HOWTO: How to configure IPSEC gateway (office) to gateway

'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 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 gateway-to-gateway

(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 shows a typical gateway-to-gateway IPSec VPN scenario:

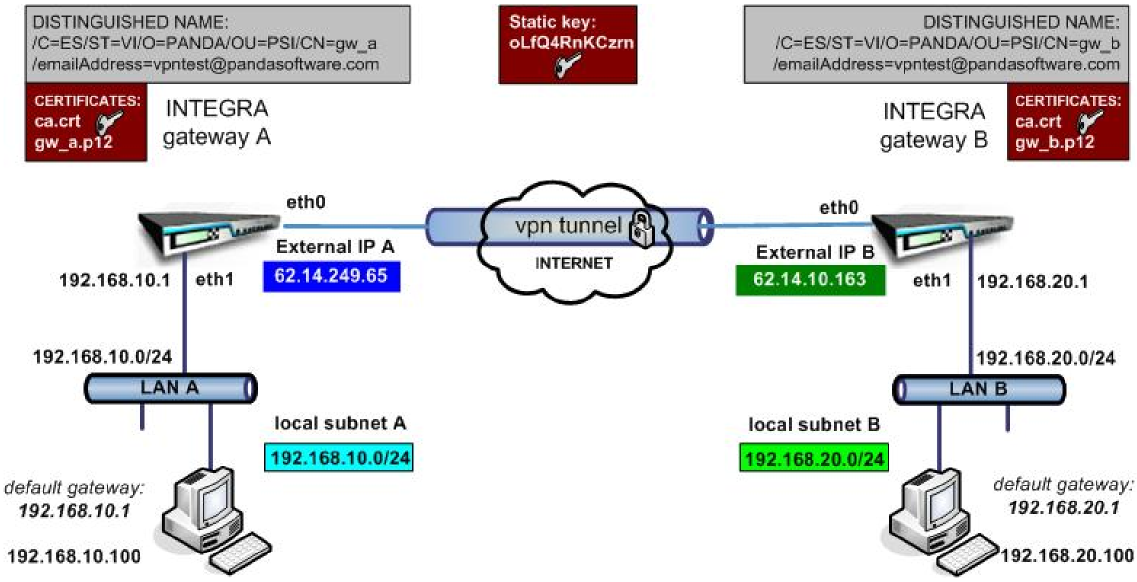


Figure 6.1 IPSec gateway-to-gateway VPN

Gateway A’s external local IP will be **62.14.249.65** and gateway B will have **62.14.10.163**

The figure shows that the eth0 interface has been assigned a public IP. In the most common configurations, Integra’s eth0/WAN interface will usually have a private IP address and will be one of the devices with the NAT option enabled located between VPN gateway and the ISP connection (for example ADSL router/modem, cable modem, etc.), which will have a public IP (dynamic or static).

This approach has been used to simplify the document and focus on the VPN configuration. For more information, refer to the How-to guides available about SNAT and DNAT configurations and port mapping.

Hosts that belong to local subnet A (identified as **192.168.10.0/24** in this how-to**)** must have configured Integra A LAN IP **192.168.10.1** as a gateway to local subnet B (identified as **192.168.20.0/24** in this how-to). The same applies to hosts on local subnet B; their gateway to local subnet A will be **192.168.20.1.** The route could be defined as a default gateway or implicit route. For the purpose of this how-to we assume that Integra’s LAN IP is the default gateway for corresponding hosts on INTEGRA’s local subnets.

In order to authenticate each gateway, you can use the static key or certificates (TLS).

Index

1.2 Gateway A setup

1.2.1 IP group configuration

The first step when configuring this kind of IPSec VPN will be to define a group of IP addresses that correspond to the IPsec local subnet (behind this gateway) and the IPsec remote subnet (behind gateway B). Hosts on those two subnets will be able to access hosts on the other side by means of the IPSec tunnel that will be created between two gateways.

In order to define the IPsec local and remote subnets, 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 included in (***ipsec gwA subnet*** will be used in this how-to) the **Name** field and 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** and then on **Add** to save the changes.
5. Click again on **Add**. This time the descriptive name of the group will be ***ipsec gwB subnet*** for this how-to and the corresponding IP range ***192.168.20.0/24*** will be used.
6. Click on **Add IP** and then on **Add** to save the changes.

IMPORTANT: Remember that the IPsec local subnet must be different from IPsec remote subnets or any other subnets that are already used in other VPN configuration (including other kind of protocols). If not, routing from local subnet A to remote subnet B would not be possible.

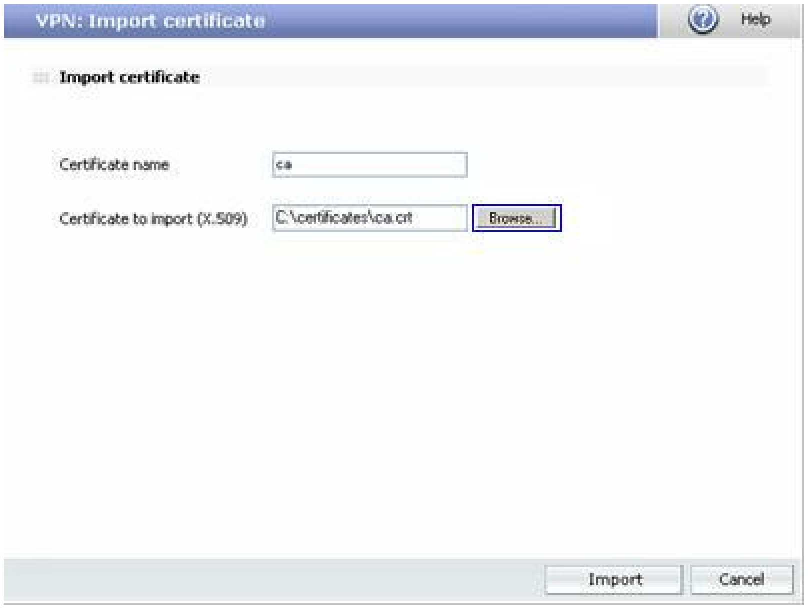
1.2.2 CA and local server certificates

If certificates will be used for authentication purposes, you need to import the public CA certificate which signed the certificate of the remote peer. It is also necessary to import the Integra VPN gateway A local certificate.

