HOWTO: Cómo configurar VPN SSL roadwarrior (usuario remoto) a gateway (oficina remota)

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 VPN SSL roadwarrior (usuario remoto) a gateway (oficina remota)

El protocolo SSL (Secure Socket Layer) salvaguarda los accesos a la información que circula por los protocolos de Internet (HTTP, SMTP, FTP, etc.) cifrando los datos de forma simétrica. El acceso a esos datos sólo será posible si se posee la clave correcta.

Panda GateDefender Integra le permite crear y modificar VPNs SSL para usuarios remotos (Roadwarriors) o para oficinas remotas (Gateway), pudiendo éstas funcionar en modo cliente y en modo servidor.

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) SSL con Panda GateDefender Integra, utilizando para ello 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.

Aviso: Panda GateDefender Integra ha de encontrarse funcionando en modo Router. De lo contrario, no podrá utilizar el sistema VPN.

1.1 Escenario

La siguiente ilustración muestra un escenario típico VPN SSL roadwarrior (usuario remoto) a gateway:

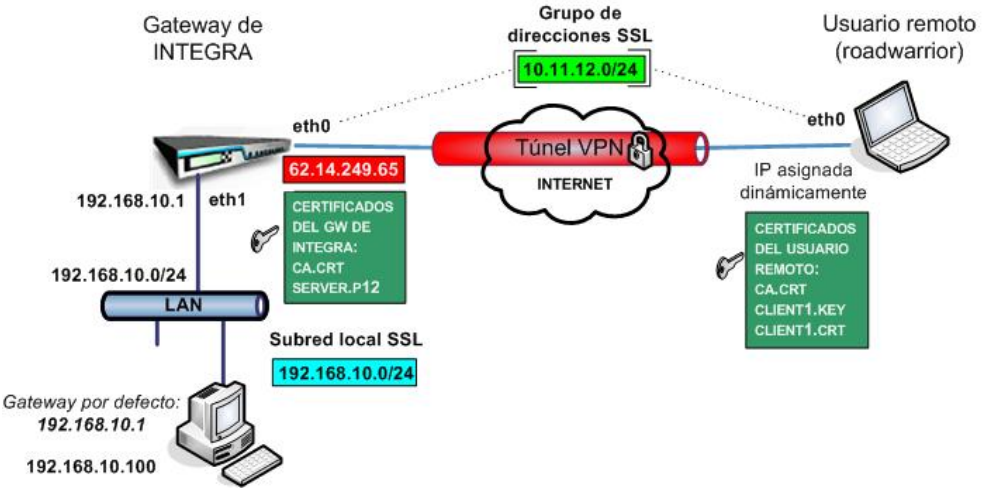


Figura 3.1: VPN usuario remoto a oficina remota SSL

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

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

El servidor escuchará el puerto UDP 1194 para recibir una solicitud de conexión del usuario remoto.

Los clientes desde la LAN de Integra tienen que haber configurado la IP **192.168.10.1** de la LAN de Integra como gateway para el grupo de direcciones SSL **10.11.12.0/24** (como ruta implícita o gateway por defecto) para que los roadwarriors puedan acceder a ellas. Lea más abajo cómo configurar rutas desde el usuario remoto.

Índice

1.2 Configuración del lado del servidor (Panda Gatedefender Integra)

1.2.1 Direcciones IP

El primer paso a la hora de configurar una VPN SSL consiste en:

- Definir el grupo de direcciones SSL que se utilizará justo después de la conexión inicial a la dirección IP local externa del servidor VPN SSL 62.14.249.65, para crear direcciones IP VPN en los dos extremos del túnel VPN.

- Definir el grupo de direcciones IP que corresponden a la subred local SSL a la que quiere que se conecte su usuario remoto (roadwarrior).

Para definir el grupo de direcciones SSL, siga los pasos que se describen a continuación:

1. Entre en el apartado **Definiciones** del menú principal de la consola de Panda GateDefender Integra.
2. Seleccione **Direcciones IP**.
3. En el apartado **Grupos**, haga clic en **Añadir**.
   Se debe dar un nombre descriptivo al grupo (en este ejemplo usaremos ***ssl address group***) en el campo **Nombre**, y un rango IP (en este ejemplo utilizaremos 10.11.12.0/24) en el campo que aparece junto al botón de selección **IP/Máscara**.
4. Haga clic en **Añadir IP**.

