TheGreenBow IPSec VPN Client

Configuration Guide

Panda GateDefender Integra

WebSite: http://www.thegreenbow.com

Contact: support@thegreenbow.com

Table of contents

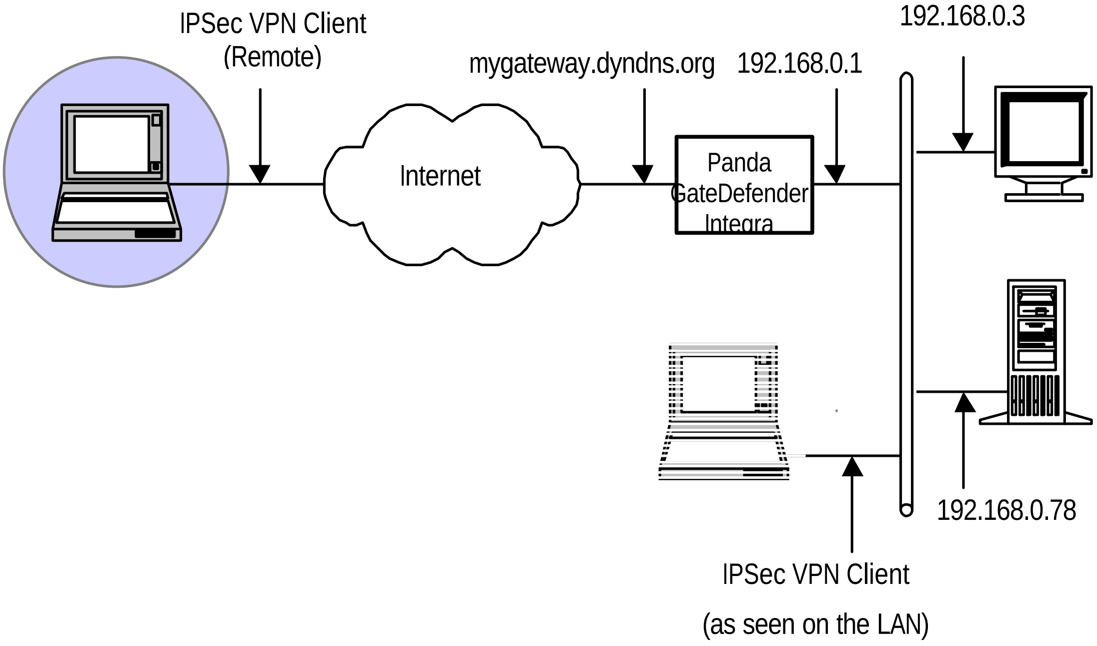
1 Introduction

1.1 Goal of this document

This configuration guide describes how to configure TheGreenBow IPSec VPN Client with a Panda GateDefender Integra 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 Panda GateDefender Integra 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 Panda GateDefender Integra Restrictions

Depending on the firmware version, Panda GateDefender Integra may not support NAT-T. The IPSec VPN Client cannot connect if it stands on a LAN.

1.4 Panda GateDefender Integra VPN Gateway

Our tests and VPN configuration have been conducted with Panda GateDefender Integra firmware release version 1.0.

2 Panda GateDefender Integra VPN configuration

This section describes how to build an IPSec VPN configuration with your Panda GateDefender Integra VPN router.

Once connected to your VPN gateway, you must follow these steps:

2.1 IP group configuration

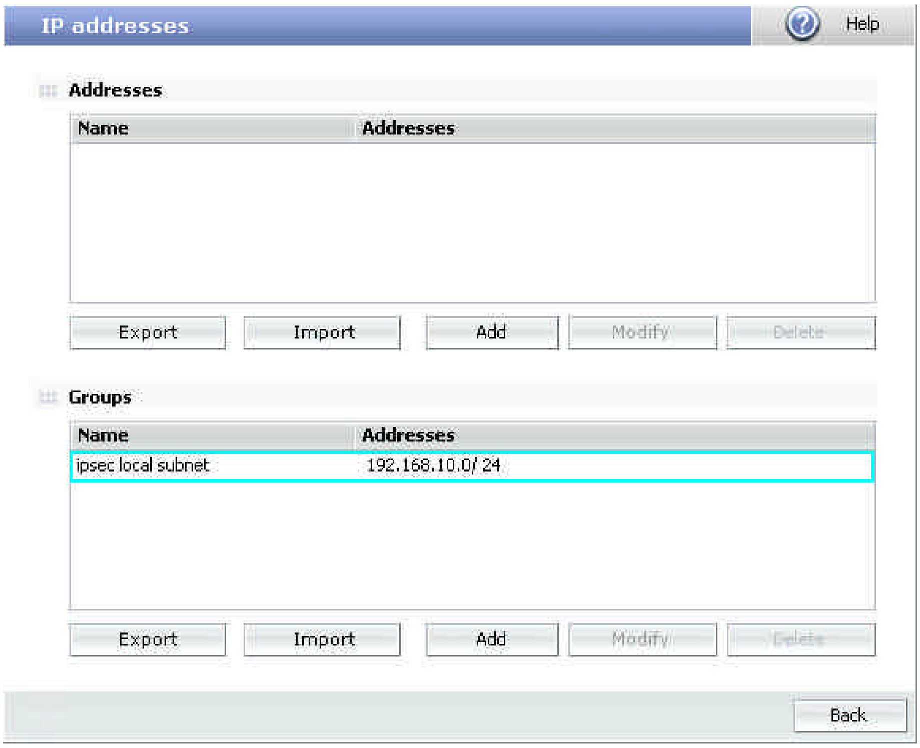
The first step when configuring IPSec VPN consists of defining IP range as a local subnet which you want your roadwarrior to be able to connect to.

To define local subnet, follow the steps described below:

1. Access the **Definitions** section of the main Panda GateDefender Integra console menu.
2. Select **IP addresses.**
3. In the **Groups** section, click on the **Add** button.
   A descriptive name of the group must be provided ***(ipsec local subnet*** will be used for this how-to) to **Name** field and ip range (***192.168.10.0/24*** will be used in this how-to) in **IP/Mask** radio button section.
4. Click on **Add IP.**

The settings will be configures as shown in figure 1

Note that you cannot use previously defined IP Group that has been already assigned to other VPN



Name	Addresses
ipsec local subnet	192.168.10.0/ 24

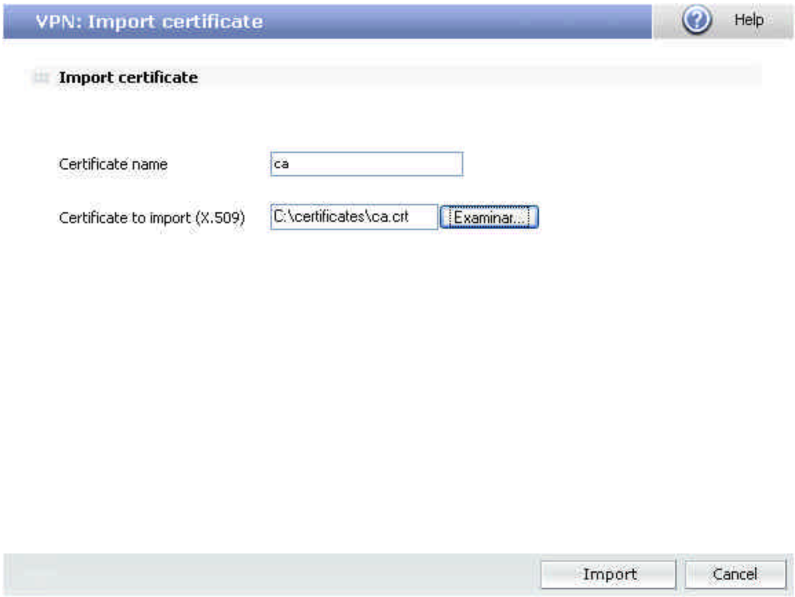
Figure 1

2.2 CA and local server certificates

Certificates are required for authentication purposes. You need to import public ca certificates which signed the roadwarrior certificates. It is also necessary to import the Integra VPN gateway local certificate that would be used to authenticate Integra VPN server itself.

In order to import CA, follow the procedure below:

1. Go to the **VPN** section of the main Panda GateDefender Integra console menu
2. Select **Digital certificate management**
3. In the **CA certificates** section, click on the **Import** button
   - Enter **Certificate name** (***ca*** will be used in this how-to)
   - Click on **Browse...** to select the certificate you want to import.
   - Click on **Import** once you have chosen a CA certificate that you wish to import



