HOWTO: Cómo configurar redes VPN IPSec de oficina remota (gateway) 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.

El software descrito en este documento se entrega bajo un Acuerdo de Licencia y únicamente puede ser utilizado una vez aceptados los términos del citado Acuerdo.

La tecnología antispam incluida en este producto pertenece a Mailshell. La tecnología de filtrado web incluida en este producto pertenece a Cobión.

Aviso de Copyright

© Panda 2007. Todos los derechos reservados. Ni la documentación, ni los programas a los que en su caso acceda, pueden copiarse, reproducirse, traducirse o reducirse a cualquier medio o soporte electrónico o legible sin el permiso previo por escrito de Panda, C/ Buenos Aires 12, 48001 Bilbao (Vizcaya) ESPAÑA.

Marca Registrada

Panda Security™. TruPrevent es una marca registrada en la Oficina de Patentes y Marcas de EEUU. Windows Vista y el logo de Windows son marcas o marcas registradas de Microsoft Corporation en los EEUU y/o otros países. Otros nombres de productos son marcas registradas de sus respectivos propietarios.
© Panda 2007. Todos los derechos reservados.

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.

1 IPSec de gateway a gateway

(IP Secure) Protocolo de seguridad que permite el intercambio seguro de paquetes en la capa IP, siendo una forma garantizada de proteger el enlace entre un dispositivo y la red. Ofrece integridad, autenticación, control de acceso y confidencialidad para el envío de paquetes IP por Internet.

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) IPsec 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 ilustración siguiente muestra un escenario típico de red VPN IPSec gateway-a-gateway (de oficina remota-a-oficina remota):

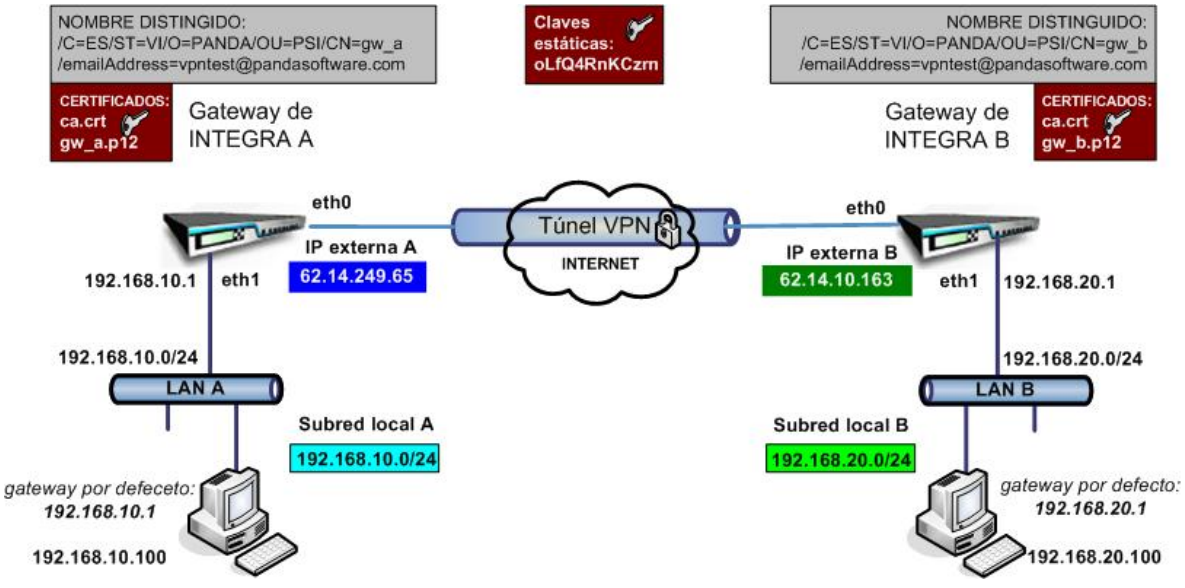

Figure 6.1 VPN IPSec gateway-a-gateway

La IP local externa del gateway A será **62.14.249.65**, mientras que el gateway B tendrá la IP **62.14.10.163**

En la figura se aprecia que los interfaces eth0/WAN de ambos gateways tienen asignada una dirección IP pública. Habitualmente, en las configuraciones reales más comunes, los interfaces eth0/WAN tienen asignados una dirección IP privada, y es otro dispositivo con la opción NAT habilitada situado entre el gateway VPN y la conexión ISP (por exemplo módem/router ADSL, cable Módem, etc), el que dispone de una dirección IP pública (dinámica o estática).
Esta aproximación se ha llevado a cabo para simplificar este documento y centrar la atención en la configuración de la VPN.
Para más detalles, se recomienda consultar howtos de configuración de SNAT, DNAT, mapeo de puertos, etc…

Los hosts que pertenezcan a la subred local A (identificada como **192.168.10.0/24** en esta guía) deben tener configurada la IP **192.168.10.1** de la LAN A de Integra como gateway a la subred local B (identificada como **192.168.20.0/24** en esta guía). Lo mismo es válido para los hosts en la subred local B; su gateway para la subred local A debe ser **192.168.20.1.** La ruta puede definirse como un gateway por defecto o una ruta implícita. Para el siguiente ejemplo supondremos que la IP de la LAN de Integra es el gateway por defecto para los hosts correspondientes de las subredes locales de Integra.

Para autenticar cada gateway pueden utilizarse claves estáticas o certificados (TLS).

Índice

1.2 Configuración del gateway A

1.2.1 Configuración de grupos de direcciones IP

El primer paso a la hora de configurar este tipo de VPN IPSec es definir un grupo de direcciones IP que correspondan a la subred local IPSec (situada detrás de este gateway) y la subred remota IPSec (situada detrás del gateway B). Los hosts de estas dos subredes podrán acceder a los hosts del otro lado por medio del túnel IPSec creado entre los dos gateways.

Para definir las subredes local y remota IPSec, siga los pasos siguientes:

1. Acceda a la sección **Definiciones** del menú principal de Panda GateDefender Integra.
2. Seleccione **Direcciones IP**.
3. En la sección **Grupos**, haga clic en **Añadir**.
   Deberá introducir un nombre descriptivo para el grupo (en este ejemplo usaremos ***ipsec gwA subnet***) en el campo **Nombre**, y un rango IP (**192.168.10.0/24** en este ejemplo) en el campo que aparece junto al botón de selección **IP/Máscara**.
4. Haga clic en **Añadir IP** y a continuación en **Añadir** para guardar los cambios.
5. Vuelva a hacer clic en **Añadir**. Esta vez, el nombre descriptivo para el grupo será ***ipsec gwB subnet*** en este ejemplo y se utilizará el rango de direcciones IP ***192.168.20.0/24***.
6. Haga clic en **Añadir IP** y a continuación en **Añadir** para guardar los cambios.

