Panda GateDefender Integra

HOWTO: How to configure L2TP VPN tunnel roadwarrior (remote user) to gateway (office)

'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

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 the L2TP VPN tunnel roadwarrior-to-gateway

The L2TP protocol (Layer 2 Tunneling Protocol) resolves interoperability problems between PPTP and L2F encapsulating the characteristics of both. It allows tunneling at the PPP link level, so that IP, IPX and AppleTalk packets sent privately can be transported via the Internet. It is supported by IPSec for data security.

Panda GateDefender Integra includes a VPN system so you can create your own virtual private networks, widening the reach of your network and ensuring confidentiality in connections.

The aim of this guide is to describe the steps needed to create a virtual private network (VPN) based on L2TP with Panda GateDefender Integra, using real data.

 **Note:** This guide assumes that the Panda GateDefender Integra unit has been configured, at least basically, and is up and running. For more information about installing and configuring Panda GateDefender Integra, refer to the Installation Guide.

 **Important:**

- GateDefender Integra must be operating in router mode. If not, you will not be able to use the VPN system.
- Panda GateDefender Integra only lets you create and modify L2TP VPNs in server mode given the limitations of the implementation of the L2TP protocol.

1.1 Scenario setup

The illustration below is a typical roadwarrior-to-gateway L2TP VPN scenario:

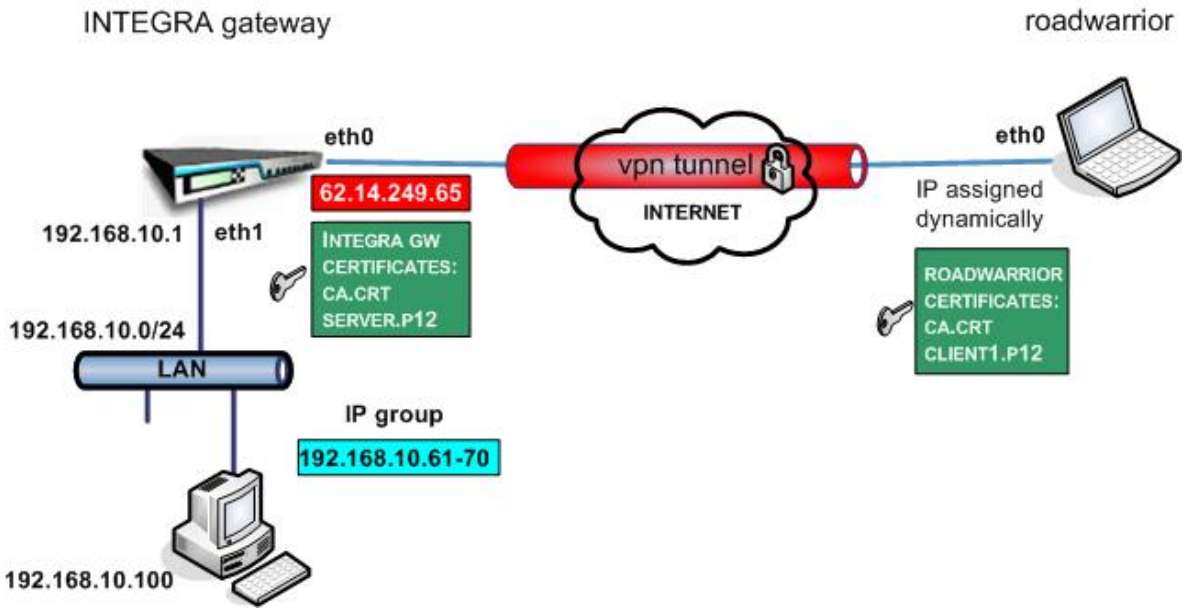


Figure 2.1: L2TP VPN

Roadwarrior has a dynamically assigned address by the ISP and will access Integra's LAN, by means of a secure tunnel using the L2TP protocol.

INTEGRA's WAN interface has the IP address **62.14.249.65.**

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.

Clients on Integra's LAN side do not need to have configured Integra's LAN IP address as its default gateway because the roadwarrior will have assigned the first available IP address from the previously defined IP group range (which itself belongs to the internal network) so it will be visible to all hosts on LAN **192.168.10.0/24**

Index

1.2 Gateway side configuration (Panda GD Integra)

The first step when configuring L2TP VPN consists of defining the group of users authorized to establish a VPN connection and defining the IP range that belongs to the LAN that you want your roadwarrior to be able to connect to.

1.2.1 Users and group configuration

1. Access the **Definitions** section of the main Panda GateDefender Integra console menu
2. Select **User management**
3. In the **Users** section, click 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 **Add** to save the changes.

As for the configuration of L2TP VPN, where defined groups of VPN users were needed, now you need to add previously defined users to the 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 the **Add** button.
4. Define a group name and add users from the box below.

Once this has been done, the configuration should be similar to that shown in figure 2.2.

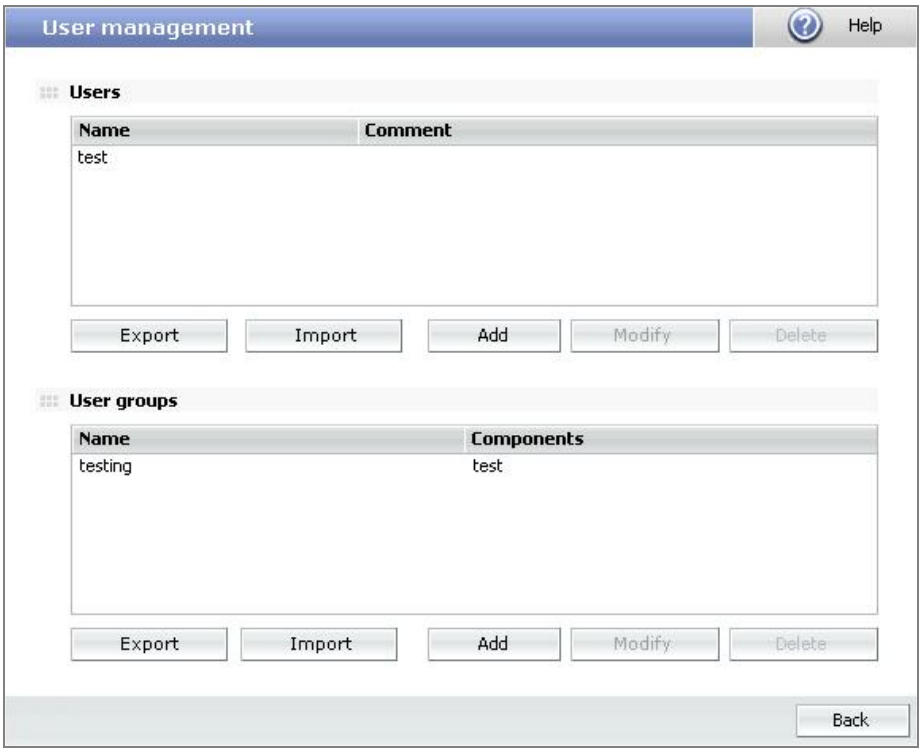


Figure 2.2

Index

1.2.2 IP group configuration

The next stage will describe the steps to configure the IP group definition:

1. Access the **Definitions** section of the main Panda GateDefender Integra console menu.
2. Select **IP addresses**
3. In the **Groups** section, click the **Add** button.
   A descriptive name of the group must be provided **(pptp vpn group** will be used for this how-to) in the **Name** field and IP range **192.168.10.61-70** in the **Use range** radio button section.
4. Click **Add IP**
5. Finally, click **Add** to save the changes.

