Panda GateDefender Integra

HOWTO: Cómo configurar el firewall para redes 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.

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 Introducción

Panda GateDefender Integra dispone del módulo VPN a través del cual se pueden implementar VPNs para arquitecturas Gateway-to-Gateway y Gateway-to-Roadwarrior.

Para construir el túnel, se puede usar cualquiera de los siguientes protocolos: PPTP, L2TP, SSL, IPSEC.

Una vez se ha configurado la VPN, Panda GateDefender Integra, de forma automática, ajusta su firewall para que los puertos necesarios para establecer el túnel con el otro extremo se encuentren abiertos y disponibles. Las reglas necesarias son introducidas en el sistema de forma totalmente transparente para el usuario y ni siquiera se visualizarán desde la consola.

Sin embargo, a pesar de que el túnel se establece sin necesidad de realizar configuración alguna en el firewall, el tráfico encriptado que llega a Integra, una vez que pasa por el módulo VPN y se desencripta, se envía internamente al firewall de nuevo. Entonces, éste le aplica las reglas de filtrado configuradas por el usuario desde la consola web.

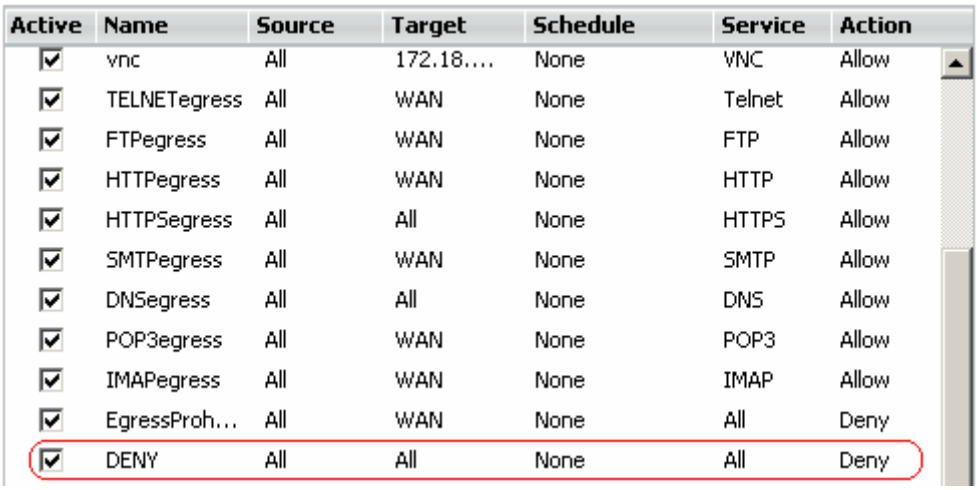
 **IMPORTANTE**: Por lo tanto, para que el tráfico del usuario pueda circular por el túnel, es necesario realizar una configuración específica.

En el siguiente documento se muestra cómo se debe configurar el firewall de GateDefender Integra cuando se está utilizando VPN (redes privadas virtuales) y el propio Panda GateDefender Integra está implicado en la implementación de los túneles bien como servidor VPN o como cliente, para que el tráfico destinado al túnel no sea filtrado.

Índice

2 Configuración del Firewall

A la hora de definir de qué forma es necesario configurar el firewall, se parte de la base de que la política por defecto del firewall es **Denegar**. Panda GateDefender Integra ya incluye esta política en su configuración de fábrica:



Active	Name	Source	Target	Schedule	Service	Action
☑	vnc	All	172.18....	None	VNC	Allow
☑	TELNETegress	All	WAN	None	Telnet	Allow
☑	FTPegress	All	WAN	None	FTP	Allow
☑	HTTPegress	All	WAN	None	HTTP	Allow
☑	HTTPSegress	All	All	None	HTTPS	Allow
☑	SMTPegress	All	WAN	None	SMTP	Allow
☑	DNSegress	All	All	None	DNS	Allow
☑	POP3egress	All	WAN	None	POP3	Allow
☑	IMAPegress	All	WAN	None	IMAP	Allow
☑	EgressProh...	All	WAN	None	All	Deny
☑	DENY	All	All	None	All	Deny

Por lo tanto, si esta regla se mantiene como la regla de menor prioridad (situada en el último lugar de las reglas de filtrado), cada vez que se configure una VPN, será necesario introducir reglas de filtrado de mayor prioridad que acepten y no denieguen el tráfico “real” que viaja dentro de los paquetes encriptados de la VPN.

