Panda GateDefender Integra

HOWTO: How to configure SSL VPN tunnel 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 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.

How to configure SSL VPNs gateway-to-gateway

(Secure Socket Layer) Security protocol safeguards access to information circulating through Internet protocols (HTTP, SMTP, FTP, etc.) symmetrically encrypting the data. Access to this data is only possible with the correct key.

Panda GateDefender Integra allows you to create and modify SSL VPNs with remote users and offices.

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 SSL 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 SSL VPN scenario:

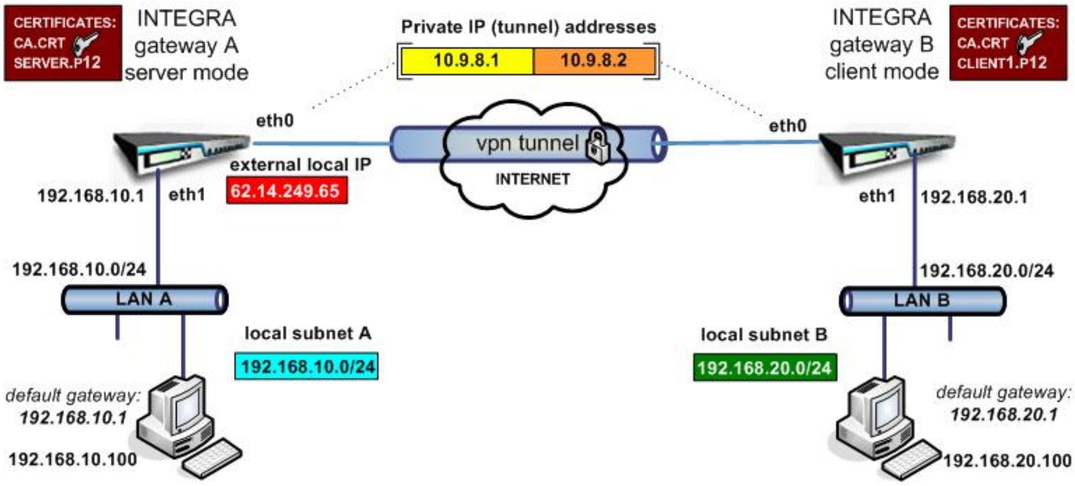


Figure 4.1 SSL gateway-to-gateway VPN

This kind of configuration requires that one of the gateways operates as a server and another one in client mode.

In this how-to, gateway A will have the server role and its external local IP will be **62.14.249.65**. The server will listen on **UDP port 1194** for an incoming connection from clients (sub-offices).

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 Integra 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 (**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 (**192.168.20.0/24**). The same is valid for the 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 following how-to, we assume that Integra's LAN IP is the default gateway for the corresponding hosts on INTEGRA's local subnets.

In order to authenticate each other, there are two possibilities to configure the SSL VPN gateway to gateway connection:

- to use static keys or
- to use certificates (TLS)

Index

1.2 Configuration using static keys

1.2.1 Gateway A Setup

The first step when configuring this kind of SSL VPN will be to define a group of IP addresses that correspond to the SSL remote subnet (that reside on other gateway); the one you want hosts from the SSL local subnet to be able to connect to.

In order to define the SSL remote subnet, follow the steps 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 (***ssl remote subnet*** will be used in this how-to) in the **Name** field and the 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.**

Finally, click on **Add** to save the changes.

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

The steps below describe how to configure SSL VPN gateway A using previously defined elements.

1. Go to the Panda GateDefender Integra administration console.
2. Click on **VPN** in the panel on the left.
3. Then, select **VPN management**.
4. Click on **SSL VPN management** and select the Remote offices tab.
5. Click on **Add** to define the new VPN.

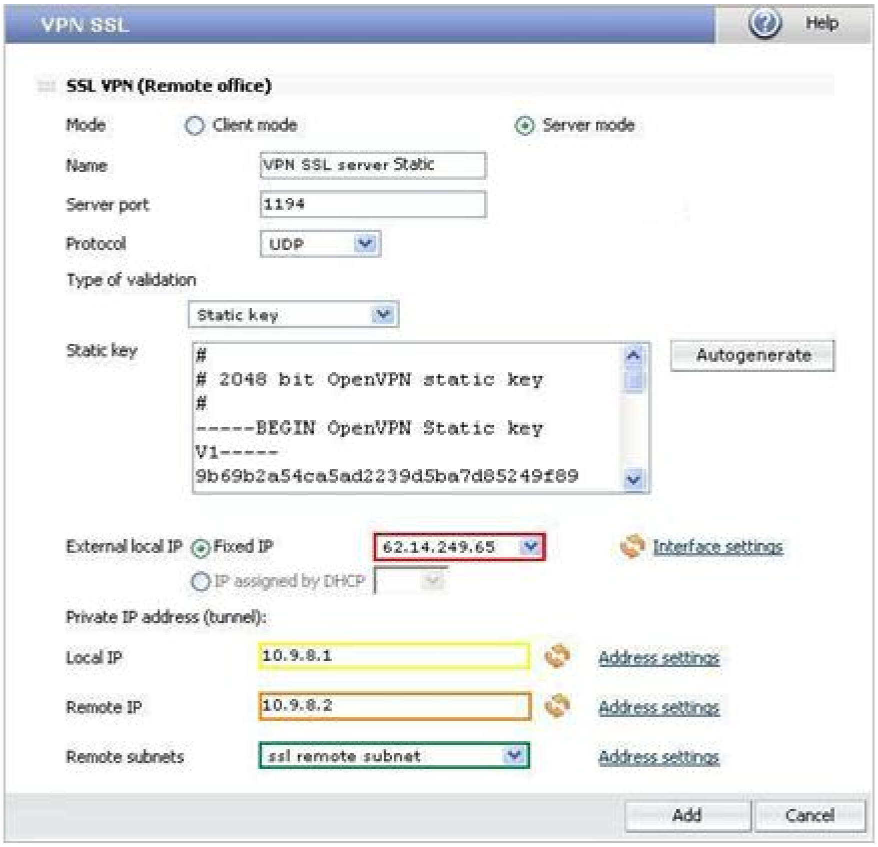
   There you will find the parameters required to configure a VPN in Panda GateDefender Integra using the SSL protocol in server mode (as shown in figure 4.2):