The settings will be configured as shown in figure 2.3.

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

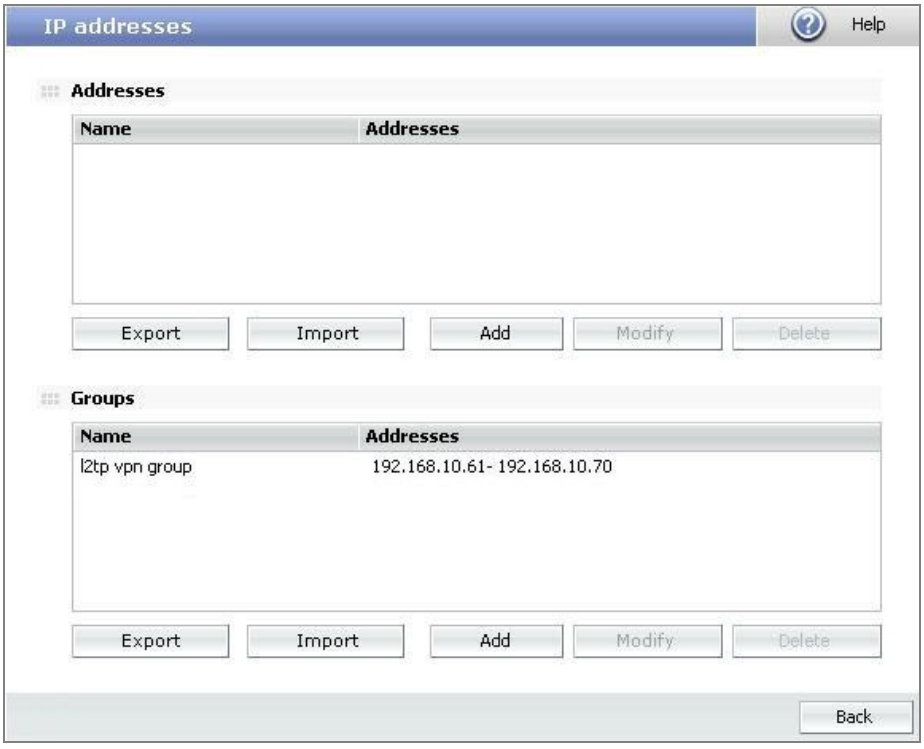


Figure 2.3

Index

1.2.3 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 would be used to authenticate the 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 the **Import** button

   - Enter **Certificate name** (**ca** will be used in this how-to)
   - Click **Browse...** to select the certificate you want to import.
   - Click **Import** once you have chosen a CA certificate that you wish to import

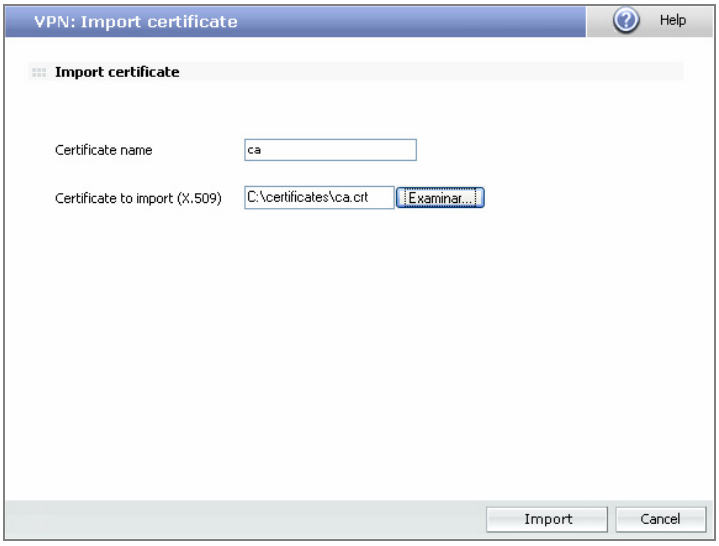


Figure 2.4

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

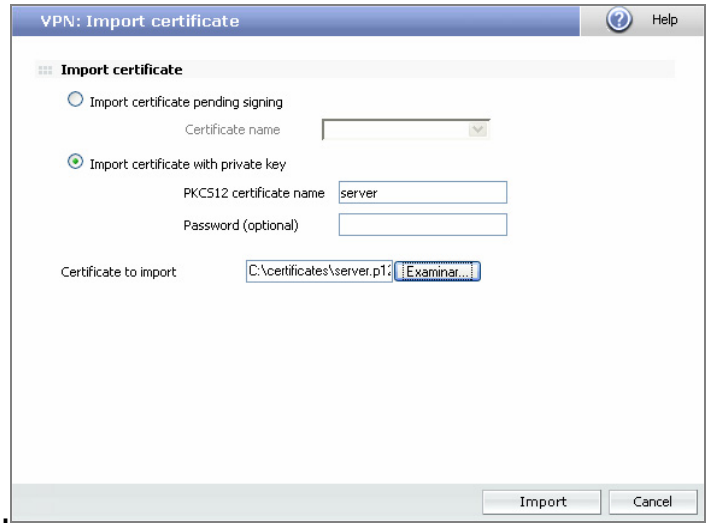


Figure 2.5

Once the CA and server certificates have been imported successfully, the corresponding configuration screen displayed is similar to that shown in figure 2.6

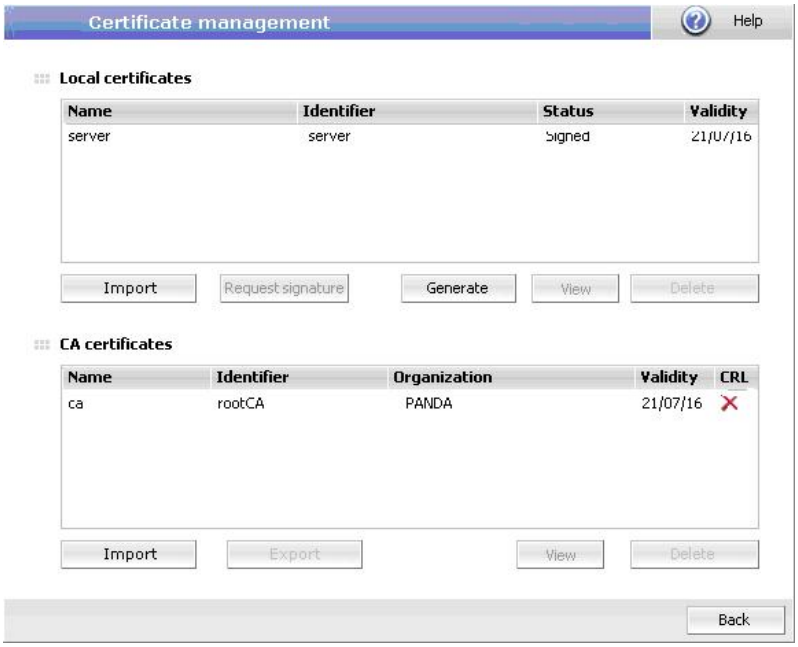


Figure 2.6

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

Index

1.2.4 L2TP/IPSec VPN configuration

This part consists of two sections, IPSEC and L2TP.

