Panda GateDefender Integra

# HOWTO: How to configure IPSEC roadwarrior to gateway using The GreenBow client


## 'How-to' guides for configuring VPNs with GateDefender Integra

Panda Security wants to ensure you get the most out of GateDefender Integra. For this reason, we offer you all the information you need about the characteristics and configuration of the product. Refer to http://www.pandasecurity.com/ and http://www.pandasecurity.com/enterprise/support/ for more information.

## 'How-to' guides for Panda GateDefender Integra

The software described in this document is delivered under the terms and conditions of the end user license agreement and can only be used after accepting the terms and conditions of said agreement.

The anti-spam technology in this product is provided by Mailshell. The web filtering technology in this product is provided by Cobion.

### Copyright notice



### Registered Trademarks

# INDEX



**Symbols and styles used in this documentation**

**Symbols used in this documentation:**

**Note**. Clarification and additional information.

**Important**. Highlights the importance of a concept.

**Tip**. Ideas to help you get the most from your program.

**Reference**. Other references with more information of interest.

**Fonts and styles used in the documentation:**

**Bold**: Names of menus, options, buttons, windows or dialog boxes.

*Codes style*: Names of files, extensions, folders, command line information or configuration files, for example, scripts.

*Italics*: Names of options related with the operating system and programs or files with their own name.

# IPSec roadwarrior-to-gateway using The GreenBow client

(IP Secure) Security protocol that allows the secure interchange of packets in the IP layer, guaranteeing the security of the link between the device and a network. It offers integrity, authentication, access control and confidentiality for sending IP packets via Internet

Panda GateDefender Integra includes a VPN system to create your own virtual private networks, widening the reach of your network and ensuring confidential connections.

The purpose of this guide is to describe the steps to create a IPsec virtual private network (VPN) with Panda GateDefender Integra, using real data.

**Note:** It is taken for granted that the Panda GateDefender Integra appliance is already configured, at least basically, and working. For further information about how to install and configure Panda GateDefender Integra, refer to the Installation Guide.

**Important:** Panda GateDefender Integra must be working in Router mode. Otherwise, you will not be able to use the VPN system.

## 1.1 Scenario setup

The illustration below is a typical roadwarrior-to-gateway IPSec VPN scenario:

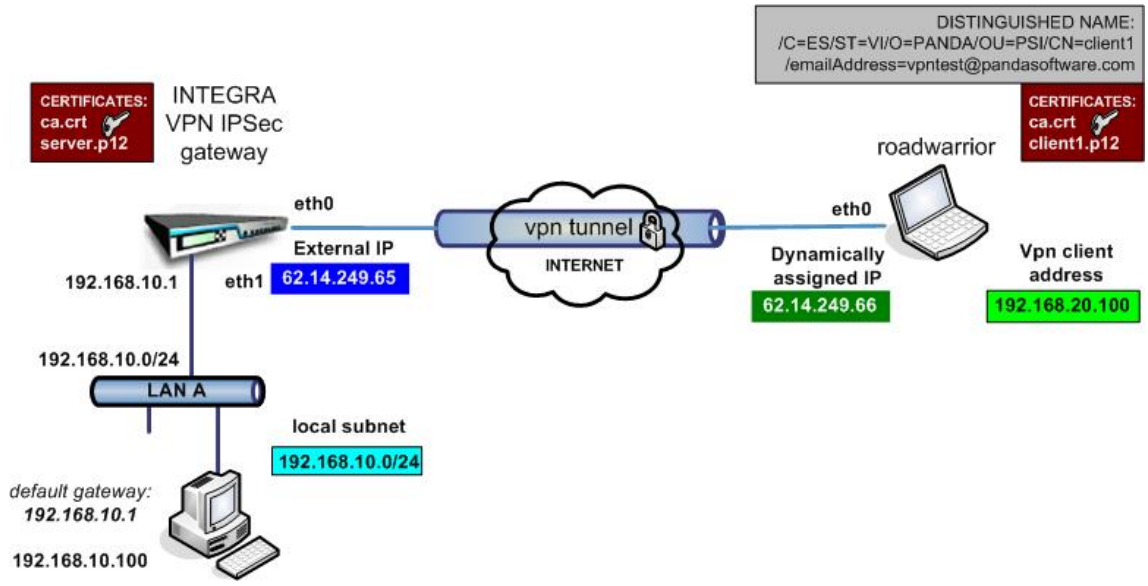



**Figure 5.1: IPSec VPN**

The roadwarrior has been dynamically assigned an address by the ISP and will access Integra's LAN by means of a secure tunnel using the IPSec protocol.

In this how-to, INTEGRA's WAN or Internet interface are assigned the IP address **62.14.249.66.**

Clients on Integra's LAN side must have configured Integra's LAN IP **192.168.10.1** as a default gateway or as an implicit route to the roadwarrior VPN client address. See the section below on how-to configure routes on the hosts on the INTEGRA LAN side.

**Index**

## 1.2 Gateway side configuration (Panda GateDefender Integra)

### 1.2.1 IP group configuration

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

To define the 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 **Add**.
   A descriptive name of the group must be provided ***(ipsec local subnet*** will be used for this how-to) in the **Name** field and the IP range (***192.168.10.0/24*** will be used in this how-to) in the **IP/Mask** radio button section.
4. Click on **Add IP.**

The settings will be configured as shown in figure 5.2

Note that you cannot use a previously defined IP Group that has been already assigned to another VPN.