Por último, haga clic en **Añadir** para guardar los cambios.

 **IMPORTANTE:** Recuerde que el rango del grupo de direcciones SSL debería ser un rango privado que no se esté utilizando en las dos redes locales (la del servidor y la del usuario remoto).
Además tiene que ser mayor de /29 por cuestiones de diseño.

Para definir la subred local SSL, siga los pasos que se describen a continuación:

1. Entre en el apartado **Definiciones** del menú principal de la consola de Panda GateDefender Integra.
2. Seleccione **Direcciones IP**.
3. En el apartado **Grupos**, haga clic en **Añadir**.
   Se debe dar un nombre descriptivo al grupo (en este ejemplo utilizaremos ***ssl local address***) en el campo **Nombre**, y un rango IP (en este ejemplo utilizaremos 192.168.10.0/24) en el campo que aparece junto al botón de selección **IP/Máscara**.
4. Haga clic en **Añadir IP**.

Por último, haga clic en **Añadir** para guardar los cambios.

Las opciones quedarán configuradas como se muestra en la figura 3.2:

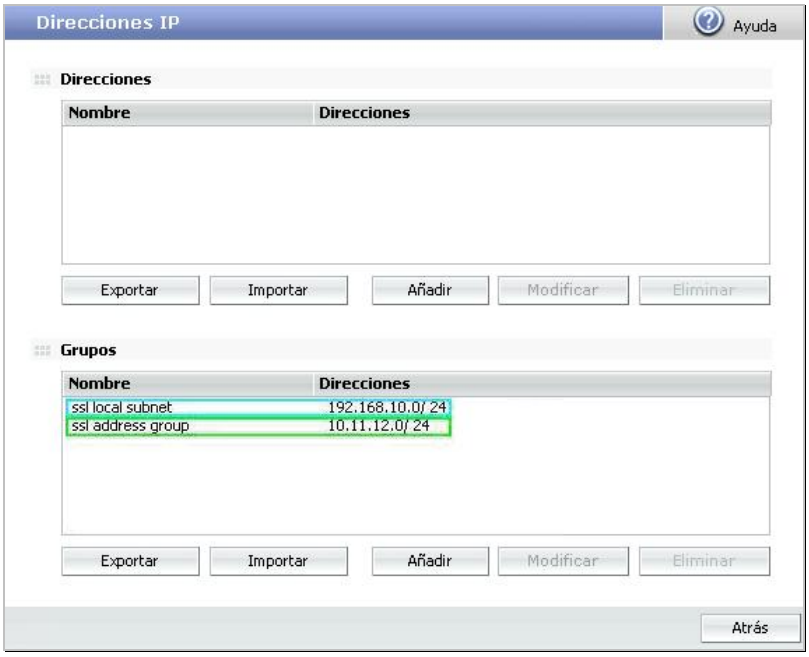


Figura 3.2

Índice

1.2.2 Certificados

Los certificados son necesarios por razones de autenticación. Debe importar el certificado públicos de CA que firmó el certificado 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.

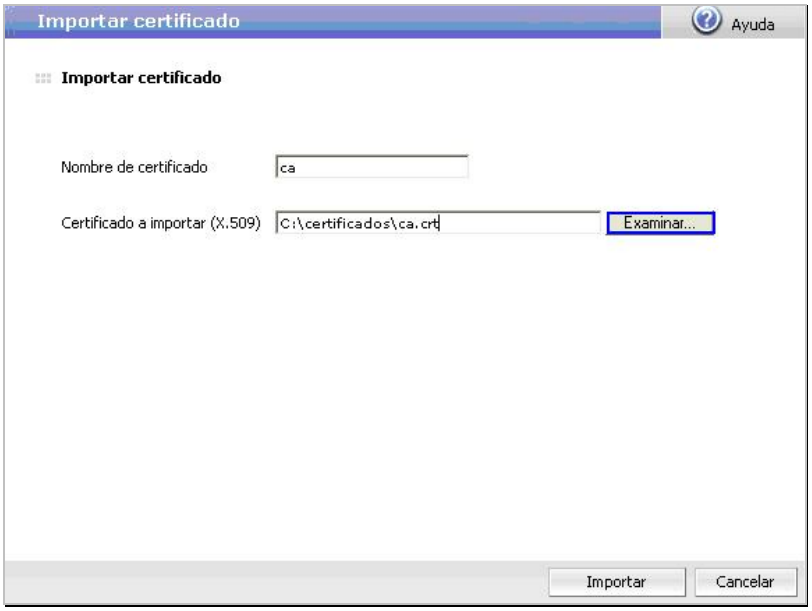


Figura 3.3

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 una **Contraseña, si esta requerida.**