1.2.4.1 IPSEC configuration

This section is related to the IPSec configuration (encryption of L2TP VPN depends on the IPSec protocol. IPSec Encapsulating Security Payload (ESP) is used to encrypt the L2TP packet. This kind of implementation is also known as L2TP/IPSec).

In order to configure IPSec, follow the instructions below:

1. Go to the Panda GateDefender Integra administration console.
2. Click **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 (in this case, L2TP will be used).
2. **IKE policies**: use the drop-down menu to select the policy to apply.(In this example, IKE 1 will be used).
3. **Phase I parameters**:

   Local IP: Enter the local public IP address or choose **IP assigned by DHCP (62.12.249.65** will be used in this how-to**)**

4. **Phase II parameters**:

Select a protocol to use: **L2TP/IPSec**

When you choose L2TP/IPSEC, the following options will be available:

- **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 roadwarrior's 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 2.7.

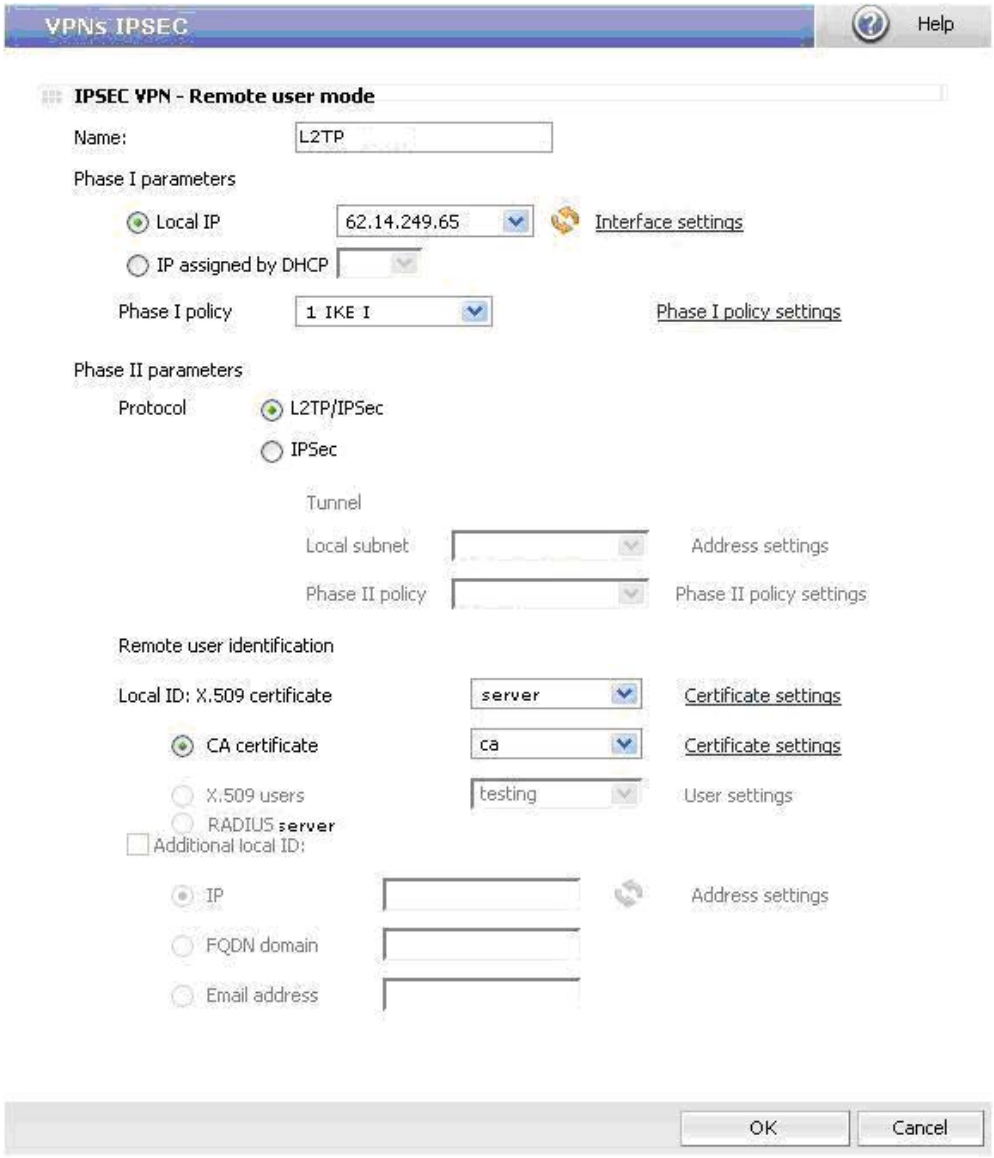


Figure 2.7

Note: 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.

Index

1.2.4.2 L2TP configuration

This section is related to the configuration of L2TP protocol itself.

In order to configure L2TP, follow the procedure below:

1. Go to the Panda GateDefender Integra administration console.
2. Click **VPN** in the panel on the left.
3. Then select **VPN management**, and then **L2TP VPN management**.

   There you will find the parameters required to configure a VPN in Panda GateDefender Integra using the L2TP protocol (as shown in figure 2.4):

   - **Name:** enter a descriptive name for the VPN (**l2tp vpn** will be used for this how-to).
   - **Active:** select this checkbox to enable the VPN.
   - **IP group:** select the range of IP addresses (**l2tp vpn group** will be used for this how-to) associated to this VPN. If you have not defined it previously click on the link **Address settings** to access the *IP address settings* screen.
   - **Users: select the desired users.**

     - **Local users:** select the user group authorized to access your VPN (**testing** will be used for this how-to). If you have not defined it previously, click on the link **User settings to access the user settings screen**.
     - **Radius server:** select the Radius server that Panda GateDefender Integra will use in order to authenticate the users.

   Once the L2TP part has been configured, the corresponding configuration screen will be displayed as shown in figure 2.8.