   - *Mode*: select the option ***Server mode***.
   - *Name***:** enter a descriptive name for the VPN (***VPN SSL server STATIC*** will be used for this how-to).
   - *Server port*: enter the connection server port (default port ***1194*** will be used for this how-to).
   - *Protocol*: choose the protocol that will be used for encapsulation (default protocol ***UDP*** will be used in this how-to).

   Note that the TCP protocol is considered more secure, but slows down communications. UDP makes fewer checks and is therefore faster.

   - *Validation type*: Choose the ***Static key*** as a type of validation to use for the VPN.

- *Static key*: Enter a static key to use in this textbox (use the same static key for gateway B).
- *External local IP*: Select the type of local IP through which it will listen, DHCP or fixed IP (for purpose of this how-to choose ***fixed IP***) and enter the fixed IP address ***62.14.249.65***
- *Local IP*: Enter the local private IP address (***10.9.8.1*** will be used for this how-to).
- *Remote IP*: Enter the remote private IP address (***10.9.8.2*** will be used for this how-to).
- *Remote subnets:* Enter local subnet B (remote subnet from the gateway A point of view). The previously defined ***SSL remote subnet*** will be used for this how-to, which is ***192.168.20.0/24***).



VPN SSL

SSL VPN (Remote office)

Mode ○ Client mode ● Server mode

Name: VPN SSL server Static

Server port: 1194

Protocol: UDP

Type of validation: Static key

Static key:

```
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key
V1-----
9b69b2a54ca5ad2239d5ba7d85249f89
```

External local IP ● Fixed IP: 62.14.249.65
○ IP assigned by DHCP

Private IP address (tunnel):

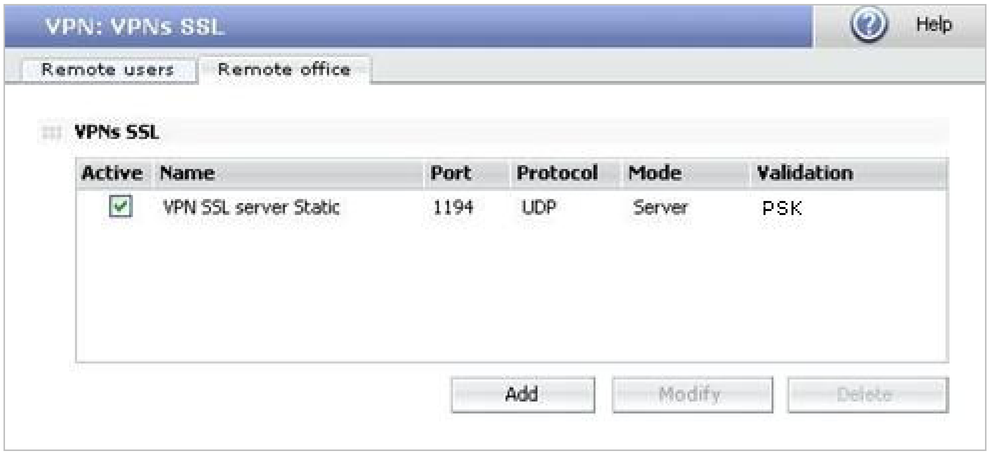
Local IP: 10.9.8.1

Remote IP: 10.9.8.2

Remote subnets: ssl remote subnet

Figure 4.2

Click on **Add** to save the changes.
Then, select the **Active** checkbox to enable the server side configuration, as shown in figure 4.3.



VPNs SSL

Active	Name	Port	Protocol	Mode	Validation
☑	VPN SSL server Static	1194	UDP	Server	PSK

Figure 4.3

Index

1.2.2 Gateway B Setup

Again, the first step in the gateway B side configuration will be to define a group of IP addresses that correspond to the SSL remote subnet (that reside on gateway A), the one you want hosts from the SSL local subnet be able to connect to.

To define the SSL remote 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 (***ssl remote 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 **IP/Mask** radio button section.
4. Click on **Add IP**.

Finally, click on **Add** to save the changes.

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

The steps below describe how to configure an SSL VPN gateway B using previously defined elements.

1. Go to the Panda GateDefender Integra administration console.
2. Click on **VPN** in the panel on the left.
3. Then, select **VPN management**.
4. Click on **SSL VPN management** and select the Remote offices tab.
5. Click on **Add** to define the new VPN.