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

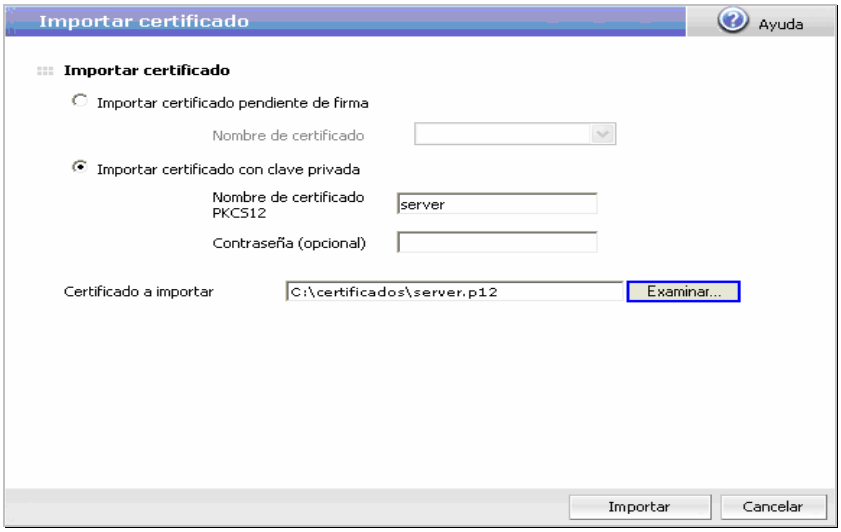


Figura 3.4

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 3.5.

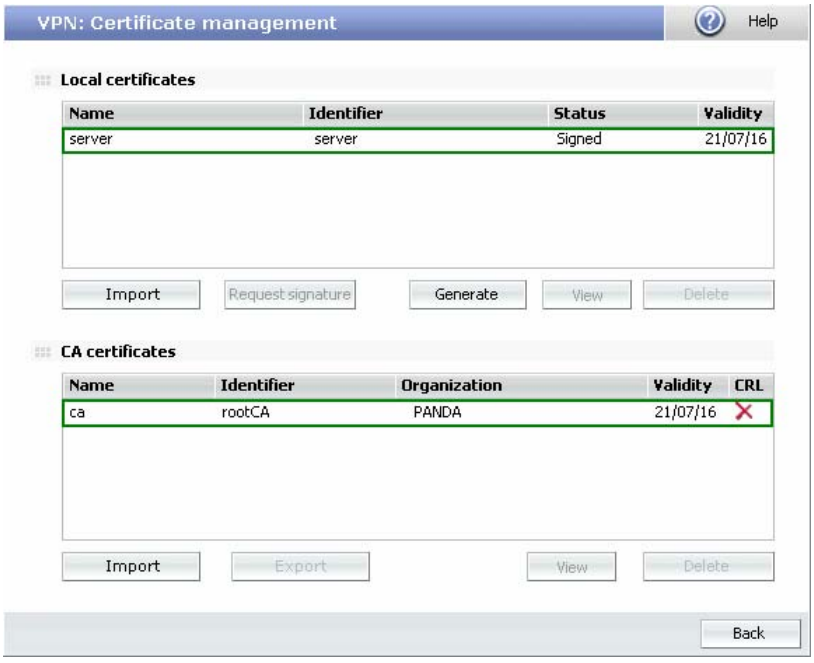


Figura 3.5

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).

1.2.3 Servidor VPN SSL

Por último, en los siguientes pasos se describe cómo configurar una VPN SSL utilizando elementos previamente definidos.