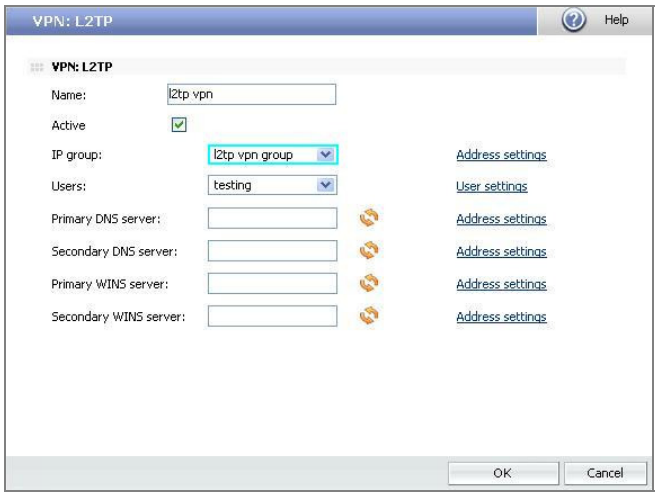


Figure 2.8

Index

1.3 Client side configuration (MS Windows 2000/XP)

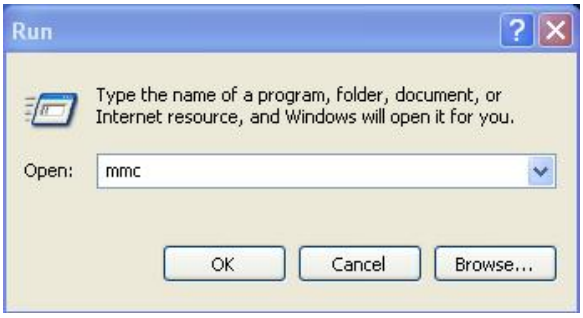
Once it has been confirmed that the connection to the Internet is correctly configured on the client computers running Microsoft Windows 2000/XP, follow the steps described below:

1.3.1 Import a local gateway certificate and the CA certificate

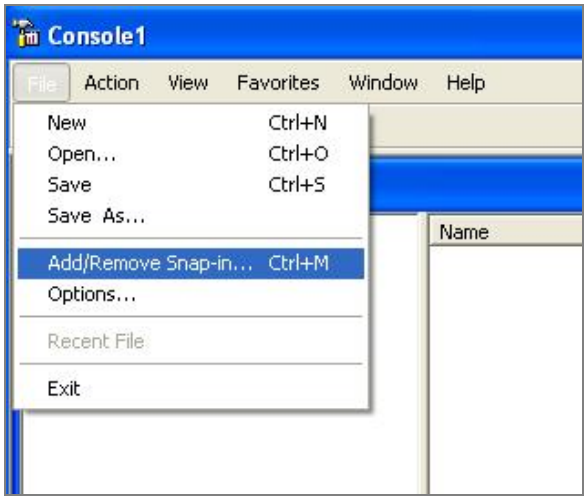
Certificates are required for authentication purposes. You need to import the trusted public CA certificates which signed the Integra VPN gateway certificate. It is also necessary to import the roadwarrior certificate that would be used to authenticate the roadwarrior itself.

In order to import local certificates for a roadwarrior, follow the procedure below:

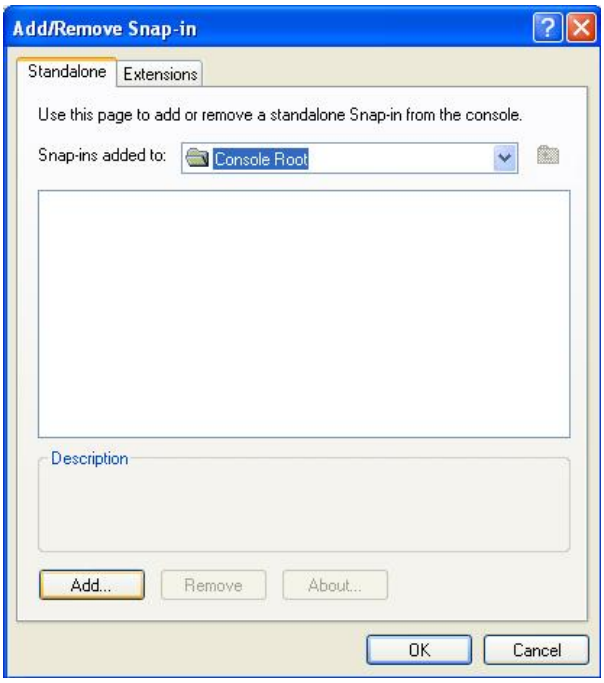
1. Click the **Start** button
2. Select **Run**
3. In the text field, type **mmc** and click **OK**



4. Click **File** and select **Add/Remove Snap-in**

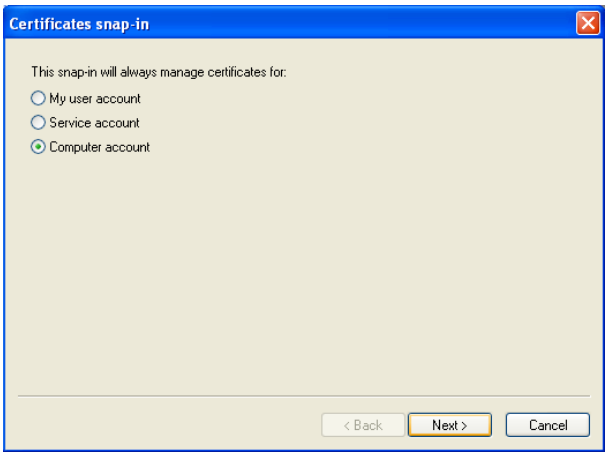


5. Click **Add...**

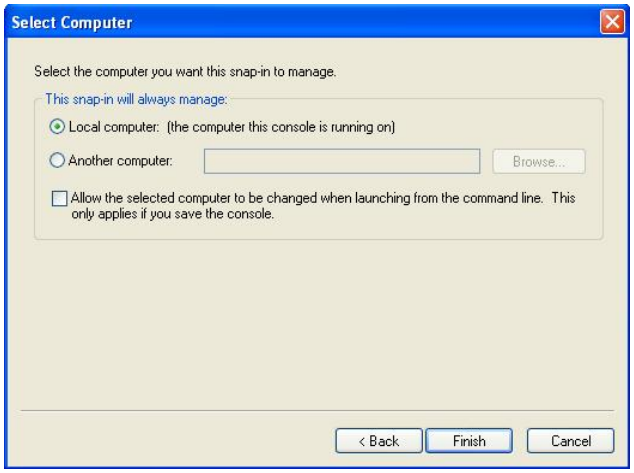


6. Select **Certificates**, and then select **Add**

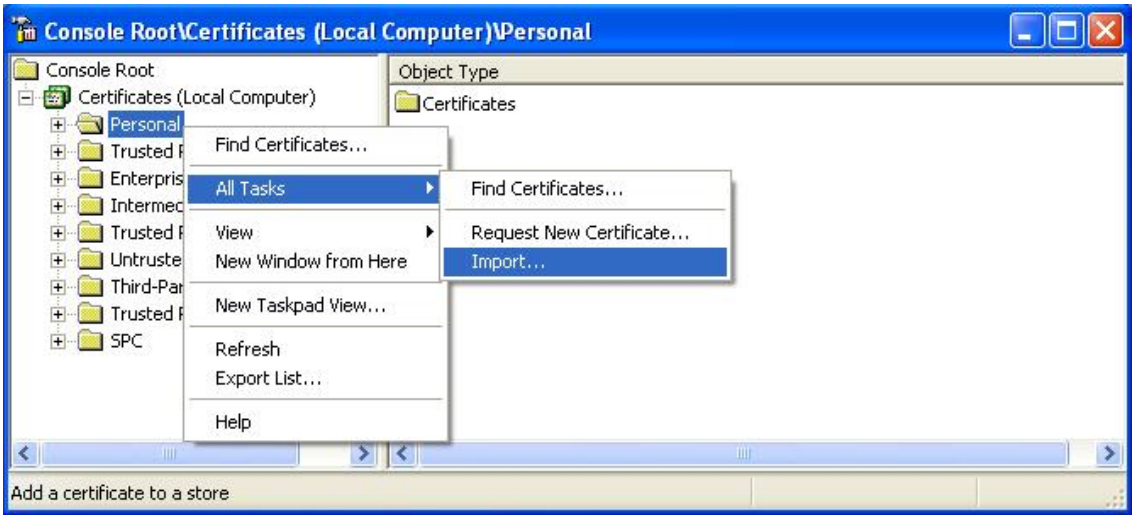
7. Select **Computer Account** and click **Next**