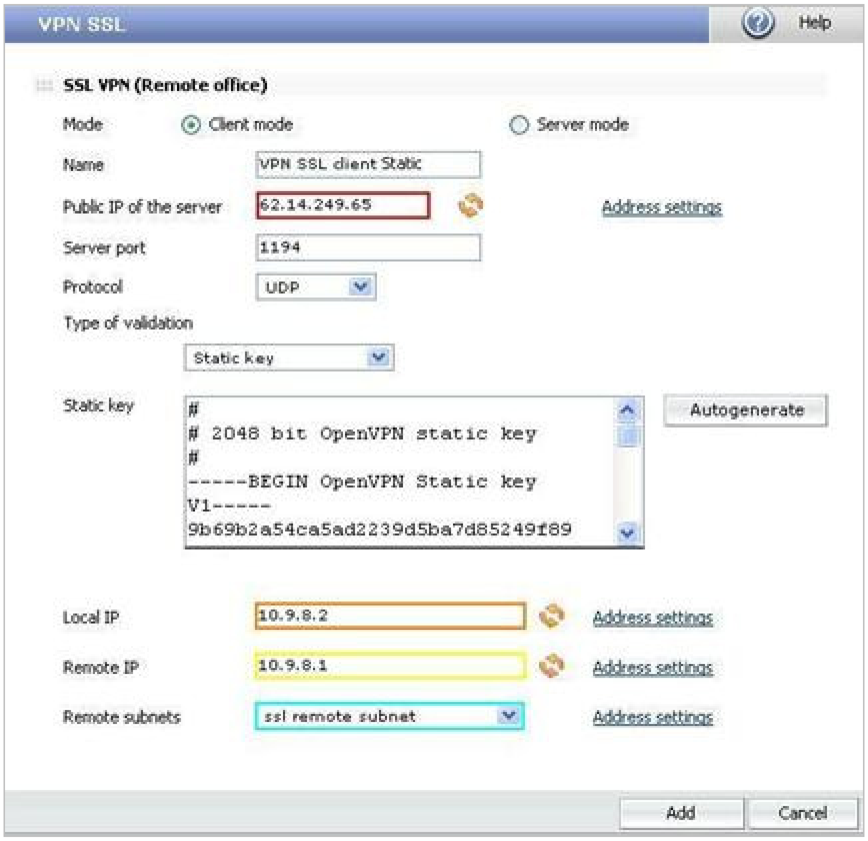
   There you will find the parameters required to configure a VPN in Panda GateDefender Integra using the SSL protocol in client mode (as shown in figure 4.4):

   - Mode: select the option **Client mode**.
   - Name**:** enter a descriptive name for the VPN (**VPN SSL client STATIC** will be used for this how-to).
   - Public IP of the server: Enter the remote public IP of the server (**65.14.249.65** will be used for this how-to).
   - Server port: enter connection server port (default port **1194** will be used for this how-to).
   - Protocol: Choose the protocol that will be used for encapsulation (default protocol **UDP** will be used in this how-to).

   Note that the TCP protocol is considered more secure, but slows down communications. UDP makes fewer checks and is therefore faster.

   - Validation type: Choose the **Static key** as a type of validation to use for the VPN.

- Static key: Enter a static key to use in this textbox (copy the same static key that was used on gateway A side).
- Local IP: Enter the local private IP address (**10.9.8.2** will be used for this how-to).
- Remote IP: Enter the remote private IP address (**10.9.8.1** will be used for this how-to).
- Remote subnets: Enter local subnet A (remote subnet from the gateway B point of view). The previously defined **SSL remote subnet** will be used for this how-to: **192.168.10.0/24**).



SSL VPN (Remote office)

Mode: ● Client mode ○ Server mode

Name: VPN SSL client Static

Public IP of the server: 62.14.249.65

Server port: 1194

Protocol: UDP

Type of validation: Static key

Static key:

```
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key
V1-----
9b69b2a54ca5ad2239d5ba7d85249f89
```

Local IP: 10.9.8.2

Remote IP: 10.9.8.1

Remote subnets: ssl remote subnet

Figure 4.4

Index

1.3 Configuration using TLS for validation

1.3.1 Gateway A Setup (Server mode)

This section will focus only on a part of the configuration of SSL VPN using TLS and which is different from the one using a static key. The part of the configuration regarding how to define an SSL remote subnet will be the same as explained in the previous section for configuration of gateway A with a static key.

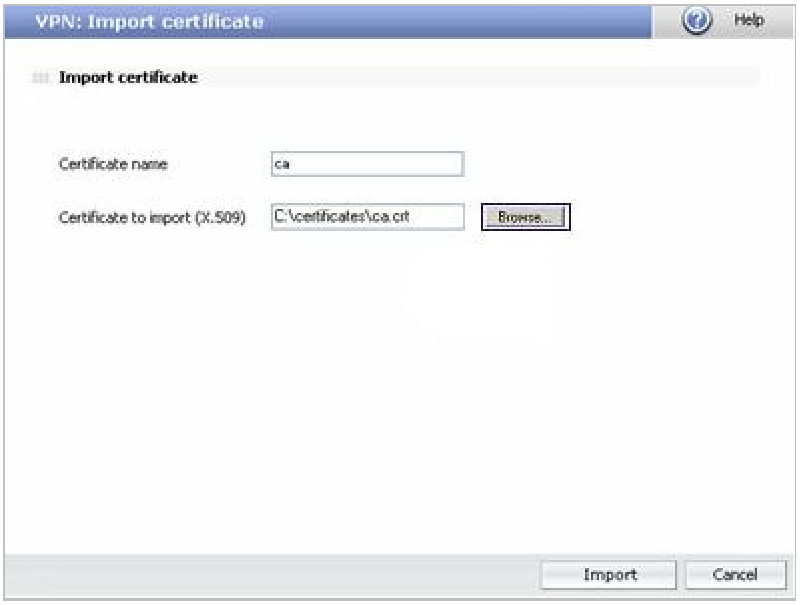
The first step to follow when configuring an SSL VPN that uses TLS for validation will be to import the required certificates.

