

Howto: Qué puertos se deben abrir en el firewall/router corporativo cuando Panda GateDefender Integra actúa como Gateway VPN



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 Cobiión.

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

1	Introducción.....	3
2	Protocolos VPN.....	3
2.1	VPN IPSEC.....	4
2.2	VPN L2TP.....	4
2.3	VPN SSL.....	5
2.4	VPN PPTP.....	6
3	Conclusiones.....	7

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.

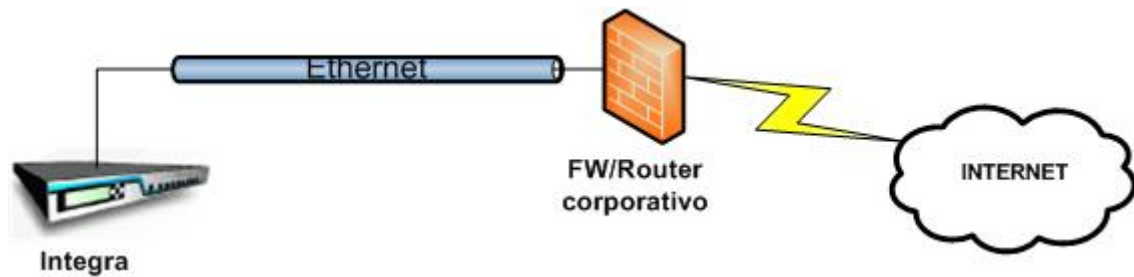
Código: Nombres de archivos, extensiones, carpetas, información de la línea de comandos o archivos de configuración como, por ejemplo, scripts.

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

1 Introducción

El siguiente documento explica cómo configurar el firewall/router corporativo situado delante de GateDefender Integra para que permita la salida del tráfico VPN cuando Integra está actuando como gateway.

El escenario que se va a describir a lo largo del documento simula una de las situaciones más habituales que se dan a la hora de instalar un dispositivo de Panda GateDefender Integra en modo router en una red corporativa:



La unidad de Panda GateDefender Integra se situará a la entrada de la red, justo detrás del firewall/router corporativo.

El dispositivo que se encuentre ubicado delante de la unidad de GateDefender Integra, bien sea un firewall o router, puede estar aplicando políticas de seguridad que controlen el tráfico tanto entrante como saliente. En este caso, si Integra está actuando como Gateway VPN, es necesario asegurarse que cierto tráfico de salida se va a permitir, para poder así establecer y utilizar la red VPN según el protocolo configurado para los túneles.

A continuación se detallan los puertos y protocolos que será necesario abrir en el firewall/router corporativo.

[Índice](#)

2 Protocolos VPN

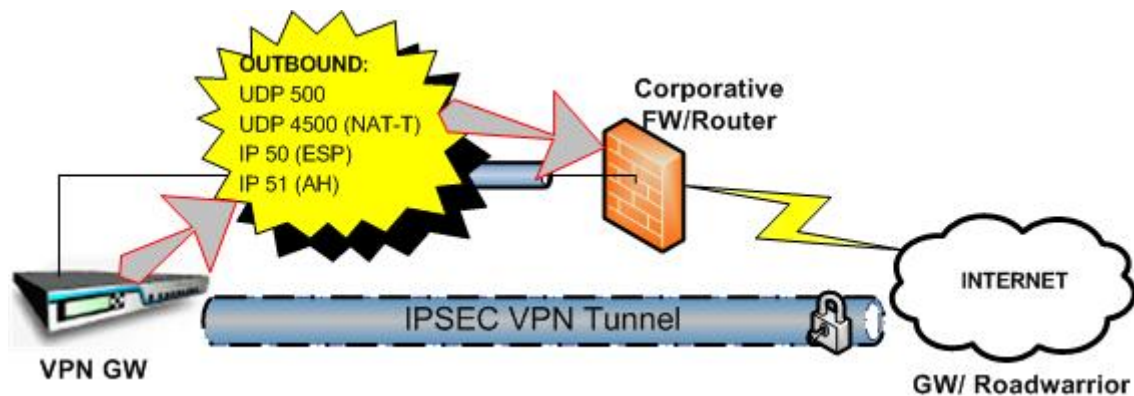
2.1 VPN IPSEC

En este primer caso, GateDefender Integra va a establecer un túnel VPN IPSEC con un dispositivo remoto, bien sea GW-GW (gateway-gateway) o bien GW-RW (gateway-roadwarrior).