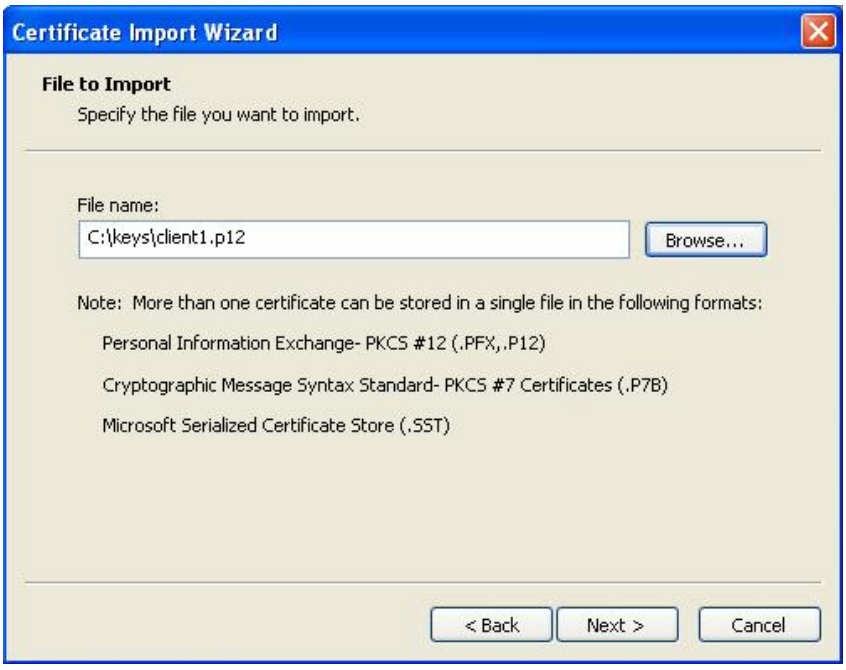
8. Select **Local computer** and click **Finish**



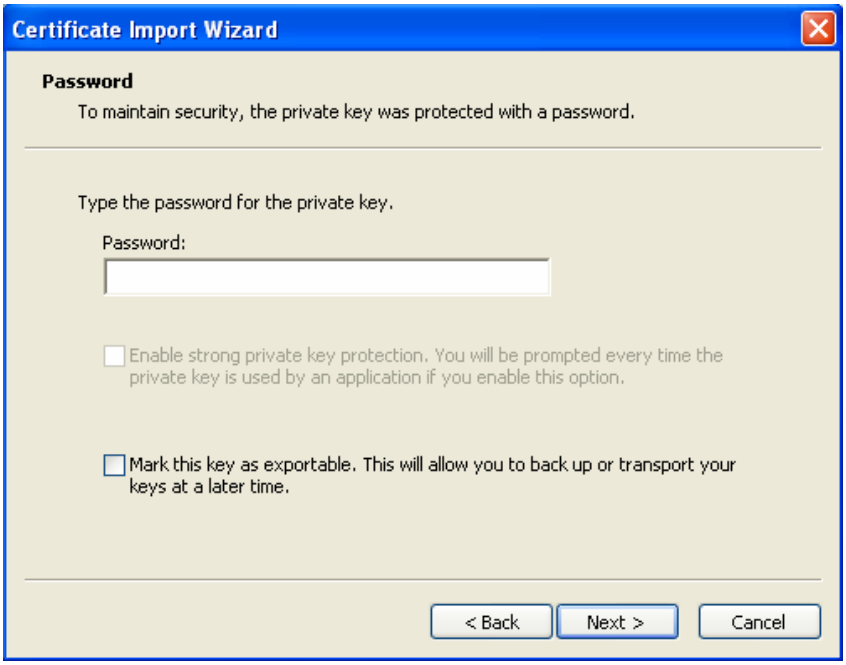
9. Click **Close** and **OK**
10. Click the plus **arrow** by **Certificates (Local Computer)**
11. Right-click **Personal** and select **All Tasks**
12. **Access Import...**



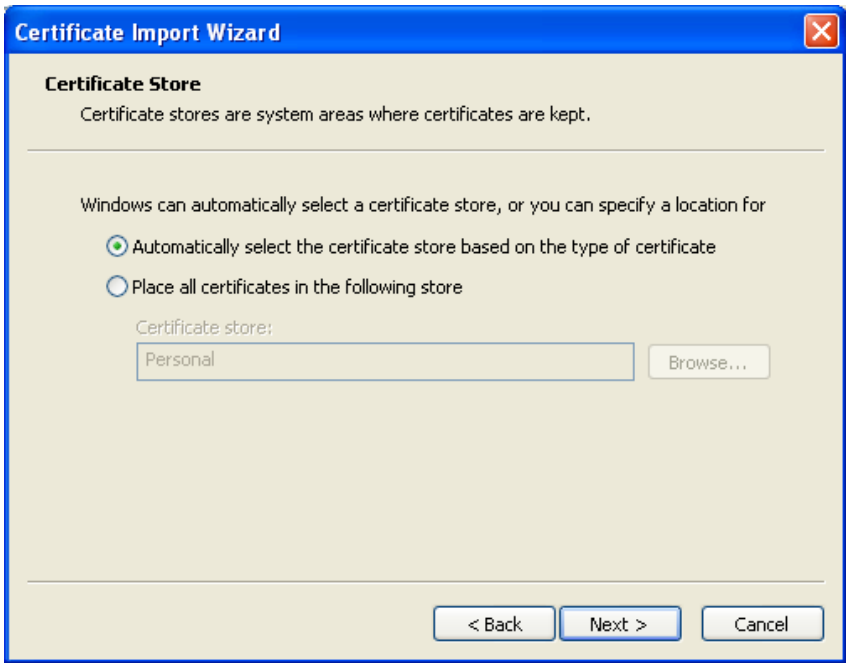
13. Click **Next**
14. Type in the path to the roadwarrior .p12 file (or browse and select the file), and click **Next**



