Panda GateDefender Integra

HOWTO: Cómo configurar el túnel VPN L2TP de usuario remoto (roadwarrior) a oficina remota (gateway)

Casos de uso para configurar VPN con GateDefender Integra

Panda Security desea que obtenga el máximo beneficio de sus unidades GateDefender Integra. Para ello, le ofrece la información que necesite sobre las características y configuración del producto. Consulte http://www.pandasecurity.com/ y http://www.pandasecurity.com/spain/enterprise/support/ para más información.

ÍNDICE

Convenciones utilizadas en este documento Iconos utilizados en esta documentación:

Nota. Aclaración que completa la información y aporta algún conocimiento de interés.

Aviso. Destaca la importancia de un concepto.

Consejo. Ideas que le ayudarán a sacar el máximo rendimiento a su programa.

Referencia. Otros puntos donde se ofrece más información que puede resultar de su interés.

Tipos de letra utilizados en esta documentación:

Negrita: Nombres de menús, opciones, botones, ventanas o cuadros de diálogo.

Código: Nombres de archivos, extensiones, carpetas, información de la línea de comandos o archivos de configuración como, por ejemplo, scripts.

Cursiva: Nombres de opciones relacionadas con el sistema operativo y programas o archivos que tienen nombre propio.

Cómo configurar L2TP de usuario remoto (roadwarrior) a oficina remota (gateway)

El protocolo L2TP (Layer 2 Tunneling Protocol) resuelve las situaciones de interoperatividad entre los protocolos PPTP y L2F, encapsulando características de ambos. Permite el túnel del nivel de enlace de PPP, de forma que los paquetes IP, IPX y AppleTalk enviados de forma privada puedan ser transportados por Internet. Para la seguridad de los datos se apoya en IPSec.

Panda GateDefender Integra incluye el sistema VPN para la creación de sus propias redes privadas virtuales, ampliando el alcance de su red y asegurando la confidencialidad de sus conexiones.

El propósito de esta guía es detallar los pasos necesarios para la creación de una red privada virtual (VPN) basándose en el protocolo L2TP con Panda GateDefender Integra, utilizando datos reales.

Nota: Se da por hecho que la unidad Panda GateDefender Integra se encuentra configurada, al menos de forma básica, y funcionando. Si desea obtener información acerca de cómo instalar y configurar Panda GateDefender Integra, consulte la Guía de Instalación.

Avisos:

- Panda GateDefender Integra ha de encontrarse funcionando en modo Router. De lo contrario, no podrá utilizar el sistema VPN.
- Panda GateDefender Integra sólo permite crear y modificar las VPNs L2TP en modo servidor debido a las limitaciones de la implantación del protocolo L2TP.

1.1 Escenario

La siguiente ilustración muestra un escenario típico de conexión VPN L2TP de usuario remoto (roadwarrior) a oficina remota (gateway)

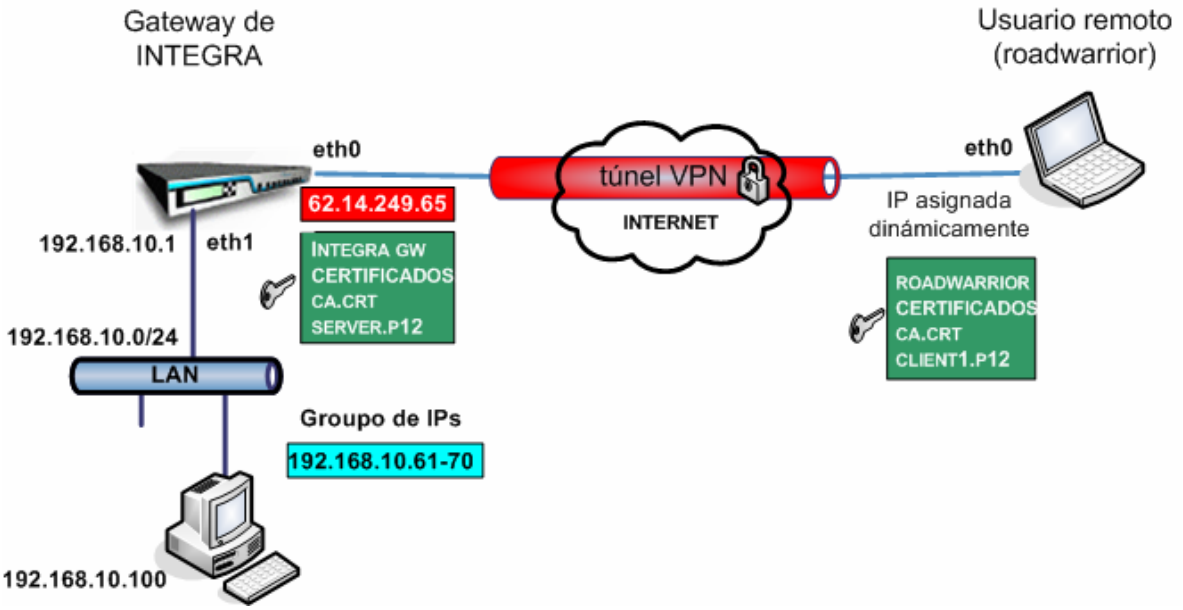


Figura 2.1: VPN L2TP

El usuario remoto (roadwarrior) tiene una dirección asignada dinámicamente por el ISP y accederá a la LAN de Integra a través de un túnel seguro utilizando el protocolo L2TP.

La interfaz WAN de INTEGRA tiene la dirección IP **62.14.249.65.**

En la figura se aprecia que el interfaz eth0 tiene asignada una dirección IP pública. Habitualmente, en las configuraciones reales más comunes, el interfaz eth0/WAN de Integra tiene asignada una dirección IP privada, y es otro dispositivo con la opción NAT habilitada situado entre Integra y la conexión ISP (por exemplo módem/router ADSL, cable Módem, etc…), que dispone de una dirección IP pública (dinámica o estática).
Esta aproximación se ha llevado a cabo para simplificar el documento y centrarlo en la configuración de la VPN.
Para más información al respecto, consulte los HOWTOS publicados que tratan los temas de las configuración de SNAT, DNAT y mapeo de los puertos.

No es necesario que los clientes situados en la LAN de Integra configuren la dirección IP de la LAN de Integra como su gateway predeterminado, ya que el usuario remoto (roadwarrior) tendrá asignada la primera dirección IP disponible del rango del grupo de direcciones IP anteriormente definido (que pertenece a la red interna) para que sea visible para todos los ordenadores de la LAN **192.168.10.0/24**

Índice

1.2 Configuración del lado del gateway (Panda GD Integra)

El primer paso a la hora de configurar VPN L2TP consiste en definir el grupo de usuarios autorizados a establecer una conexión VPN e indicar el rango de direcciones IP que pertenece a la LAN a la que quiere que se conecte su usuario remoto (roadwarrior).

1.2.1 Configuración de usuarios y grupos

1. Acceda a la sección **Definiciones** del menú principal de la consola de Panda GateDefender Integra.
2. Seleccione **Gestión de usuarios**.
3. En el apartado **Usuarios**, haga clic en el botón **Añadir**.
4. Se abrirá una pantalla en la que deberá introducir datos, como mínimo, en los tres primeros cuadros de texto:

    - Nombre (en este ejemplo utilizaremos ***test***)
    - Contraseña (en este ejemplo utilizaremos ***testing***)
    - Repetir contraseña.

5. Cuando haya terminado la configuración, haga clic en **Añadir** para guardar los cambios.

En cuanto a la configuración de VPN L2TP, en los casos en los que se necesiten grupos definidos de usuarios de VPN, deberá añadir los usuarios anteriormente definidos al grupo.

Para ello, siga los pasos que se indican a continuación:

1. Acceda a la sección **Definiciones** del menú principal de la consola de Panda GateDefender Integra.
2. Seleccione **Gestión de usuarios**.
3. En el apartado **Grupos de usuarios**, haga clic en el botón **Añadir**.
4. Defina el nombre del grupo y añada usuarios del cuadro inferior.

Cuando haya terminado, la configuración debería ser similar a la que se muestra en la figura 2.2.

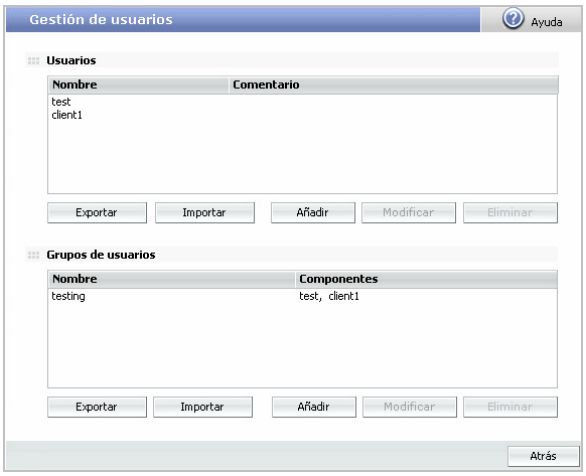


Figura 2.2

1.2.2 Configuración del grupo IP

A continuación se describen los pasos para configurar la definición del grupo IP:

1. Acceda al apartado **Definiciones** del menú principal de la consola de Panda GateDefender Integra.
2. Seleccione **Direcciones IP**.
3. En el apartado **Grupos**, haga clic en el botón **Añadir**.
   Introduzca un nombre descriptivo para el grupo (*en este ejemplo, utilizaremos **pptp vpn group***) en el campo **Nombre** y un rango de IP ***192.168.10.61-70*** en el cuadro de texto situado junto al botón de selección **Usar rango**.
4. Haga clic en **Añadir IP**.
5. Por último, haga clic en **Añadir** para guardar los cambios.