In order to import the CA certificate, 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 the **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.



VPN: Import certificate

Import certificate

Certificate name: ca

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

Figure 6.2

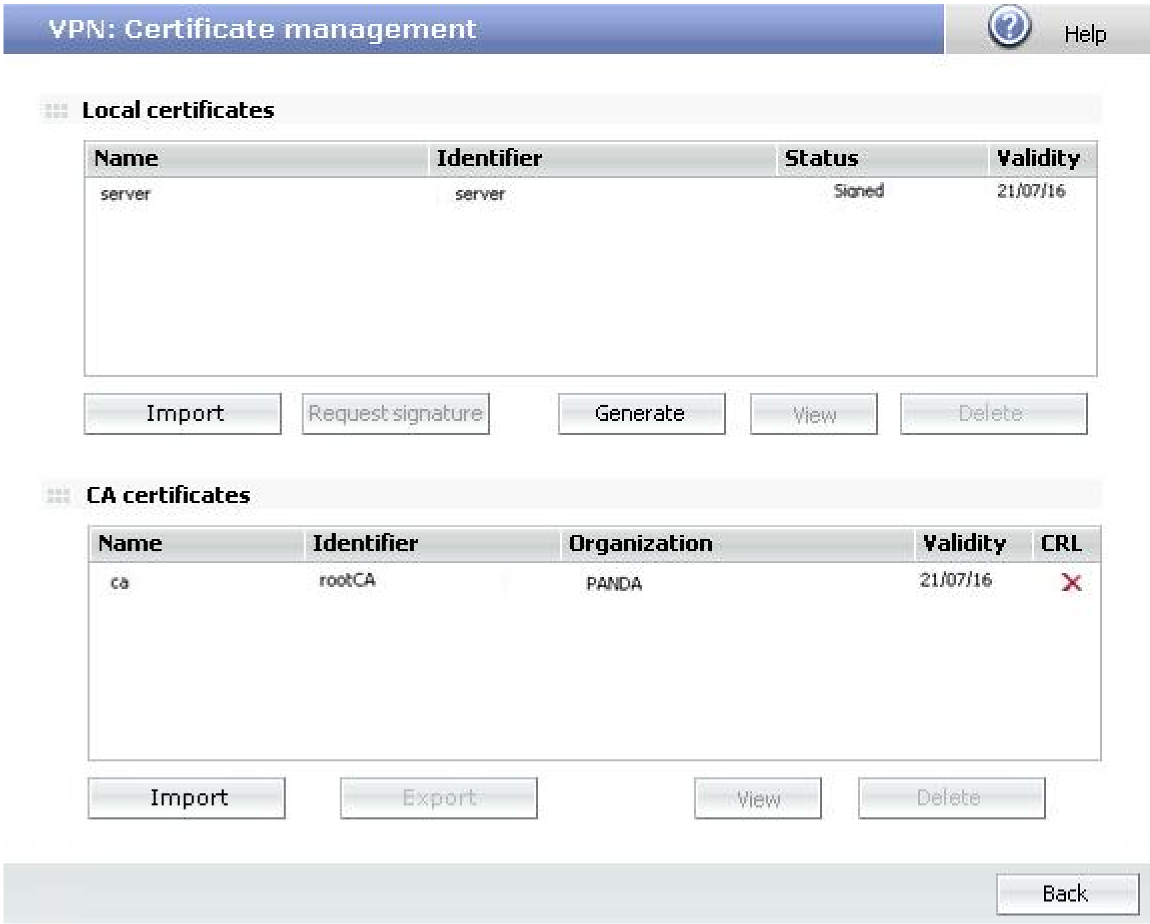
In order to import the local gateway A certificate, follow the procedure below:

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**.

   a. Select if you want to **Import a certificate pending signing** or **Import a certificate with private key** issued by a CA.
   b. If you select **Import certificate with private key**, enter 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.

Once the CA and local gateway A certificates have been imported successfully, a screen similar to the one shown below (figure 6.3) is displayed.



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 6.3

Note that if you select **Import certificate with private key,** you can only import PKCS12 format local certificates (the file has .p12 or .pfx extension).

Index

1.2.3 IKE policies

Panda GateDefender Integra lets you define the Phase I and Phase II IKE security policies required for IPSec VPN connection.

To add a new IKE Phase I policy, follow the instructions below:

1. Click on the **VPN** option in the main menu of the Panda GateDefender Integra console and then click on **IPSEC VPN** in the **VPN management** section.
2. Go to the **IKE** policies tab.
3. Click on **Add**. This will take you to a screen with the following options:

    - **Name:** Descriptive name of the policy. (***1 IKE I*** will be used in this how-to)
    - **Force algorithms:** Leave this checkbox disabled not to force the selected algorithms. The two sides of the tunnel will try to use the first of the selected algorithms in order and if this negotiation is not successful, other possibilities that both sides have will be used.
    - **Key Lifetime for Phases I and II**: Optional. Leave these options unchecked.

Click on **Add** to save the changes.

Index

1.2.4 IPSec VPN configuration on gateway A

Using the static key

This section is related to the IPSec configuration using the static key.

In order to configure IPSec using the static key with 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 VPN1*** will be used in this how-to)

2. **IKE policy**: Use the drop-down menu in order to select the IKE policy that you want to apply (in this case, IKE will be used).

3. **Phase I parameters:**

   Local IP: Enter the local public address or choose the option IP assigned by DHCP (in this case, the local public IP 62.14.249.65 will be used).