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**.
4. Haga clic en **Gestión de VPN SSL** y seleccione la pestaña **Usuarios remotos**.
5. Haga clic en **Añadir** para definir la nueva VPN

   Encontrará los parámetros necesarios para configurar una VPN en Panda GateDefender Integra utilizando el protocolo SSL (como se muestra en la figura 3.6):

   - **Nombre**: introduzca un nombre descriptivo para la VPN (en este ejemplo utilizaremos ***VPN ssl RW***).
   - **Puerto del servidor:** introduzca el puerto del servidor de la conexión (en este ejemplo utilizaremos ***1194***).
   - **Protocolo:** elija entre los protocolos TCP y UDP (en este ejemplo utilizaremos ***UDP***).
   - **Certificado local del servidor:** utilice el menú desplegable para seleccionar el nombre del certificado que quiera (en este ejemplo utilizaremos ***server***).
   - **Certificado CA de los usuarios:** el usuario remoto identificado con un certificado debe presentar la firma CA. Utilice el menú desplegable para seleccionar el certificado CA que quiera (en este ejemplo utilizaremos ***ca***).
   - **Grupo de usuarios:** lista de los Nombres comunes de los certificados X.509 con los que se identificarán los usuarios. Estos Common names se pueden obtener del campo *CN* del certificado **client.crt**. Este campo es opcional.(En este ejemplo no utilizaremos ninguno).
   - **Grupos de direcciones:** introduzca el rango de direcciones IP (máscara de red y de subred) desde el que se asignará la IP a los usuarios remotos. (en este ejemplo utilizaremos ***ssl address group***, que corresponde con ***10.11.12.0/24***. De hecho, se utilizará la subred /30 debido a las limitaciones de los dispositivos virtuales TUN/TAP.)
   - **IP local externa:** introduzca la dirección IP externa del servidor VPN SSL (en este ejemplo utilizaremos ***62.14.249.65***)
   - **Subredes locales***:* direcciones de subred que se enviarán a los usuarios remotos para que puedan introducirlas en sus propias tablas de enrutamiento. (En este ejemplo utilizaremos ***ssl local subnet***, que corresponde con ***192.168.10.0/24***).

   También existe la opción de incluir las direcciones IP de los servidores DNS y WINS. Al hacer clic en el icono asociado con las opciones DNS y WINS, puede cambiar el campo de texto del menú desplegable y elegir el valor que quiera asignar a cada opción. Haga clic en **Aceptar** para guardar los cambios.