Las opciones quedarán configuradas como se muestra en la figura 2.3.

Aviso: Tenga en cuenta que no puede utilizar un Grupo IP previamente definido que ya se haya asignado a otra VPN.

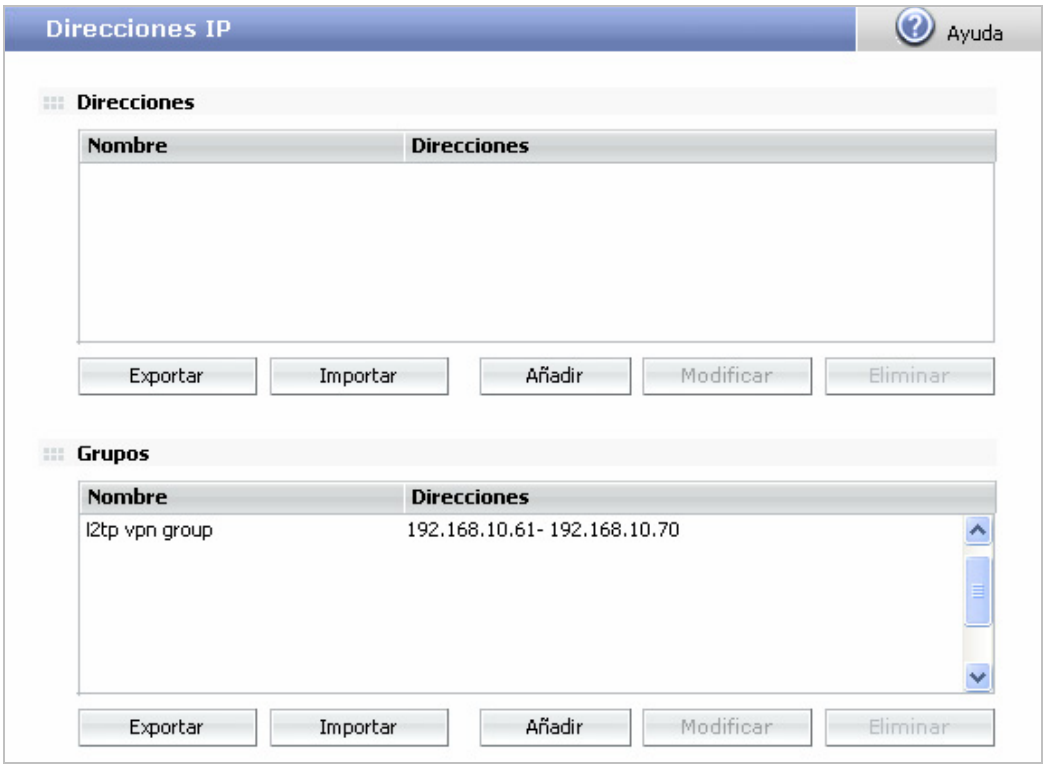


Figura 2.3

1.2.3 Certificados CA y certificados locales de servidor

Los certificados son necesarios por razones de autenticación. Se debe importar los certificados de CA públicos que firmaron los certificados del usuario remoto. También se debe importar el certificado local del gateway VPN de Integra que se utilizará para autenticar el propio servidor VPN de Integra.

Para importar los certificados CA, siga el procedimiento que se indica a continuación:

1. Vaya al apartado **VPN** del menú principal de la consola de Panda GateDefender Integra.
2. Seleccione **Gestión de certificados digitales**.
3. En el apartado **Certificados CA**, haga clic en **Importar**.

   - Introduzca el **Nombre de certificado** (en este ejemplo utilizaremos ***ca***)
   - Haga clic en **Examinar...** para seleccionar el certificado que quiere importar.
   - Haga clic en **Importar** cuando haya elegido un certificado para importar.

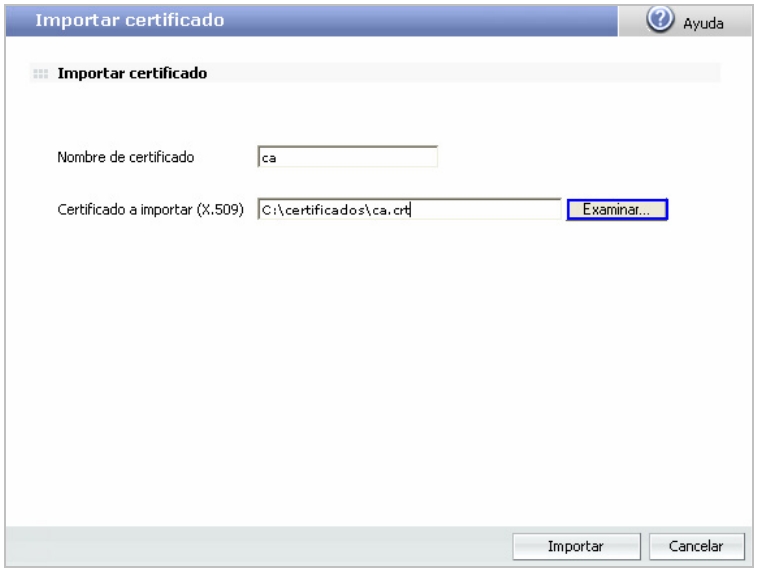


Figura 2.4

Para importar certificados de servidor locales, siga el procedimiento que se indica a continuación:

1. Vaya al apartado **VPN** del menú principal de la consola de Panda GateDefender Integra.
2. Seleccione Gestión de certificados digitales y, en el apartado Certificados locales, haga clic en Importar.

   - Seleccione si quiere Importar un certificado pendiente de firma o Importar un certificado con clave privada emitido por una CA.

   - Si selecciona **Importar certificado con clave privada**, introduzca el Nombre de certificado PKCS12 (en este ejemplo utilizaremos ***server***) y, si es necesario, una **Contraseña**.

3. Haga clic en **Examinar...** para seleccionar el certificado que quiere importar.
4. Haga clic en **Importar** cuando haya elegido un certificado.

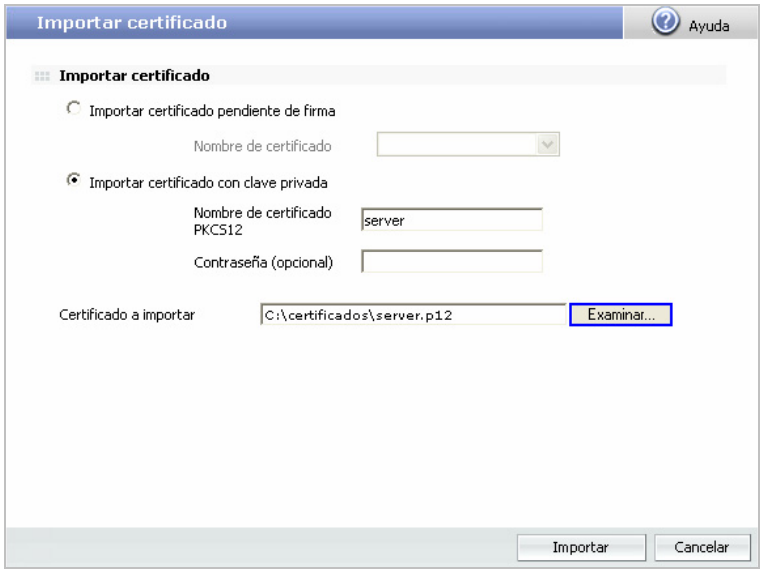


Figura 2.5

Una vez se hayan importado correctamente los certificados CA y de servidor, la pantalla con la configuración será similar a la que se muestra en la figura 2.6.

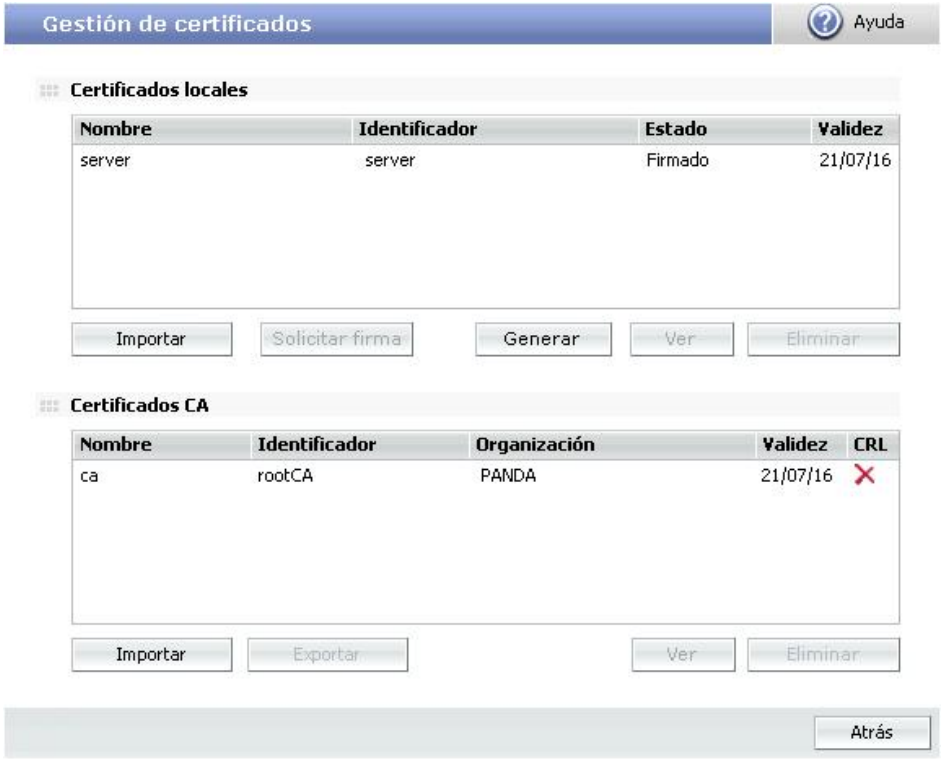


Figura 2.6

Tenga en cuenta que si selecciona **Importar certificado con clave privada**, sólo podrá importar certificados locales que se ajusten al formato PKCS12 (el archivo tiene la extensión .p12 o .pfx).