   Remote IP: Enter the remote public IP address or choose the option IP assigned by DHCP (in this case, the remote public IP 62.14.10.163 will be used)

   Select an authentication type to use: **Static key.**

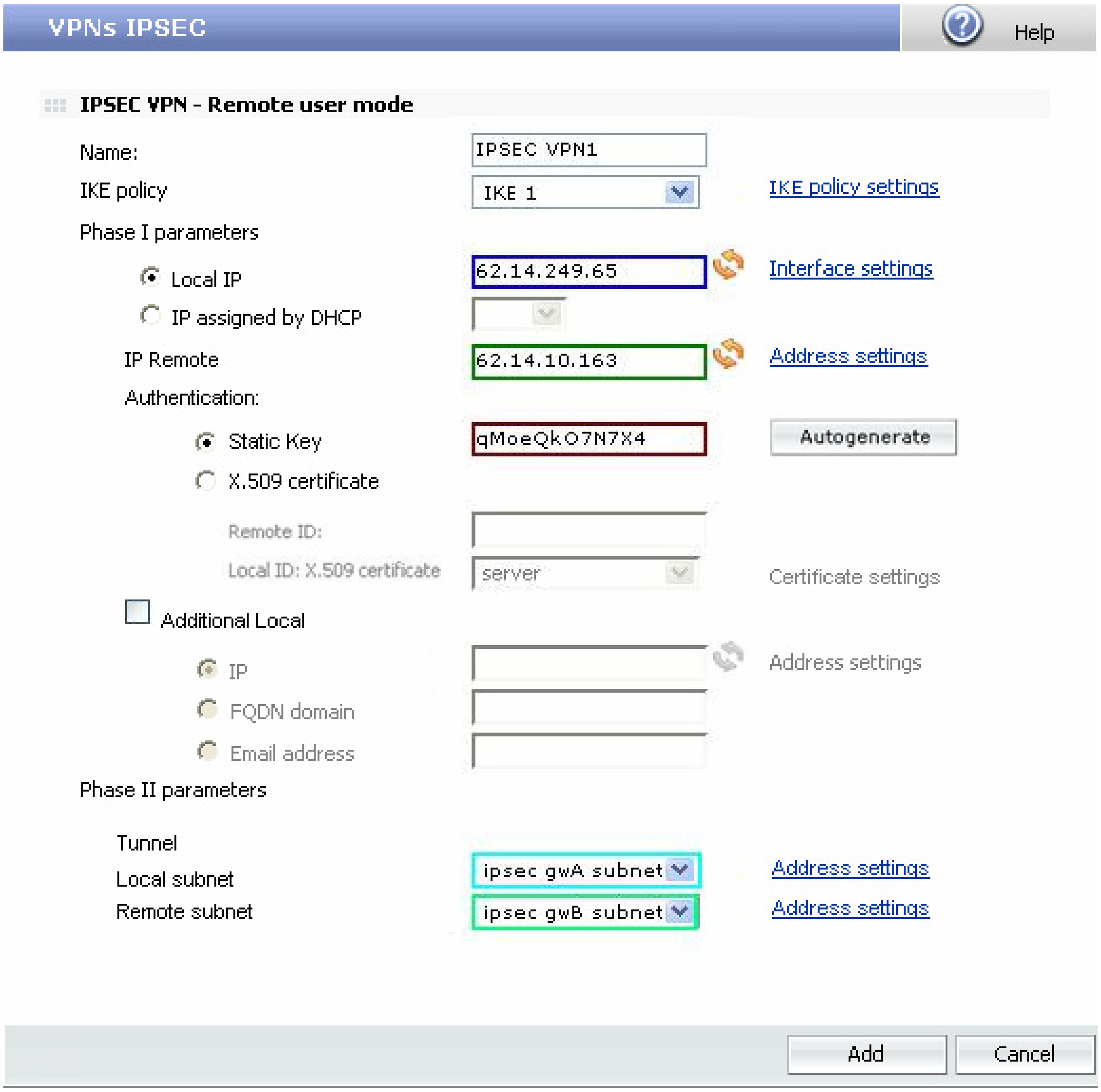
4. When you choose **Static key**, enter a static key to use. If you want, click on the **Autogenerate** button to create a key automatically (the static key used for this how-to will be ***qMoeQkO7N7X4*****).**

5. **Phase II parameters:**

   Local subnet: Select a subnet from those defined in the drop-down menu. (***ipsec gwA subnet*** will be used in this how-to).

   Remote subnet: Select a subnet from those defined in the drop-down menu. (***ipsec gwB subnet*** will be used in this how-to).

Once the IPSEC part has been configured, the corresponding configuration screen will be similar to figure **6.4**



IPSEC VPN - Remote user mode

Name: IPSEC VPN1

IKE policy: IKE 1 — IKE policy settings

Phase I parameters

- ● Local IP: 62.14.249.65 — Interface settings
- ○ IP assigned by DHCP

IP Remote: 62.14.10.163 — Address settings

Authentication:

- ● Static Key: qMoeQkO7N7X4 — Autogenerate
- ○ X.509 certificate

Remote ID:

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

□ Additional Local

- ● IP — Address settings
- ○ FQDN domain
- ○ Email address

Phase II parameters

Tunnel

Local subnet: ipsec gwA subnet — Address settings

Remote subnet: ipsec gwB subnet — Address settings

Figure 6.4

Using TLS

This section is related to the IPSec configuration using TLS.

In order to configure IPSec using TLS with 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 VPN1*** will be used in this how-to)

2. **IKE policy**: Use the drop-down menu in order to select the IKE policy that you want to apply (in this case, IKE 1 will be used).
3. **Phase I parameters:**

   Local IP: Enter the local public IP or choose the option IP assigned by DHCP (in this case the local public IP 62.14.249.65 will be used).

   Remote IP: Enter the remote public IP or choose the option IP assigned by DHCP (in this case, the remote public IP address 62.14.10.163 will be used).

4. Select an authentication type to use: **X.509 certificate** and you will have the following options:

   - **Remote ID**: Specify distinguished gateway B name. (following remote ID will be used in this how-to:

     C=ES, ST=VI, O=PANDA, OU=PSI, CN= client, emailAddress=vpntest@pandasoftware.com

     You can obtain it from the gateway B certificate client, using the following command from the ms-command prompt and assuming that you have installed an openssl or openvpn program:

     # openssl x509 –in client.crt –text –noout

   - **Local ID: X-509 certificate**: Use the drop-down menu to select the certificate you want. (***client*** will be used in this how-to).

   Additional local ID: You also have the following options:

   IP: Enter the local IP address. By default, you will see the IP entered in the IPSec global configuration screen.

FQDN domain (Fully Qualified Domain Name): Name of the fully qualified domain.