15. Optionally, type the export **password** if required, and click **Next**

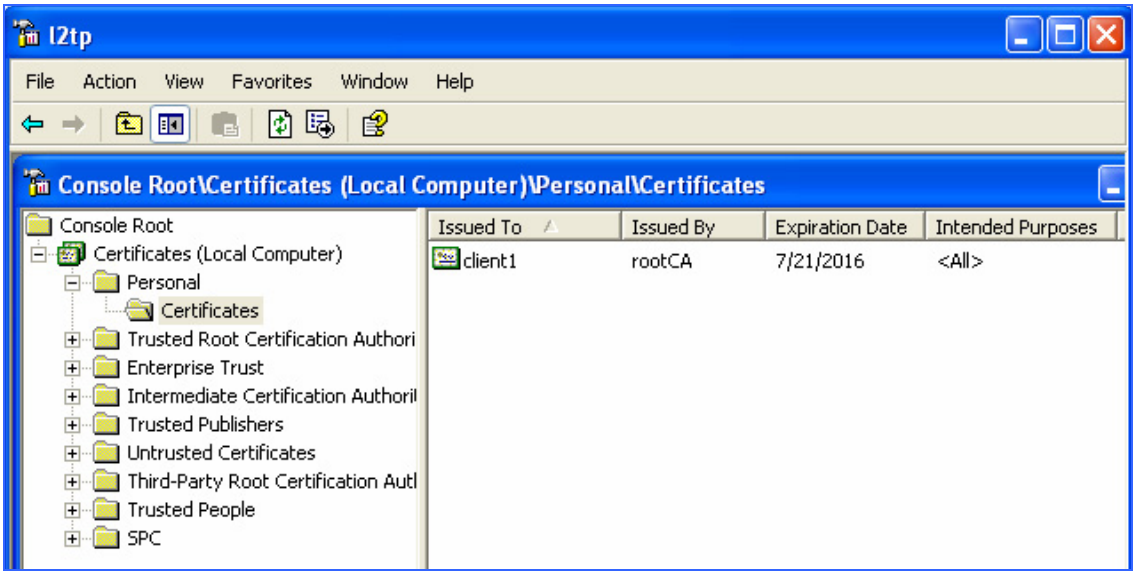


16. Select **Automatically select the certificate store based on the type of certificate** and click **Next**



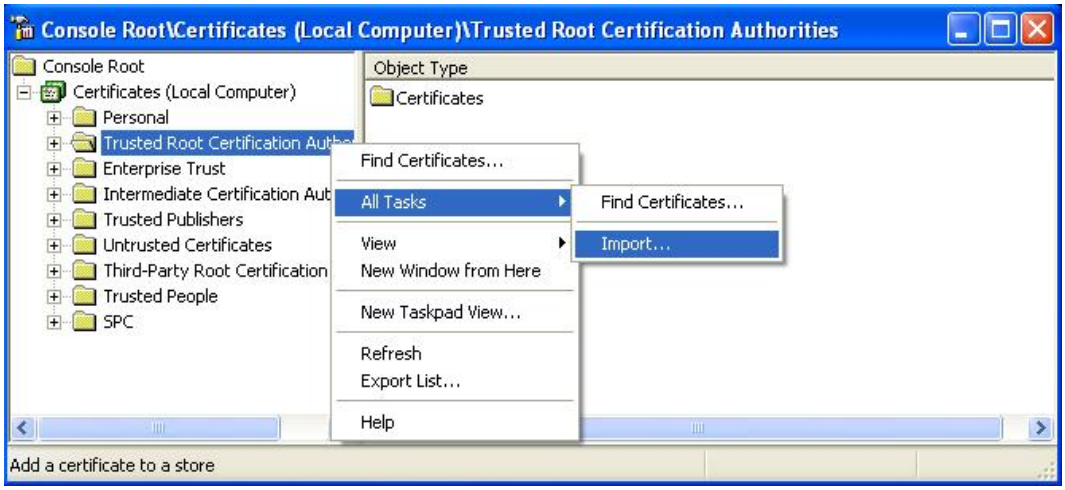
17. Click **Finish**, and confirm the next pop-ups by selecting **Yes**.
18. Click **OK**.

If your certificate has been imported successfully, the corresponding screen will be similar to the one below.

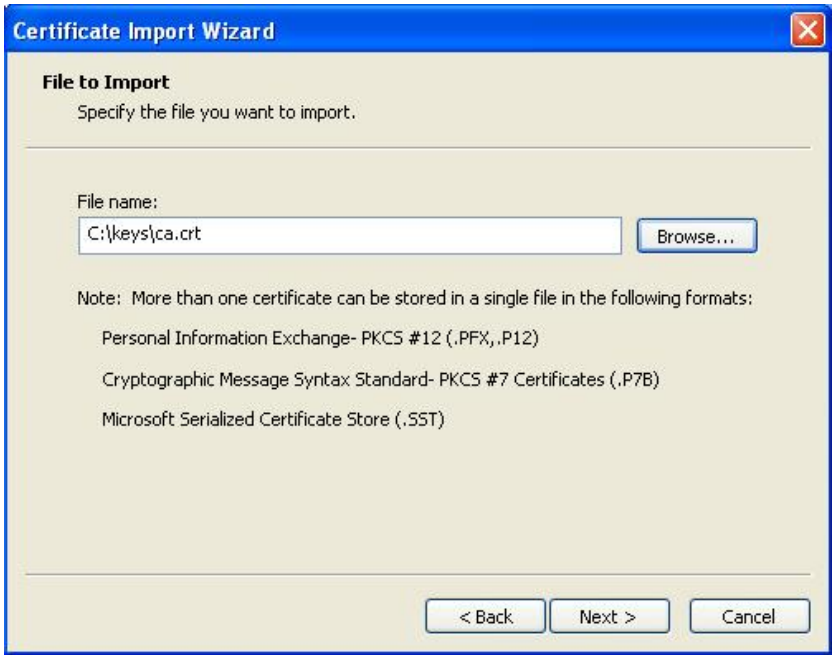


If a CA that has been used to sign your roadwarrior certificate is different from the one that has been used to sign the Integra VPN gateway certificate, you must then follow the instructions below. Otherwise, simply skip the following part and continue with section ***Connection configuration.***

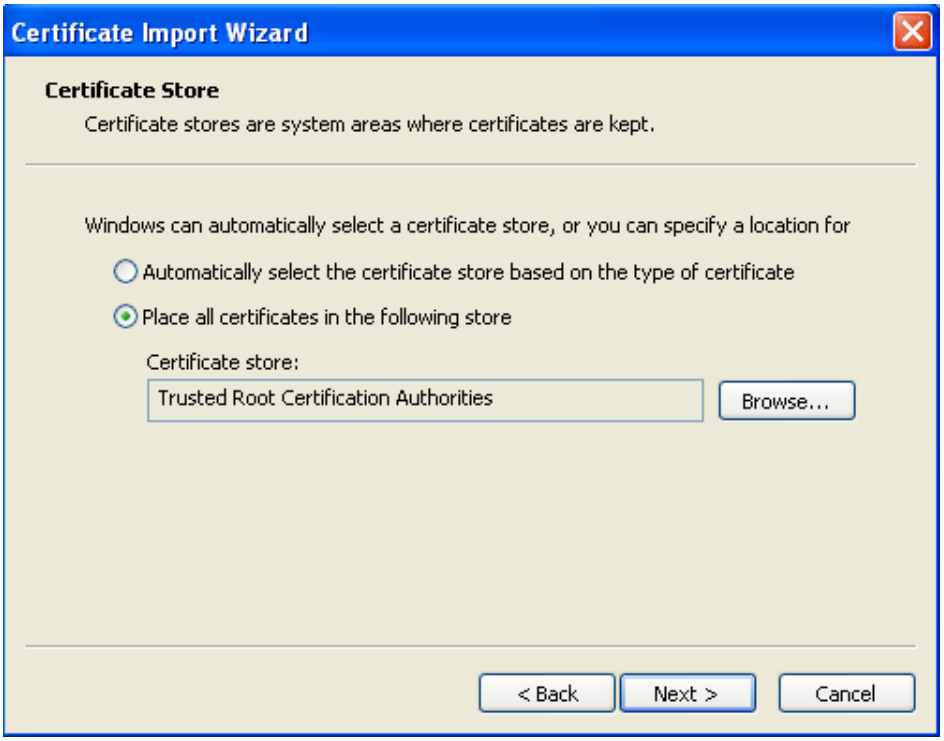
1. Right-click **Trusted Root Certification Authority** and select **All Tasks.**
2. Then, click **Import...** and **Next**.