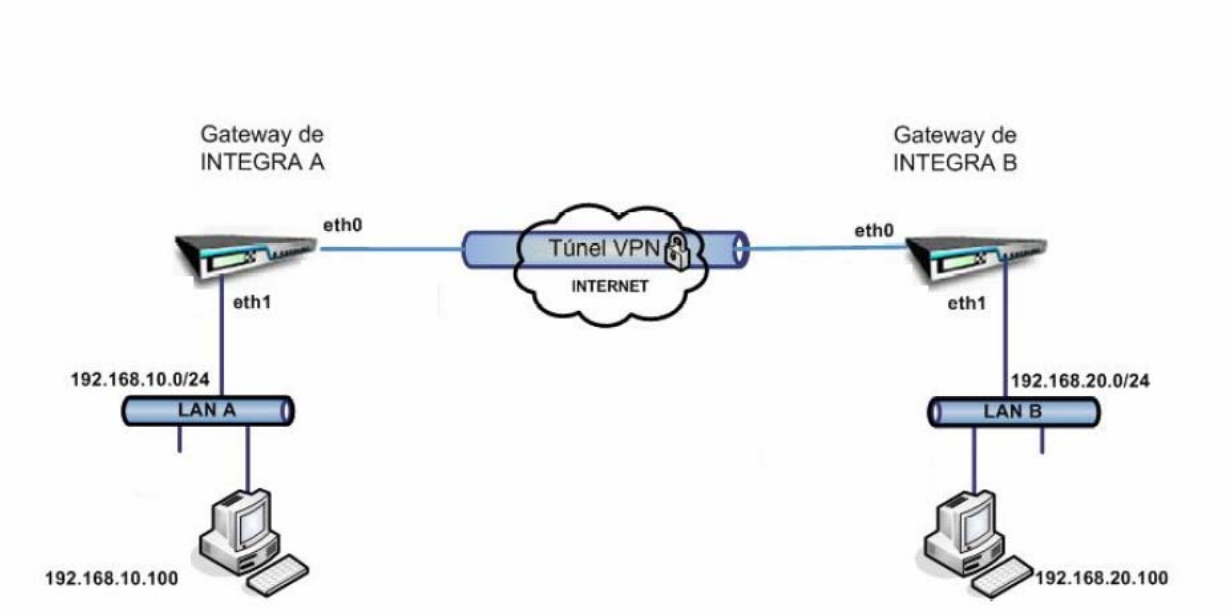
Índice

2.1 VPN IPSEC

Panda GateDefender Integra permite implementar dos arquitecturas diferentes para este protocolo:

Gateway (oficina)-to-gateway (oficina), y Gateway (oficina)-Roadwarrior:

2.1.1 Gateway-to-gateway



En el escenario de la figura, se establece un túnel IPSEC entre dos dispositivos de Panda GateDefender Integra.

En ambas unidades se han definido previamente desde el menú **Definiciones** varios grupos de direcciones que recogen el rango de direcciones locales y remotas respectivamente:

Integra A: Local_A= 192.168.10.0/24
Remota_B= 192.168.20.0/24

Integra B: Local_B= 192.168.20.0/24
Remota_A= 192.168.10.0/24

Para que desde la LAN A se pueda alcanzar la LAN B, no basta únicamente con establecer el túnel que las comunica a través de Internet de forma segura, sino que será necesario configurar el firewall con las reglas adecuadas.

- **Caso 1: Desde la LAN A se quiere acceder a la LAN B**

Las siguientes políticas de filtrado deben ser configuradas:

Integra A: **Permitir** el tráfico desde el **origen** *lanA* al **destino** *LanB* para aquellos servicios que se desee.