Para establecer y posteriormente utilizar el túnel de forma correcta, es necesario abrir los siguientes puertos en el firewall/router corporativo para que se permita la salida del tráfico a GateDefender Integra:

- UDP 500 para el establecimiento del túnel
- Protocolo IP 50 si se está usando ESP (Encapsulating Security Payload), o bien protocolo IP 51 en caso de usar AH (Authentication Header).
- En caso de emplear NAT-T (Nat transversal) en aquellos casos en los que sea necesario, además de usar paquetes UDP 500, se usarán paquetes UDP 4500.

El siguiente diagrama ilustra este escenario:



[Índice](#)

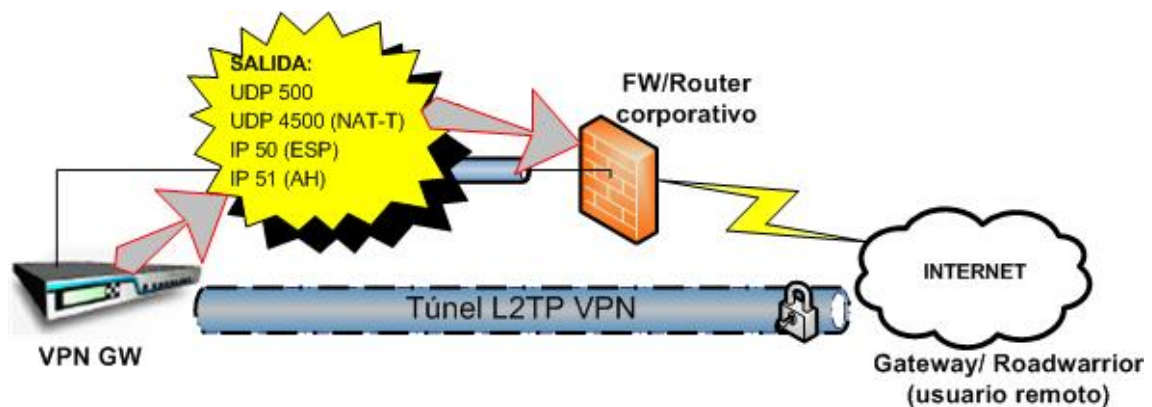
2.2 VPN L2TP

Para el protocolo L2TP, el funcionamiento es similar al caso anterior, ya que L2TP funciona sobre IPSEC.

Por lo tanto, los puertos que tendrán que estar abiertos en el firewall/router corporativo para que la VPN L2TP se establezca y funcione de forma correcta son los siguientes:

- UDP 500 para el establecimiento del túnel
- Protocolo IP 50 si se está usando ESP, o bien protocolo IP 51 en caso de usar AH.
- En caso de emplear NAT-T (Nat transversal) en aquellos casos en los que sea necesario, además de usar paquetes UDP 500, se usarán paquetes UDP 4500.

El siguiente diagrama resume esta situación:



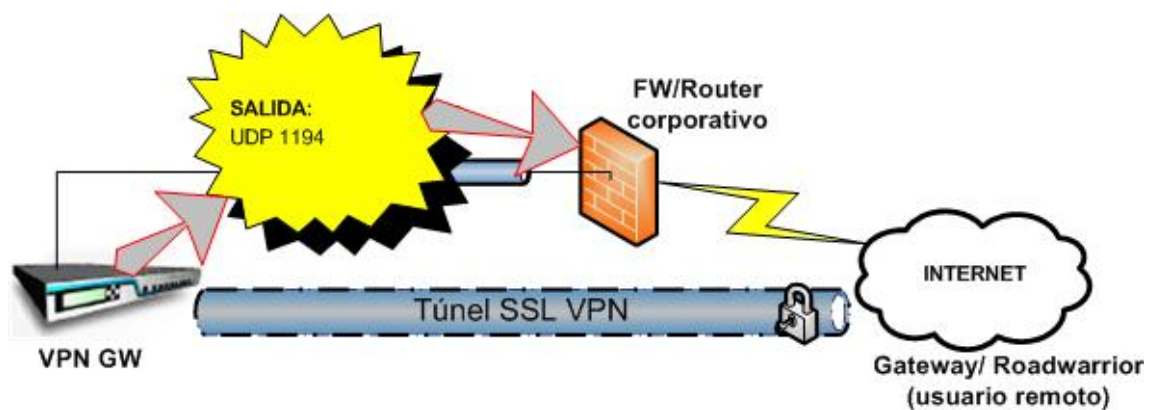
[Índice](#)