1.2.4 Configuración de VPN L2TP/IPSec

Este apartado se divide en dos secciones: IPSEC y L2TP.

1.2.4.1 Configuración de IPSEC

Este apartado está relacionado con la configuración IPSec (el cifrado de VPN L2TP depende del protocolo IPSec. IPSec Encapsulating Security Payload (ESP) se utiliza para cifrar el paquete L2TP. Este tipo de implementación también se conoce como L2TP/IPSec).

Para configurar IPSec, siga las instrucciones que se indican a continuación:

1. Vaya a la consola de administración de Panda GateDefender Integra.
2. Haga clic en **VPN** en el panel de la izquierda.
3. Seleccione **Gestión de VPN** y, a continuación, **Gestión de VPN IPSEC**.

Las opciones disponibles son:

1. **Nombre**: introduzca el nombre descriptivo de la VPN (en este ejemplo utilizaremos **L2TP**)
2. **Políticas IKE:** utilice el menú desplegable para seleccionar la política IKE que desee aplicar. (En este ejemplo utilizaremos ***IKE I***)
3. **Parametros de Fase I**

   IP local: introduzca la dirección IP pública local o elija **IP asignada por DHCP** (en este ejemplo utilizaremos **62.12.249.65**).

4. **Parámetros de Fase II**

   Seleccione el protocolo que vaya a utilizar: **L2TP/IPSec**

   Cuando elija L2TP/IPSEC, tendrá disponibles las siguientes opciones:

   - **ID local: Certificado X-509:** utilice el menú desplegable para seleccionar el certificado local del servidor (en este ejemplo utilizaremos ***server***).

   - **Certificado CA**: los usuarios remotos que se autentiquen con un certificado X-509, también deben presentar la firma de una CA. Utilice el menú desplegable para seleccionar el certificado del CA que firmó el certificado del usuario remoto (roadwarrior). En este ejemplo utilizaremos ***ca.crt***.

Cuando haya configurado la parte IPSEC, la pantalla de configuración correspondiente será similar a la de la figura 2.7

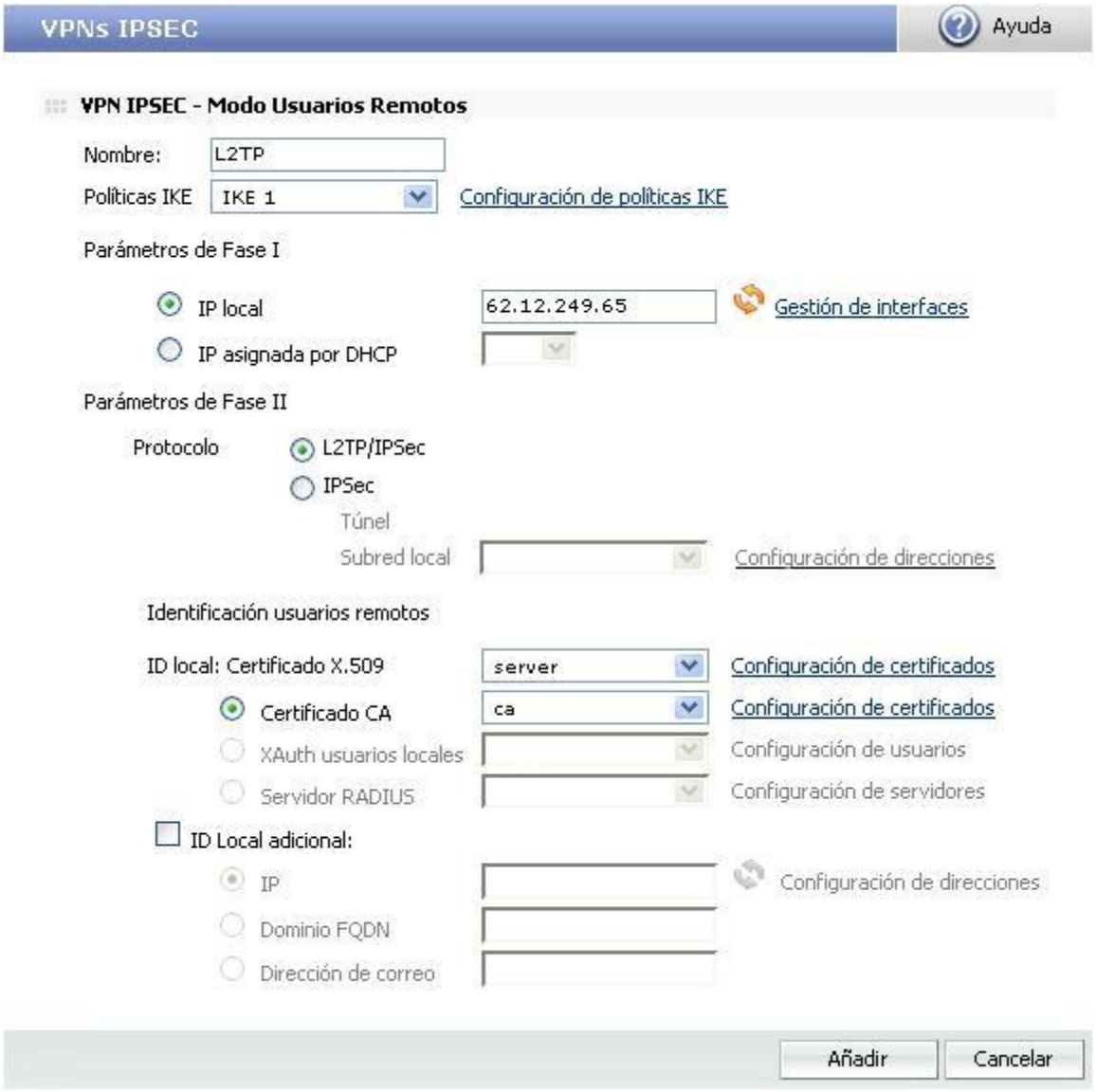


Figura 2.7

Nota: si hay algún dispositivo NAT entre un usuario remoto y un gateway VPN de Integra, debería activar la casilla NAT transversal tal y como se muestra a continuación.

1.2.4.2 Configuración L2TP

Este apartado está relacionado con la configuración del propio protocolo L2TP.

Para configurar L2TP, siga el procedimiento que se indica a continuación:

1. Vaya a la consola de administración de Panda GateDefender Integra.
2. Haga clic en **VPN** en el panel de la izquierda.
3. Seleccione **Gestión de VPN** y, a continuación, **Gestión de VPN L2TP**.

   Encontrará los parámetros necesarios para configurar una VPN en Panda GateDefender Integra utilizando el protocolo L2TP (como se muestra en la figura 2.4).

   - **Nombre:** introduzca un nombre descriptivo para la VPN (en este ejemplo utilizaremos ***l2tp vpn***).
   - **Activa:** seleccione esta casilla de verificación para activar la VPN.
   - **Grupo de IPs:** seleccione el rango de direcciones IP (en este ejemplo utilizaremos ***l2tp vpn group***) asociado a esta VPN. Si no lo ha definido anteriormente, haga clic en el enlace **Configuración de direcciones** para acceder a la pantalla que le permitirá definir las direcciones IP.
   - **Usuarios:** Seleccione el tipo de usuario que desee:

     - **Usuarios locales:** seleccione el grupo de usuarios autorizados a acceder a su VPN (en este ejemplo utilizaremos ***testing***). Si no lo ha definido anteriormente, pulse el enlace **Configuración de usuarios** para acceder a la pantalla de gestión de usuarios.

     - **Servidor Radius:** seleccione el servidor RADIUS que utilizará Panda GateDefender Integra para autenticar a los usuarios.

   Cuando haya configurado la parte L2TP, la pantalla de configuración correspondiente será similar a la de la figura 2.8.

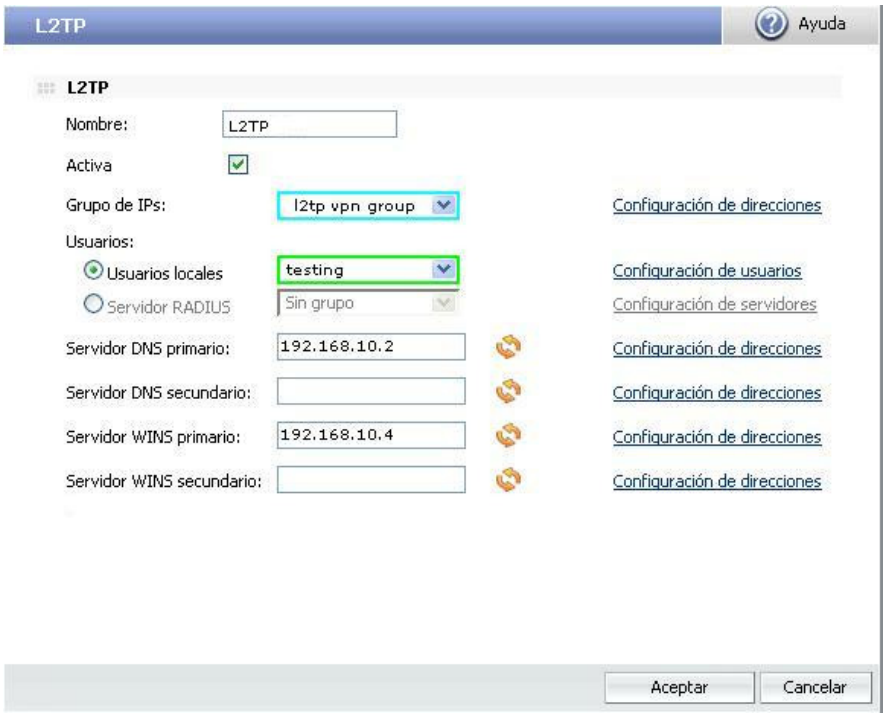


Figura 2.8

Índice

1.3 Configuración del lado del cliente (MS Windows 2000/XP)

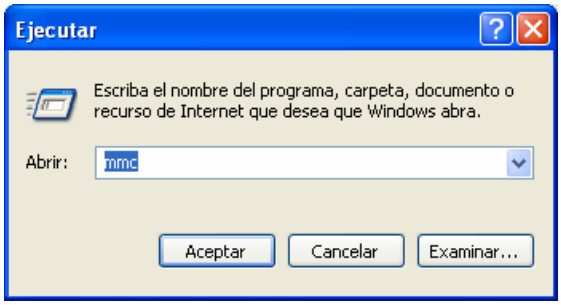
Una vez se ha confirmado que la conexión a Internet se ha configurado correctamente en los ordenadores cliente con Microsoft Windows 2000/XP, siga los pasos que se indican a continuación:

1.3.1 Importar un certificado local de gateway y un certificado CA

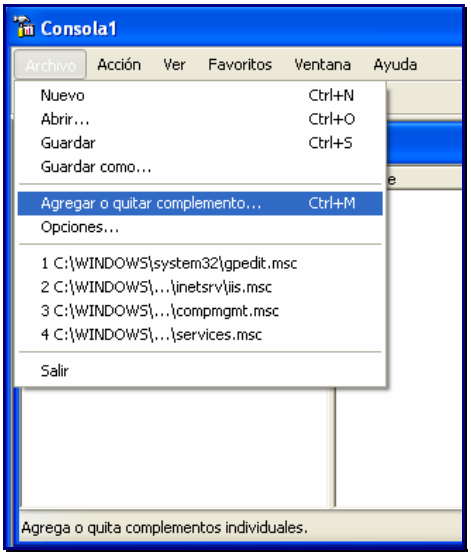
Los certificados son necesarios por razones de autenticación. Debe importar los certificados de los CA públicos que firmaron el certificado del gateway VPN de Integra. También será necesario importar el certificado del usuario remoto (roadwarrior) que se utilizaría para autenticar al propio usuario remoto.

Para importar certificados locales para un usuario remoto (roadwarrior), siga el procedimiento que se indica a continuación:

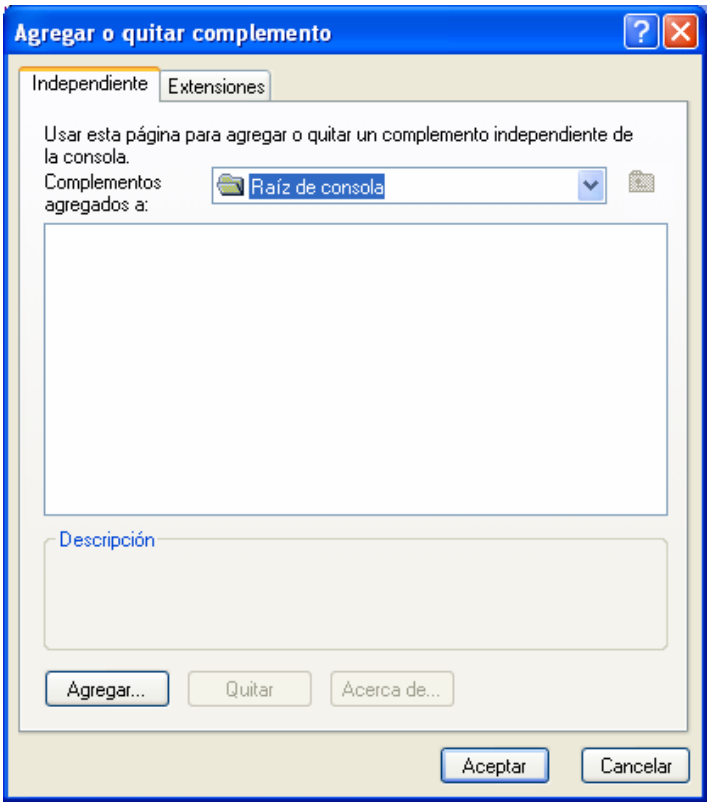
1. Haga clic en el botón **Inicio**.
2. Seleccione **Ejecutar**.
3. En el campo de texto, escriba **mmc** y haga clic en **Aceptar**.



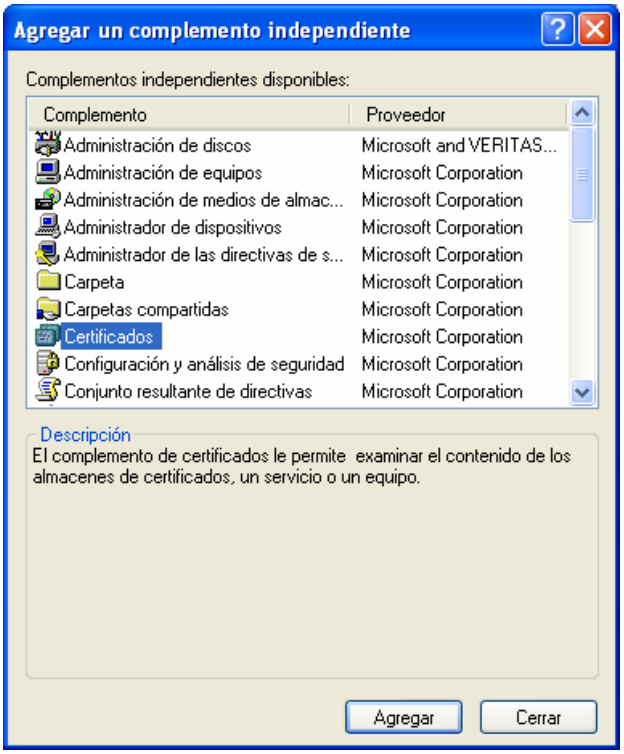
4. Haga clic en **Archivo** y seleccione **Agregar o quitar complemento**.