Certificate name: ca

Certificate to import (X.509): C:\certificates\ca.crt

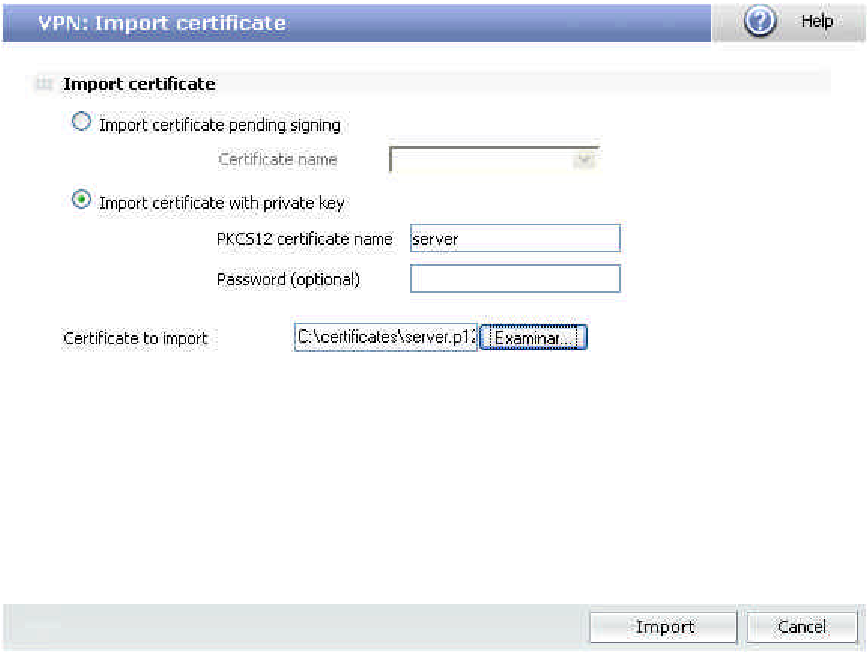
Figure 2

In order to import local server certificates, follow the procedure below:

1. Go to the **VPN** section of the main Panda GateDefender Integra console menu
2. Select **Digital certificate management** and, in the **Local certificates** section, click on the **Import** button.

   - Select if you want to **Import a certificate pending signing** or **Import a certificate with private key** issued by a CA.
   - If you select **Import certificate with private key**, enter PKCS12 Certificate Name (***server*** will be used in this how-to) and optionally **Password**

1. Click on **Browse...** to select the certificate you want to import
2. Click on **Import** once you have chosen a certificate.



VPN: Import certificate

Import certificate

○ Import certificate pending signing

Certificate name

● Import certificate with private key

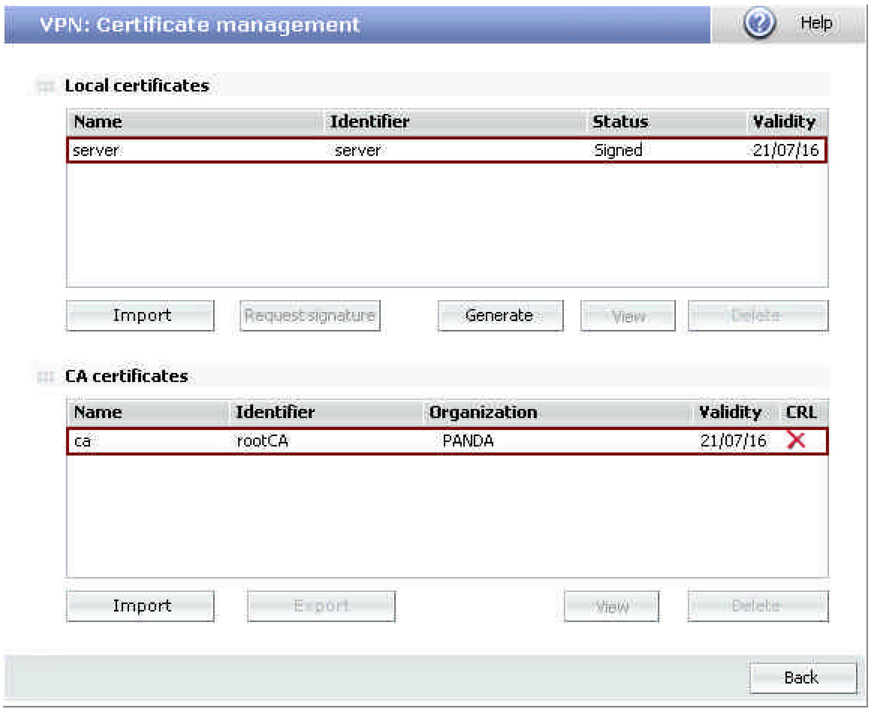
PKCS12 certificate name: server

Password (optional):

Certificate to import: C:\certificates\server.p12

Figure 3

Once the CA and server certificates have been imported successfully, the corresponding configuration screen displayed is similar as shown in figure 4



VPN: Certificate management

Local certificates

Name	Identifier	Status	Validity
server	server	Signed	21/07/16

CA certificates

Name	Identifier	Organization	Validity	CRL
ca	rootCA	PANDA	21/07/16	✗

Figure 4

Note that if you select **Import certificate with private key,** it is allowed to import only local certificates that are conformed with PKCS12 format (file has p12 or pfx extension).