Certificates are required for authentication purposes. You need to import the public certificate of CA 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 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 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.



Certificate name: ca

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

Figure 4.5

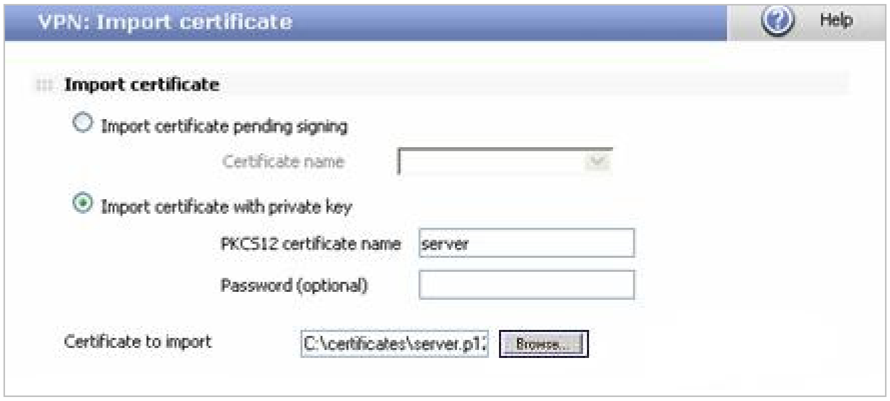
In order to import the local gateway A certificate, follow the procedure below:

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

3. Click on **Browse…** to select the certificate you want to import.
4. 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

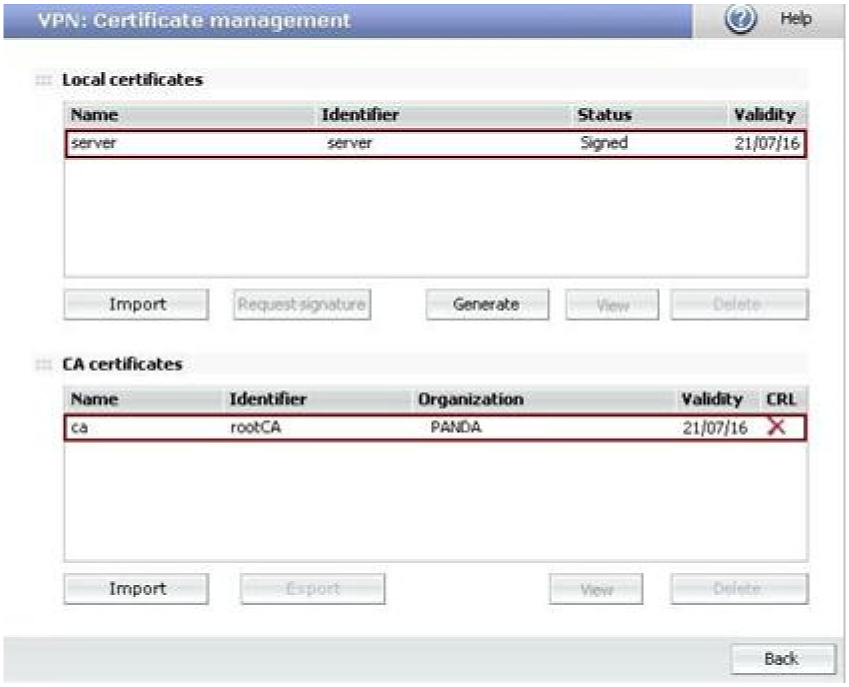
PKCS12 certificate name: server

Password (optional):

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

Figure 4.6

Once the CA and local gateway A certificates have been imported successfully, a screen similar to the one shown below (figure 4.7) 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	✗