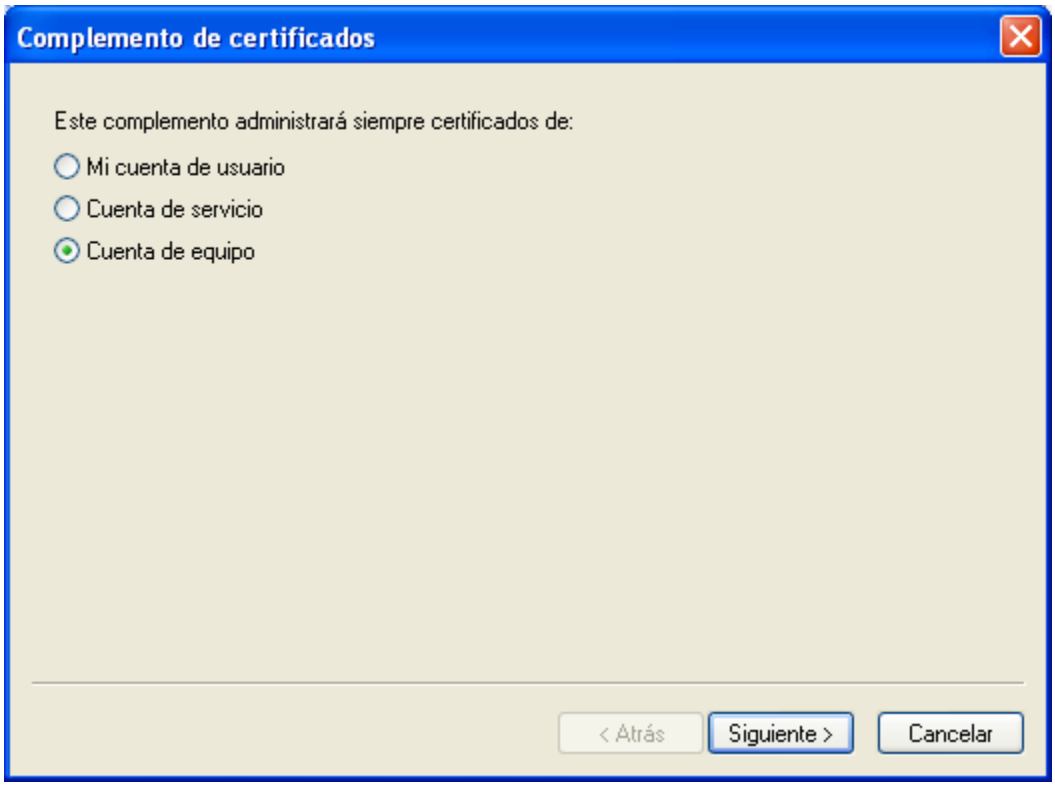
5. Haga clic en **Agregar...**



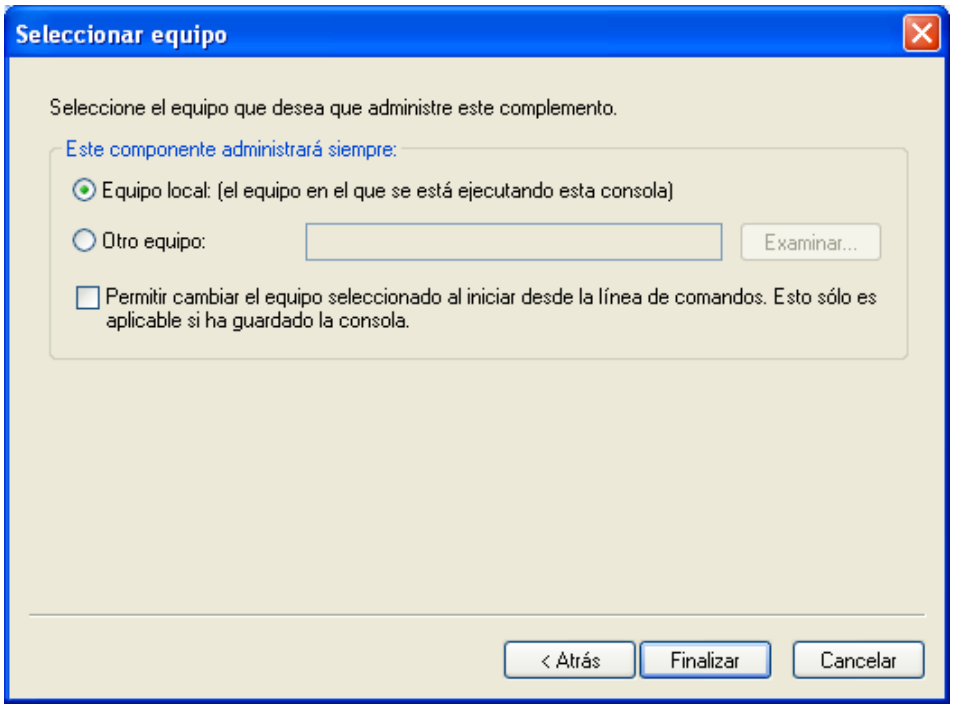
6. Seleccione **Certificados** y, a continuación, seleccione **Agregar**.



7. Seleccione **Cuenta de equipo** y haga clic en **Continuar.**

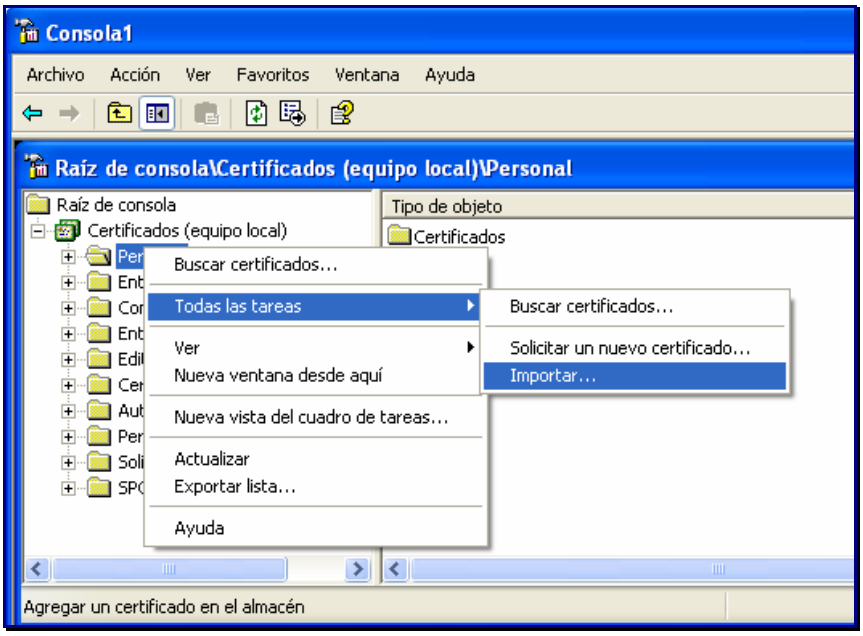


8. Seleccione **Equipo local** y haga clic en **Finalizar**.

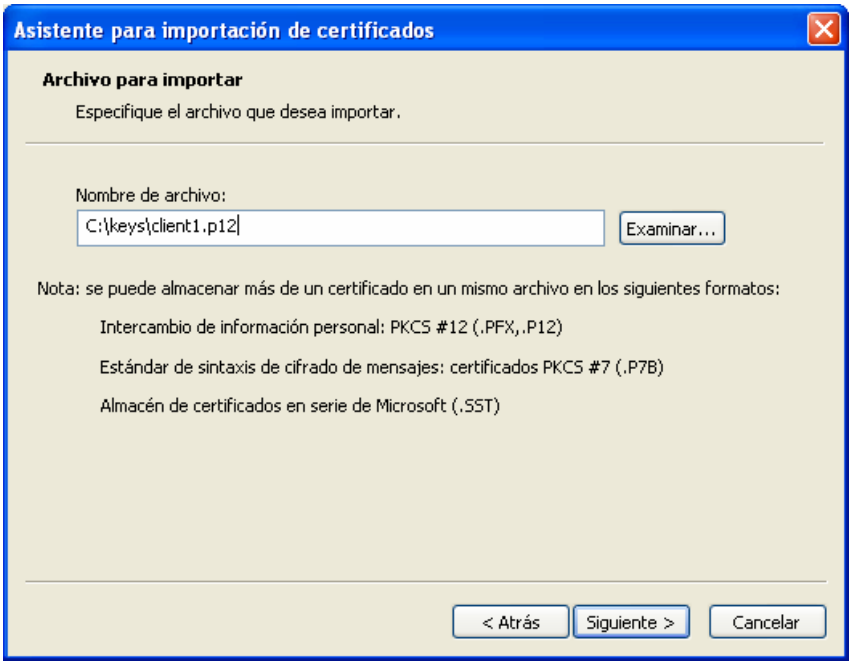


9. Haga clic en **Cerrar** y en **Aceptar**.

10. Haga clic en la casilla **más** situada junto a **Certificados (equipo local)**.
11. Haga clic con el botón derecho del ratón en **Personal** y seleccione **Todas las tareas**.
12. Pulse **Importar...**

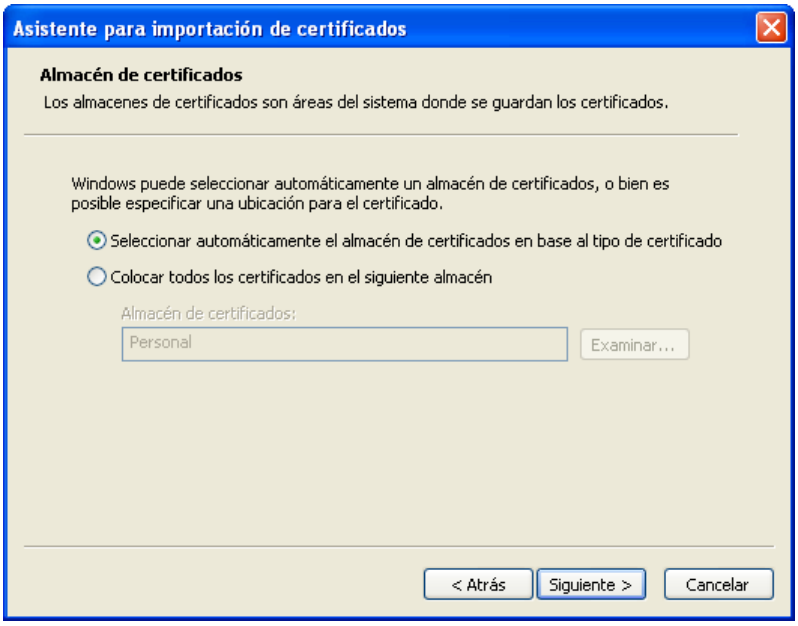


13. Haga clic en **Siguiente.**
14. Escriba la ruta del archivo .p12 del usuario remoto (o examine el ordenador y seleccione el archivo) y haga clic en **Siguiente.**



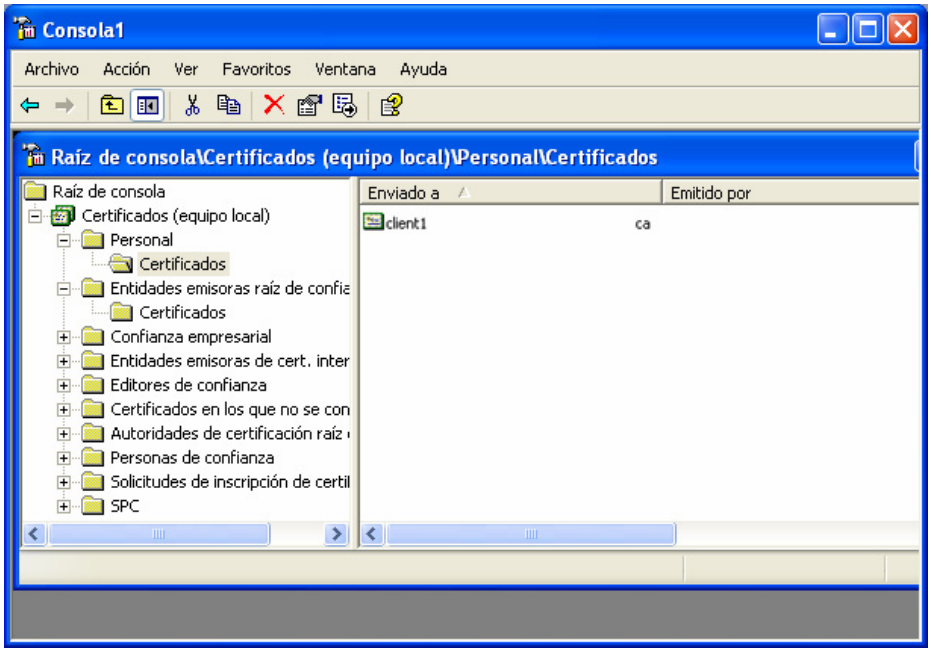
15. Opcionalmente, escriba la **contraseña** de exportación, si es necesario, y haga clic en **Siguiente.**