2.3 Users and group configuration (optionally)

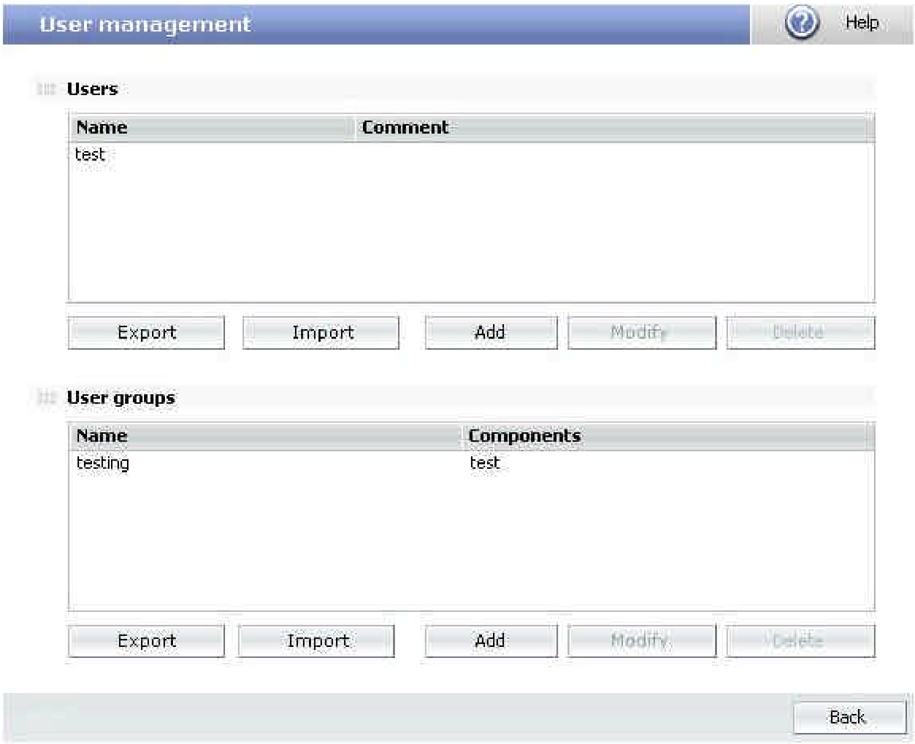
1. Access the **Definitions** section of the main Panda GateDefender Integra console menu
2. Select **User management**
3. In the **Users** section, click on the **Add** button.
4. This will take you to a screen where you should provide data for at least the first three textboxes:
   - ✍ Name (***test*** will be used for this how-to)
   - ✍ Password ***(testing*** will be used for this how-to)
   - ✍ Repeat password.
5. Once you have configured it, click on Add to save the changes.

As defined groups of vpn users were needed, now we need to add previously defined users to our group.

In order to do this, follow the steps below:

1. Access the **Definitions** section of the main Panda GateDefender Integra console menu
2. Select **User management**
3. In the **User Groups** section, click on the **Add** button.
4. Define a group name and add users from the box bellow.

Once this has been done, configuration should be similar as shown in figure 5



Users

Name	Comment
test	

User groups

Name	Components
testing	test

Figure 5

2.4 IPSec configuration on server side

This section is related to the IPSec configuration.

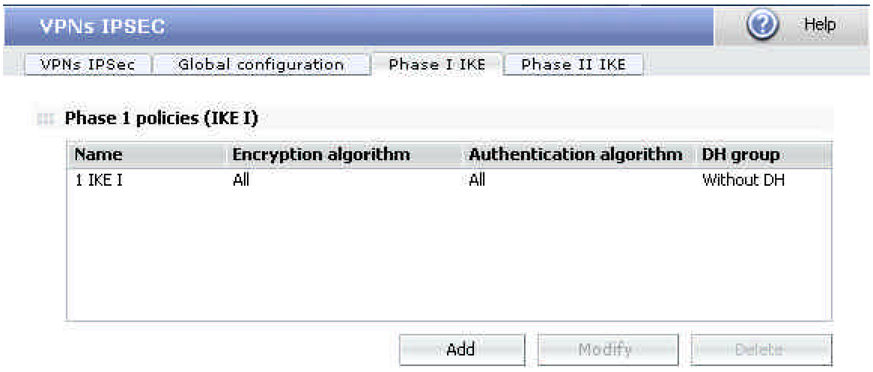
In order to configure IPSec using previously defined elements follow the instructions below:

1. Go to the Panda GateDefender Integra administration console.
2. Click on VPN in the panel on the left.
3. Then select VPN management, and then IPSEC VPN management.