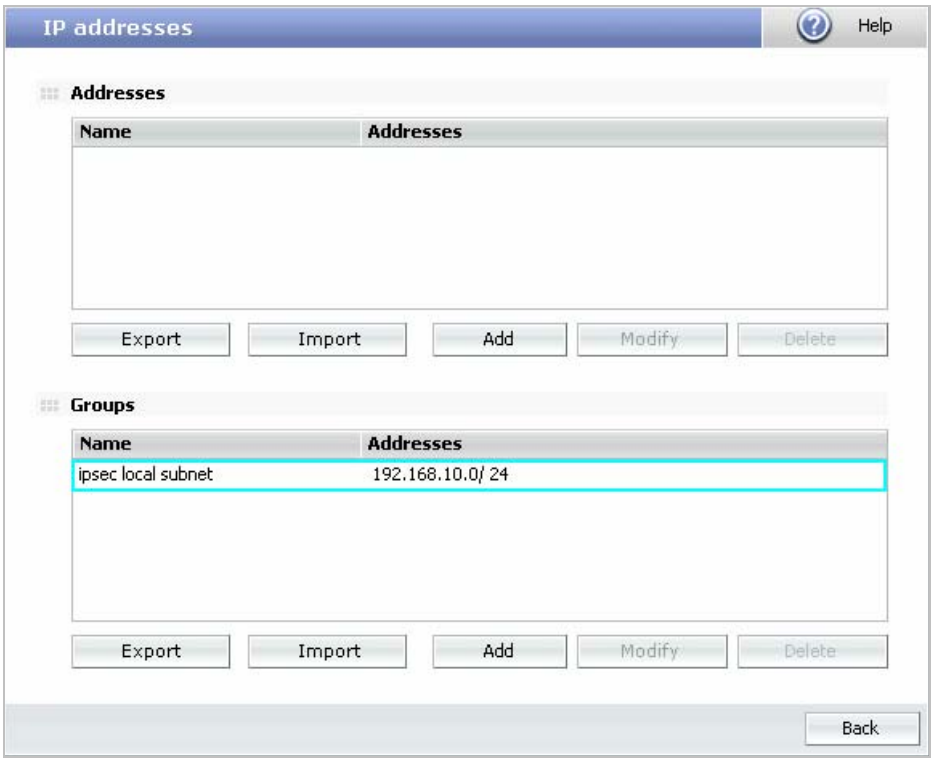



**Figure 5.2**

### 1.2.2 CA and local server certificates

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

In order to import the 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 **Import**.

    - 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.

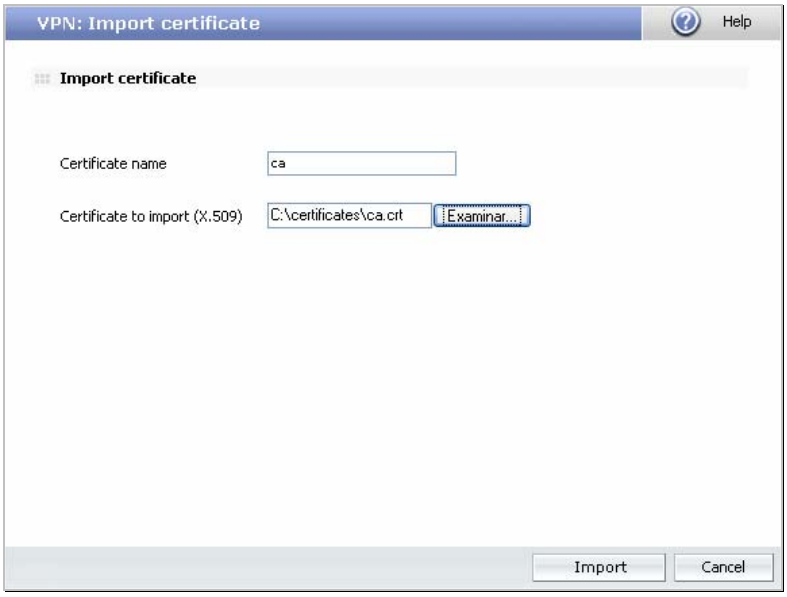



**Figure 5.3**

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 **Import**.

    - 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 the PKCS12 Certificate Name (***server*** will be used in this how-to) and optionally **Password**.

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


**Figure 5.4**

Once the CA and server certificates have been imported successfully, the corresponding configuration screen displayed is similar to that shown in figure 5.5