16. Elija **Seleccionar el almacenamiento del certificado automáticamente según el tipo de certificado** y haga clic en **Siguiente.**



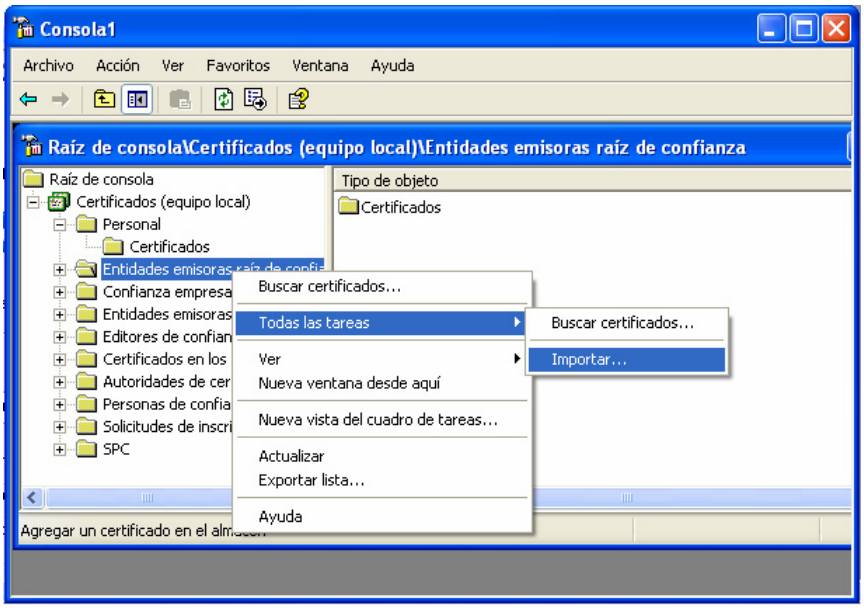
17. Haga clic en **Finalizar** y confirme las ventanas emergentes que aparecen pulsando **Sí**.
18. Haga clic en **Aceptar**.

Si ha importado el certificado correctamente, la pantalla que visualizará será similar a la que se muestra a continuación.



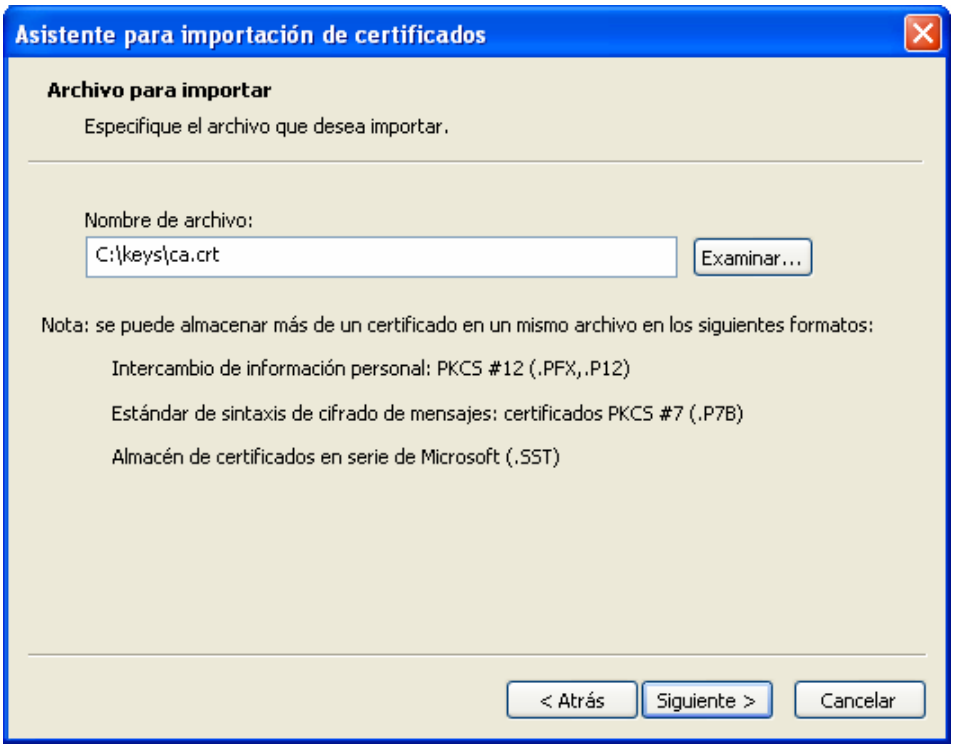
Si para firmar su certificado de roadwarrior se ha utilizado una CA diferente a la que se ha utilizado para firmar el certificado del gateway VPN de Integra, deberá seguir las instrucciones que aparecen a continuación. Si este no es el caso, vaya directamente al apartado ***1.3.2 Configuración de la conexión***.

1. Haga clic con el botón derecho del ratón en **Entidades emisoras de certificados raíz de confianza** y seleccione **Todas las tareas**.
2. Haga clic en **Importar...** y en **Siguiente**.

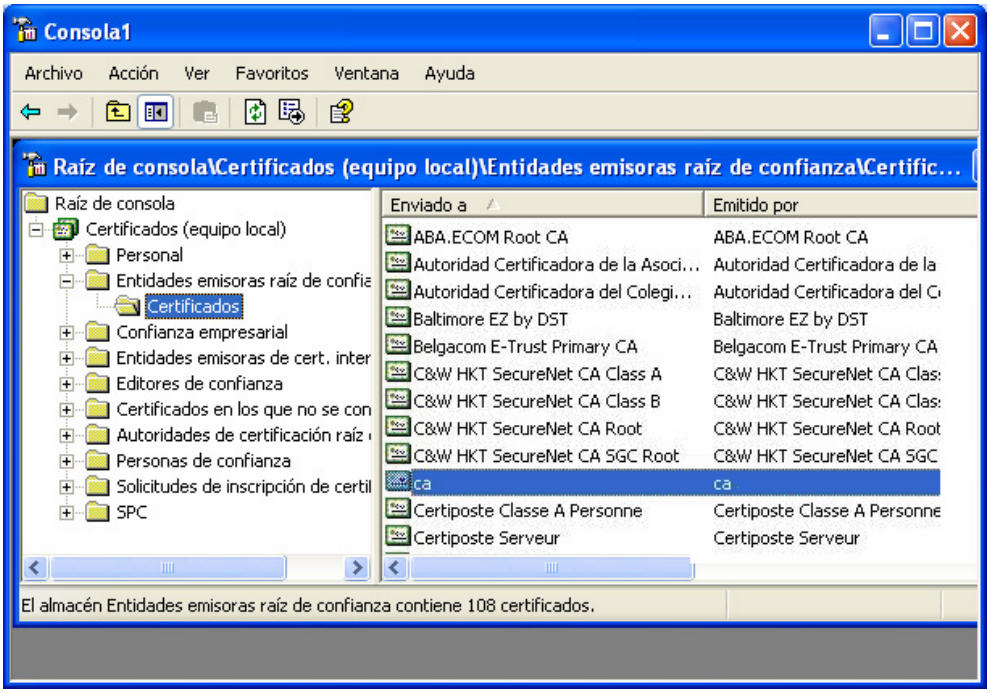


3. Escriba la ruta del archivo .crt que corresponda a la CA del gateway VPN de Integra (o examine el equipo y seleccione el archivo) y haga clic en **Siguiente**.

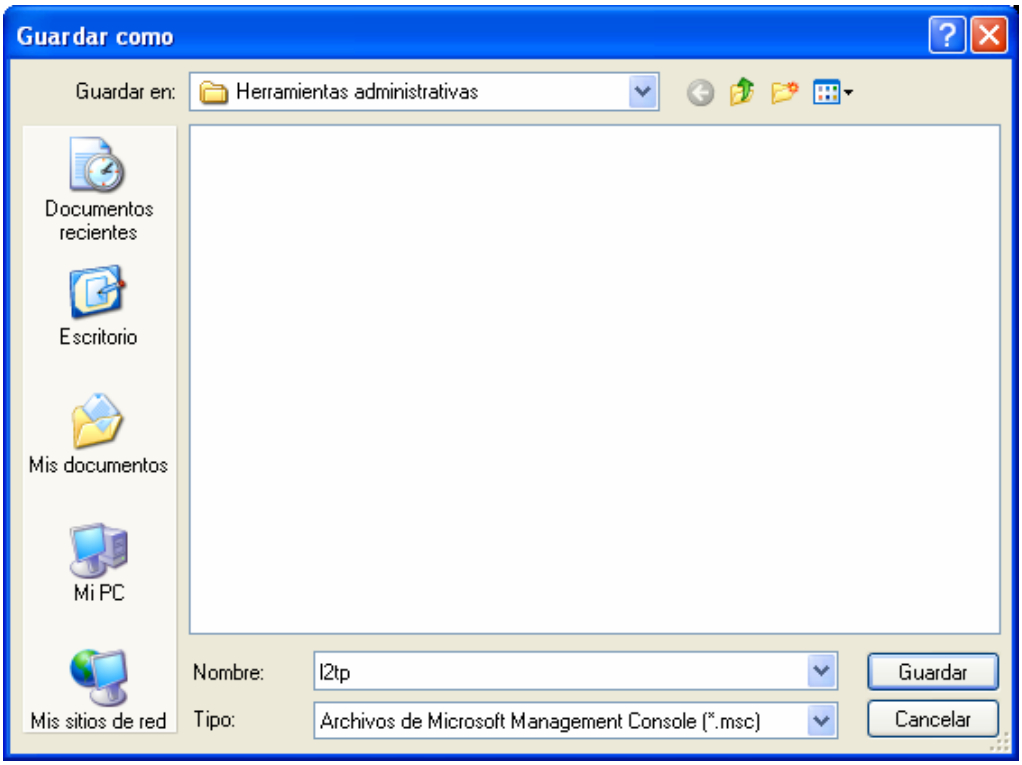
4. Seleccione **Colocar todos los certificados en el siguiente almacén** y haga clic en **Siguiente**.