 **IMPORTANTE:** Recuerde que la subred local IPSec debe ser distinta de las subredes remotas IPSec o de cualquier otra subred que esté ya en uso en cualquier otra configuración VPN (incluyendo otros tipos de protocolo). En caso contrario sería imposible lograr el enrutamiento de la subred local A a la subred local B.

1.2.2 Certificados CA y certificados locales de servidor

Si se van a emplear certificados para la autenticación, necesitará importar el certificado CA público que firmó el certificado del par remoto. También deberá importar el certificado local del gateway A VPN de Integra.

Para importar el certificado 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.

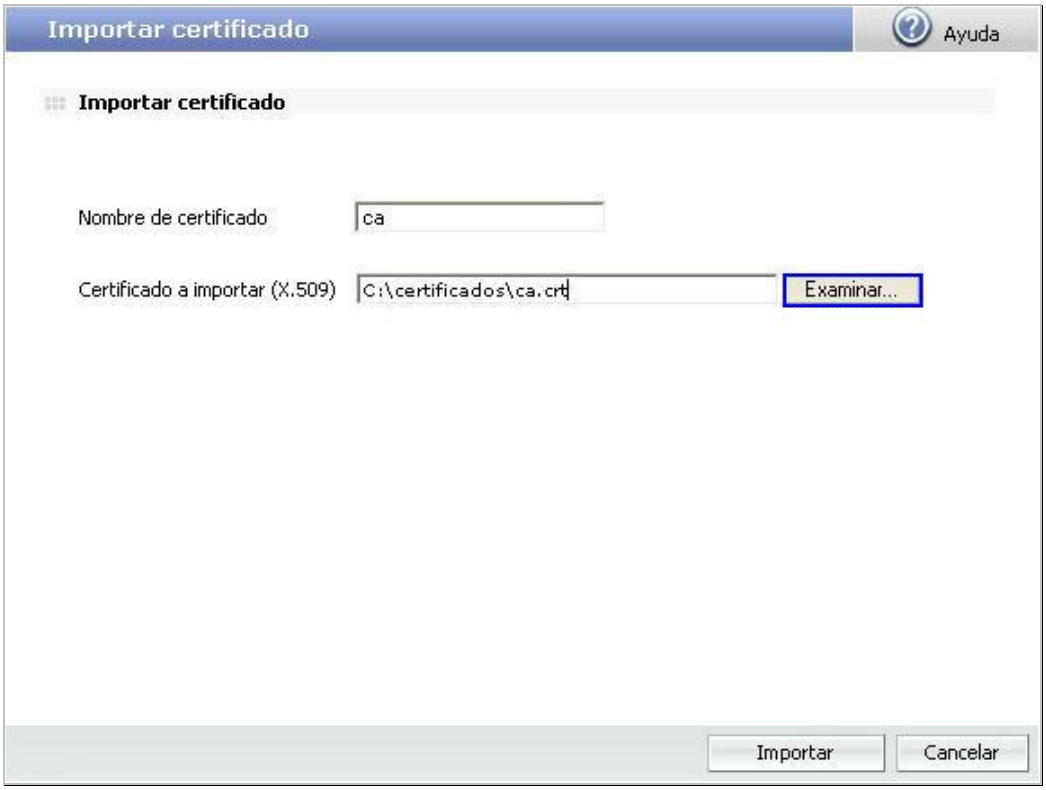

Figura 6.2

Para importar el certificado local del gateway A, siga el procedimiento que se indica a continuación:

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

    a. Seleccione si quiere **Importar un certificado pendiente de firma** o **Importar un certificado con clave privada** emitido por una CA.
    b. Si selecciona **Importar certificado con clave privada**, introduzca el Nombre de certificado PKCS12 (en este ejemplo utilizaremos ***server***) y, si lo desea, una **Contraseña**.

3. Haga clic en **Examinar**… para seleccionar el certificado que desea importar.
4. Haga clic en **Importar** una vez haya elegido un certificado.

Una vez se hayan importado correctamente los certificados CA y el certificado local del gateway A, la pantalla con la configuración será similar a la que se muestra en la figura 6.3.

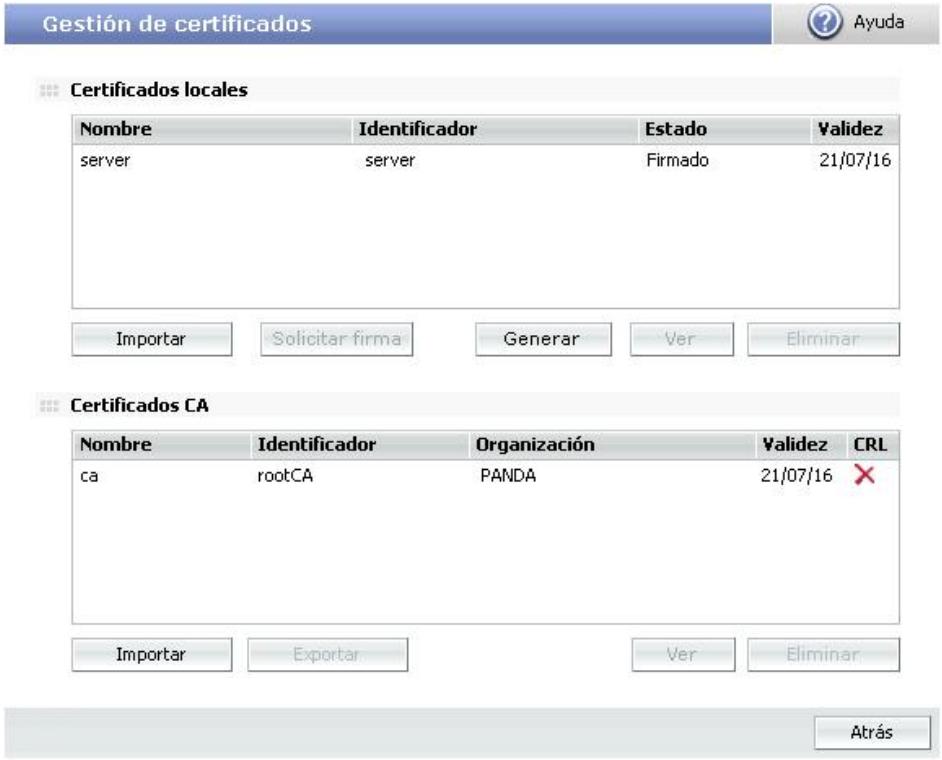

Figura 6.3

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).