The available options are:

1. **Name**: Enter the descriptive name of the VPN. (***IPSec RW GreenBow*** will be used in this how-to)
2. **Local IP**: Enter the **local public IP** address or choose **IP assigned by DHCP (*Local public IP 62.12.249.65*** will be used in this how-to**)**
3. **Phase 1 policy**: Use the drop-down menu to select the IKE I policy you want to apply. (***1 IKE I*** will be used in this configuration).

   Here is the screenshot of the 1 IKE I policy (with a default options)



Phase 1 policies (IKE I)

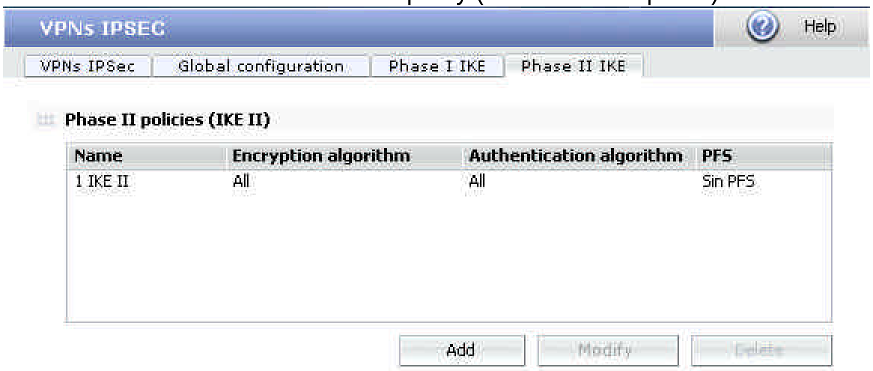
Name	Encryption algorithm	Authentication algorithm	DH group
1 IKE I	All	All	Without DH

4. Select a protocol to use: **IPSec**
5. When you choose IPSEC, the following options will be available:

? **Local subnet**: Select a subnet from those defined in the drop-down menu.

? **Phase II policy**: IKE II policy identifier of this tunnel.

Here is the screenshot of the 1 IKE II policy (with a default options)



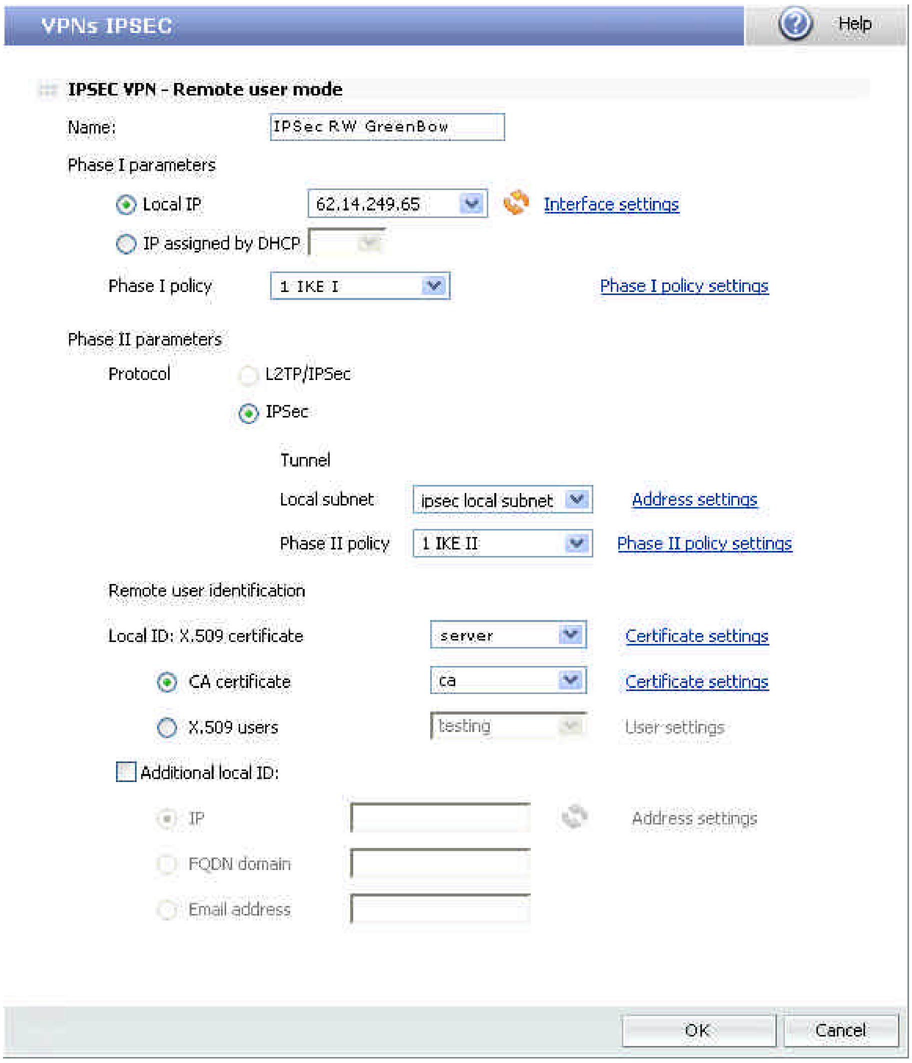
Phase II policies (IKE II)