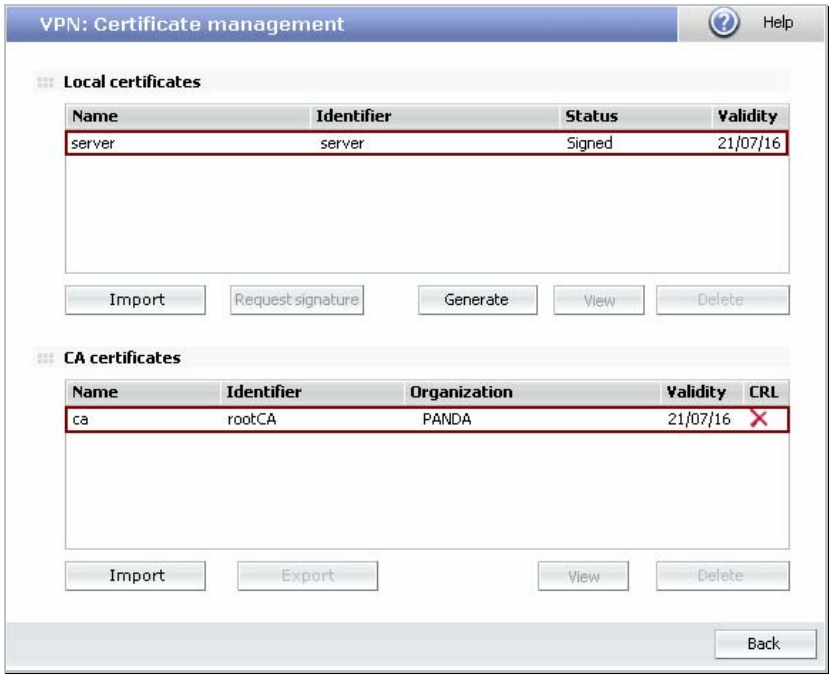



**Figure 5.5**

Note that if you select **Import certificate with private key,** you can only import local PKCS12 format certificates (files have p12 or pfx extensions).

**Index**

### 1.2.3 Users and group configuration (optional)

1. Access the **Definitions** section of the main Panda GateDefender Integra console menu.
2. Select **User management**.
3. In the **Users** section, click on **Add**.
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, you need to add previously defined users to your 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 **Add**.
4. Define a group name and add users from the box below.

Once this has been done, configuration should be similar to that shown in figure 5.6

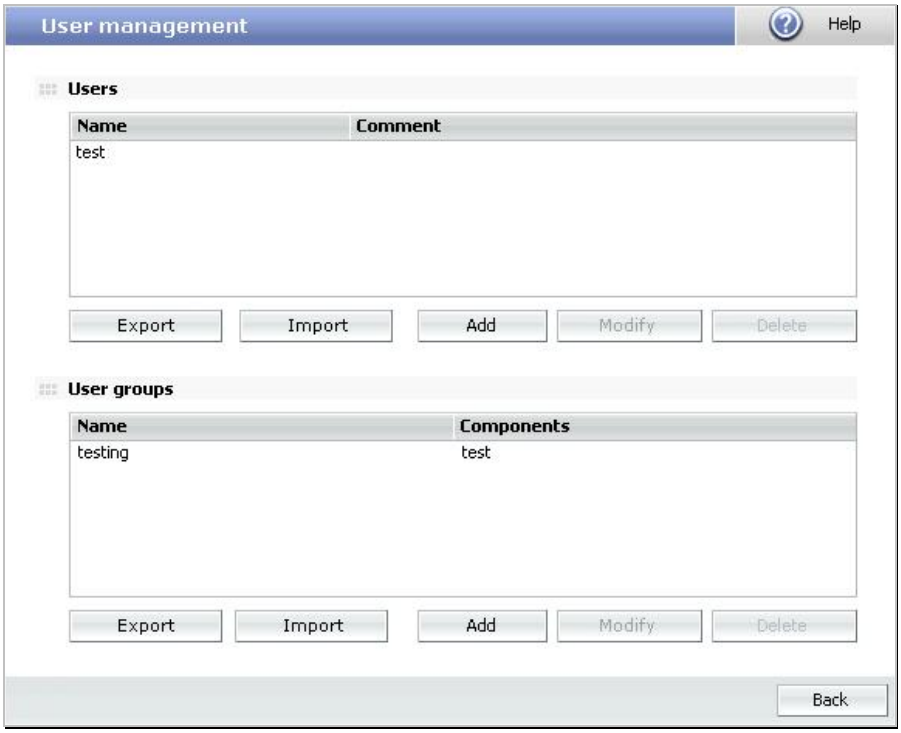



**Figure 5.6**

### 1.2.4 IPSec configuration on the 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:

   - **Name**: Enter the descriptive name of the VPN. ( ***IPSec RW GreenBow*** will be used in this how-to).
   - **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).
   - **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 how-to).

     Here is the screenshot of the 1 IKE I policy (with a default options) used in this how-to.

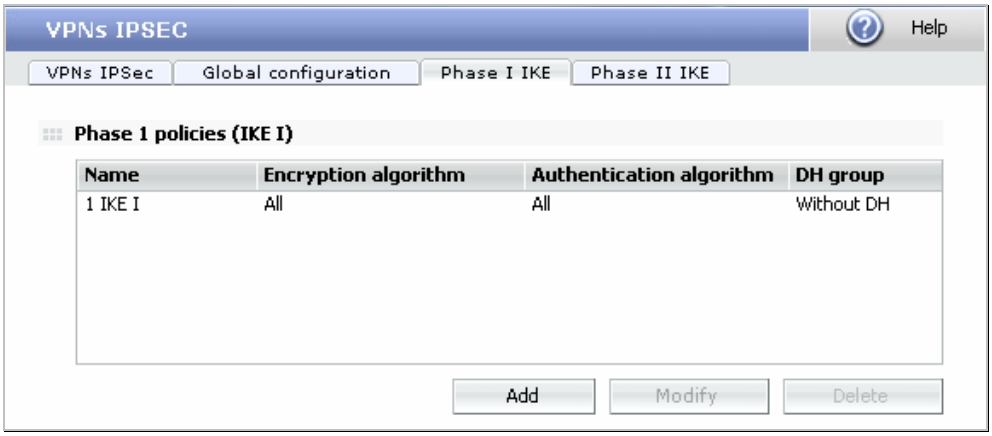



**Figure 5.7**

1. Select a protocol to use: **IPSec**
2. 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) used in this how-to.


**Figure 5.8**

- **Local ID: X-509 certificate:** Use the drop-down menu to select the 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 the 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 displayed will be similar to figure 5.9