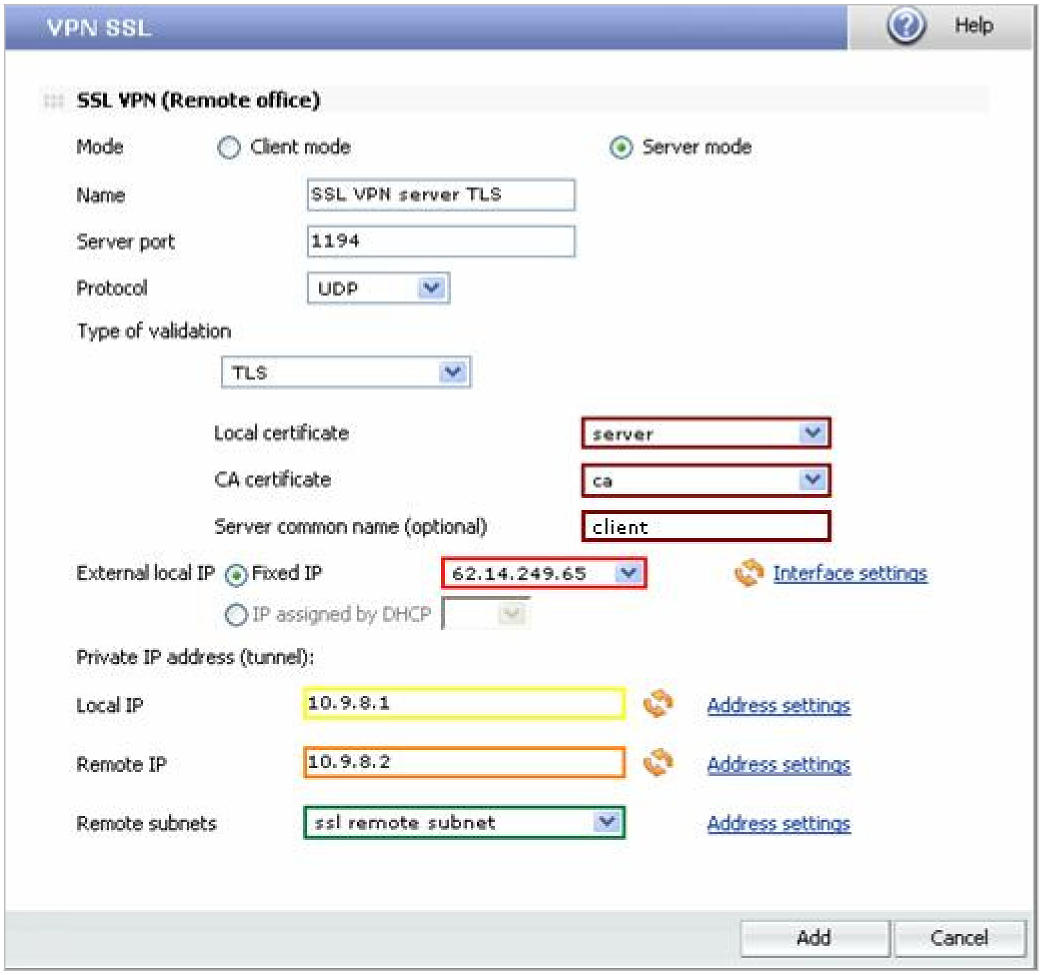
Figure 4.7

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

The steps below describe how to configure SSL VPN gateway A with TLS using previously defined elements.

1. Go to the Panda GateDefender Integra administration console.
2. Click on **VPN** in the panel on the left.
3. Then, select **VPN management**.
4. Click on **SSL VPN management** and select the **Remote offices** tab.
5. Click on **Add** to define new VPN.

There you will find the parameters required to configure a VPN in Panda GateDefender Integra using the SSL protocol in server mode (as shown in figure 4.8):



VPN SSL

Help

SSL VPN (Remote office)

Mode ○ Client mode ● Server mode

Name: SSL VPN server TLS

Server port: 1194

Protocol: UDP

Type of validation: TLS

Local certificate: server

CA certificate: ca

Server common name (optional): client

External local IP ● Fixed IP 62.14.249.65 — Interface settings

○ IP assigned by DHCP

Private IP address (tunnel):

Local IP: 10.9.8.1 — Address settings

Remote IP: 10.9.8.2 — Address settings

Remote subnets: ssl remote subnet — Address settings

Figure 4.8

- Mode: select the option **Server mode**.
- Name**:** enter a descriptive name for the VPN (**SSL VPN server TLS** will be used for this how-to).
- Server port: enter connection server port (default port **1194** will be used for this how-to).
- Protocol: choose the protocol that will be used for encapsulation (default protocol **UDP** will be used in this how-to).

Note that the TCP protocol is considered more secure, but slows down communications. UDP makes fewer checks and is therefore faster.

- Validation type: Choose **TLS** as a type of validation to use for the VPN.
- Local certificate: Use the drop-down menu to select the certificate you want (**server** will be used in this how-to).
- Validation CA of the remote certificate: The remote office identified with a certificate must present the CA signature. Use the drop-down menu to select the CA certificate you want. (**ca** will be used in this how-to).

- Server Common Name:. In this field it is compulsory to enter the CN (Common name) of the other gateway, in this case, the client. The CN field of the certificate can be obtained from the client´s .CRT.
- External local IP**:** Select the type of local IP through which it will listen, DHCP or fixed IP (for purpose of this how-to, choose **fixed IP**) and enter the fixed IP address **62.14.249.65**
- Local IP: Enter the local private IP address (**10.9.8.1** will be used for this how-to).
- Remote IP: Enter the remote private IP address (**10.9.8.2** will be used for this how-to).
- Remote subnets: Enter local subnet B (remote subnet from the gateway A point of view). The previously defined **SSL remote subnet** will be used for this how-to which is **192.168.20.0/24**).

Index

1.3.2 Gateway B Setup (Client mode)

This section will focus only on a part of the configuration of an SSL VPN using TLS and which is different from the one using a static key. The part of configuration referring to defining an SSL remote subnet will be the same as explained above in corresponding section for a configuration of gateway B with a static key.

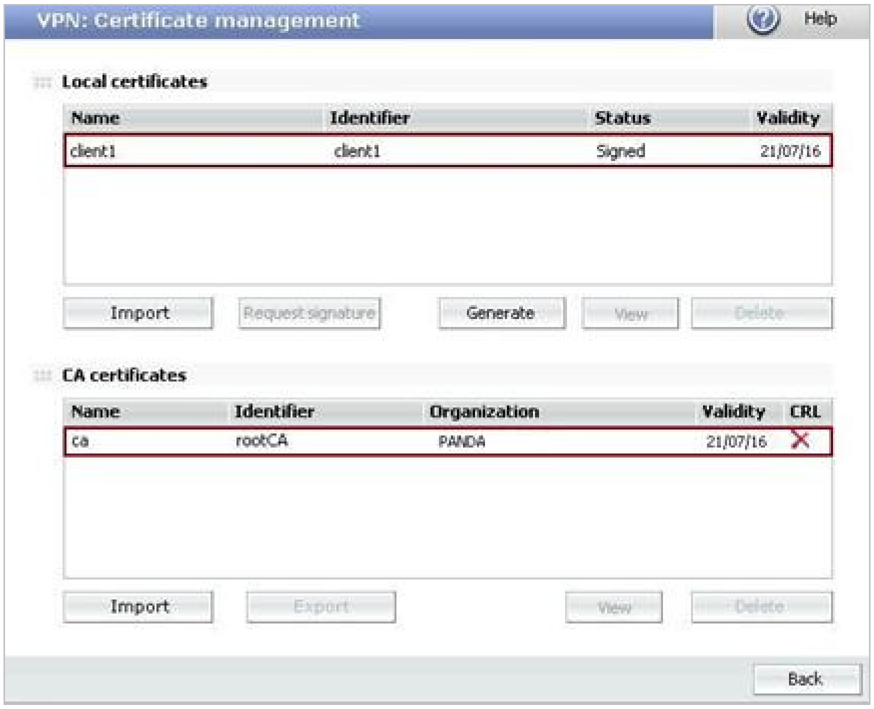
The first step when configuring an SSL VPN that uses TLS for validation will be to import the required certificates.

