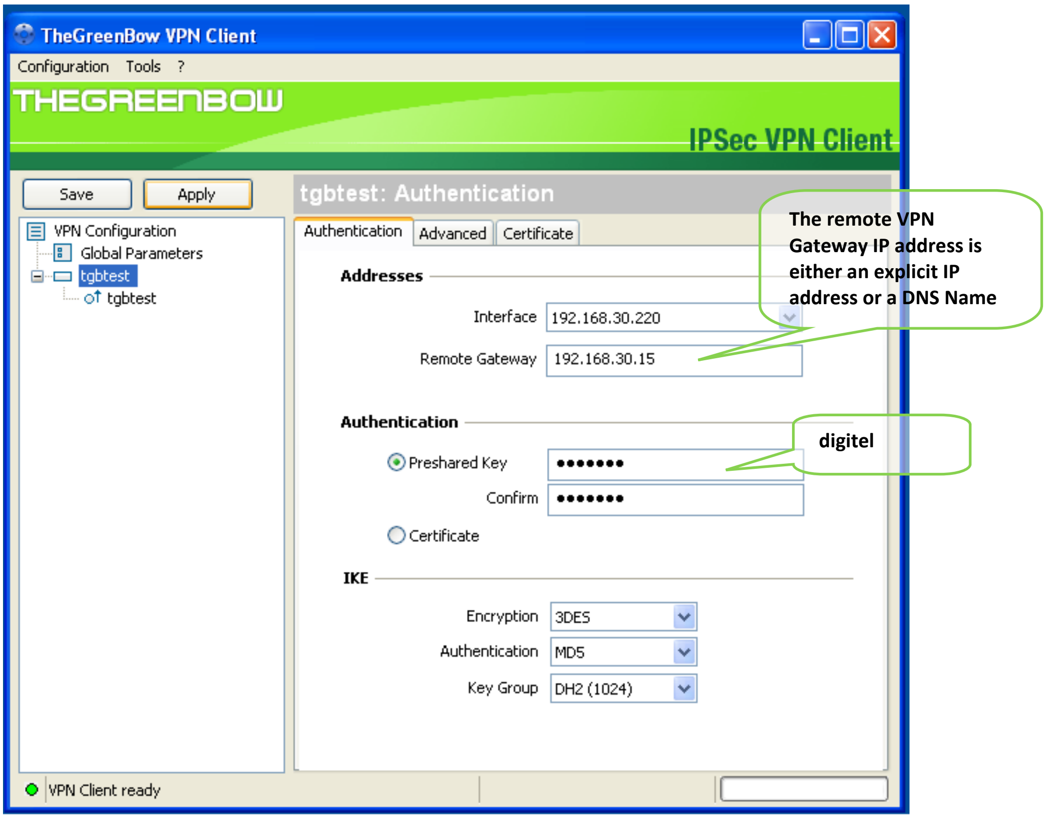
• PURGE: This option clears the setting for IPSECn.

4 TheGreenBow IPSec VPN Client configuration

This section describes the required configuration to connect to a Digitel NRX 5122 VPN router via VPN connections.

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

4.1 VPN Client Phase 1 (IKE) Configuration



tgbtest: Authentication

Addresses

Interface: 192.168.30.220

Remote Gateway: 192.168.30.15

Authentication

● Preshared Key: •••••••

Confirm: •••••••

○ Certificate

IKE

Encryption: 3DES

Authentication: MD5

Key Group: DH2 (1024)