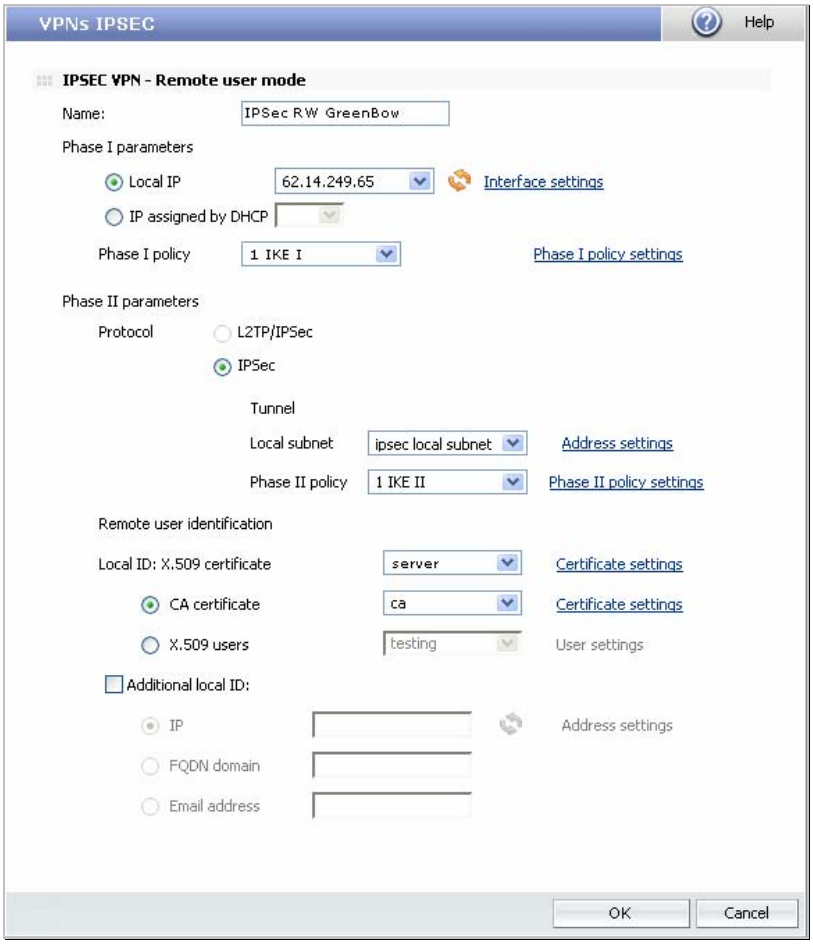



**Figure 5.9**

Optionally, a previously defined group of users can be provided, if option **X.509 users** is 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.


**Figure 5.10**

**Index**

## 1.3 Client side configuration (TheGreenBow client)

Once it has been confirmed that the connection to the Internet is correctly configured on the client computers running Microsoft Windows 2000/XP, and you install TheGreenBow IPSec client, follow the steps described below to configure the client side.

**Note:** For the correct functioning of The GreenBow client it is essential to disable the IPSEC services (Control Panel--> Administrative Tools--> Services)