2.3 VPN SSL

El protocolo SSL se comporta de forma más sencilla que IPSEC.

Para que la red VPN SSL se establezca y funcione de forma correcta, únicamente será necesario permitir un tipo de paquetes de salida: UDP 1194

Por lo tanto, el firewall/router corporativo debe permitir en sus políticas de seguridad la salida de estos paquetes:



[Índice](#)

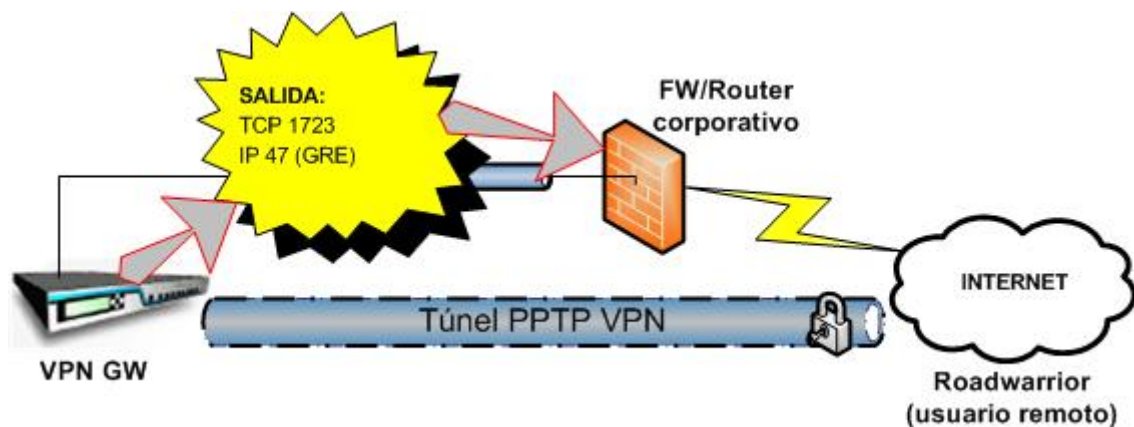
2.4 VPN PPTP

El protocolo PPTP utiliza dos paquetes diferentes para implementar los túneles:

- TCP 1723 para el canal de control
- IP 47 (GRE) para el canal de datos

Para que el túnel se establezca correctamente, es necesario que dichos paquetes pasen a través del router/firewall corporativo.

La siguiente figura detalla esta situación:




[Índice](#)

3 Conclusiones

A lo largo de este documento, se ha mostrado cómo configurar el router/firewall corporativo para que no se bloqueen los paquetes de la red VPN en el caso de que las políticas de seguridad estén aplicando restricciones sobre el tráfico saliente.

Si las políticas de seguridad recaen sobre la propia unidad de Integra y no existe ningún otro dispositivo que restrinja el tráfico, no es necesario realizar estas configuraciones en el firewall de Integra, ya que la propia configuración de la VPN introduce las reglas necesarias en su sistema para permitir la salida de estos paquetes.

 **NOTA: Con la configuración de la VPN, Integra prepara automáticamente su firewall para que la VPN se pueda establecer. Sin embargo, es necesario definir a posteriori las reglas adecuadas si queremos aplicar políticas de seguridad sobre el tráfico transportado dentro de la VPN, una vez que éste ha sido descifrado.**

Para que la red VPN se establezca correctamente, además de permitir cierto tráfico de salida para cada escenario y protocolo utilizado, puede que sea necesario realizar configuraciones adicionales que se apliquen sobre los paquetes entrantes.

[Índice](#)