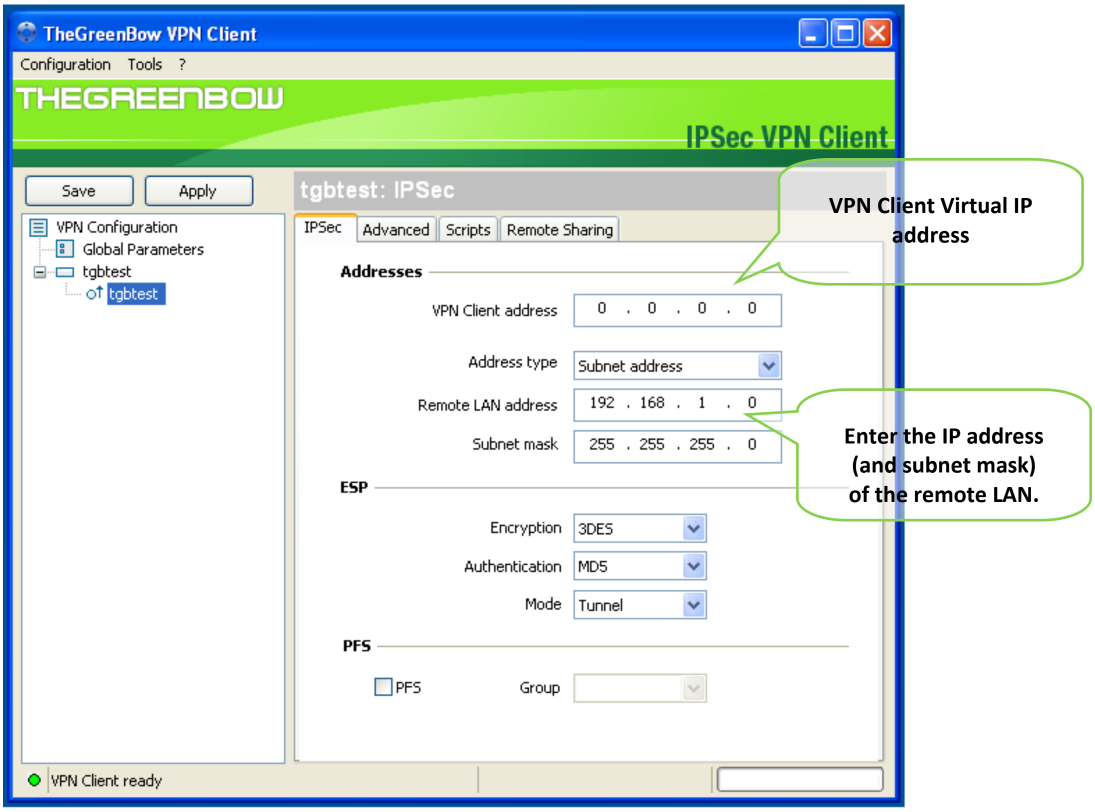
The remote VPN Gateway IP address is either an explicit IP address or a DNS Name

digitel

Phase 1 configuration

You may use either Preshared key, Certificates, USB Tokens, OTP Token (One Time Password) or X-Auth combined with RADIUS Server for User Authentication with the Digitel NRX 5122 router. This configuration is one example of what can be accomplished in term of User Authentication. You may want to refer to either the Digitel NRX 5122 router user guide or TheGreenBow IPSec VPN Client software User Guide for more details on User Authentication options.

4.2 VPN Client Phase 2 (IPSec) Configuration



Addresses

VPN Client address: 0 . 0 . 0 . 0

Address type: Subnet address

Remote LAN address: 192 . 168 . 1 . 0

Subnet mask: 255 . 255 . 255 . 0

ESP

Encryption: 3DES

Authentication: MD5

Mode: Tunnel

PFS

□ PFS Group:

VPN Client Virtual IP address

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

Phase 2 Configuration

4.3 Open IPSec VPN tunnels

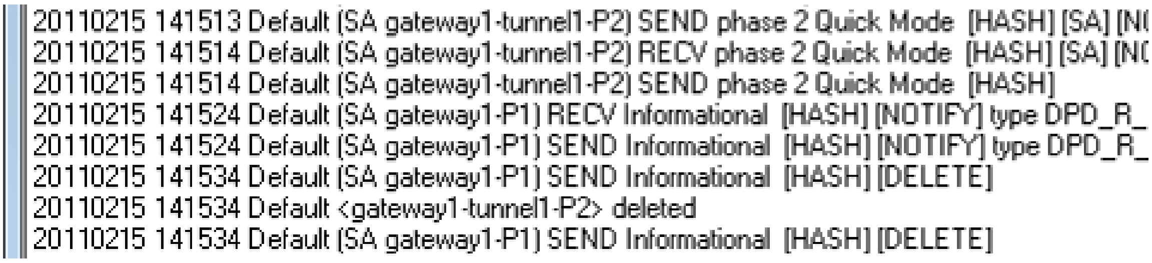
Once both Digitel NRX 5122 router and TheGreenBow IPSec VPN Client software have been configured accordingly, you are ready to open VPN tunnels. First make sure you enable your firewall with IPSec traffic.

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 Digitel NRX 5122 VPN router.



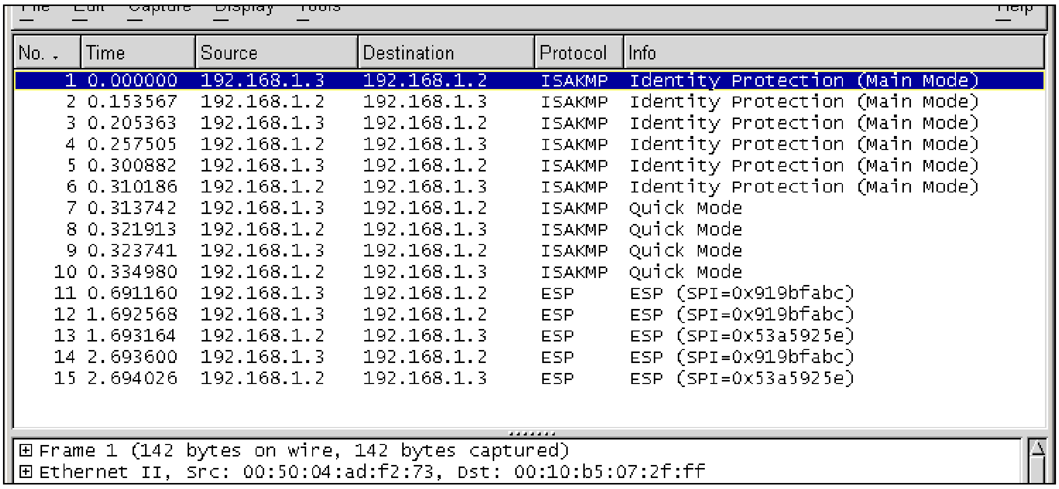
```
20110215 141513 Default (SA gateway1-tunnel1-P2) SEND phase 2 Quick Mode  [HASH] [SA] [N
20110215 141514 Default (SA gateway1-tunnel1-P2) RECV phase 2 Quick Mode  [HASH] [SA] [N
20110215 141514 Default (SA gateway1-tunnel1-P2) SEND phase 2 Quick Mode  [HASH]
20110215 141524 Default (SA gateway1-P1) RECV Informational  [HASH] [NOTIFY] type DPD_R_
20110215 141524 Default (SA gateway1-P1) SEND Informational  [HASH] [NOTIFY] type DPD_R_
20110215 141534 Default (SA gateway1-P1) SEND Informational  [HASH] [DELETE]
20110215 141534 Default <gateway1-tunnel1-P2> deleted
20110215 141534 Default (SA gateway1-P1) SEND Informational  [HASH] [DELETE]
```

5 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.

5.1 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   192.168.1.3    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
```

6 VPN IPSec Troubleshooting

6.1 « 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.

6.2 « 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.

6.3 « 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.

6.4 « 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.

6.5 « 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
```

6.6 « 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).

6.7 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).

6.8 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 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.

7 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

News and updates on Digitel web site: http://www.digitel.com.br

Technical support by email at: suporte@digitel.com.br

Sales contacts by email at: vendas_digitel@digitel.com.br

Secure, Strong, Simple.

TheGreenBow Security Software