TheGreenBow IPSec VPN Client

Configuration Guide

Cisco ASA 5510

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

Configuration Guide written by:

Writer:	Carlos Astor
Company:	www.integrasti.com.br

Table of contents

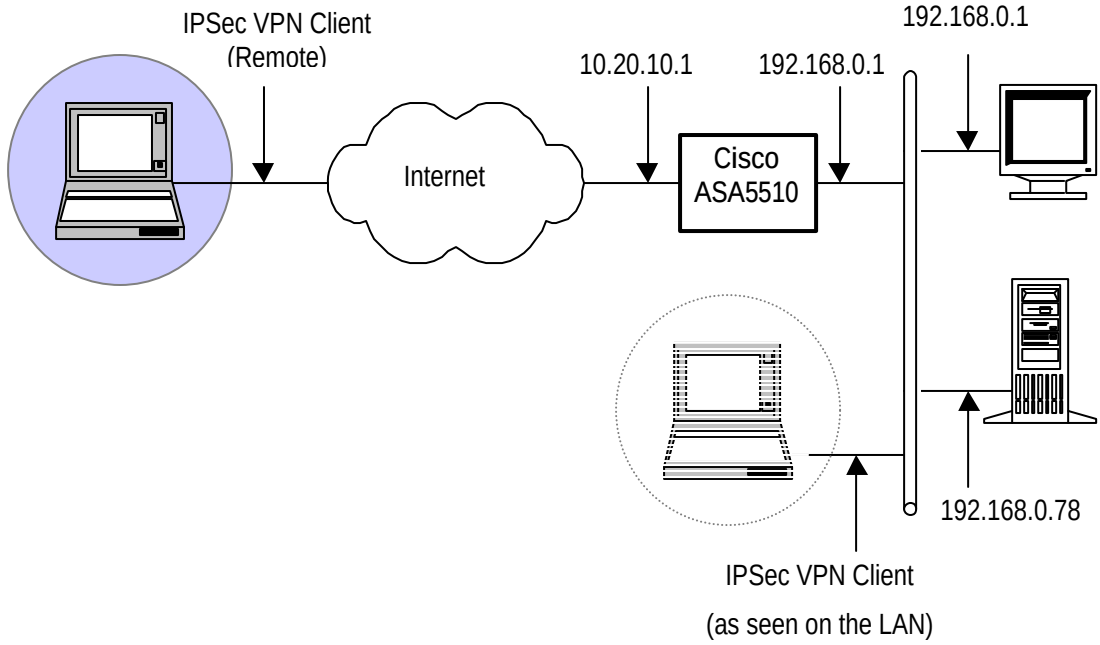
1 Introduction

1.1 Goal of this document

This configuration guide describes how to configure TheGreenBow IPSec VPN Client with a Cisco ASA 5510 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 Cisco ASA 5510 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 Cisco ASA 5510 VPN Gateway

Our tests and VPN configuration have been conducted with Cisco ASA 5510 software release ASA 8.0(2), ASDM6.0(2).

1.4 Cisco ASA 5510 VPN Gateway product info

It is critical that users find all necessary information about Cisco ASA 5510 VPN Gateway. All product info, User Guide and knowledge base for the Cisco ASA 5510 VPN Gateway can be found on the Cisco ASA 5510 website: http://www.cisco.com/en/US/products/ps6120/index.html

Cisco ASA 5510 Product page	http://www.cisco.com/en/US/products/ps6120/prod_literature.html
Cisco ASA 5510 User Guide	http://www.cisco.com/en/US/products/ps6120/products_installation_and_configuration_guides_list.html
Cisco ASA 5510 FAQ/Knowledge Base	http://www.cisco.com/en/US/products/ps6120/tsd_products_support_series_home.html

2 Cisco ASA 5510 VPN configuration

This section describes how to build an IPSec VPN configuration with your Cisco ASA 5510 VPN router.

Once connected to your Cisco ASA 5510 VPN gateway, here are the command lines.