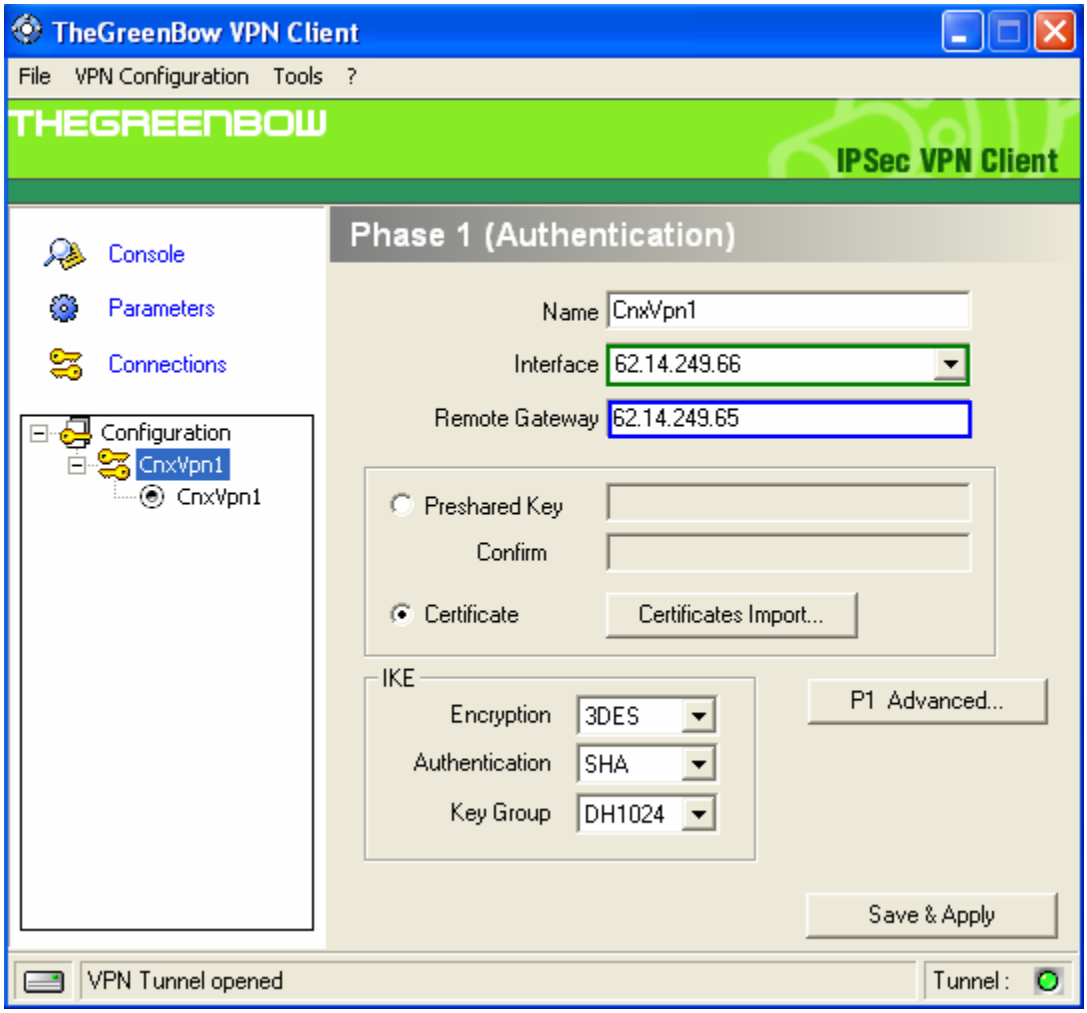



**Figure 5.11**

Certificates are required for authentication purposes. You need to import the trusted public CA certificates which signed the Integra VPN gateway certificate. It is also necessary to import the roadwarrior certificate and its corresponding private key that would be used to authenticate the roadwarrior itself.

In order to import CA and local certificates for a roadwarrior, click on **Certificate Import...**

Once the certificates have been imported you must provide at least **local ID** by clicking on **P1 Advanced...** Then, choose the **DER ASN1 DN** ID type and enter the corresponding ID for a local certificate as shown in figure 5.14.

DER ASN1 DN ID or **Distinguished Name** can be read from the local client certificate using openssl command:

***# openssl x509 –in client1.crt –noout –subject***

It is possible to access the whole subnet or just one specific host on Panda GD Integra LAN as shown in figures 5.12 and 5.13.