Name	Encryption algorithm	Authentication algorithm	PFS
1 IKE II	All	All	Sin PFS

? **Local ID: X-509 certificate:** Use the drop-down menu to select local server certificate (***server.p12*** will be used in this how-to).

? **CA certificate**: Remote users authenticating using an X-509 certificate must also present the signature of a CA. Use the drop-down menu to select the CA certificate that signed roadwarriors certificate (***ca.crt*** will be used in this how-to)

Once the IPSEC part has been configured, the corresponding configuration screen which will be the following:



VPNs IPSEC

IPSEC VPN - Remote user mode

Name: IPSec RW GreenBow

Phase I parameters

● Local IP: 62.14.249.65 — Interface settings

○ IP assigned by DHCP

Phase I policy: 1 IKE I — Phase I policy settings

Phase II parameters

Protocol: ○ L2TP/IPSec ● IPSec

Tunnel

Local subnet: ipsec local subnet — Address settings

Phase II policy: 1 IKE II — Phase II policy settings

Remote user identification

Local ID: X.509 certificate: server — Certificate settings

● CA certificate: ca — Certificate settings

○ X.509 users: testing — User settings

□ Additional local ID:

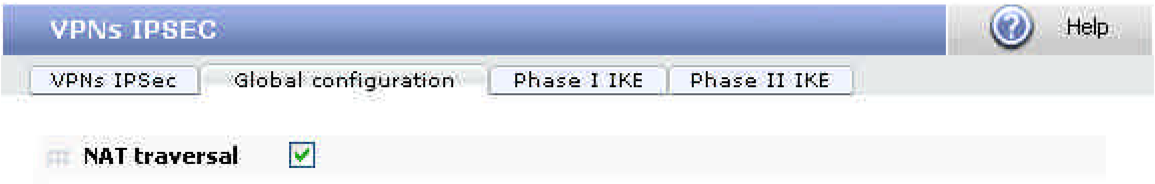
● IP — Address settings

○ FQDN domain

○ Email address

Optionally can be provided previosly defined group of users if option **X.509 users** are selected.

Note that if there is any NAT device between a roadwarrior and Integra VPN gateway, then you should enable the NAT transversal verification checkbox as shown below.