Certificates are required 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.

Note: This Gateway B certificate must be a client certificate, not another Server certificate.

In order to import CA and local gateway B certificates (remember that gateway B will act as a client in this configuration), follow the procedures already explained when configuring gateway A.

Once the CA and local gateway B certificates have been imported successfully, you will see a screen similar to the one shown below (figure 4.9).



Local certificates

Name	Identifier	Status	Validity
client1	client1	Signed	21/07/16

CA certificates

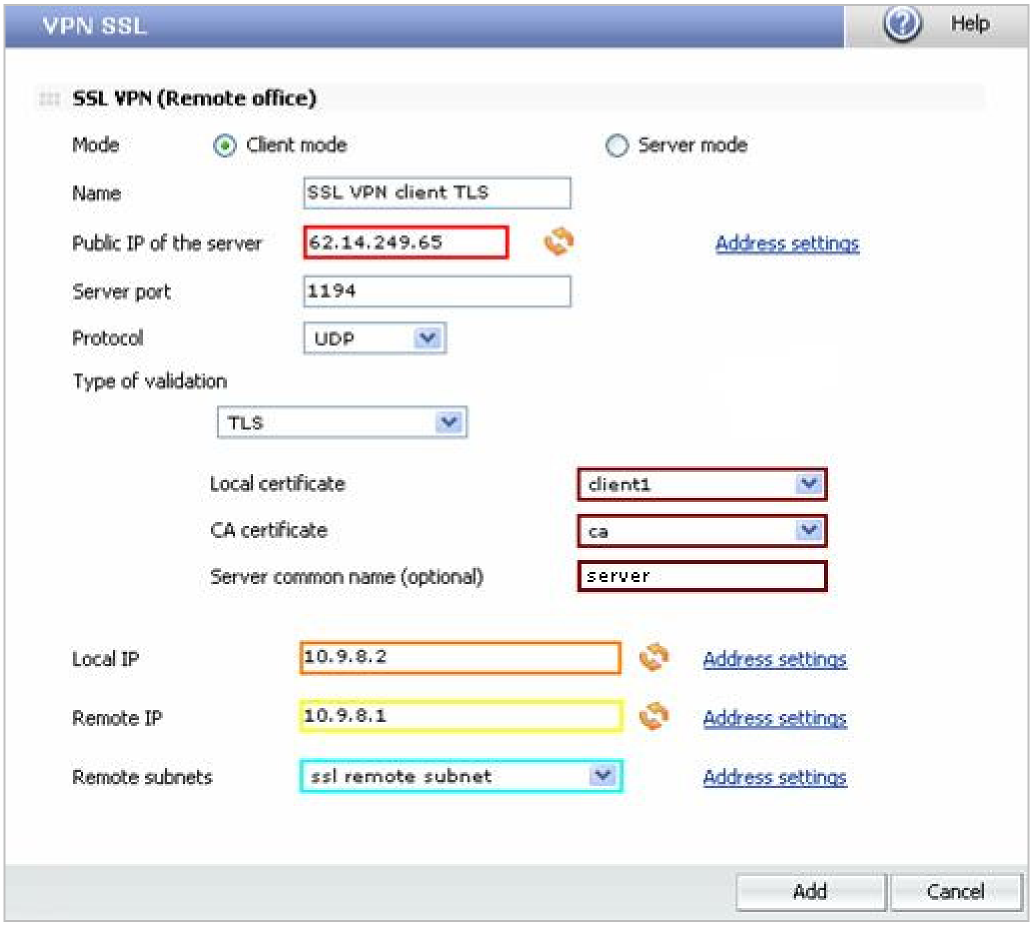
Name	Identifier	Organization	Validity	CRL
ca	rootCA	PANDA	21/07/16	✗

Figure 4.9

The steps below describe how to configure an SSL VPN gateway B with TLS using previously defined elements.

a. Go to the Panda GateDefender Integra administration console.
b. Click on **VPN** in the panel on the left.
c. Then, select **VPN management**.
d. Click on **SSL VPN management** and select the Remote offices tab.
e. Click on **Add** to define the new VPN.