Índice

1.2.3 Políticas IKE

Panda GateDefender Integra le permite definir las políticas de seguridad IKE necesarias para la conexión VPN IPSec.

Para añadir una nueva política IKE, siga las siguientes instrucciones:

1. Haga clic en la opción **VPN** del menú principal de la consola de Panda GateDefender Integra y a continuación haga clic en **VPN IPSEC** en la sección **Gestión de VPN.**
2. Vaya a la pestaña **Políticas IKE**.
3. Haga clic en **Añadir**. Aparecerá una pantalla con las siguientes opciones:

    - **Nombre:** Nombre descriptivo de la política (en esta guía se empleará ***IKE***).
    - **Forzar algoritmos:** Deje esta opción sin marcar para no forzar los algoritmos seleccionados. Los dos lados del túnel intentarán utilizar el primero de los algoritmos seleccionados en orden, y, en caso de que esta negociación no tenga éxito, se emplearán otras posibilidades con las que cuentan ambos lados.
    - **Tiempo de vida de las claves para las Fases I y II**: Opcional. Deje estas opciones sin marcar.

4. Haga clic en **Añadir** para guardar los cambios.

Índice

1.2.4 Configuración de VPN IPSec en el gateway A

Utilizando clave estática

Esta sección trata de la configuración de IPSec utilizando clave estática.

Para configurar IPSec con clave estática utilizando elementos previamente definidos, siga las siguientes instrucciones:

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 un nombre descriptivo para la VPN. (en este caso se utilizará **IPSEC VPN1**).
2. **Política IKE**: Utilice el menú desplegable para seleccionar la política IKE que desee aplicar (en este ejemplo se utilizará IKE)
3. **Parámetros de Fase I:**

   IP Local: Introduzca la **dirección IP pública local** o elija la opción **IP asignada por DHCP** (en este caso se utilizará **la *IP pública local 62.14.249.65)***.

   IP Remota: Introduzca la **dirección IP pública remota** o elija la opción **IP asignada por DHCP** (en este caso se utilizará **la *IP pública remota 62.14.10.163)***.

   Seleccione un tipo de autenticación a utilizar: **Clave estática**.

4. Después de seleccionar **Clave estática**, introduzca una clave estática que quiera utilizar. Si lo desea, haga clic en el botón **Autogenerar** para crear una clave automáticamente (la clave estática utilizada en este ejemplo será ***qMoeQkO7N7X4*)**.
5. **Parámetros de Fase II:**

   Subred Local: Seleccione una subred de aquellas definidas en el menú desplegable (en este ejemplo se utilizará ***ipsec gwA subnet***).

   Subred Remota: Seleccione una subred de aquellas definidas en el menú desplegable (en este ejemplo se utilizará ***ipsec gwB subnet***).

Cuando haya configurado la parte IPSEC, la pantalla de configuración correspondiente será similar a la de la figura **6.4**.

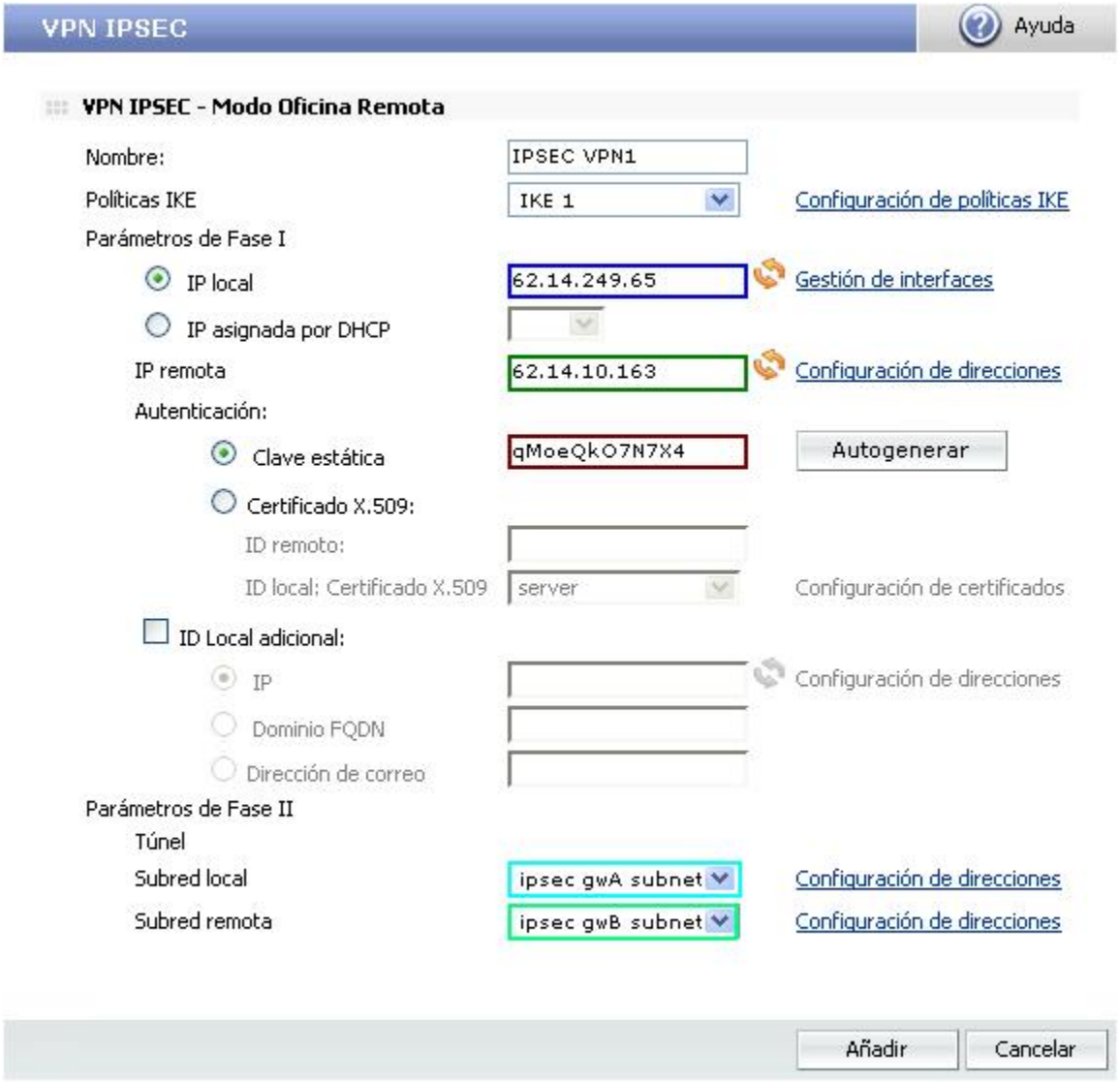
VPN IPSEC
Ayuda
VPN IPSEC - Modo Oficina Remota
Nombre:
IPSEC VPN1
Políticas IKE
IKE 1
Configuración de políticas IKE
Parámetros de Fase I
IP local
62.14.249.65
Gestión de interfaces
IP asignada por DHCP
IP remota
62.14.10.163
Configuración de direcciones
Autenticación:
Clave estática
qMoeQkO7N7X4
Autogenerar
Certificado X.509:
ID remoto:
ID local: Certificado X.509
server
Configuración de certificados
ID Local adicional:
IP
Configuración de direcciones
Dominio FQDN
Dirección de correo
Parámetros de Fase II
Túnel
Subred local
ipsec gwA subnet
Configuración de direcciones
Subred remota
ipsec gwB subnet
Configuración de direcciones
Añadir
Cancelar