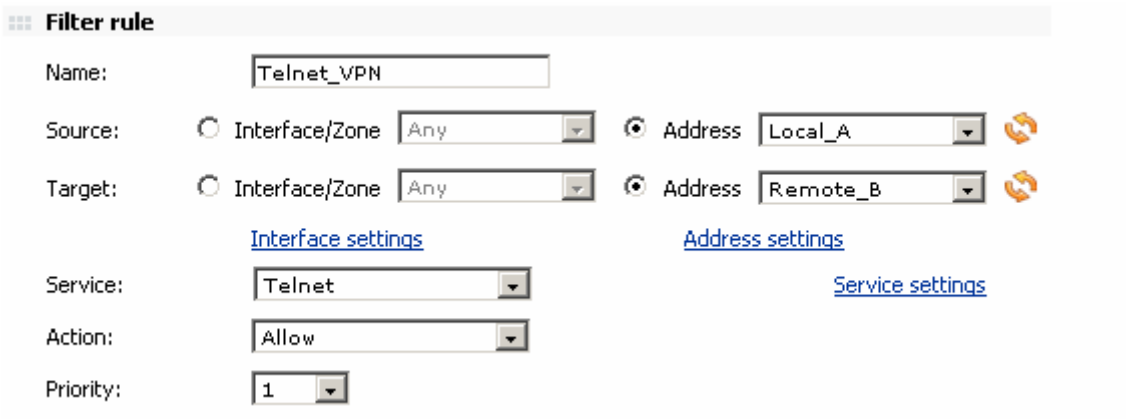
Integra B: **Permitir** el tráfico desde el **origen** *lanA* al **destino** *LanB* para aquellos servicios que se desee.

Nota: No es necesario habilitar una regla explícita en el firewall para permitir las respuestas a las sesiones ya establecidas con las reglas de filtrado inversas ya que Integra ya dispone de la opción interna de seguimiento de conexiones (Connection tracking) que se encarga de ello.

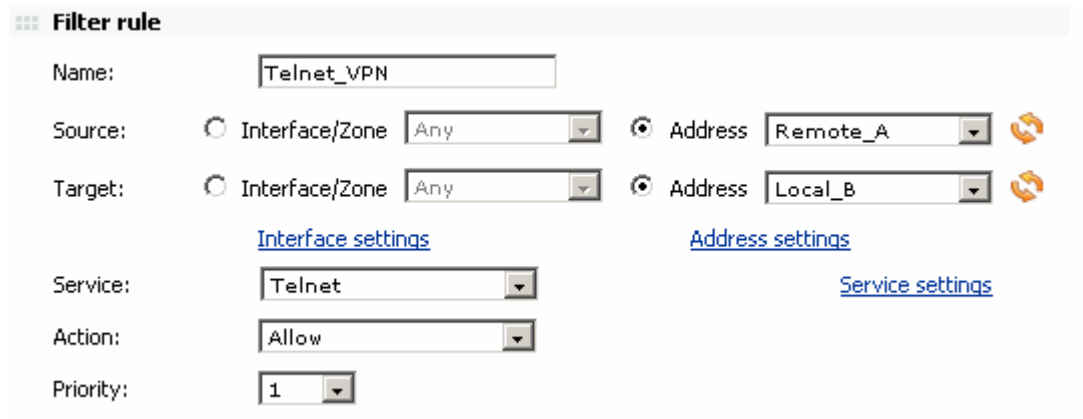
Ejemplo: ¿Qué reglas habría que añadir en los firewalls de ambos Integras para que el host de la red A (192.168.10.100) pueda llegar por Telnet (TCP 23) al host de la red B? (192.168.20.100)?

Solución:

Firewall de Integra A:



Firewall de Integra B:



Estas reglas permitirán que el host de la red local A acceda por Telnet al host de la red B.

- **Caso 2: Desde la LAN B se quiere acceder a la LAN A**

Las siguientes políticas de filtrado deben ser configuradas:

Integra B: **Permitir** el tráfico desde el **origen** *LANB* al **destino** *LANA* para aquellos servicios que se desee.