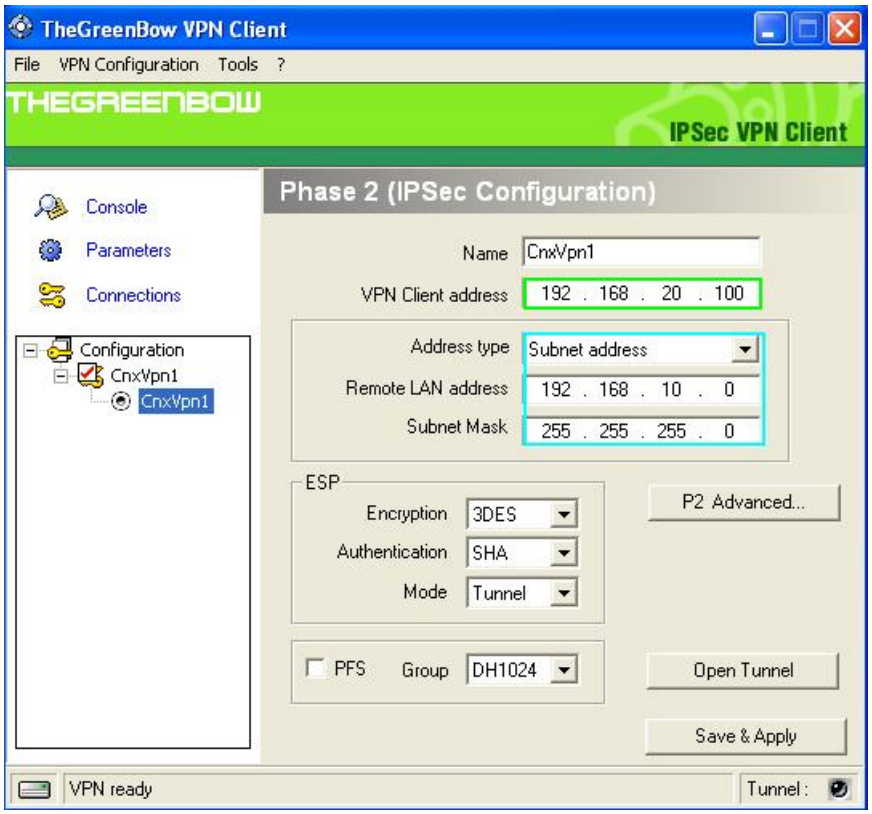



**Figure 5.12**

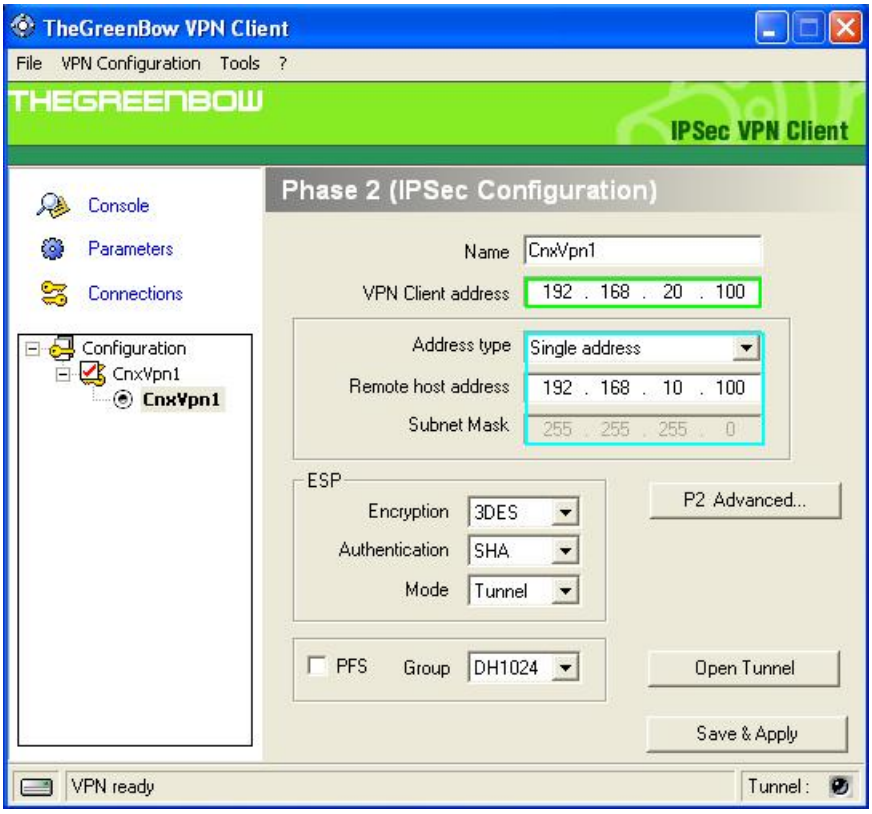



**Figure 5.13**

If Xauth is used as an authentication option on Panda GateDefender Integra then you should configure it also on the client side, as shown in figure 5.14.

Note that Aggressive Mode is not supported by Panda GateDefender Integra for security reasons.