There you will find the parameters required to configure a VPN in Panda GateDefender Integra using the SSL protocol in client mode (as shown in figure 4.10):



SSL VPN (Remote office)

Mode ● Client mode ○ Server mode
Name: SSL VPN client TLS
Public IP of the server: 62.14.249.65 Address settings
Server port: 1194
Protocol: UDP
Type of validation: TLS
Local certificate: client1
CA certificate: ca
Server common name (optional): server
Local IP: 10.9.8.2 Address settings
Remote IP: 10.9.8.1 Address settings
Remote subnets: ssl remote subnet Address settings

Figure 4.10

- Mode: select the option **Client mode**.
- Name**:** enter a descriptive name for the VPN (**VPN SSL client TLS** will be used for this how-to).
- Public IP of the server: Enter the remote public IP of the server (**62.14.249.65** will be used in this how-to).

- Server port: enter connection server port (default port **1194** will be used for this how-to).
- Protocol: choose the protocol that will be used for encapsulation (default protocol **UDP** will be used in this how-to).

Note that the TCP protocol is considered more secure, but slows down communications. UDP makes fewer checks and is therefore faster.

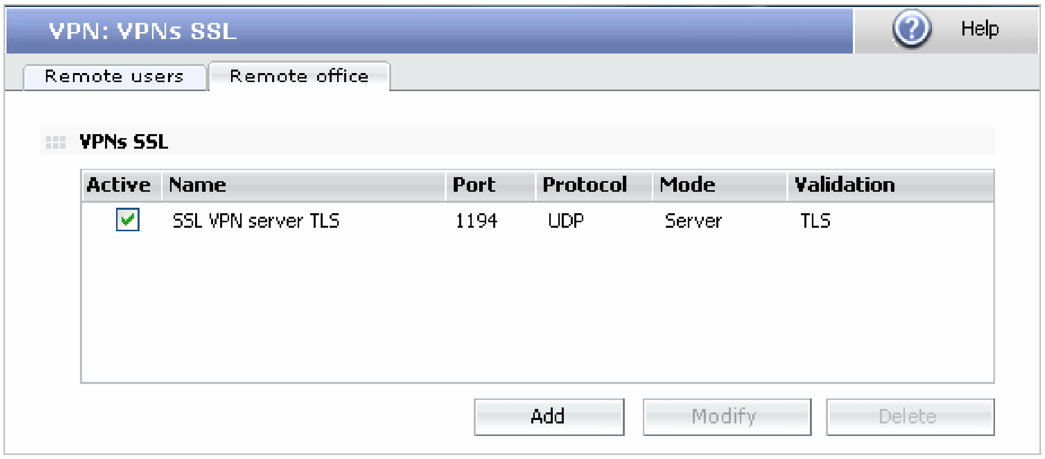
- Validation type: Choose **TLS** as a type of validation to use for the VPN.
- Local certificate: Use the drop-down menu to select the certificate you want (**client1** will be used in this how-to).
- Validation CA of the remote certificate: The remote office identified with a certificate must present the CA signature. Use the drop-down menu to select the CA certificate you want. (**ca** will be used in this how-to).
- Remote gateway Common Name: It is compulsory to enter the CN (Common name) of thegateway A-, in this case, server. The certificate can be obtained from the CN field of the server´s .CRT .
- Common Name del gateway remoto. En este campo se debe introducir el CN (Common name) del gateway A- en este caso server . Se puede obtener del campo CN del certificado .CRT del servidor
-
- IP: Enter the local private IP address (**10.9.8.2** will be used for this how-to).
- Remote IP: Enter the remote private IP address (**10.9.8.1** will be used for this how-to).
- Remote subnets: Enter local subnet A (remote subnet from the gateway B point of view). The previously defined **SSL remote subnet** will be used for this how-to which is **192.168.10.0/24**).

Index

1.4 Establishing a VPN connection

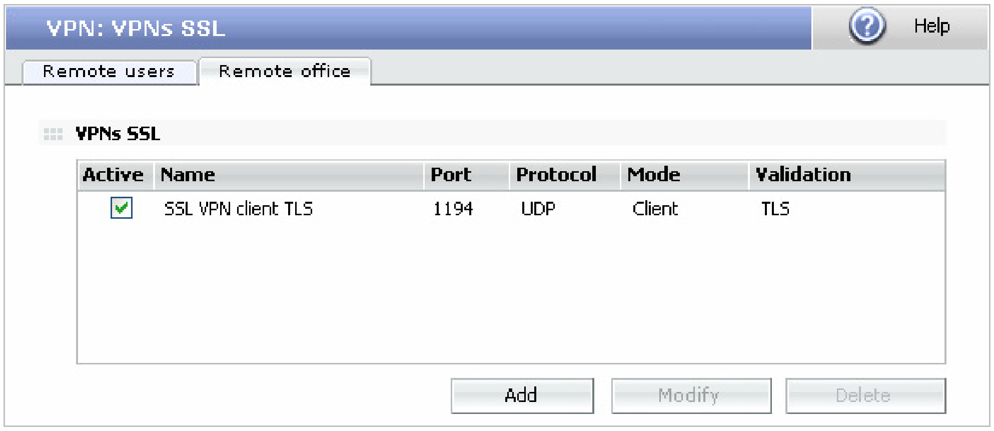
In order to initiate SSL VPN between two gateways, follow these instructions:

Select the **Active** checkbox on both gateways to enable the server and client side configuration, as shown in figures 4.11 and 4.12.