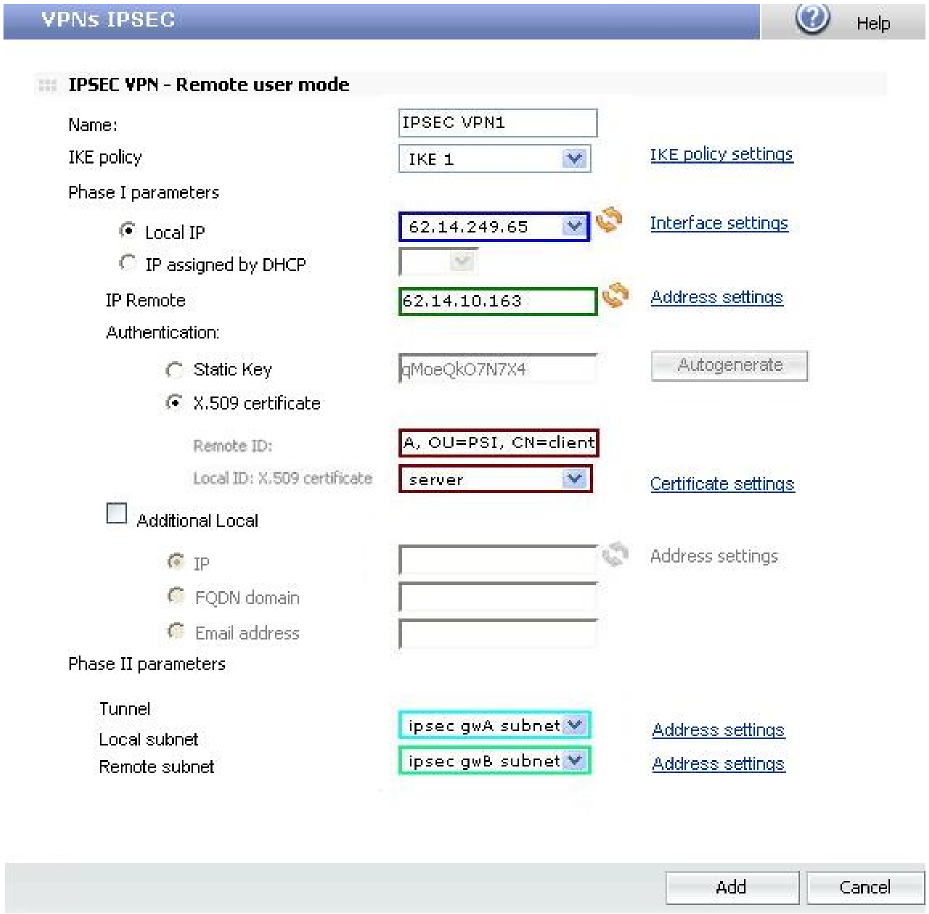
1. Email address. Email address used for the identification.

5. **Phase II parameters:**

Local Subnet: Select a subnet from the drop-down menu (in this case, ipsec gwA subset will be used).

Remote Subnet: Select a subnet from the drop-down menu (in this case, ipsec gwB subset will be used).

Once the IPSEC part has been configured, the corresponding configuration screen will be similar to figure **6.5**



IPSEC VPN - Remote user mode

Name: IPSEC VPN1

IKE policy: IKE 1 — IKE policy settings

Phase I parameters

● Local IP: 62.14.249.65 — Interface settings

○ IP assigned by DHCP

IP Remote: 62.14.10.163 — Address settings

Authentication:

○ Static Key: qMoeQkO7N7X4

● X.509 certificate

Remote ID: A, OU=PSI, CN=client

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

☐ Additional Local

● IP — Address settings

○ FQDN domain

○ Email address

Phase II parameters

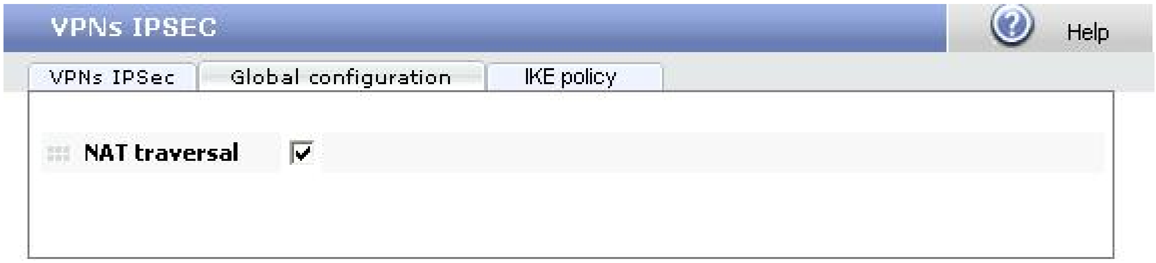
Tunnel

Local subnet: ipsec gwA subnet — Address settings

Remote subnet: ipsec gwB subnet — Address settings

Figure 6.5

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



NAT traversal ☑

Figure 6.6

Index

1.3 Gateway B setup

1.3.1 IP group configuration

Once again, define a group of IP addresses that correspond to the IPsec local subnet (behind this gateway) and remote subnet (behind gateway A). Hosts on those two subnets will be able to access hosts on the other side by means of IPSec tunnel that will be created between two gateways.

In order to define the IPsec local and remote subnets 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 gwB subnet*** will be used in this how-to) in the **Name** field and IP range (**192.168.20.0/24** will be used in this how-to) in the **IP/Mask** radio button section.
4. Click on **Add IP** and then on **Add** to save the changes.
5. Click again on **Add**. This time the descriptive name of the group will be ***ipsec gwA subnet*** for this how-to and the corresponding IP range ***192.168.10.0/24*** will be used.
6. Click on **Add IP** and then on **Add** to save the changes.

⚠ **IMPORTANT:** Remember that the IPsec local subnet must be different from the IPsec remote subnets or any other subnets that are already used in other VPN configuration (including other kind of protocols). If not, routing from local subnet B to remote subnet A would not be possible.