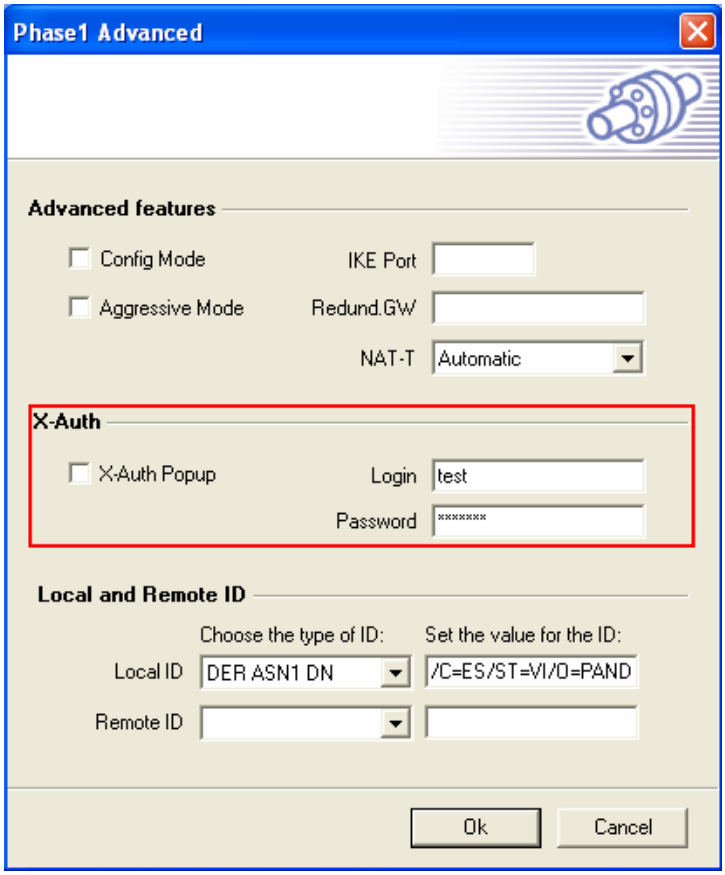



**Figure 5.14**

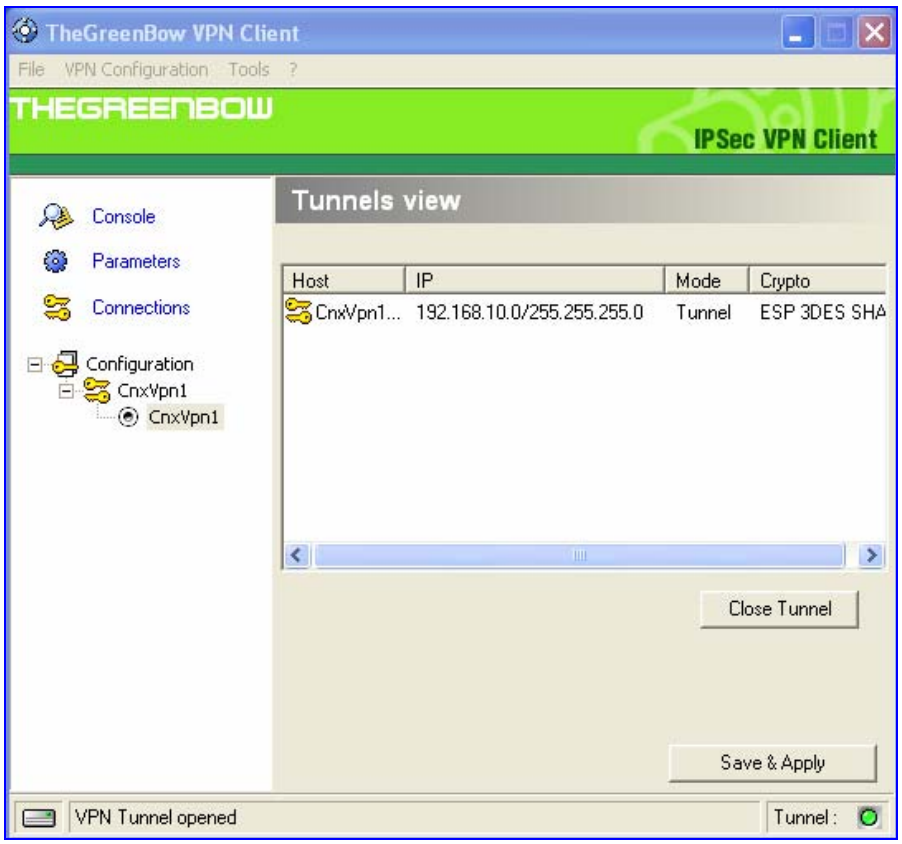
More details about configuration issues can be found on TheGreenBow website: *www.thegreenbow.com*

**Index**

## 1.4 Establishing IPSec VPN connection

Use the following procedure in order to establish IPSec VPN connection which has been previously defined:

1. Click on "**Save & Apply**" to take into account all modifications 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 open 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 Panda GateDefender Integra.

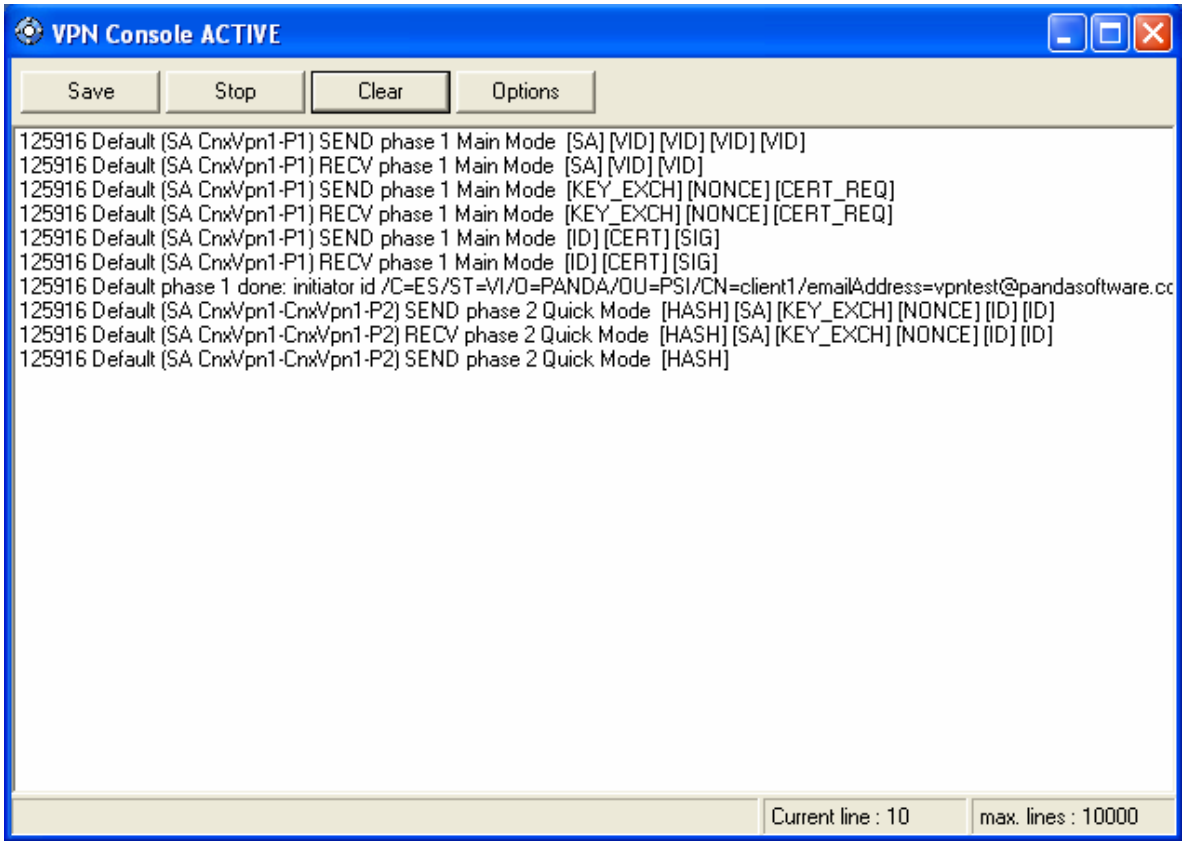



**Figure 5.15**

Once the VPN tunnel has been established, specific network resources should be available to you as they are when you connect directly to the network.

In order to disconnect, right-click on the TheGreenBow icon that appears in the bottom right corner, and then select **Quit** or just press **Close Tunnel** in TheGreenBow client window.