2.1 Cisco ASA 5510 Router command lines

```
: Saved
:
ASA Version 8.0(2)
!
hostname ciscoasa
domain-name default.domain.invalid
enable password 123456789 encrypted
names
dns-guard
!
interface Ethernet0/0
 nameif Interna
 security-level 100
 ip address 192.168.0.1 255.255.255.0
!
interface Ethernet0/1
 nameif Externa
 security-level 0
 ip address 10.20.10.1 255.255.255.0
!
interface Ethernet0/2
 shutdown
 no nameif
 security-level 0
 no ip address
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 nameif management
 security-level 100
 no ip address
 management-only
!
passwd 12345678 encrypted
boot system disk0:/asa802-K8.bin
ftp mode passive
dns server-group DefaultDNS
 domain-name default.domain.invalid
access-list   150   extended   permit   ip   192.168.0.0   255.255.255.0   192.168.11.0
255.255.255.0
access-list pocket@vpn.com_splitTunnelAcl standard permit 192.168.0.0 255.255.255.0
pager lines 24
logging enable
logging buffered debugging
logging asdm informational
mtu Interna 1500
mtu Externa 1500
mtu management 1500
ip local pool vpnpool 192.168.11.1-192.168.11.254
ip verify reverse-path interface Interna
ip verify reverse-path interface Externa
icmp unreachable rate-limit 1 burst-size 1
```

```
asdm image disk0:/asdm521.bin
no asdm history enable
arp timeout 14400
route Externa 0.0.0.0 0.0.0.0 10.20.10.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy
nac-policy DfltGrpPolicy-nac-framework-create nac-framework
 reval-period 36000
 sq-period 300
aaa authentication telnet console LOCAL
aaa authentication ssh console LOCAL
aaa authentication http console LOCAL
aaa authentication enable console LOCAL
http server enable
http 0.0.0.0 0.0.0.0 Interna
no snmp-server location
no snmp-server contact
sysopt connection permit-vpn
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac
crypto ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto ipsec transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto ipsec transform-set myset esp-3des esp-sha-hmac
crypto ipsec transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto ipsec transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-hmac
crypto ipsec transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac
crypto ipsec transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-hmac
crypto ipsec transform-set ESP-AES-128-MD5 esp-aes esp-md5-hmac
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set pfs
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set transform-set ESP-AES-128-
SHA ESP-AES-128-MD5 ESP-AES-192-SHA ESP-AES-192-MD5 ESP-AES-256-SHA ESP-AES-256-MD5
ESP-3DES-SHA ESP-3DES-MD5 ESP-DES-SHA ESP-DES-MD5
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set nat-t-disable
crypto map mymap 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTO_MAP
crypto map mymap interface Externa
crypto isakmp enable Externa
crypto isakmp policy 65535
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
no crypto isakmp nat-traversal
telnet timeout 5
ssh timeout 5
ssh version 2
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
!
class-map class_sip_tcp
 match port tcp eq sip
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect icmp
  inspect dns preset_dns_map
```