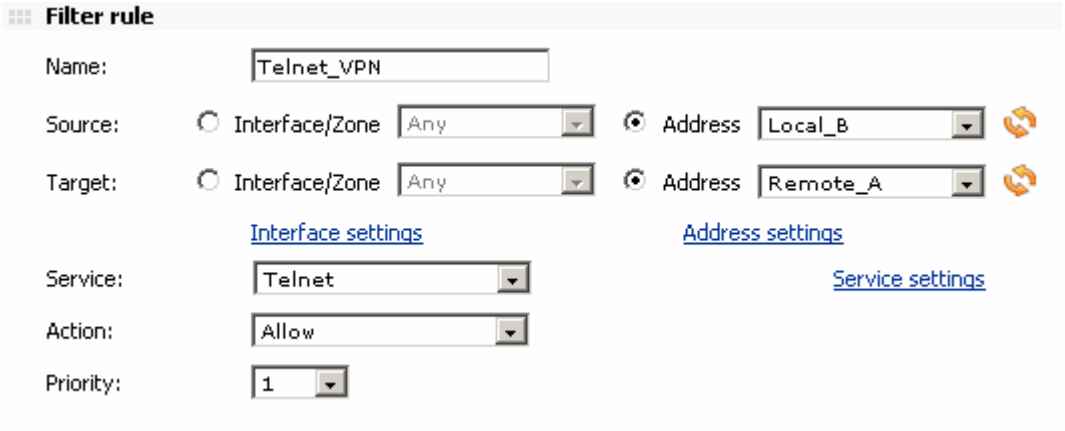
Integra A: **Permitir** el tráfico desde el **origen** *LANB* al **destino** *LanA* para aquellos servicios que se desee.

Ejemplo:

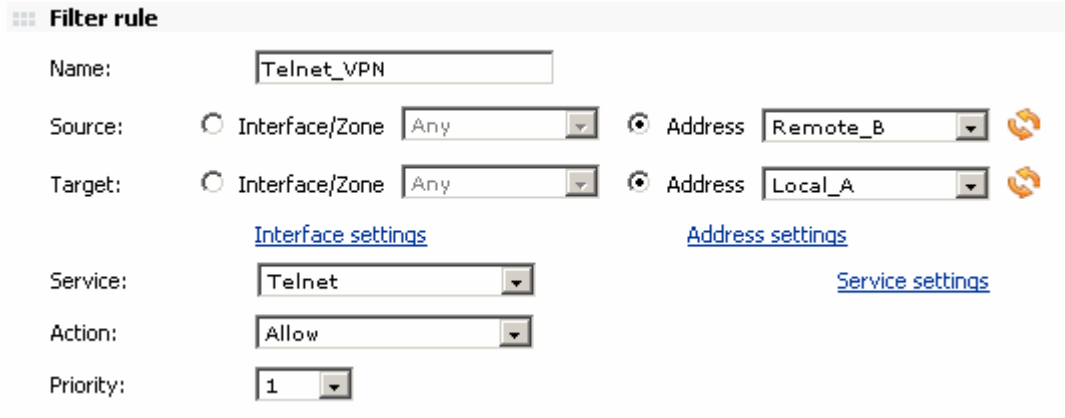
Si se desea acceder vía Telnet del host de la red B al host de la red A, se debe cambiar el origen y el destino de los paquetes respecto al caso anterior:

Solución:

Firewall de Integra B:

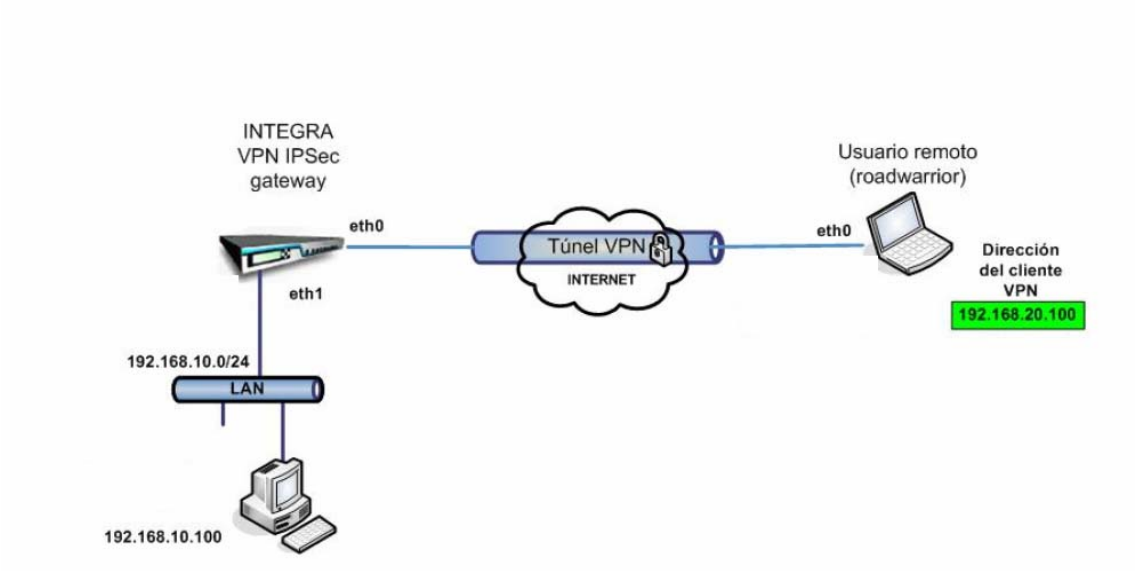


Firewall de Integra A:



Índice

2.1.2 Gateway-to-Roadwarrior



En el escenario de la figura, un dispositivo de Panda GateDefender Integra actúa como servidor VPN para clientes remotos (roadwarriors) entre los que se acaba de establecer un túnel IPSEC.

En el caso de IPSEC, el roadwarrior accede a la red local VPN con la dirección IP real que tenga asignada en su propia red, normalmente una dirección IP privada. Como estas direcciones IP son las que se usarán en la lan local del servidor VPN, se deberán utilizar dichas direcciones para establecer las políticas de seguridad.

Nota*:* Para verificar qué dirección IP tiene cada roadwarrior, se puede acceder al **submenú Monitor VPN** desde el **menú VPN** de la consola web.

Para simplificar la gestión de las reglas del firewall, desde el **menú Definiciones** de Integra se definen los siguientes grupos de direcciones:

- Virtual_IPSEC = 192.168.20.10 (para el ejemplo de la figura)
- Local=192.168.10.0/24

Si se quiere permitir que el roadwarrior una vez que haya establecido el túnel VPN con el servidor VPN IPSEC pueda acceder a la red local con determinados servicios, es necesario configurar las políticas de seguridad en Panda GateDefender Integra como se muestra a continuación:

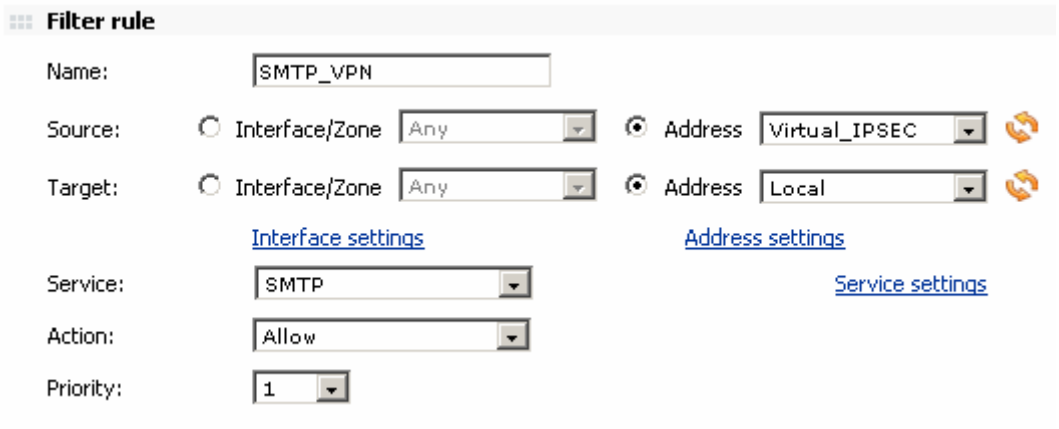
> Integra: **Permitir** el tráfico desde el **origen** *roadwarrior* al **destino** *Lan* para aquellos servicios que se desee.

Nota: No es necesario habilitar una regla explícita en el firewall para permitir las respuestas a las sesiones ya establecidas con las reglas de filtrado inversas ya que Integra ya dispone de la opción interna de seguimiento de conexiones (Connection tracking) que se encarga de ello.

Ejemplo: ¿Qué reglas habrá que añadir en el firewall de Integra para que el roadwarrior pueda acceder por SMTP (TCP 25) a la red local de Integra?