Active	Name	Port	Protocol	Mode	Validation
☑	SSL VPN server TLS	1194	UDP	Server	TLS

Figure 4.11



Active	Name	Port	Protocol	Mode	Validation
☑	SSL VPN client TLS	1194	UDP	Client	TLS

Figure 4.12

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

Index

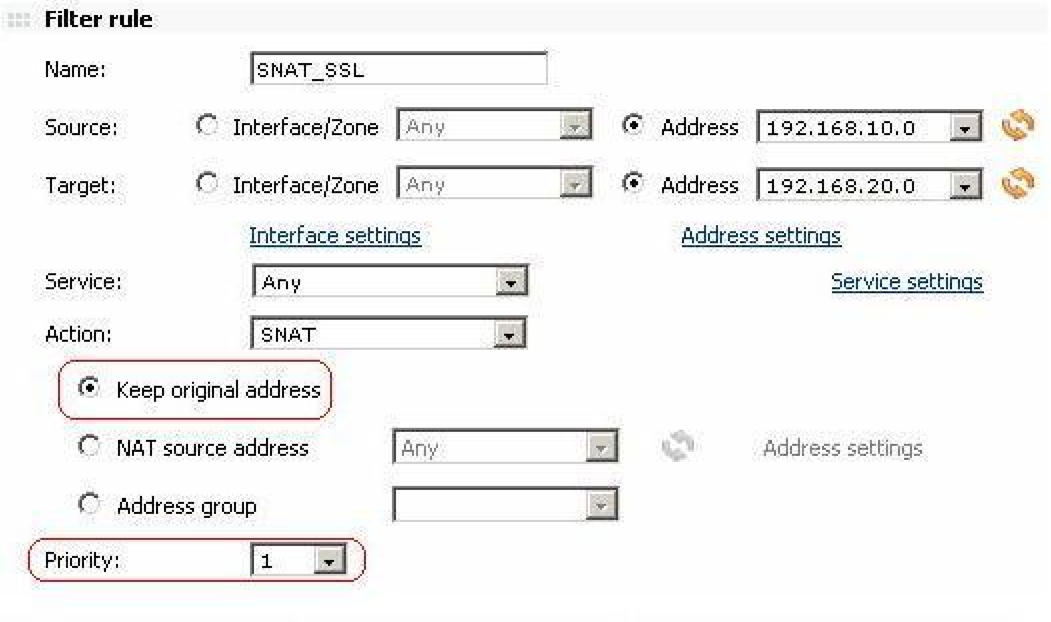
1.5 Further considerations

If Panda GateDefender Integra's firewall capabilities are used, then all the corresponding configuration rules of its firewall will be automatically entered.

If there are routers or firewalls between the two gateways, the following port and protocol must be enabled for SSL VPN to work properly:

Port / Protocol
1194/UDP.

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 SNAT 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_SSL

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

Figure 4.13

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.

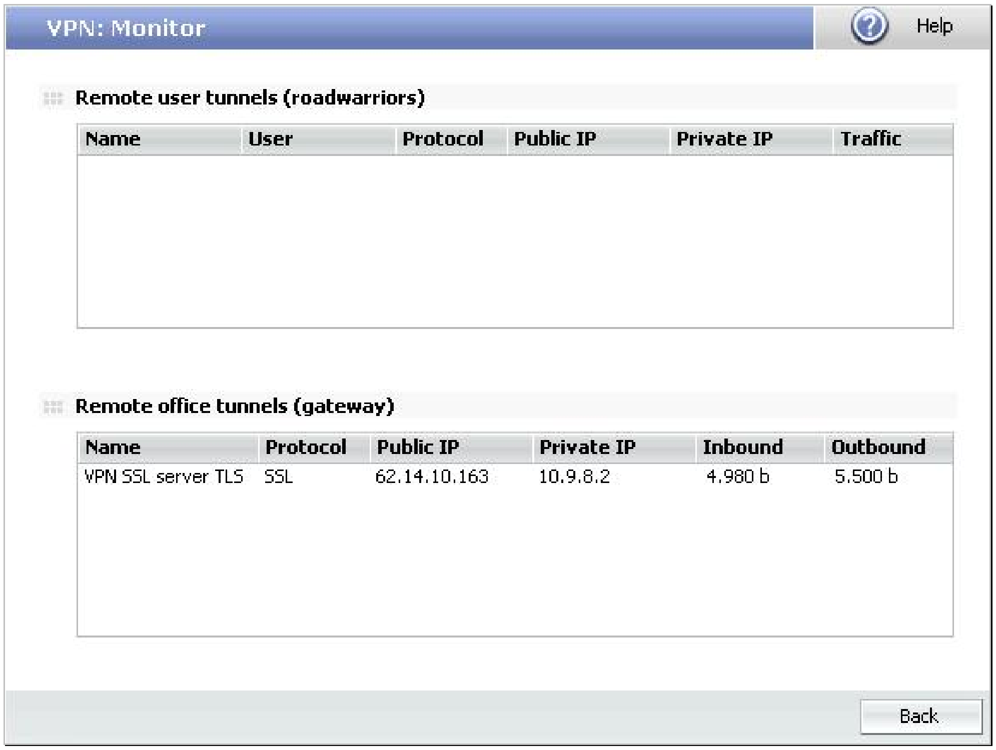
Index

1.6 Configuration checking

To check your **SSL** 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.

Then select **VPN Monitor** which will allow you to see the status of all established VPN connections (figure 4.14 shows the status of the gateway A monitor window).



Remote user tunnels (roadwarriors)

Name	User	Protocol	Public IP	Private IP	Traffic

Remote office tunnels (gateway)

Name	Protocol	Public IP	Private IP	Inbound	Outbound
VPN SSL server TLS	SSL	62.14.10.163	10.9.8.2	4.980 b	5.500 b

Figure 4.14

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

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

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, host that belongs to the gateway A should see the icmp response message.

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

Index

0707-PGDIHT04-03-EN