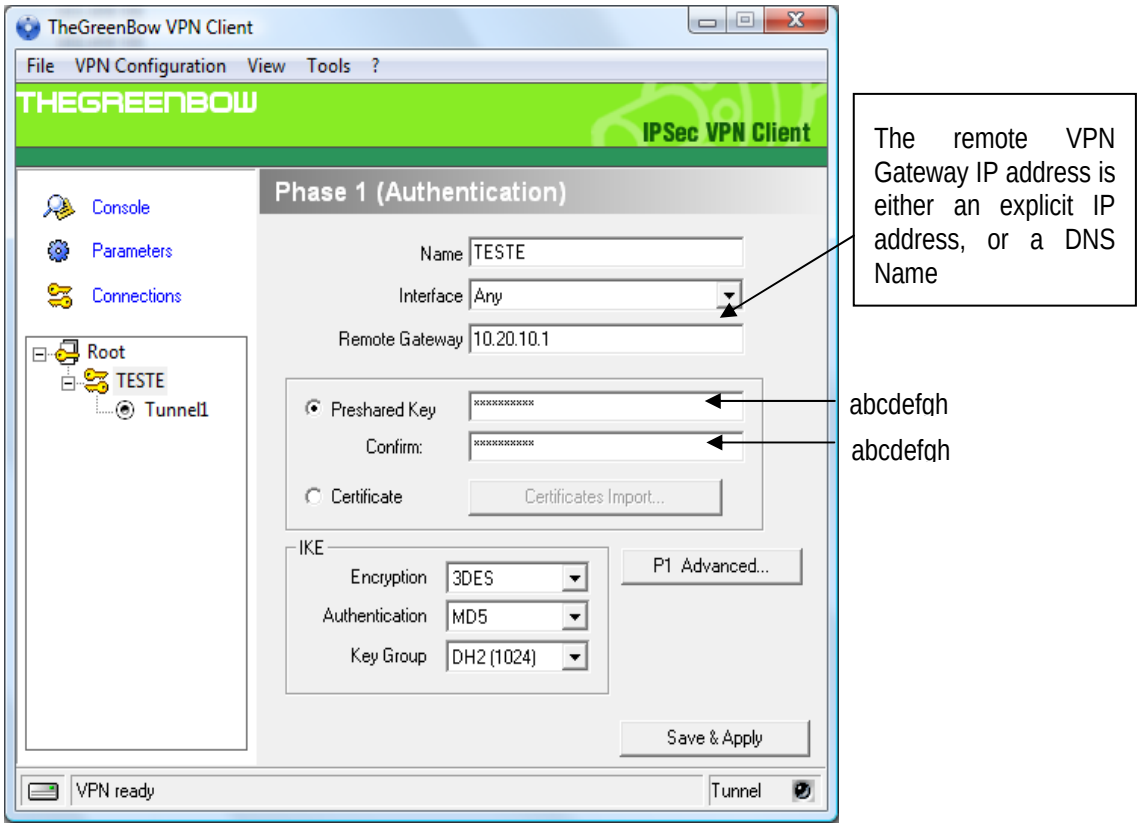
```
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
 class class_sip_tcp
  inspect sip
policy-map type inspect dns migrated_dns_map_1
 parameters
  message-length maximum 512
!
service-policy global_policy global
group-policy DfltGrpPolicy attributes
 vpn-simultaneous-logins 20
 vpn-tunnel-protocol IPSec l2tp-ipsec
 nac-settings value DfltGrpPolicy-nac-framework-create
 webvpn
  svc dpd-interval client none
  svc dpd-interval gateway none
group-policy pocket@vpn.com internal
group-policy pocket@vpn.com attributes
 vpn-tunnel-protocol IPSec
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value pocket@vpn.com_splitTunnelAcl
username pocketvpn password ltT0Umxsjt92h2um encrypted privilege 0
username pocketvpn attributes
 vpn-group-policy pocket@vpn.com
tunnel-group DefaultL2LGroup ipsec-attributes
 isakmp keepalive threshold 60 retry 2
tunnel-group DefaultRAGroup ipsec-attributes
 isakmp keepalive threshold 60 retry 2
tunnel-group pocket@vpn.com type remote-access
tunnel-group pocket@vpn.com general-attributes
 address-pool vpnpool
 default-group-policy pocket@vpn.com
tunnel-group pocket@vpn.com ipsec-attributes
 pre-shared-key *
tunnel-group-map enable rules
prompt hostname context
Cryptochecksum:75c4246e0696f8d6b8a627f1fa419e15
: end
```

3 TheGreenBow IPSec VPN Client configuration

This section describes the required configuration to connect to a Cisco ASA 5510 VPN router.

To download the latest release of TheGreenBow IPSec VPN Client software, please go to http://www.thegreenbow.com/vpn_down.html or http://www.thegreenbow.com/mobile_down.html for VPN Mobile software. They both use the same VPN Configuration file.

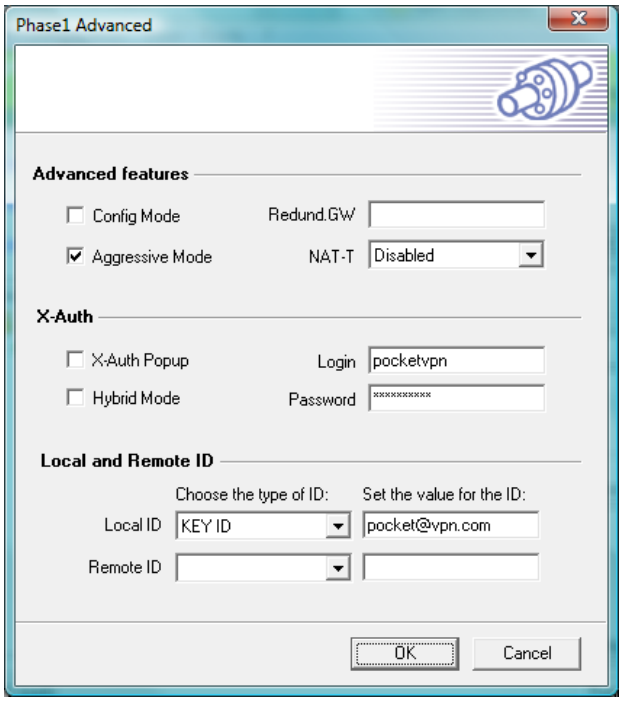
3.1 VPN Client Phase 1 (IKE) Configuration