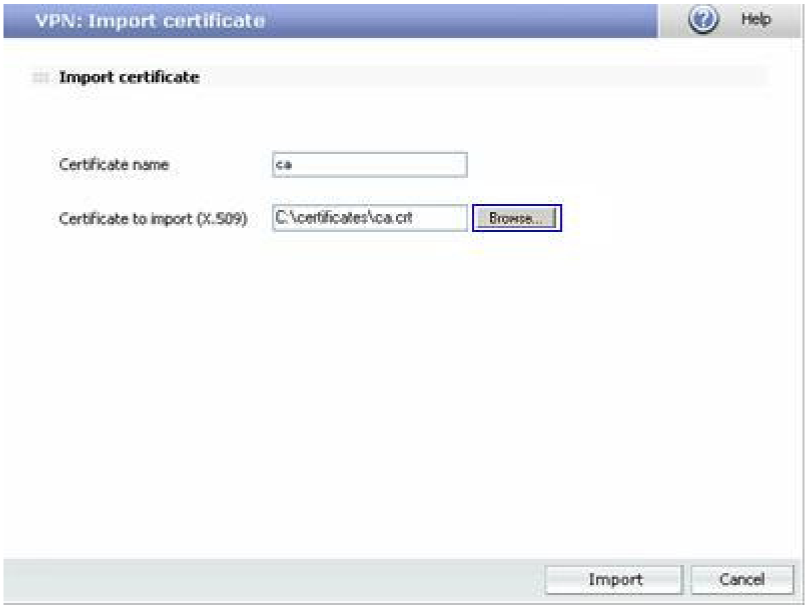
1.3.2 CA and local server certificates

If certificates will be used for authentication purposes, you need to import the public CA certificate which signed the certificate of the remote peer. It is also necessary to import the Integra VPN gateway B local certificate.

In order to import CA certificate, 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*** would 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 6.7

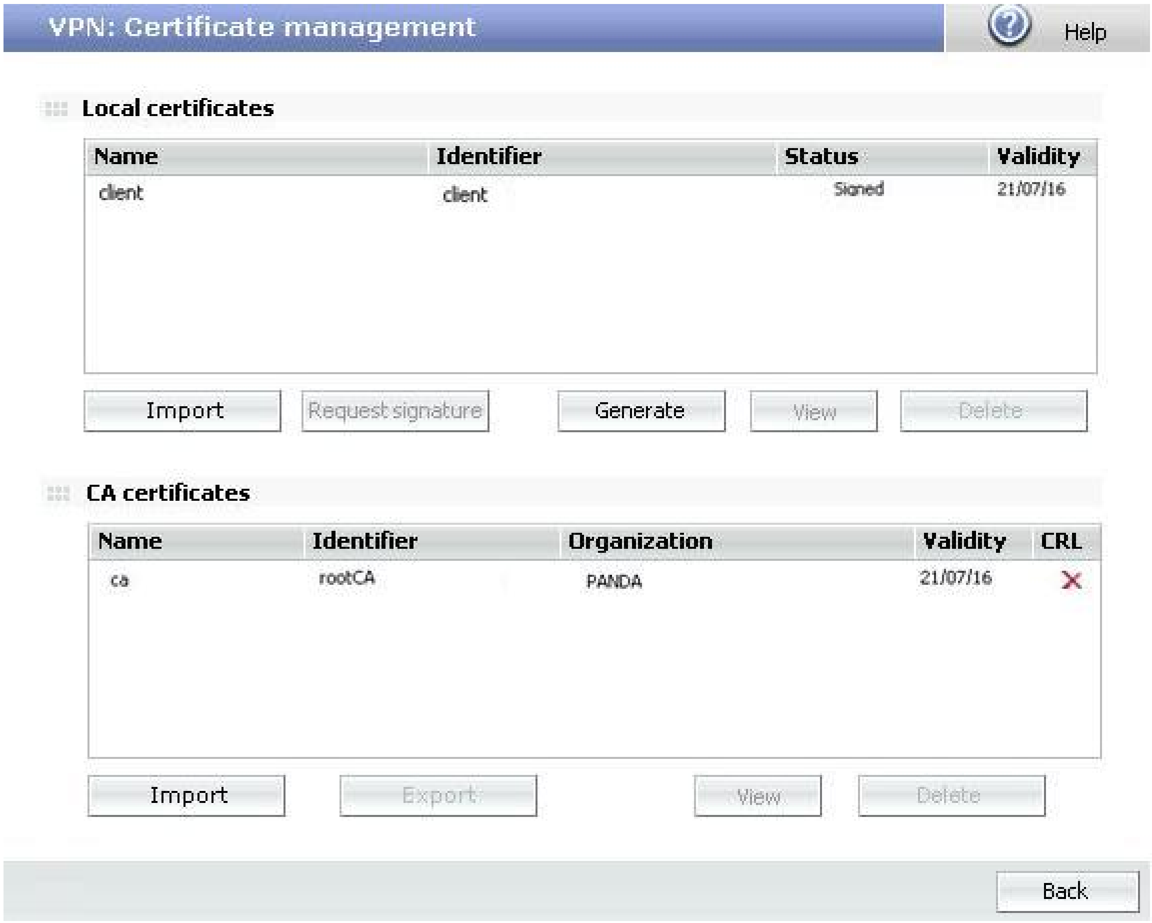
In order to import local gateway B certificate, follow the procedure below:

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**.

    a. Select if you want to **Import a certificate pending signing** or **Import a certificate with private key** issued by a CA.
    b. If you select **Import certificate with private key**, enter PKCS12 Certificate Name (***client*** 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.

Once the CA and local gateway B certificates have been imported successfully, a screen similar to the one shown below (figure 6.8) is displayed.



VPN: Certificate management

Local certificates

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

CA certificates

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

Figure 6.8

Note that if you select **Import certificate with private key,** you can only import PKCS12 format local certificates (the file has p12 extension).

Index

1.3.3 IPSec VPN configuration on gateway B

Using the static key

This section is related to the IPSec configuration using the static key.

In order to configure IPSec using the static key with 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 VPN1*** will be used in this how-to)
2. **IKE policy**: Use the drop-down menu to select the IKE policy you want to apply. (***1IKE*** will be used in this how-to).
3. **Phase I parameters:**

   Local IP: Enter the local public IP or choose the option IP assigned by DHCP (in this case the local public IP *62.14.10.163* will be used).