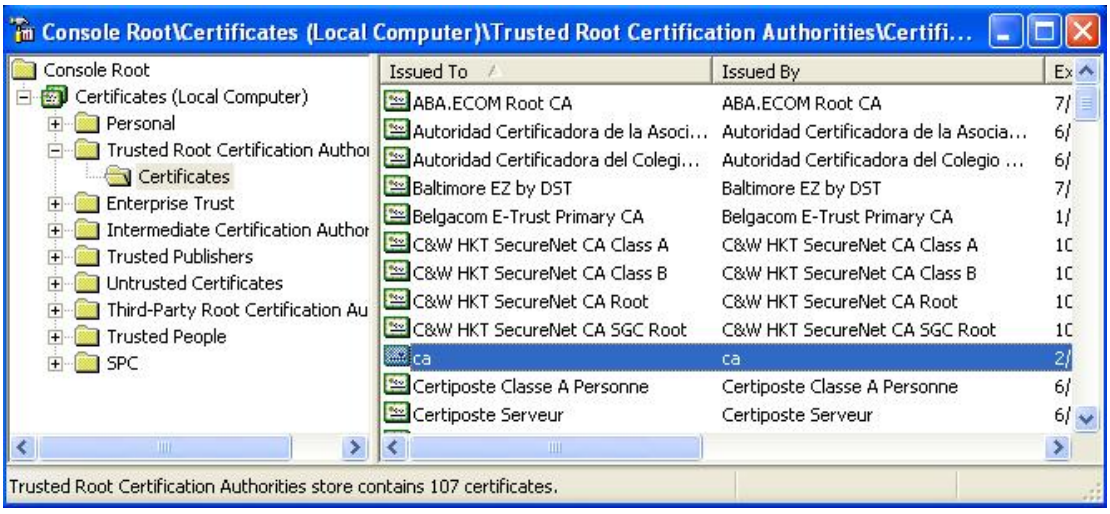
3. Type in the path to the .crt file that corresponds to the Integra VPN gateway CA (or browse and select the file), and click **Next**.



4. Select **Place all certificates in the following store** and click **Next**.

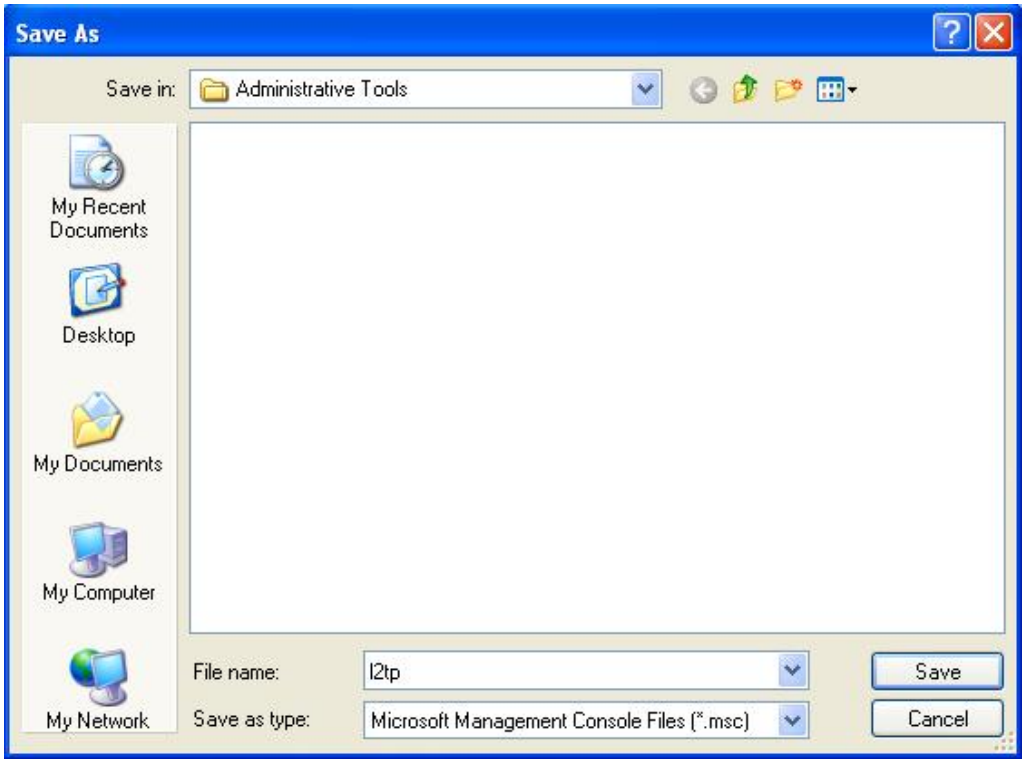


5. Click **Finish**, and confirm the next pop-ups by selecting **Yes**. Then click **OK**.



6. Save the current configuration settings as a file so you don't have to re-add the Snap Ins each time.

7. Type the name and click **Save**.



Index

1.3.2 Connection configuration

1. Click the **Start** button
2. Select the **Control Panel**.
3. In Control Panel, double-click **Network Connections**
4. Then, click **Create a new connection**.

5. In the Network Connection Wizard, click **Next**.

6. Click **Connect to the network at my workplace**, and then click **Next**.

7. Click **Virtual Private Network connection**, and then click **Next**.

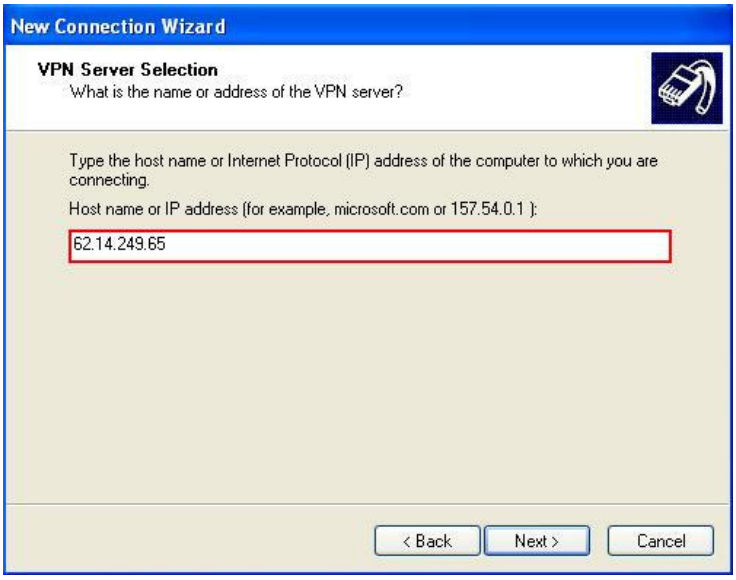
If you use a dial-up connection to connect to the Internet, click on **Automatically dial this initial connection**, and then, from the list, select your dial-up Internet connection.