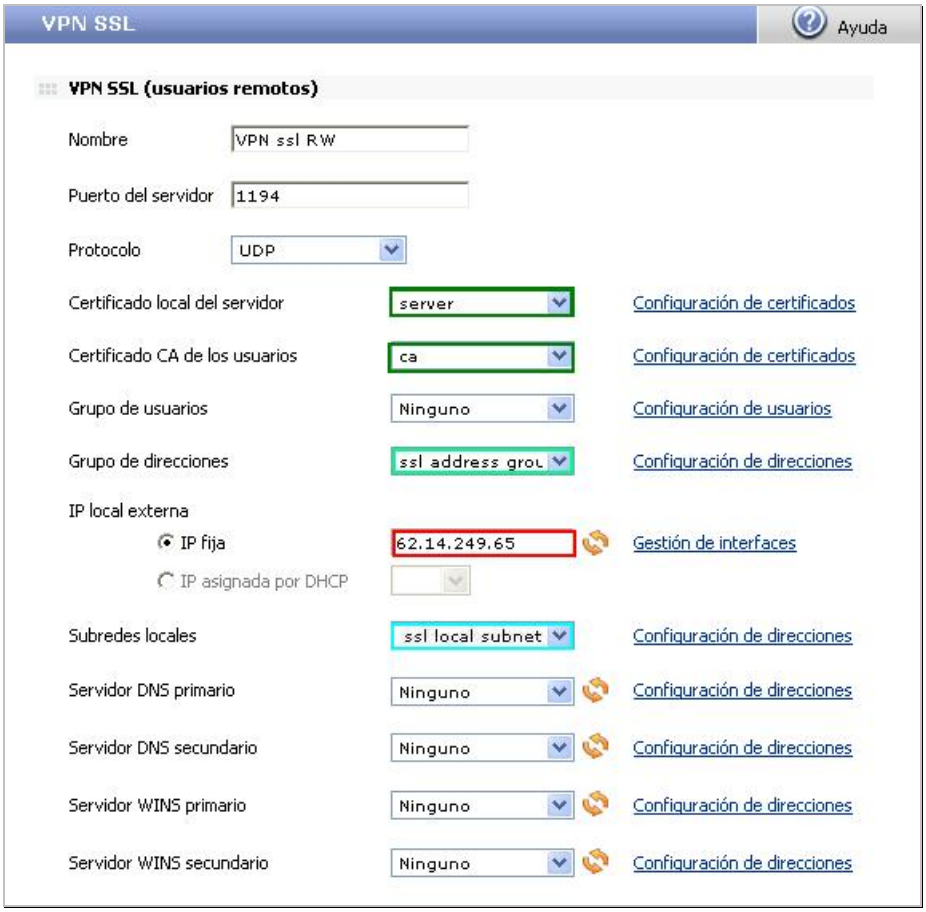


Figura 3.6

Índice

1.3 Configuración del lado del cliente

1.3.1 MS Windows 2000/XP

En el lado del usuario remoto se utilizará OpenVPN para la implementación del protocolo SSL/TLS.

Los archivos de instalación pueden encontrarse en: http://www.openvpn.se/

Tanto OpenVPN como OpenVPN GUI son un proyecto de código abierto y tienen licencia GPL.

Una vez instalado OpenVPN, aparte de los archivos binarios y de configuración, también se instala el adaptador TUN/TAP. Debería comprobarlo en la configuración de red.

En los siguientes pasos se describe cómo configurar un usuario remoto SSL utilizando OpenVPN.

Guarde los siguientes certificados en la carpeta *C:\Archivos de programa\OpenVPN\config* (o en la ruta que elija durante la instalación):

1- ***client1.crt*** --> certificado del cliente (clave pública firmada)
2-***client1.key*** --> clave del cliente (clave secreta privada que en ningún momento deberá salir del ordenador del usuario remoto.
3-***ca.crt*** --> certificado CA (certificado de la CA que firmó el certificado de servidor; en este ejemplo utilizaremos el mismo para el servidor y el usuario remoto)

Copie el archivo ***client.ovpn*** del directorio *C:\Archivos de programa\OpenVPN\sample-config* y realice los cambios necesarios para que el contenido quede como se indica a continuación:

```
##############################################
# Sample client-side OpenVPN 2.0 config file #
# for connecting to multi-client server. #
# #
# This configuration can be used by multiple #
# clients, however each client should have #
# its own cert and key files. #
# #
# On Windows, you might want to rename this #
# file so it has a .ovpn extension #
##############################################
# Specify that we are a client and that we
# will be pulling certain config file directives
# from the server.
client
# Use the same setting as you are using on
# the server.
# On most systems, the VPN will not function
# unless you partially or fully disable
# the firewall for the TUN/TAP interface.
;dev tap
dev tun
# Windows needs the TAP-Win32 adapter name
```

```
# from the Network Connections panel
# if you have more than one. On XP SP2,
# you may need to disable the firewall
# for the TAP adapter.
;dev-node MyTap
# Are we connecting to a TCP or
# UDP server? Use the same setting as
# on the server.
;proto tcp
proto udp
# The hostname/IP and port of the server.
# You can have multiple remote entries
# to load balance between the servers.
remote 62.14.249.65 1194
;remote my-server-2 1194
# Choose a random host from the remote
# list for load-balancing. Otherwise
# try hosts in the order specified.
;remote-random
# Keep trying indefinitely to resolve the
# host name of the OpenVPN server. Very useful
# on machines which are not permanently connected
# to the internet such as laptops.
resolv-retry infinite
# Most clients don't need to bind to
# a specific local port number.
nobind
# Downgrade privileges after initialization (non-Windows only)
;user nobody
;group nobody
# Try to preserve some state across restarts.
persist-key
persist-tun
# If you are connecting through an
# HTTP proxy to reach the actual OpenVPN
# server, put the proxy server/IP and
# port number here. See the man page
# if your proxy server requires
# authentication.
;http-proxy-retry # retry on connection failures
;http-proxy [proxy server] [proxy port #]
# Wireless networks often produce a lot
# of duplicate packets. Set this flag
# to silence duplicate packet warnings.
;mute-replay-warnings
# SSL/TLS parms.
# See the server config file for more
# description. It's best to use
# a separate .crt/.key file pair
# for each client. A single ca
# file can be used for all clients.
ca ca.crt
cert client1.crt
```