   Remote IP: Enter the remote public IP or choose the option IP assigned by DHCP (in this case, the remote public IP address *62.14.249.65* will be used).

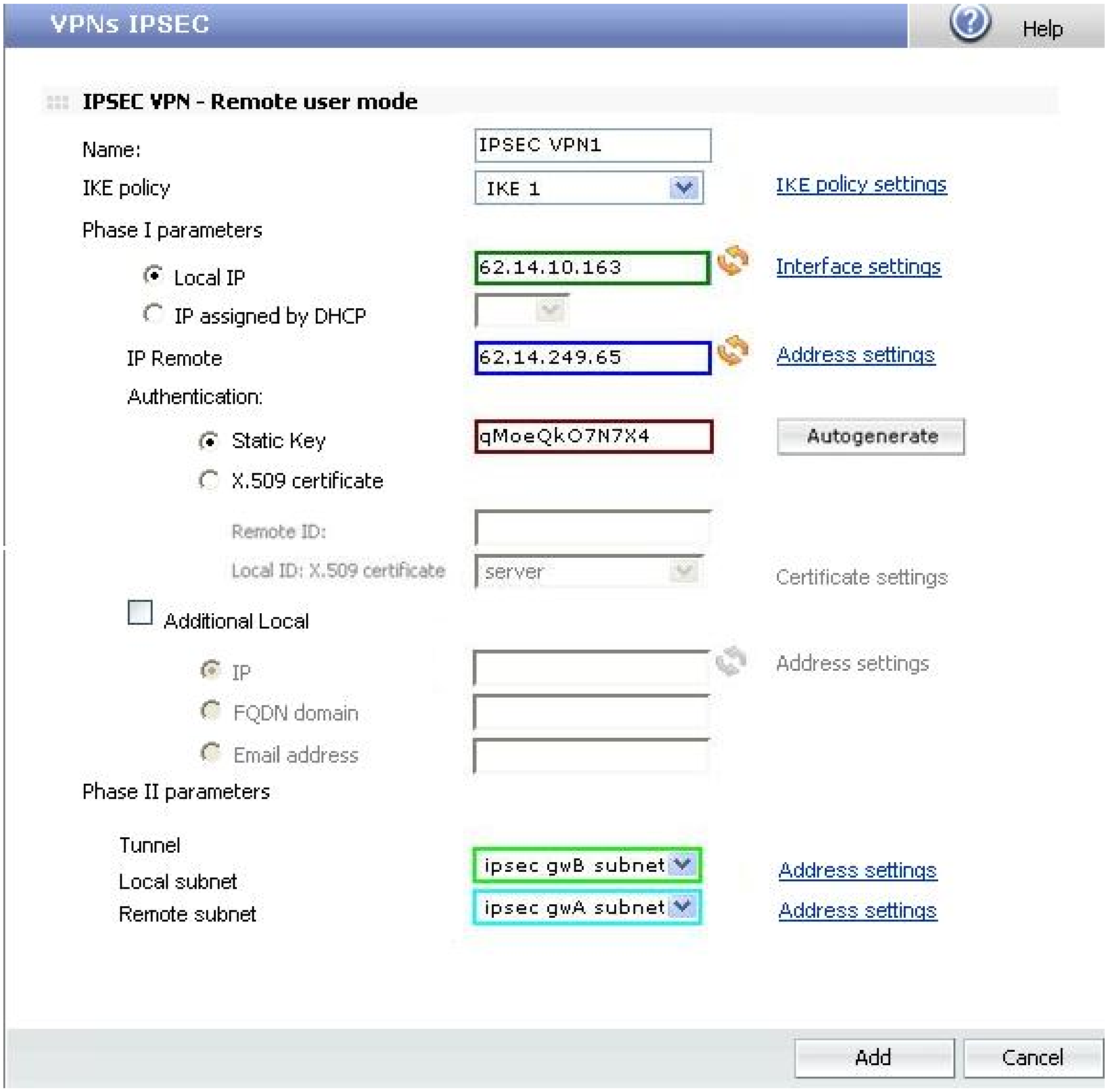
   Select an authentication type to use: **Static key.**

4. When you choose **Static key**, enter a static key to use. If you want, click on the **Autogenerate** button to create a key automatically (static key used for this how-to will be ***qMoeQkO7N7X4***)).
5. **Phase II parameters:**

   Local Subnet: Select a subnet from the drop-down menu (in this case, ***ipsec gwB subnet*** will be used).

   Remote Subnet: Select a subnet from the drop-down menu (in this case, ***ipsec gwA subnet*** will be used).

Once the IPSEC part has been configured, the corresponding configuration screen will be similar to figure **6.9**



VPNs IPSEC

IPSEC VPN - Remote user mode

Name: IPSEC VPN1

IKE policy: IKE 1 — IKE policy settings

Phase I parameters

- ● Local IP: 62.14.10.163 — Interface settings
- ○ IP assigned by DHCP
- IP Remote: 62.14.249.65 — Address settings
- Authentication:
  - ● Static Key: qMoeQkO7N7X4 — Autogenerate
  - ○ X.509 certificate
    - Remote ID:
    - Local ID: X.509 certificate: server — Certificate settings
- □ Additional Local
  - ● IP — Address settings
  - ○ FQDN domain
  - ○ Email address

Phase II parameters

- Tunnel
- Local subnet: ipsec gwB subnet — Address settings
- Remote subnet: ipsec gwA subnet — Address settings

Figure 6.9

Using TLS

This section is related to the IPSec configuration using TLS.

In order to configure IPSec using TLS with 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 a descriptive name for the VPN (in this case, IPSEC VPN1 will be used).
2. **IKE policy**: Use the drop-down menu in order to select the IKE policy that you want to apply (in this case, IKE 1 will be used).
3. **Phase I parameters:**

   Local IP: Enter the local IP address or choose IP assigned by DHCP (in this case, the local public IP *62.14. 10.163 will be used)* .