Solución:

Firewall de Integra:

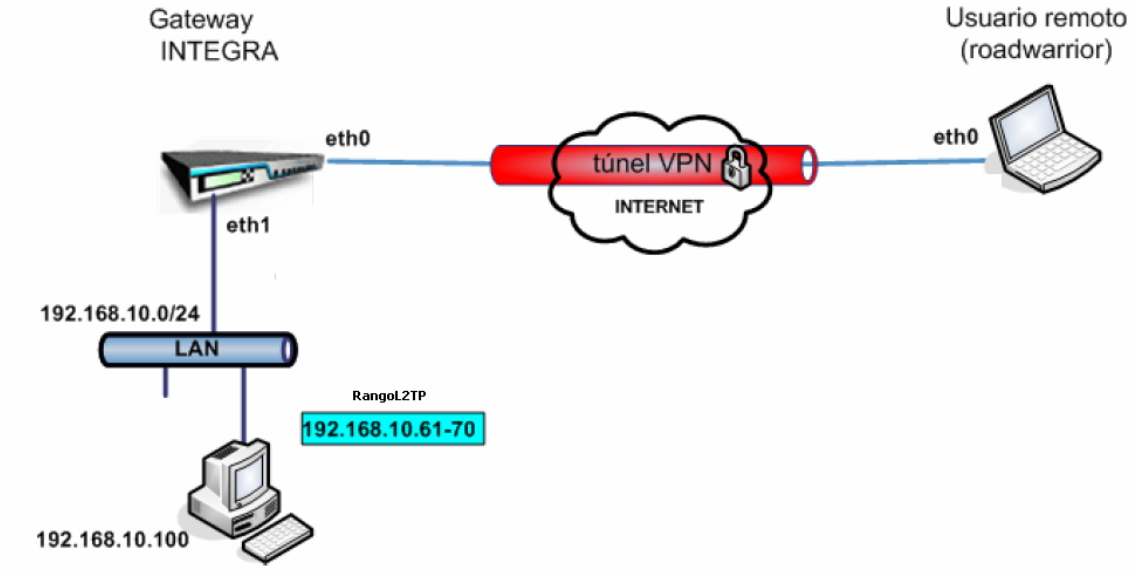


Índice

2.2 VPN L2TP

Panda GateDefender Integra permite implementar una única arquitectura para este protocolo:

Gateway (oficina)-Roadwarrior:



En el escenario de la figura, se encuentra un dispositivo de Panda GateDefender Integra que actúa como servidor VPN para clientes remotos (roadwarriors) entre los que se acaba de establecer un túnel L2TP.

El grupo de rango L2TP (ver la figura) se utilizará para asignar direcciones IP a los diferentes roadwarriors que se conecten al servidor. Estas direcciones IP, serán las que se utilicen en la red local del servidor VPN.

Nota: Para verificar qué dirección IP se le ha asignado a cada roadwarrior se puede acceder al **submenú Monitor VPN** desde el **menú VPN** de la consola web.

Para simplificar la gestión de las reglas del firewall, desde el **menú Definiciones** de Integra se definen los siguientes grupos de direcciones:

- Range_L2TP = 192.168.10.61-70
- Local=192.168.10.0/24

Si se quiere permitir que el roadwarrior pueda acceder a la red local con determinados servicios una vez que haya establecido el túnel VPN con el servidor VPN L2TP, es necesario configurar las políticas de seguridad en Panda GateDefender Integra como se muestra a continuación:

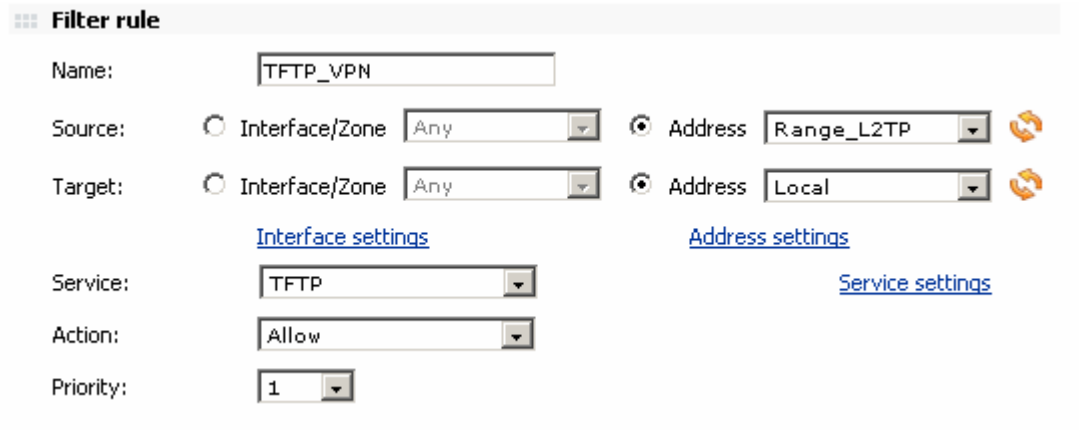
> Integra: **Permitir** el tráfico desde el **origen** *roadwarrior* al **destino** *Lan* para aquellos servicios que se desee.