key client1.key

```
# Verify server certificate by checking
# that the certicate has the nsCertType
# field set to "server". This is an
# important precaution to protect against
# a potential attack discussed here:
# http://openvpn.net/howto.html#mitm
#
# To use this feature, you will need to generate
# your server certificates with the nsCertType
# field set to "server". The build-key-server
# script in the easy-rsa folder will do this.
;ns-cert-type server
# If a tls-auth key is used on the server
# then every client must also have the key.
;tls-auth ta.key 1
# Select a cryptographic cipher.
# If the cipher option is used on the server
# then you must also specify it here.
;cipher x
# Enable compression on the VPN link.
# Don't enable this unless it is also
# enabled in the server config file.
comp-lzo
# Set log file verbosity.
verb 3
# Silence repeating messages
;mute 20
```

Índice

1.3.2 Linux (distribución Debian 3.1 Sarge)

En el lado del usuario remoto se utilizará OpenVPN para la Implementación del protocolo SSL/TLS.

Para los paquetes fuente y rpm, puede consultar la página de OpenVPN: www.openvpn.net

Tanto OpenVPN como OpenVPN GUI son proyectos de código abierto y tienen licencia GPL.

- Instale openvpn con:

  #apt-get install openvpn

- Primero debería comprobar si los módulos TUN se incluyeron al instalar el kernel:

  # cat /boot/config-2.4.x-x-x | grep CONFIG_TUN

  (pudieron ser instalados como un módulo ***CONFIG_TUN=m*** o como parte integrante del kernel ***CONFIG_TUN=y***)

En caso contrario, tendrá que activar **CONFIG_TUN** en el archivo de configuración del kernel (*Device Drivers -> Network device support -> Universal TUN/TAP device driver support*) y volver a compilarlo o instalarlo.

- A continuación, compruebe si existe el dispositivo TUN:

  # ls –la /dev /net

Si no es así, créelo con:

```
# mkdir /dev/net
# mknod /dev/net/tun c 10 200
# chmod 0700 /dev/net/tun
```

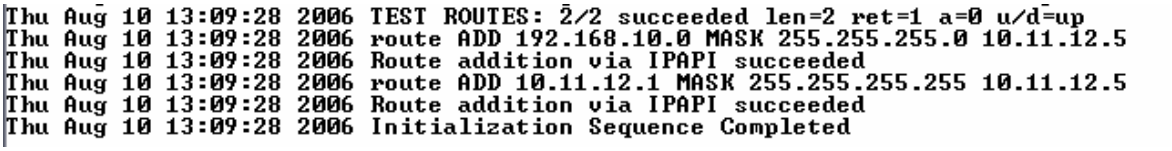
- El último paso sería realizar las mismas modificaciones en el archivo **/etc/openvpn/client.conf** que se han descrito anteriormente para el archivo de configuración de MS Windows 2000/XP **client1.ovpn**.

Índice

1.4 Establecer una conexión VPN

Para iniciar un túnel VPN SSL desde un usuario remoto MS Windows 2000/XP:

- Haga clic con el botón derecho del ratón en el archivo **client1.ovpn** de OpenVPN.
- Del menú emergente desplegado, seleccione "**Connect**". Si todo está bien configurado, se conectará a la nueva red virtual.
- Si todo está bien configurado, aparecerá una ventana con un mensaje que termina con la línea **Initialization Sequence Completed** (secuencia de inicialización completada), tal como se muestra a continuación:



Cuando se ejecuta de este modo, hay muchos comandos de teclado disponibles:

- **F1** -- Reinicio condicional (no cierra o vuelve a abrir el adaptador TAP)
- **F2** -- Mostrar estadísticas de conexión
- **F3** -- Reinicio
- **F4** -- Salir

Tenga en cuenta que OpenVPN también se puede iniciar como un servicio de Windows.

Para iniciar un túnel VPN SSL desde un usuario remoto Linux:

```
# cd /etc/openvpn
# openvpn client.conf
```

(los certificados client1.crt y ca.crt y la clave client1.key tienen que estar en el mismo directorio).