   Remote IP: Enter the public remote IP address or choose IP assigned by DHCP (in this case, the remote public IP address will be *62.14. 249.65).*

4. Select the type of authentication to use: **X.509 Certificate**. **The following options are available:**

   - **Remote ID**: Specify the name of the gateway B. In this example, the following remote identification will be used:

     C=ES, ST=VI, O=PANDA, OU=PSI, CN=server, emailAddress=vpntest@pandasoftware.com

     You can obtain it from the gateway B client certificate, by typing the following command in the MS-DOS console, provided programs such as openssl or openvpn are installed:

     ```
     # openssl x509 –in server.crt –text –noout
     ```

   - **Local ID: X-509 certificate**: Use the drop-down menu in order to select the desired certificate (in this case, client will be used).

   - **Additional local ID Local**: The following options are also available:

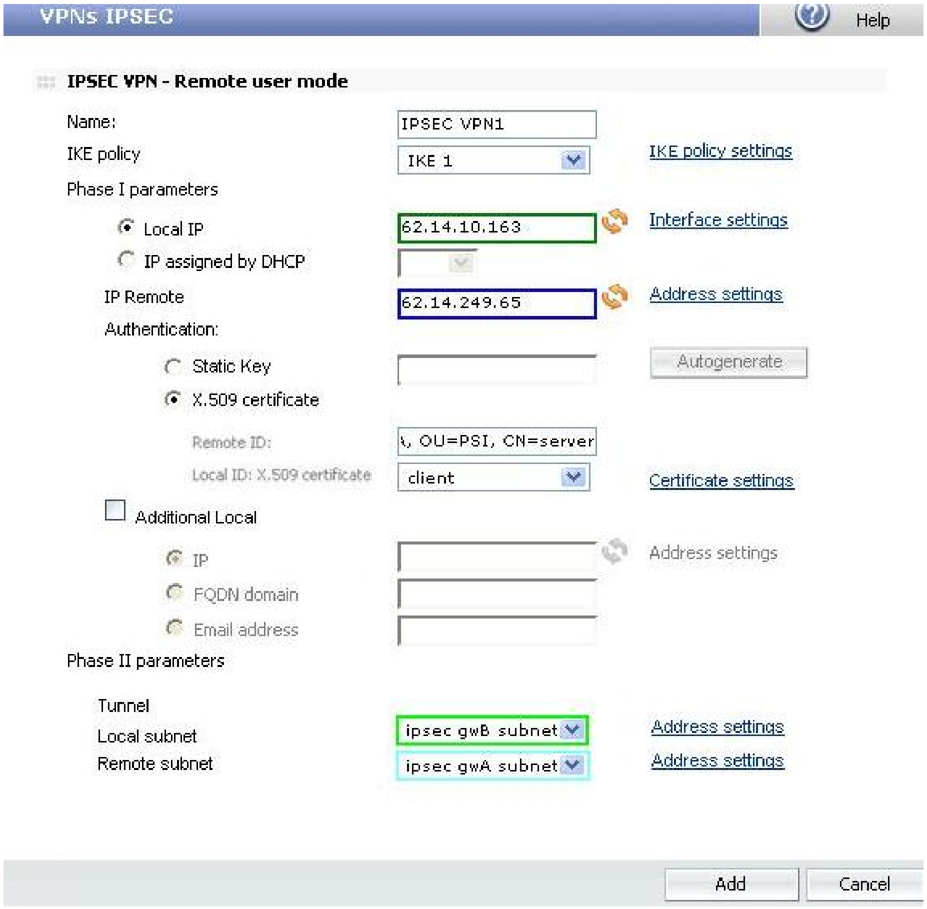
     - **IP**: Enter the local Ip address. By default, the Ip address entered in the IPSec global settings screen will be displayed.
     - **FQDN domain** (Fully Qualified Domain Name): Full name of the domain.
     - **Email address**. Electronic address used for identification purposes.

5. **Phase II parameters:**

   Local Subnet: Select a subset from the drop-down menu (in this case, **ipsec gwB subnet** will be used).

   Remote Subnet: Select a subset from the drop-down menu (in this case, **ipsec gwA subnet** will be used).

Once the IPSEC part has been configured, the corresponding configuration screen will be similar to figure **6.10**



VPNs IPSEC

IPSEC VPN - Remote user mode

Name: IPSEC VPN1

IKE policy: IKE 1

Phase I parameters

● Local IP: 62.14.10.163

○ IP assigned by DHCP

IP Remote: 62.14.249.65

Authentication:

○ Static Key

● X.509 certificate

Remote ID: \, OU=PSI, CN=server

Local ID: X.509 certificate: client

□ Additional Local

● IP

○ FQDN domain

○ Email address

Phase II parameters

Tunnel

Local subnet: ipsec gwB subnet

Remote subnet: ipsec gwA subnet

Figure 6.10

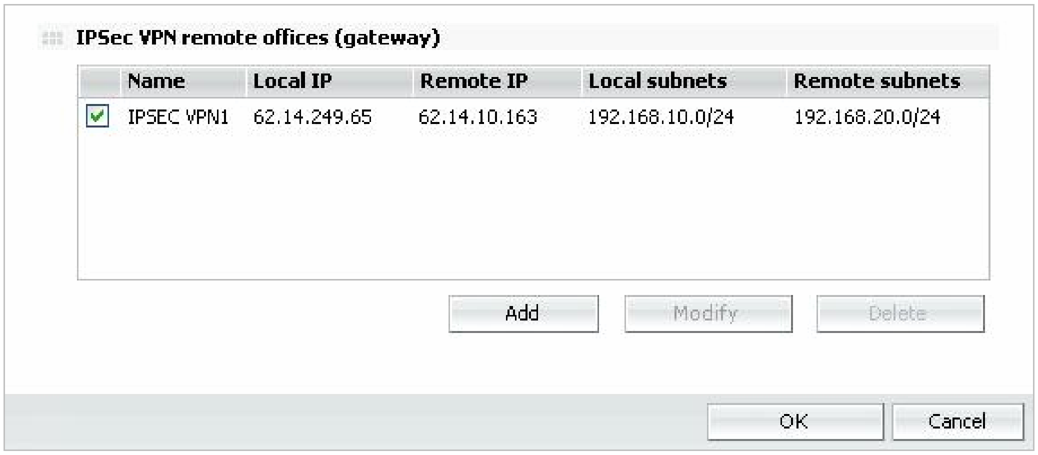
Note that if there is any NAT device between a two Integra VPN gateways, then you should enable the NAT transversal verification checkbox as shown in Figure 6.7.