Figura 6.4

Utilizando TLS

Esta sección trata de la configuración de IPSec utilizando TLS.

Para configurar IPSec con TLS utilizando elementos previamente definidos, siga las siguientes instrucciones:

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 un nombre descriptivo para la VPN. (en este caso se utilizará **IPSEC VPN1**).
2. **Política IKE**: Utilice el menú desplegable para seleccionar la política IKE que desee aplicar. (en este ejemplo se utilizará **IKE 1**)
3. **Parámetros de Fase I:**

   IP Local: Introduzca la **dirección IP pública local** o elija la opción **IP asignada por DHCP** (en este caso se utilizará **la dirección *IP pública local 62.14.249.65)***.

   IP Remota: Introduzca la **dirección IP pública remota** o elija la opción **IP asignada por DHCP** (en este caso se utilizará **la dirección *IP pública remota 62.14.10.163)***.

4. Seleccione un tipo de autenticación a utilizar: **Certificado X.509**. Dispondrá de las siguientes opciones:

   - **ID remoto**: Especifique el nombre distinguido del gateway B. En este ejemplo se utilizará la siguiente identificación remota:

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

     Puede obtenerlo del certificado client del gateway B, tecleando el comando siguiente en la consola de comandos de MS-DOS, siempre y cuando tenga instalados un programa openssl o openvpn:

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

   - **ID local: X-509 certificate**: Utilice el menú desplegable para seleccionar el certificado que desea (en esta guía se utilizará server).

   - **ID Local adicional**: También dispone de las siguientes opciones:

     - **IP**: Introduzca la dirección IP local. Por defecto aparecerá la dirección IP introducida en la pantalla de la configuración global de IPSec.
     - **Dominio FQDN** (Fully Qualified Domain Name): Nombre del dominio completo.
     - **Dirección de correo**. Dirección de correo electrónico utilizada para la identificación.

5. Parametros de Fase II

Subred Local: Seleccione una subred de aquellas definidas en el menú desplegable (en este ejemplo se utilizará **ipsec gwA subnet**).

Subred Remota: Seleccione una subred de aquellas definidas en el menú desplegable (en este ejemplo se utilizará **ipsec gwB subnet)**.

Cuando haya configurado la parte IPSEC, la pantalla de configuración correspondiente será similar a la de la figura **6.5**