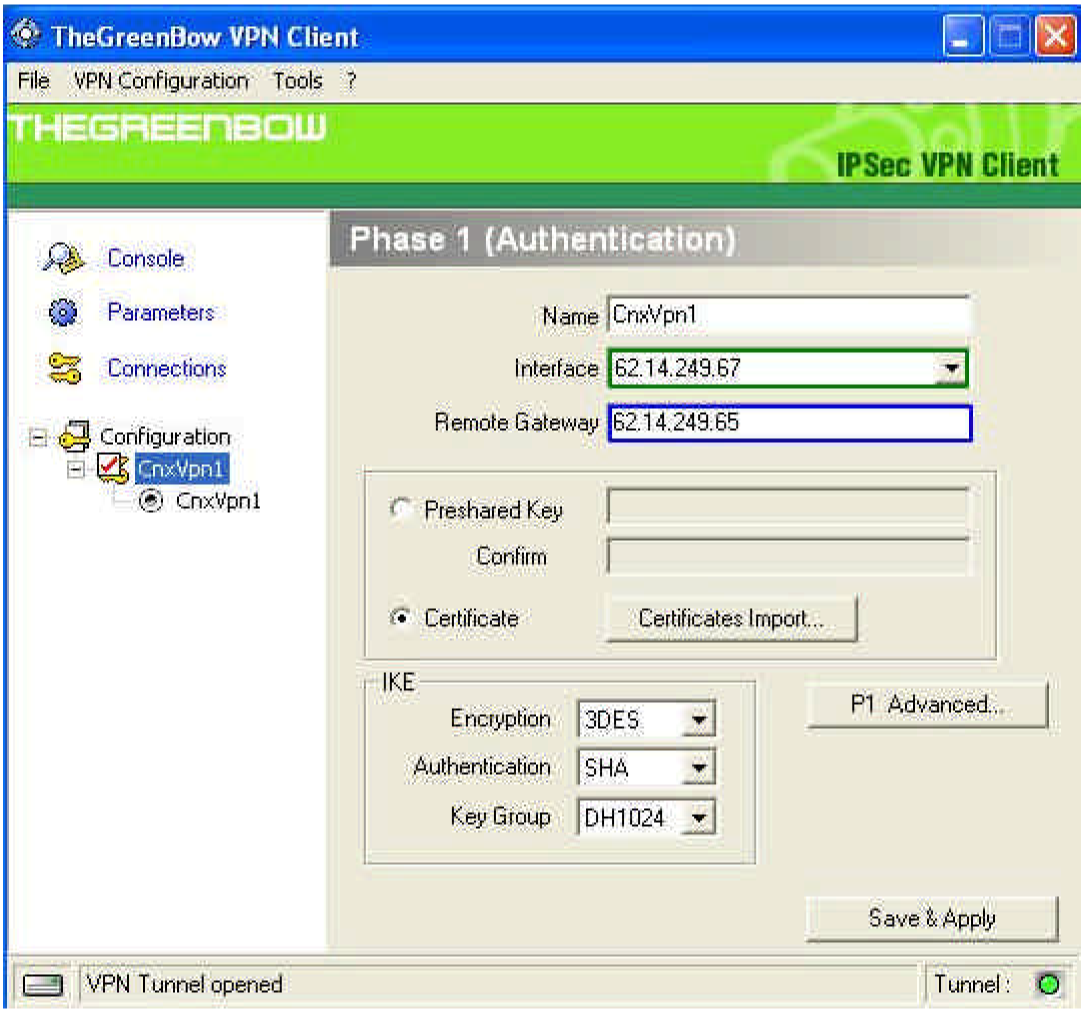


VPNs IPSEC

NAT traversal ☑

3 TheGreenBow IPSec VPN Client configuration

3.1 VPN Client Phase 1 (IKE) Configuration



Phase 1 (Authentication)