Index

1.4 Establishing a VPN connection

To initiate IPSec VPN between two gateways, proceed as follows:

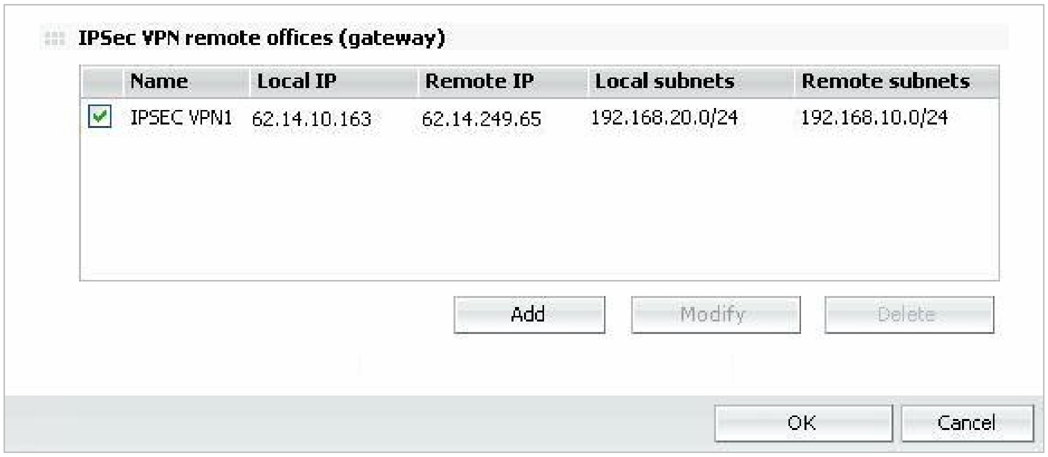
Mark the **Active** checkbox on both gateways to enable configuration, as shown in corresponding figures **6.11** and **6.12**



IPSec VPN remote offices (gateway)

	Name	Local IP	Remote IP	Local subnets	Remote subnets
☑	IPSEC VPN1	62.14.249.65	62.14.10.163	192.168.10.0/24	192.168.20.0/24

Figure 6.11



IPSec VPN remote offices (gateway)

	Name	Local IP	Remote IP	Local subnets	Remote subnets
☑	IPSEC VPN1	62.14.10.163	62.14.249.65	192.168.20.0/24	192.168.10.0/24

Figure 6.12

In order to disconnect it, just disable the **Active** checkbox on any side of the tunnel and then click on **OK**.

Index

1.5 Further considerations

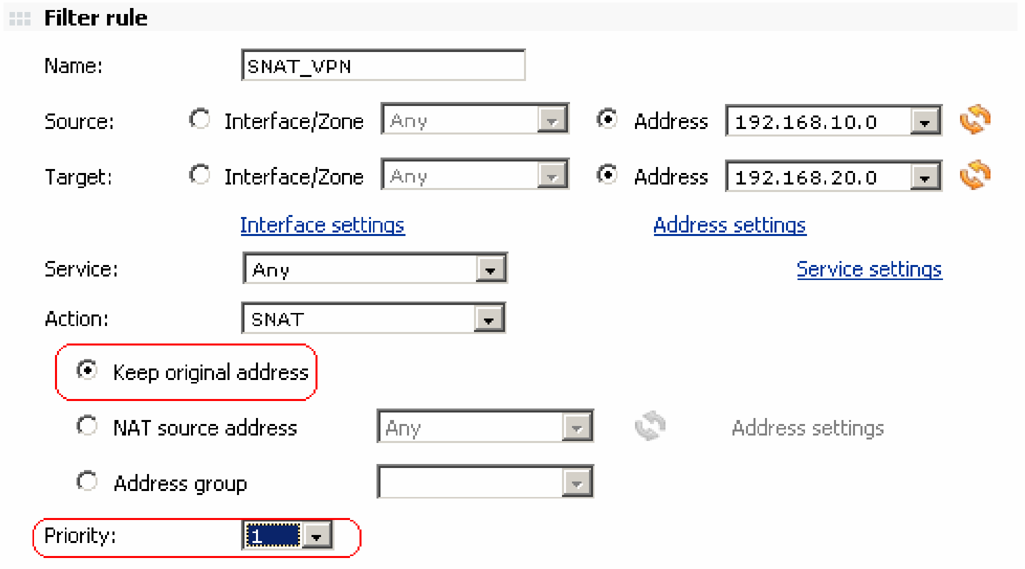
If the Integra firewall is used, the encryption protocol configuration rules will automatically be entered in the firewall.

If there are routers or firewalls between the two gateways, the following ports and protocols must be enabled for IPSec VPN to work properly:

- 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:



Filter rule

Name: SNAT_VPN

Source: ○ Interface/Zone Any ● Address 192.168.10.0

Target: ○ Interface/Zone Any ● Address 192.168.20.0

Interface settings Address settings

Service: Any Service settings

Action: SNAT

● Keep original address

○ NAT source address Any Address settings

○ Address group

Priority: 1

The example in the screenshot shows the rule to add to ensure that traffic from network 192.168.10.0 can be correctly routed through the VPN tunnel to the roadwarriors' network 192.168.20.0

Index

1.6 Configuration checking

To check your IPSec VPN configuration, please follow the procedure 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.

   Once the VPN tunnel has been established between two gateways, the following test should be performed on each local VPN subnetworks, in order to reach the remote one.

   In order to carry out such a task, the command prompt that should be used is the following:

   ```
   ping –n 10 192.168.20.100
   ```

   When running this command, it pings from the host that belongs to the gateway A VPN subnetwork to the host that resides on the internal network behind VPN gateway B, and gateway A should see the icmp response message.

   Note that only those packets from the local VPN subnet to the remote one will be encrypted. This means that if you ping between hosts that belong to one of the gateway’s internal VPN subnetworks and an external IP address of another gateway the traffic will not be encrypted at all because the purpose of a gateway to gateway (or as mentioned, subnet to subnet) VPN tunnel is to ensure privacy only between two subnets.

Index

0707-PGDIHT08-03-EN