5. Haga clic en **Finalizar** y confirme las ventanas emergentes que aparecen pulsando **Sí**. Haga clic en **Aceptar**.



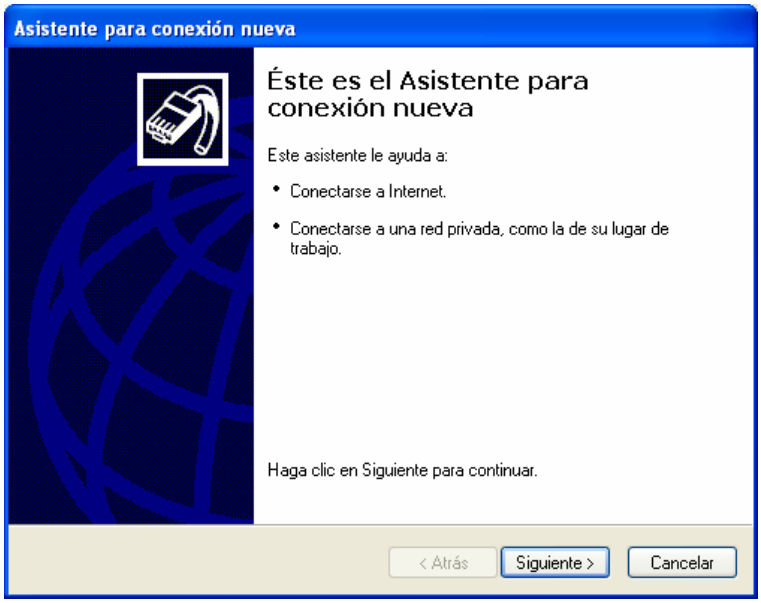
6. Guarde la configuración actual como un archivo para que no tenga que volver a agregar los complementos cada una de las veces.
7. Escriba el nombre y haga clic en **Guardar**.



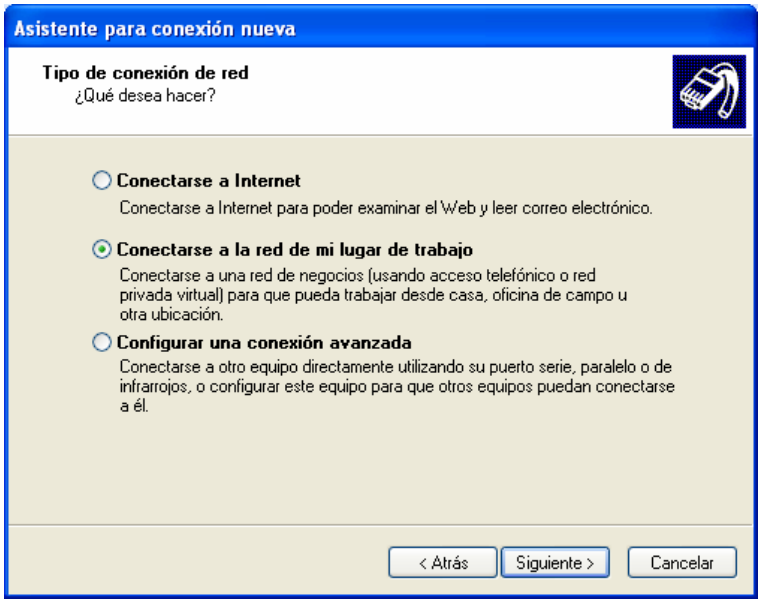
1.3.2 Configuración de la conexión

1. Haga clic en el botón **Inicio**.
2. Seleccione el **Panel de control**.
3. En el Panel de control, haga doble clic en **Conexiones de red**.
4. Haga clic en **Crear una conexión nueva**.

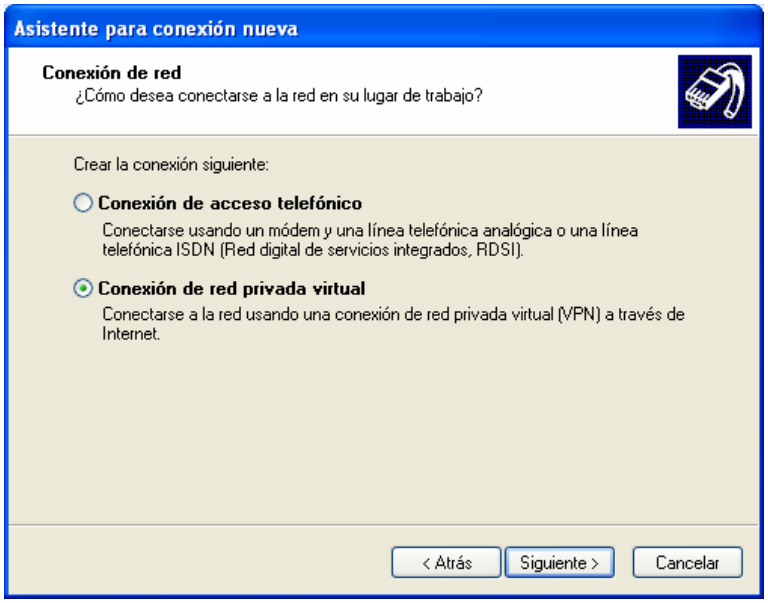
5. En el Asistente para conexión nueva, haga clic en **Siguiente**.



6. Haga clic en **Conectarse a la red de mi lugar de trabajo** y después haga clic en **Siguiente.**



7. Haga clic en **Conexión de red privada virtual** y después haga clic en **Siguiente.**

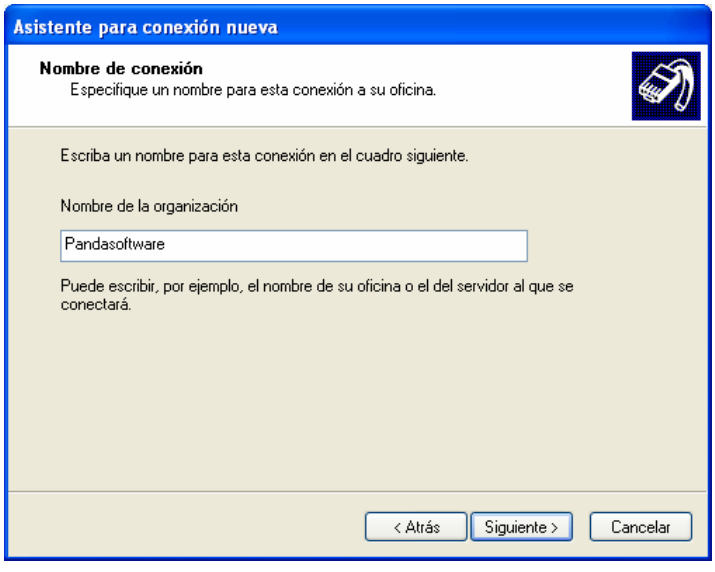


Si utiliza una conexión de acceso telefónico para conectarse a Internet, haga clic en **Usar automáticamente esta conexión inicial** y después seleccione de la lista su conexión de acceso telefónico a Internet.

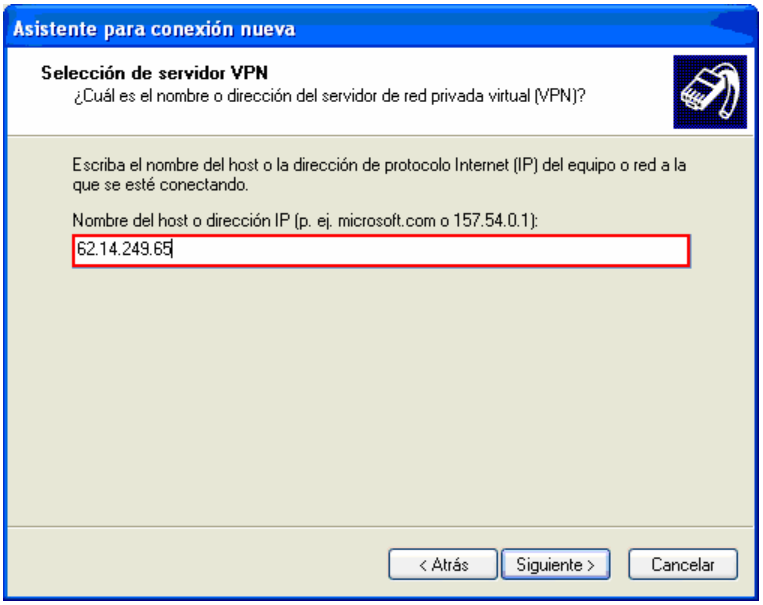
Si utiliza una conexión permanente (como un módem ADSL o por cable), seleccione la casilla de verificación **No usar la conexión inicial**.