Name: CnxVpn1

Interface: 62.14.249.67

Remote Gateway: 62.14.249.65

○ Preshared Key

Confirm

● Certificate

IKE

Encryption: 3DES

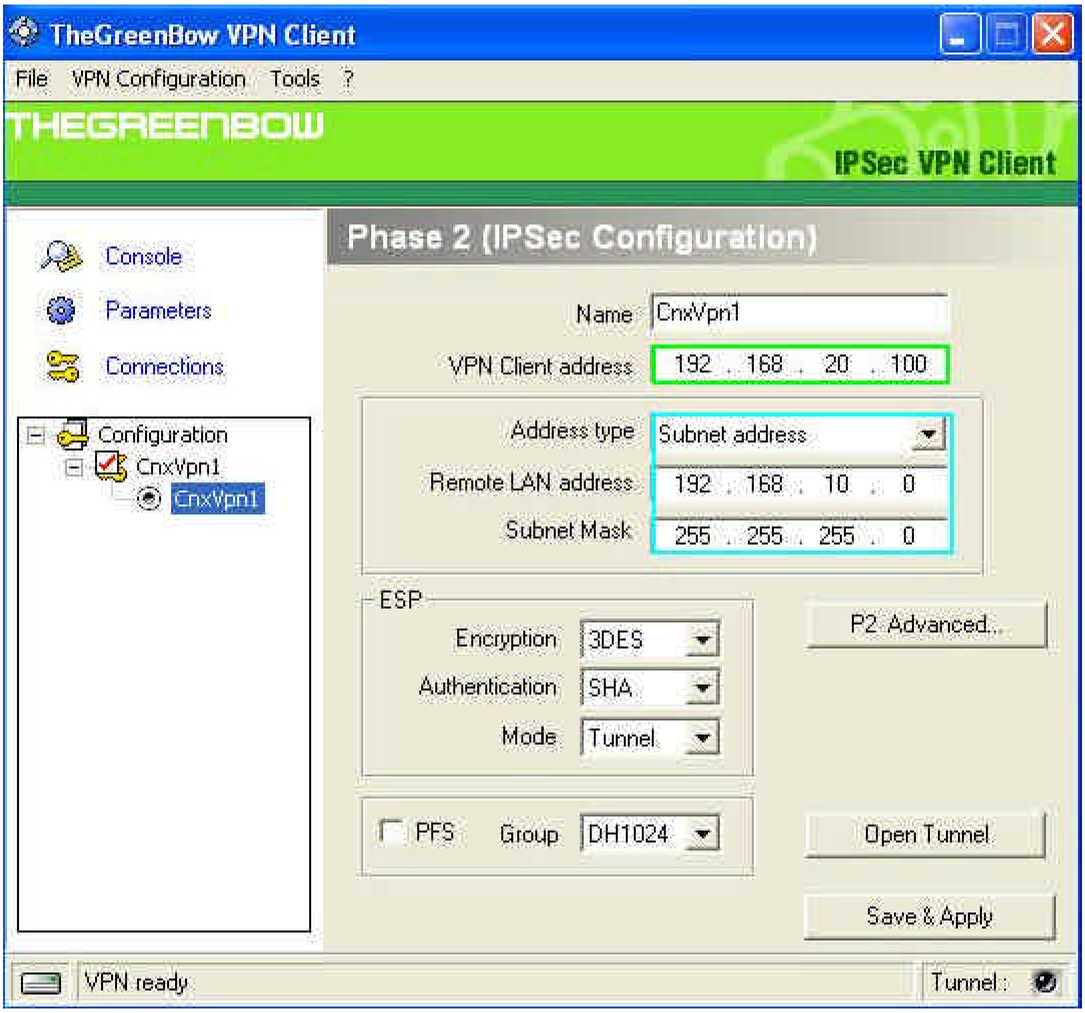
Authentication: SHA

Key Group: DH1024

VPN Tunnel opened

Phase 1 configuration

3.2 VPN Client Phase 2 (IPSec) Configuration



Name: CnxVpn1

VPN Client address: 192 . 168 . 20 . 100

Address type: Subnet address

Remote LAN address: 192 . 168 . 10 . 0

Subnet Mask: 255 . 255 . 255 . 0

ESP

Encryption: 3DES

Authentication: SHA

Mode: Tunnel

□ PFS Group: DH1024

VPN ready

Tunnel :

Phase 2 Configuration

3.3 Open IPSec VPN tunnels

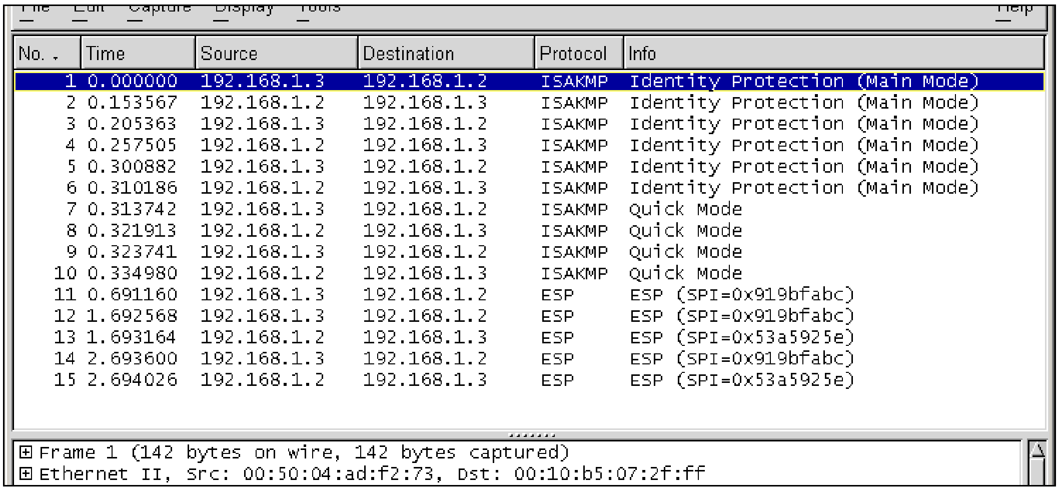
Once both Panda GateDefender Integra router and TheGreenBow IPSec VPN Client have been configured accordingly, you are ready to open VPN tunnels. First make sure you enable your firewall with IPSec traffic.

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 Microsoft Windows 2000 Server.



```
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
```

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