If you use a permanent connection (such as an ADSL or cable modem), select the verification checkbox **Do not dial the initial connection**.

8. Click **Next**.

9. Type in the name of your company or a descriptive name for the connection, and then click on **Next**.

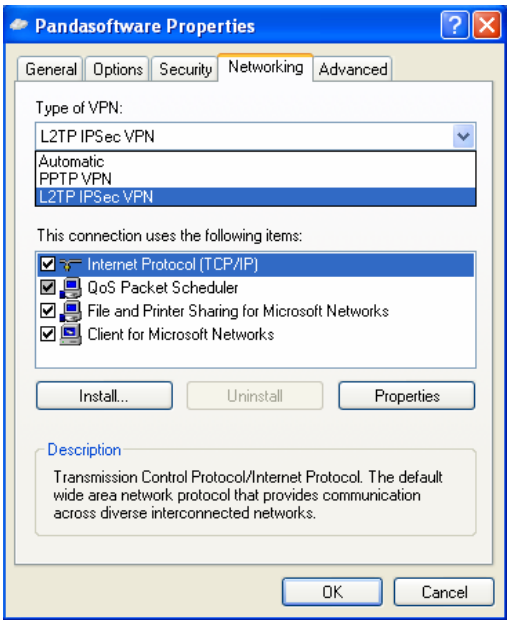
10. Type in the IP address of VPN server (**62.14.249.65** will be used for this how-to), and then click **Next**.



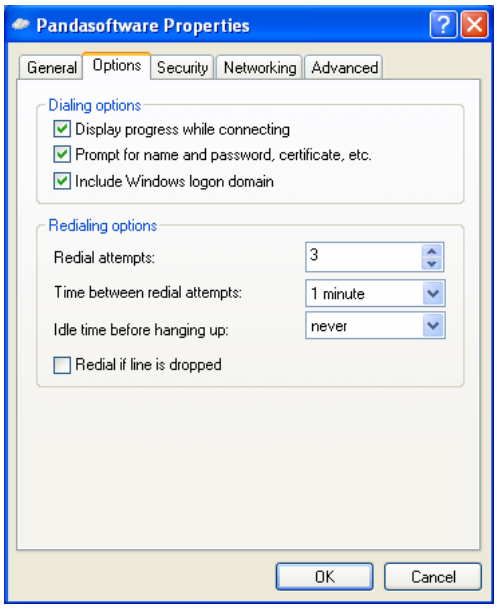
11. Enable the verification **Add a shortcut to this connection to my desktop** checkbox if you want to create a shortcut on the desktop, and then click **Finish**.

12. If you are prompted to connect, select **No.**
13. In the Network Connections window, right-click on the new connection.
14. Click **Properties**, and then configure further options for the connection:

15. Select the **Networking** tab and then, from the Type of VPN list, choose **L2TP IPSec VPN**.



16. If you are connecting to a domain, click the **Options** tab, and then click to select the **Include Windows logon domain** checkbox to specify whether to request Windows 2000/XP logon domain information before attempting to connect.



Index

1.4 Establishing L2TP VPN connection

Use the following procedure in order to establish the L2TP VPN connection which has previously been defined:

1. Click on the **Start** button, then **Settings, Network Connections**, and then click on the connection that you configured before.
2. If you added a connection shortcut to the desktop, double-click on the shortcut on the desktop.

If you are not currently connected to the Internet, Windows offers to connect to the Internet.

After your computer connects to the Internet, the Integra VPN gateway will prompt you for your user name and password (the user must be previously defined on Integra side. Type your user name and password, and then click on **Connect**. Your network resources should be available to you as they are when you connect directly to the network.

In order to disconnect from the VPN, right-click on the icon for the connection that appears on the lower right corner, and then select **Disconnect**.

Index

1.5 Further considerations

If the Integra firewall is used, the encryption protocol configuration rules will automatically be entered in the firewall. But if the DNS and WINS servers have been entered (see figure 2.8) you will have to enter the rules manually.

But if you use a personal firewall or a broadband router with firewall features or if there are routers or firewalls between the VPN client and the Integra VPN gateway server, the following ports and protocols must be enabled for L2TP on all firewalls and routers that are between the VPN client and the Integra VPN gateway server:

For L2TP you need to open the **same** protocols and ports as for plain IPSec:

- 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*.

Index

1.6 Configuration checking

In order to check the L2TP VPN configuration please proceed as described below:

1. Access the Panda GateDefender Integra administration console.
2. Click **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 on figure 1.4).

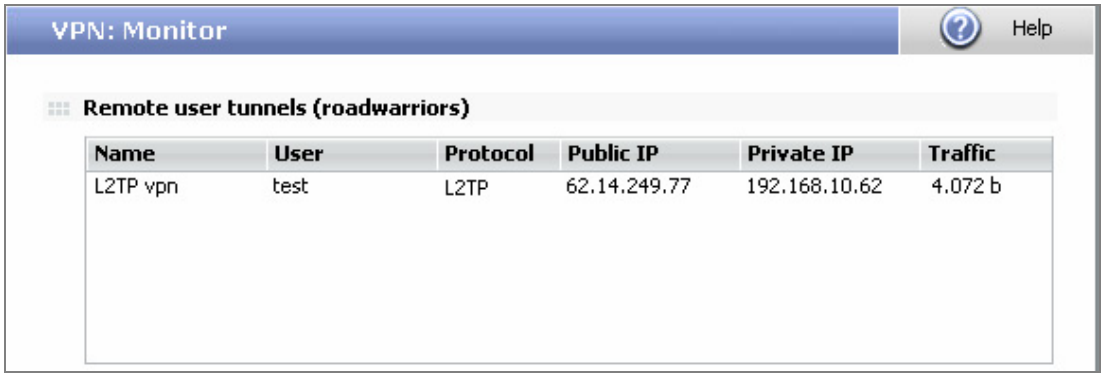


Figure 2.8

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 **ipconfig /all** command **shows that** an additional IP address has been assigned to your external interface (ppp adapter l2tp). If you are the first roadwarrior connected, it would be 192.168.10.62.

- The **ping –n 10 192.168.10.100** command pings from 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 an 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 only be seen when observing traffic in the external network interface, whereas the unencrypted packets (in this case icmp reply and response packets) will usually be seen in virtual ppp adapter I2p interface.

Index

0707-PGDIHT01-04-EN