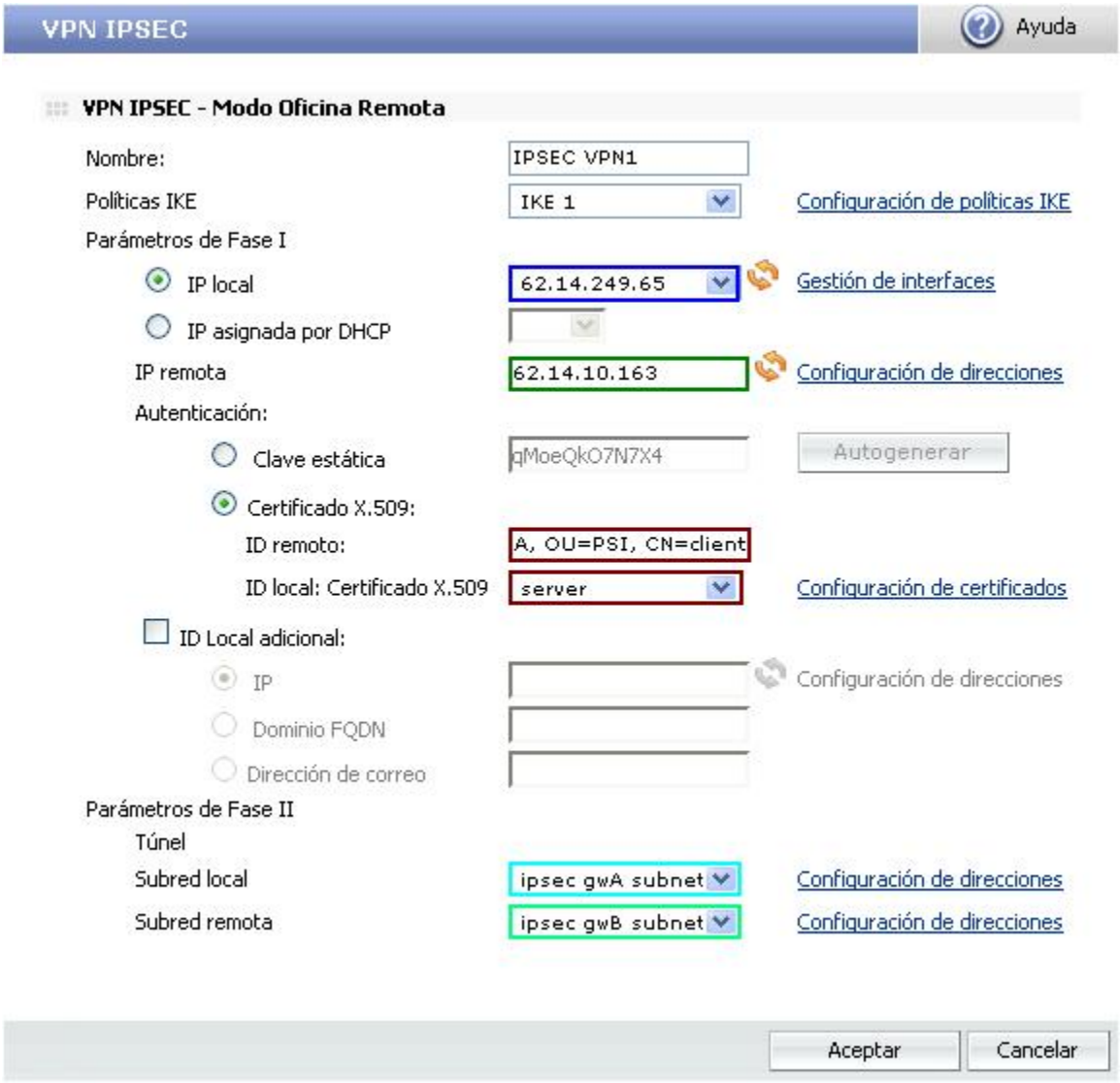

Figura 6.5

Nota: Si existe algún dispositivo NAT entre los dos gateways VPN de Integra, deberá activar la casilla NAT transversal tal y como se muestra a continuación.

Figura 6.6

Índice

1.3 Configuración del gateway B

1.3.1 Configuración de grupos de direcciones IP

Una vez más, deberá definir un grupo de direcciones IP que correspondan a la subred local IPSec (situada detrás de este gateway) y la subred remota IPSec (situada detrás del gateway A). Los hosts de estas dos subredes podrán acceder a los hosts del otro lado por medio del túnel IPSec creado entre los dos gateways.

Para definir las subredes local y remota IPSec, siga los pasos siguientes:

1. Acceda a la sección **Definiciones** del menú principal de Panda GateDefender Integra.
2. Seleccione **Direcciones IP**.
3. En la sección **Grupos**, haga clic en **Añadir**.
   Deberá introducir un nombre descriptivo para el grupo (en este ejemplo usaremos ***ipsec gwB subnet***) en el campo **Nombre**, y un rango IP (**192.168.20.0/24** en este ejemplo) en el campo que aparece junto al botón de selección **IP/Máscara**.
4. Haga clic en **Añadir IP** y a continuación en **Añadir** para guardar los cambios.
5. Vuelva a hacer clic en **Añadir**. Esta vez, el nombre descriptivo para el grupo será ***ipsec gwA subnet*** en este ejemplo y se utilizará el rango de direcciones IP ***192.168.10.0/24***.

Haga clic en **Añadir IP** y a continuación en **Añadir** para guardar los cambios.

 **IMPORTANTE:** Recuerde que la subred local IPSec debe ser distinta de las subredes remotas IPSec o de cualquier otra subred que esté ya en uso en cualquier otra configuración VPN (incluyendo otros tipos de protocolo). En caso contrario sería imposible lograr el enrutamiento de la subred local B a la subred local A.

1.3.2 Certificados CA y certificados locales de servidor

Si se van a emplear certificados para la autenticación, necesitará importar el certificado CA público que firmó el certificado del par remoto. También deberá importar el certificado local del gateway A VPN de Integra.

Para importar el certificado 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.

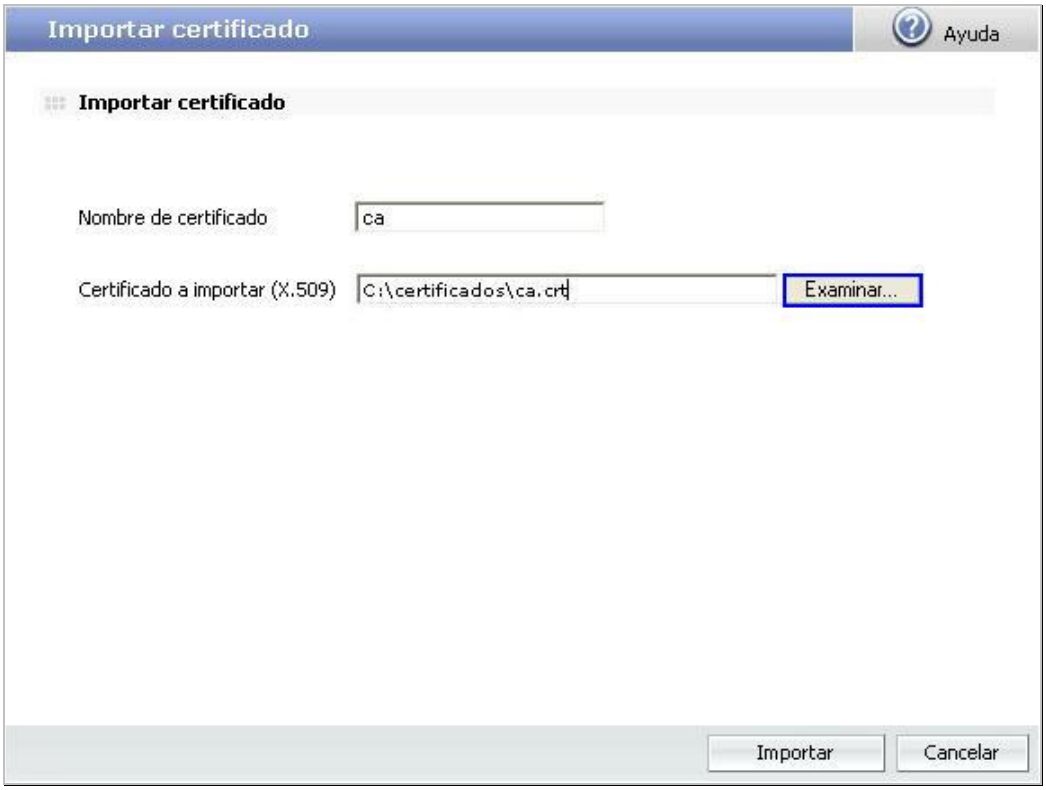

Figura 6.7

Para importar el certificado local del gateway B, siga el procedimiento que se indica a continuación:

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

    a. Seleccione si quiere **Importar un certificado pendiente de firma** o **Importar un certificado con clave privada** emitido por una CA.
    b. Si selecciona **Importar certificado con clave privada**, introduzca el Nombre de certificado PKCS12 (en este ejemplo utilizaremos ***client***) y, si lo desea, una **Contraseña.**

3. Haga clic en **Examinar**… para seleccionar el certificado que desea importar.
4. Haga clic en **Importar** una vez haya elegido un certificado.