8. Haga clic en **Siguiente.**

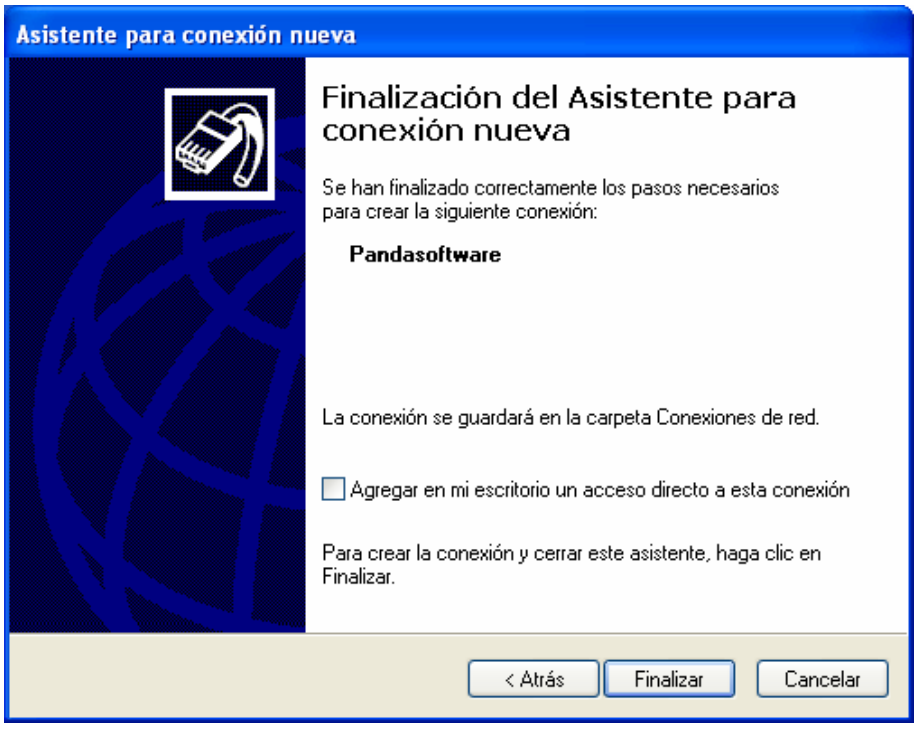
9. Escriba el nombre de su organización o un nombre descriptivo para la conexión (en este ejemplo utilizaremos ***Pandasoftware***) y después haga clic en **Siguiente**.



10. Escriba la dirección IP del servidor VPN (en este ejemplo utilizaremos ***62.14.249.65***) y después haga clic en **Siguiente**.

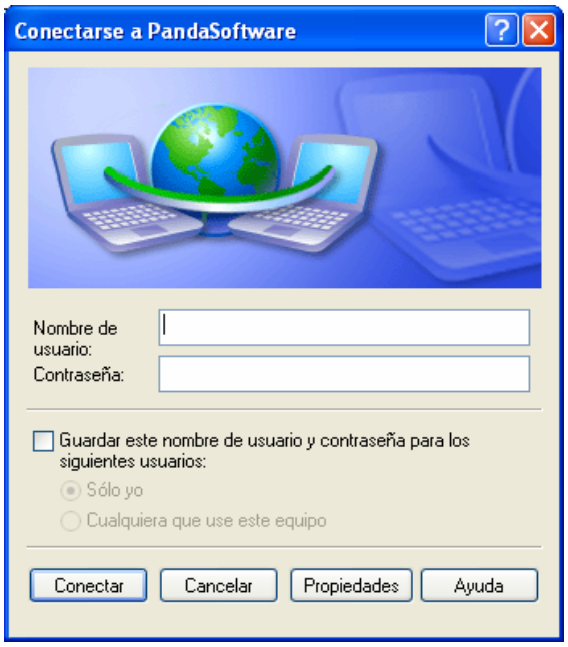


11. Marque la casilla de verificación **Agregar a mi escritorio un acceso directo a esta conexión** si quiere crear un acceso directo desde su escritorio y después haga clic en **Finalizar**.



12. Si se le pide conectarse, seleccione **No**.
13. En la ventana de Conexiones de red, haga clic con el botón derecho del ratón en la nueva conexión.

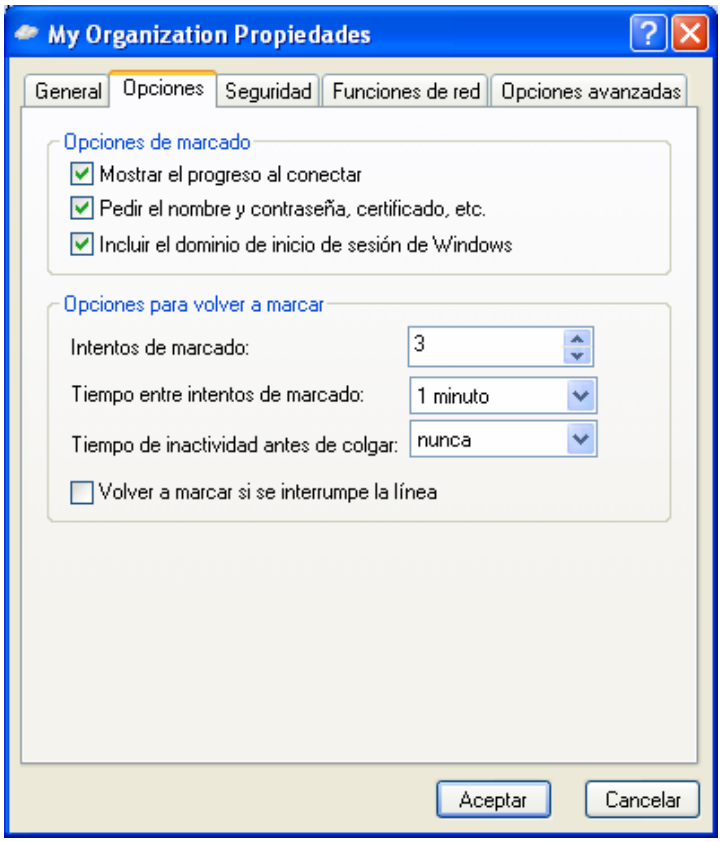
14. Haga clic en **Propiedades** y, a continuación, configure la credenciales de acceso para la conexión:



15. Seleccione la pestaña **Funciones de red** y, de la lista Tipo de red privada virtual (VPN), elija **L2TP IPSec VPN**.

16. Si se va a conectar a un dominio, haga clic en la pestaña **Opciones** y después active la casilla de verificación **Incluir el dominio de inicio de sesión de Windows** para

especificar si quiere que se le pida el dominio de inicio de sesión de Windows 2000/XP antes de conectarse.



Índice

1.4 Establecer una conexión VPN L2TP

Utilice el siguiente procedimiento para establecer la conexión VPN L2TP que ha definido anteriormente.

1. Haga clic en el botón **Inicio** y después en **Configuración, Conexiones de red**, a continuación haga clic en la conexión que ha configurado anteriormente.
2. Si agregó un acceso directo al escritorio, haga doble clic sobre él.
   Si no está conectado a Internet, Windows le ofrecerá conectarse.

Después de que su equipo se conecte a Internet, el gateway VPN de Integra le solicitará el nombre de usuario y la contraseña (hay que definir previamente el usuario desde Integra. Escriba su nombre de usuario y contraseña y, después, haga clic en **Conectar**. Los recursos de la red remota deberían estar disponibles para usted del mismo modo que cuando se conecta directamente a la red.

Para descontarse de la VPN, haga clic con el botón derecho del ratón en el icono de la conexión que aparece en la esquina inferior derecha y seleccione **Desconectar**.

Índice

1.5 Otras consideraciones

Si se utiliza el firewalll de Integra, las reglas de configuración correspondientes a los protocolos de encriptación se introducirán automáticamente en el firewall. Pero si se han introducido los servidores DNS y WINS (ver imagen 2.8) habrá que introducir las reglas manualmente.

Pero si utiliza un firewall personal, o un router de banda ancha con firewall, o si hay routers o firewalls entre el cliente VPN y el servidor del gateway VPN de Integra, habrá que activar los siguientes puertos y protocolos para L2TP en todos los firewalls y routers que haya entre el cliente VPN y el servidor gateway VPN de Integra:

Para L2TP tiene que abrir los **mismos** puertos y protocolos que para IPSec:

1. Puerto UDP 500 (IKE)

2. Protocolo IP 50 (ESP), 51 (AH) ó

   Puerto UDP 4500 (NAT-T): necesario cuando entre dos gateways se encuentra por lo menos un dispositivo SNAT (el caso habitual)

Tenga en cuenta que IP 50 es un *protocolo*, no un *puerto*.

Índice

1.6 Comprobación de la configuración

Para comprobar la configuración de la VPN L2TP, siga los pasos que se indican a continuación:

1. Abra la consola de administración de Panda GateDefender Integra.
2. Haga clic en **VPN** en el panel de la izquierda.
3. Seleccione **Monitor VPN**, lo que le permitirá ver el estado de todas las conexiones VPN (como se muestra en la figura 1.4).

Figura 2.8

Cualquiera de los usuarios remotos puede verificar la configuración en su Windows 2000/XP de forma independiente.

Para realizar esta tarea, habría que utilizar los siguientes comandos:

- El comando **ipconfig /all** muestra que se ha asignado una dirección IP adicional a su interfaz externo (adaptador ppp l2tp). Si usted es el primer usuario remoto (roadwarrior) conectado, sería 192.168.10.62 (la primera IP del rango, es decir, 61, está reservada para el servidor VPN.)

- El **comando ping –n 10 192.168.10.100 comprueba el estado de la conexión** desde el usuario remoto a uno de los ordenadores que residen en la red interna detrás del gateway VPN de Integra y debería obtener una respuesta del equipo remoto.

Al mismo tiempo, se puede utilizar una herramienta de monitorización del tráfico de red como, por ejemplo, Ethereal, para comprobar si el tráfico entre el usuario remoto (roadwarrior) y la oficina remota (gateway) está cifrado.
Los paquetes cifrados ESP (Encapsulating Security Payl) sólo se verán al observar el tráfico en el interfaz de la red externa, mientras que los paquetes no cifrados (en este caso los paquetes ICMP de respuesta) normalmente se verán en el interfaz del adaptador virtual ppp l2p.

Índice