**Index**

## 1.5 Further considerations

If Integra's firewall is used, all the corresponding configuration rules will automatically be entered in the firewall.

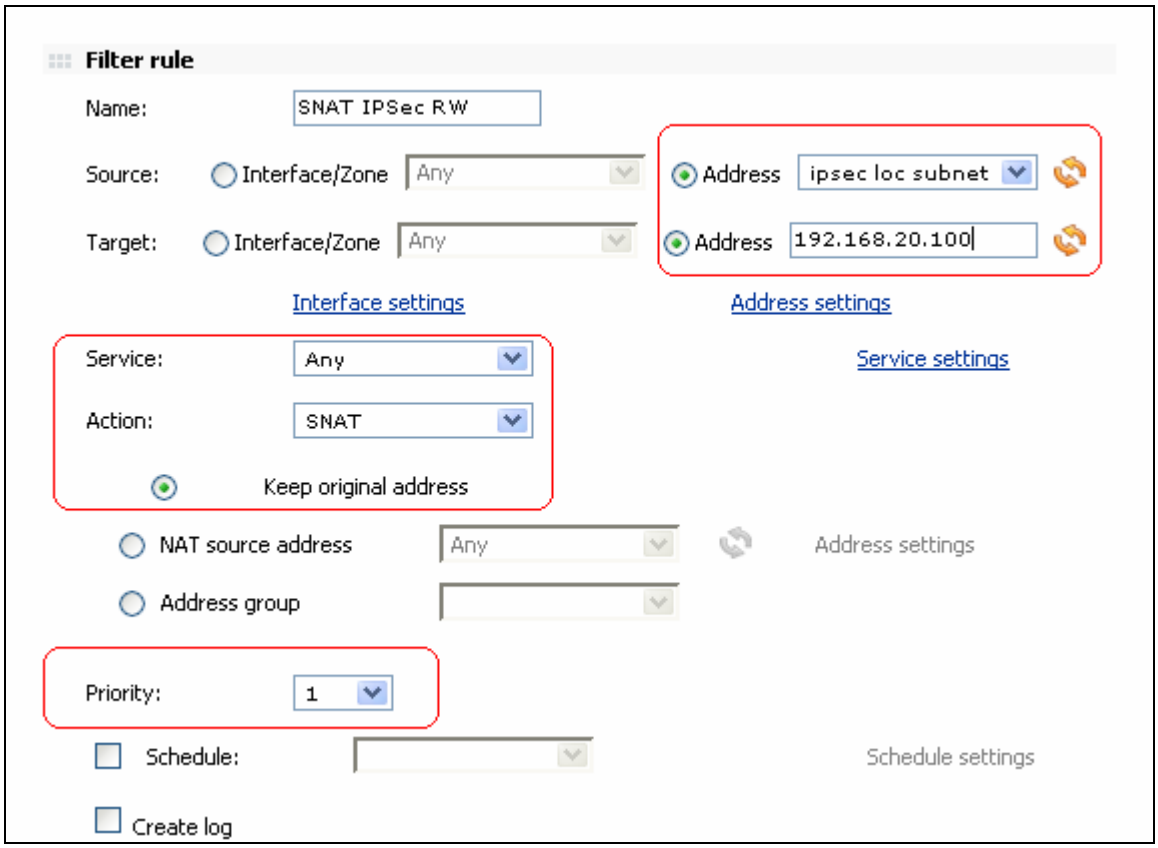
But if you use a personal firewall or broadband router with firewall features or if there are routers or firewalls between TheGreenBow client and the Integra VPN gateway server, the following ports and protocols must be enabled for IPSec on all firewalls and routers between them:

- UDP port 500 (IKE)
- IP protocol 50 (ESP), 51 (AH) or

  UDP port 4500 (NAT-T): needed when there is at least a SNAT device between two gateways (the usual situation)

Note that IP 50 is a *protocol*, not a *port*.

If the SNAT option is enabled for the local network that intervenes in the VPN in any of the GateDefender Integra configurations -the Static key or certificates-, you need to add a NAT rule with a higher priority than the previous rule. This rule should ensure that the change of source IP header belonging to SNAT is not applied to the VPN traffic before the packets are routed to the tunnel. To do this, the *Keep original address* check box must be selected:



The example in the screenshot shows the rule to add to ensure that traffic from the local IPSEC subnet can be correctly routed through the VPN tunnel to the roadwarriors' network **192.168.20.100.**

**Index**

## 1.6 Configuration checking

In order to check the IPSec VPN configuration please proceed as described below::

1. Access the Panda GateDefender Integra administration console.
2. Click on **VPN** in the panel on the left.
3. Then select **VPN Monitor** which will allow you to see the status of all established VPN connections (as shown in figure 5.16).


**Figure 5.16**

Any of the roadwarriors can verify the configuration settings of its Windows 2000/XP independently.

In order to carry out that task, the command prompt should be used:

The **ping –n 10 192.168.10.100 command** pings from the roadwarrior to one of the hosts that reside on the internal network behind Integra VPN gateway and should see a response from the remote host.

At the same time, a network traffic monitoring tool such as Ethereal can be used to check if all the traffic between a roadwarrior and the gateway is encrypted.

The encrypted ESP (Encapsulating Security Payload) packets will be seen when observing traffic in the external network interface

More details about troubleshooting issues of TheGreenBow client can be found on its website: *www.thegreenbow.com*

**Index**


0707-PGDIHT09-03-EN