Phase 1 configuration

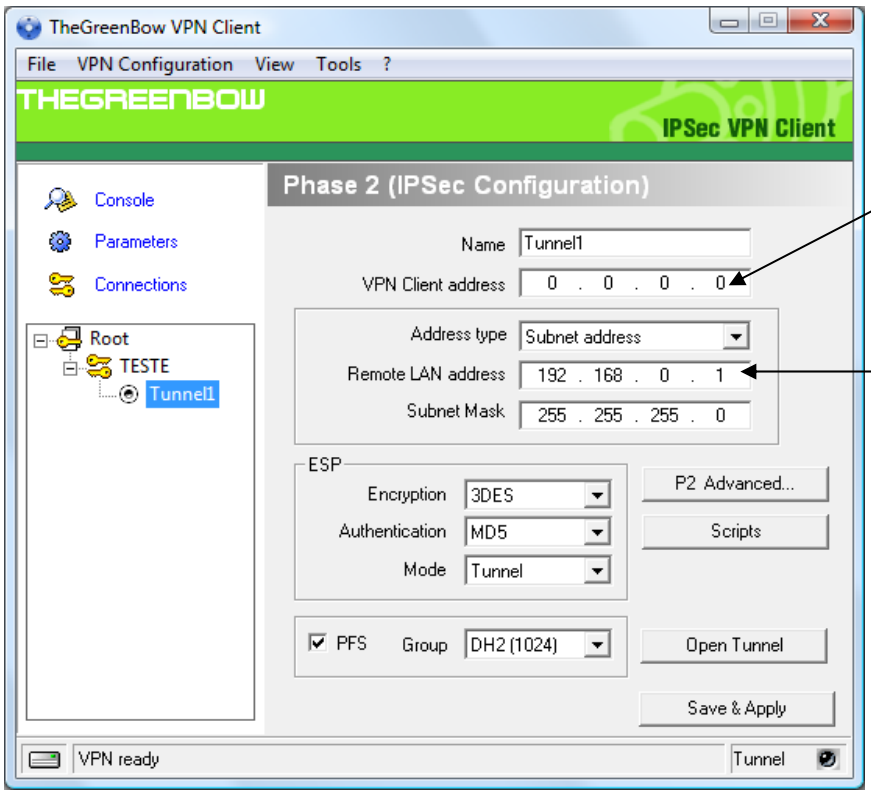
You may use either Preshared, Certificates, USB Tokens or X-Auth for User Authentication with the Cisco ASA 5510 router. This configuration is one example of can be accomplished in term of User Authentication. You may want to refer to either the Cisco ASA 5510 router user guide or TheGreenBow IPSec VPN Client User Guide for more details on User Authentication options.

3.2 VPN Client Phase 1 (IKE) Advanced



In this Cisco ASA 5510 VPN configuration, the Aggressive Mode is selected, NAT-T is disabled, and X-Auth authentication method is used.

3.3 VPN Client Phase 2 (IPSec) Configuration



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

3.4 Open IPSec VPN tunnels

Once both Cisco ASA 5510 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.

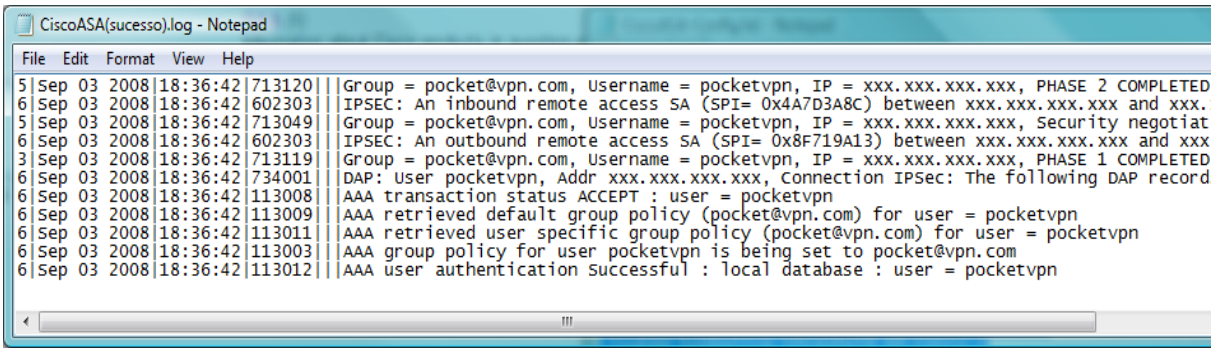
1. Click on "Save & Apply" to take into account all modifications we've made on your VPN Client configuration

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 Cisco ASA 5510 VPN router.

Here are the Cisco ASA 5510 logs:



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/).

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 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.

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