Una vez se hayan importado correctamente los certificados CA y el certificado local del gateway B, la pantalla con la configuración será similar a la que se muestra en la figura 6.8.

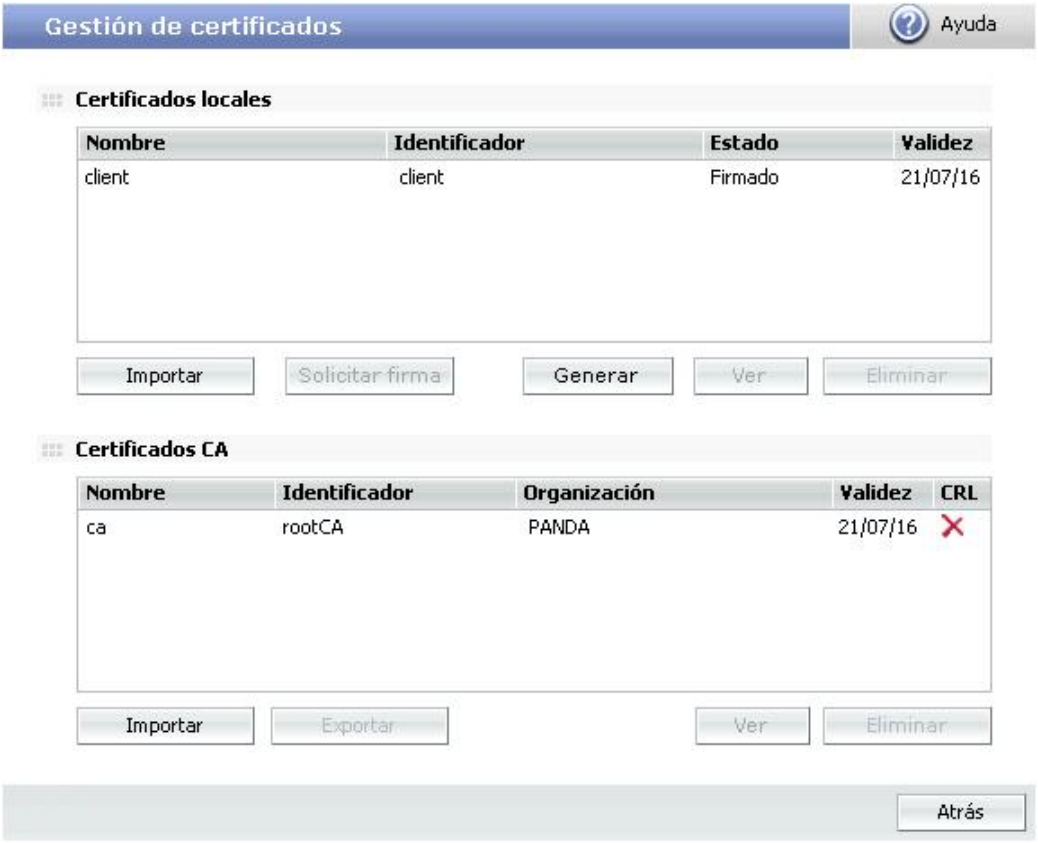

Figura 6.8

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).

1.3.3 Configuración de VPN IPSec en el gateway B

Utilizando clave estática

Esta sección trata de la configuración de IPSec utilizando clave estática.

Para configurar IPSec con clave estáttica utilizando elementos previamente definidos, siga las siguientes instrucciones:

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 un nombre descriptivo para la VPN. (en este caso se utilizará **IPSEC VPN1**).
2. **Política IKE**: Utilice el menú desplegable para seleccionar la política IKE que desee aplicar. (en este ejemplo se utilizará **IKE 1**)
3. **Parametros de Fase I:**

   IP Local: Introduzca la **dirección IP pública local** o elija la opción **IP asignada por DHCP** (en este caso se utilizará **la dirección *IP pública local 62.14.10.163)***.

   IP Remota: Introduzca la **dirección IP pública remota** o elija la opción **IP asignada por DHCP** (en este caso se utilizará **la dirección *IP pública remota 62.14.249.65)***.

   Seleccione un tipo de autenticación a utilizar: **Clave estática**.

4. Después de seleccionar **Clave estática**, introduzca una clave estática que quiera utilizar. Si lo desea, haga clic en el botón **Autogenerar** para crear una clave automáticamente (la clave estática utilizada en este ejemplo será ***qMoeQkO7N7X4*)**.
5. **Parametros de Fase II:**

   Subred Local: Seleccione una subred de aquellas definidas en el menú desplegable (en este ejemplo se utilizará ***ipsec gwB subnet***).

   Subred Remota: Seleccione una subred de aquellas definidas en el menú desplegable (en este ejemplo se utilizará ***ipsec gwA subnet***).

Cuando haya configurado la parte IPSEC, la pantalla de configuración correspondiente será similar a la de la figura **6.9**.