Si desea más información acerca de la gestión de un cliente openvpn, consulte la página: www.openvpn.net

Índice

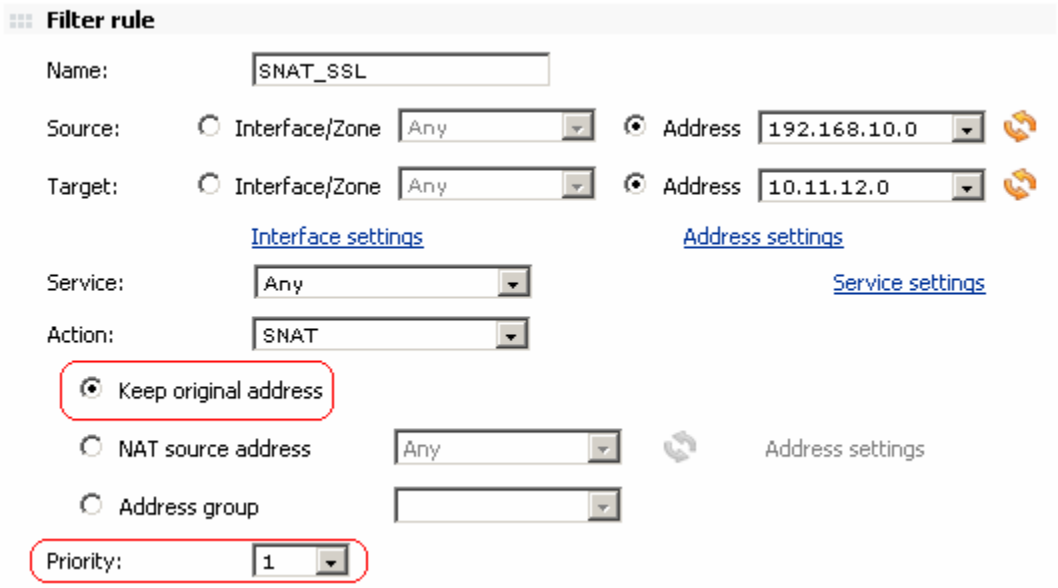
1.5 Otras consideraciones

Si se utilizan todas las funcionalidades del firewall de Panda GateDefender Integra, todas las reglas de configuración correspondientes se introducirán automáticamente en el firewall.
Pero si utiliza un firewall personal o un router de banda ancha con firewall o si hay routers o firewalls situados entre el cliente VPN y el servidor gateway VPN de Integra, debe activar un puerto y protocolo para VPN SSL en todos los firewalls y routers que haya entre el cliente VPN y el servidor gateway VPN de Integra:

En este ejemplo, hay que abrir el puerto/protocolo del servidor **1194/UDP.**

Tenga en cuenta que si activa las opciones de firewall en Windows XP, tendrá que desactivar la casilla que corresponda al adaptador TAP-Win32.
Se puede acceder al firewall desde el **Panel de control -> Centro de seguridad -> Firewall de Windows -> Opciones avanzadas**.

Si, en cualquiera de sus configuraciones – ya sea Clave estática o certificados-, GateDefender Integra tiene habilitada la opción de SNAT para la red local que interviene en la VPN, será necesario añadir una regla SNAT de mayor prioridad que la anterior, que haga que al tráfico de la VPN no se le aplique el cambio de encabezado IP origen propio de SNAT antes de enrutar los paquetes hacia el túnel. Para ello sólo se debe activar el botón *Mantener dirección original:*



En el ejemplo de la figura, vemos cómo sería la regla a añadir para que el tráfico de la red 192.168.10.0 pudiera enrutarse de forma correcta por el túnel VPN hacia la red 10.11.12.0 de los roadwarriors.

Índice

1.6 Comprobación de la configuración

Para comprobar su configuración VPN **SSL**, siga el procedimiento que se describe a continuación:

1. Aceda a 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 3.7).

Figura 3.7

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 al adaptador TAP-Win32 (si usted es el primer usuario remoto que se conecta utilizando la configuración que se ha explicado en este ejemplo, su dirección IP será 10.11.12.6 y la siguiente 10.11.12.10, ya que se usa la subred /30 en lugar de la /24 debido a los límites de implementación de la interfaz TAP).

- 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 control del tráfico de red como, por ejemplo, Ethereal, para comprobar si el tráfico entre el usuario remoto (roadwarrior) y a oficina remota (gateway) está cifrado.

Los paquetes cifrados SSL 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) se verán en la interfaz TAP-Win32.

Índice

0707-PGDIHT03-03-SP