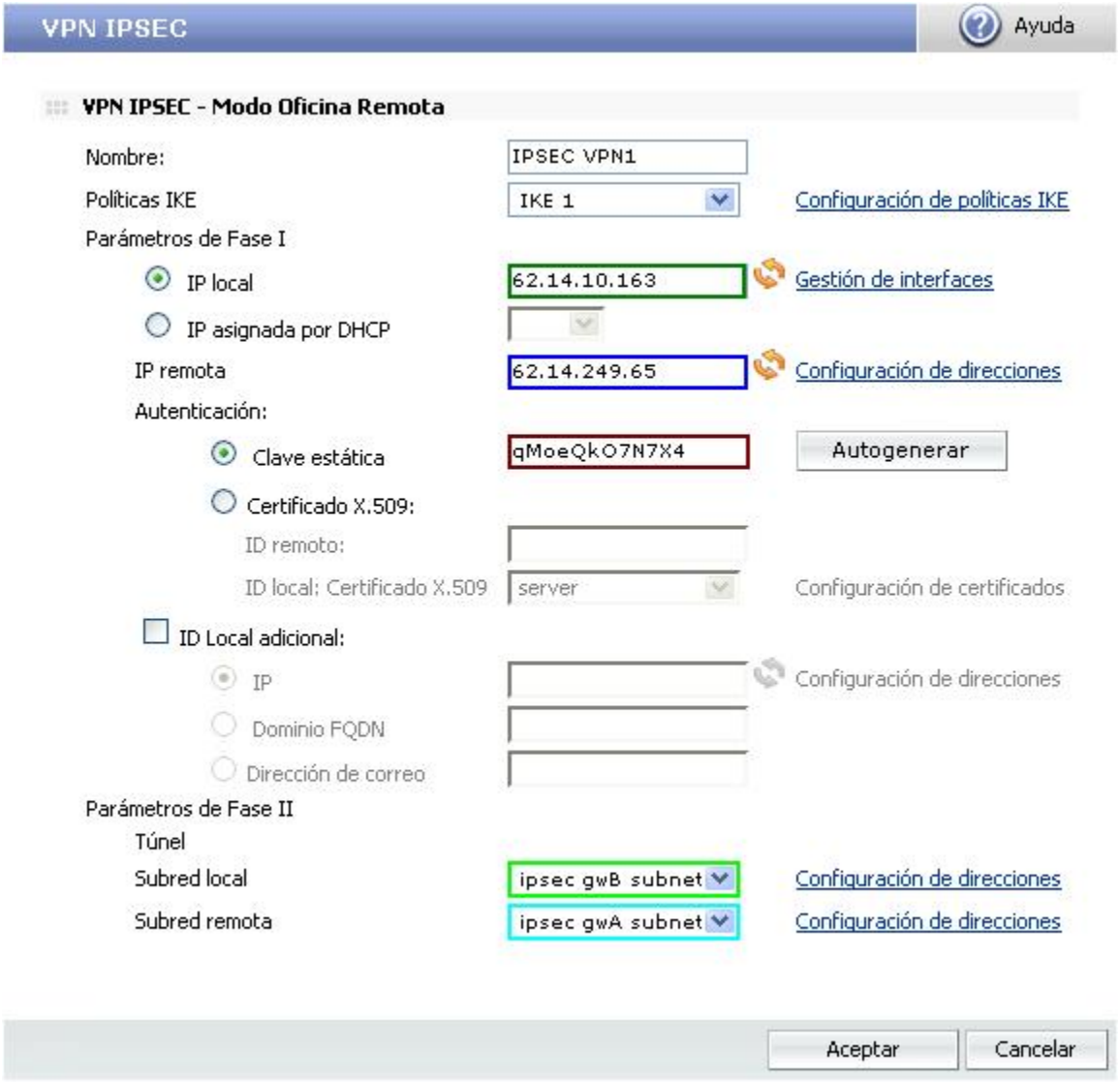
VPN IPSEC
Ayuda
VPN IPSEC - Modo Oficina Remota
Nombre:
IPSEC VPN1
Políticas IKE
IKE 1
Configuración de políticas IKE
Parámetros de Fase I
IP local
62.14.10.163
Gestión de interfaces
IP asignada por DHCP
IP remota
62.14.249.65
Configuración de direcciones
Autenticación:
Clave estática
qMoeQkO7N7X4
Autogenerar
Certificado X.509:
ID remoto:
ID local: Certificado X.509
server
Configuración de certificados
ID Local adicional:
IP
Configuración de direcciones
Dominio FQDN
Dirección de correo
Parámetros de Fase II
Túnel
Subred local
ipsec gwB subnet
Configuración de direcciones
Subred remota
ipsec gwA subnet
Configuración de direcciones
Aceptar
Cancelar

Figura 6.9

Utilizando TLS

Esta sección trata de la configuración de IPSec utilizando TLS.

Para configurar IPSec con TLS utilizando elementos previamente definidos, siga las siguientes instrucciones:

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:

Las opciones disponibles son:

1. **Nombre**: Introduzca un nombre descriptivo para la VPN. (en este caso se utilizará **IPSEC VPN1**).

2. **Política IKE**: Utilice el menú desplegable para seleccionar la política IKE que desee aplicar. (en este ejemplo se utilizará **IKE 1**).

3. **Parámetros de Fase I:**

   IP Local: Introduzca la **dirección IP pública local** o elija **IP asignada por DHCP** (en este caso se utilizará **la dirección *IP pública local 62.14. 10.163)***.

   IP Remota: Introduzca la **dirección IP pública remota** o elija **IP asignada por DHCP** (en este caso se utilizará **la dirección *IP pública remota 62.14. 249.65)***.

4. Seleccione un tipo de autenticación a utilizar: **Certificado X.509**. Dispondrá de las siguientes opciones:

   - **ID remoto**: Especifique el nombre distinguido del gateway B. En este ejemplo se utilizará la siguiente identificación remota:

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

     Puede obtenerlo del certificado client del gateway B, tecleando el comando siguiente en la consola de comandos de MS-DOS, siempre y cuando tenga instalados un programa openssl ó openvpn:

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

   - **ID local: X-509 certificate**: Utilice el menú desplegable para seleccionar el certificado que desea (en esta guía se utilizará **client**).

- **ID Local adicional**: También dispone de las siguientes opciones:

    - **IP**: Introduzca la dirección IP local. Por defecto aparecerá la dirección IP introducida en la pantalla de la configuración global de IPSec.
    - **Dominio FQDN** (Fully Qualified Domain Name): Nombre del dominio completo.
    - **Dirección de correo**. Dirección de correo electrónico utilizada para la identificación.

5. Parametros de Fase II

Subred Local: Seleccione una subred de aquellas definidas en el menú desplegable (en este ejemplo se utilizará **ipsec gwB subnet**).

Subred Remota: Seleccione una subred de aquellas definidas en el menú desplegable (en este ejemplo se utilizará **ipsec gwA subnet)**.

Cuando haya configurado la parte IPSEC, la pantalla de configuración correspondiente será similar a la de la figura **6.10**

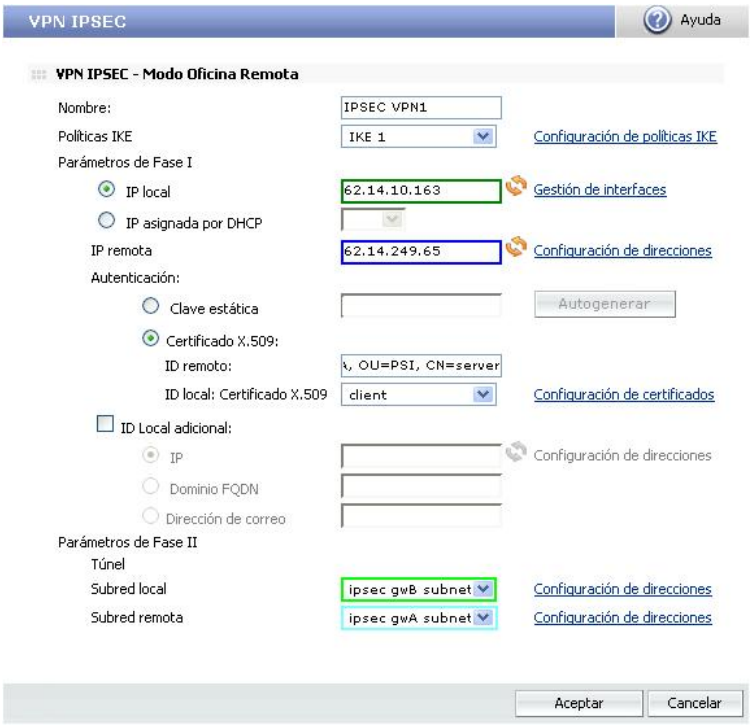

Figura 6.10

Nota: Si existe algún dispositivo NAT entre los dos gateways VPN de Integra, deberá activar la casilla NAT transversal tal y como se muestra en la Figura 6.7.

Índice

1.4 Establecimiento de una conexión VPN

Para poder iniciar una conexión VPN IPSec entre dos oficinas remotas (gateways), siga estas instrucciones:

1. Marque la casilla **Activa** en ambos gateways para activar la configuración, como se muestra en las figuras **6.11** y **6.12**

Figura 6.11

Figura 6.12

2. Para desconectar, desmarque la casilla **Activa** en ambos lados del túnel y haga clic en **Aceptar**.

Índice

1.5 Consideraciones adicionales

Si se utilizan las funciones de firewall de Panda GateDefender Integra, se pondrán en marcha automáticamente todas las reglas de configuración del firewall correspondientes.

Si hay routers o firewalls entre las dos oficinas remotas (gateways), deberán activarse los siguientes puertos y protocolos para que la VPN IPSec funcione correctamente:

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*.

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:*

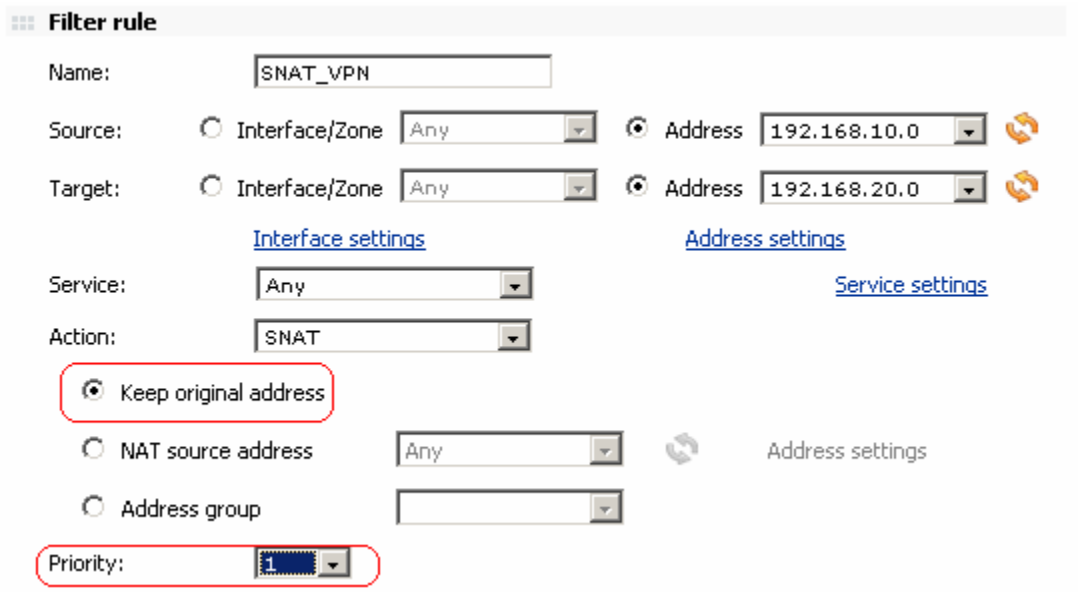

Figura 6.13

En el ejemplo de la figura, se muestra la regla a añadir para que el tráfico de la red 192.168.10.0 pueda enrutarse de forma correcta por el túnel VPN hacia el roadwarrior 192.168.20.100.

Índice

1.6 Comprobación de la configuración

Para comprobar la configuración de la red VPN ISPec, siga los pasos que se describen a continuación:

1. Acceda a la consola de administración de Panda GateDefender.
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 establecidas.

   Una vez establecido el túnel VPN entre las dos oficinas remotas (gateways), deberá ejecutar el test siguiente en cada subred local de la VPN para alcanzar la subred remota.

   Para realizarlo, utilice el siguiente comando:

   ping –n 10 192.168.20.100

   Cuando se ejecuta este comando, se hace un ping desde el host que pertenece a la subred VPN del gateway A al host que reside en la red interna detrás del gateway B VPN. El gateway A debería poder ver el mensaje de respuesta ICMP.

   Ten en cuenta que sólo estarán encriptados aquellos paquetes que vayan de una subred local a una subred remota o viceversa. Esto significa que si se hace ping entre hosts que pertenecen a una de las subredes VPN internas del gateway y una dirección IP externa de otro gateway, el tráfico no irá encriptado en ningún momento, ya que el propósito de un tunel VPN gateway a gateway (o como también hemos mencionado anteriormente, subred a subred) es asegurar la privacidad entre dos subredes.

Índice

© Panda 2007