Nota: No es necesario habilitar explícitamente la vuelta de la misma sesión con las reglas de filtrado inversas, ya que Integra con la opción interna de seguimiento de conexiones (Connection tracking) ya se encarga de ello.

Ejemplo: ¿Qué reglas será necesario añadir en el firewall de Panda GateDefender Integra para que el roadwarrior pueda acceder por TFTP(UDP 69) a la red local de Integra?

Solución:

Firewall de Integra:

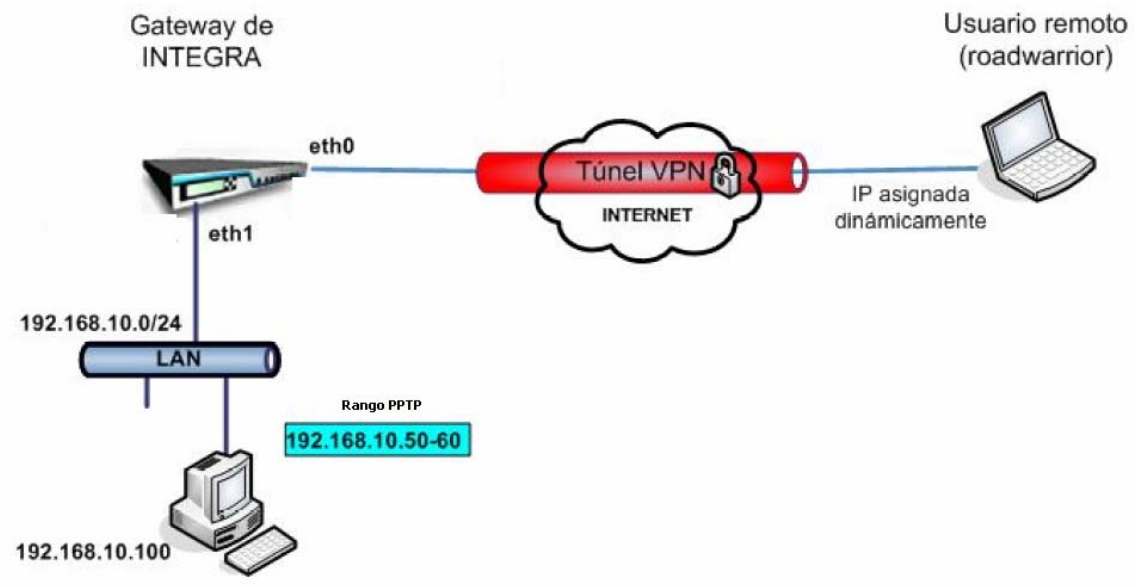


Índice

2.3 VPN PPTP

Panda GateDefender Integra permite implementar una única arquitectura para este protocolo:

Gateway (oficina)-Roadwarrior:



Pongamos por ejemplo el escenario de la figura, en el que un dispositivo de Panda GateDefender Integra actúa como servidor VPN para clientes remotos (roadwarriors) entre los que se acaba de establecer un túnel PPTP.

El grupo de rango PPTP (ver la figura) se utilizará para asignar direcciones IP a los diferentes roadwarriors que se conecten al servidor. Estas direcciones IP, serán las que utilicen en la lan local del servidor VPN.

Nota: Para verificar qué dirección IP se le ha asignado a cada roadwarrior se puede acceder al **submenú Monitor VPN** desde el **menú VPN** de la consola web.

Para simplificar la gestión de las reglas del firewall, desde el **menú Definiciones** de Integra se definen los siguientes grupos de direcciones:

- Range_PPTP= 192.168.10.50-60
- Local=192.168.10.0/24

Si se quiere permitir que el roadwarrior pueda acceder a la red local con determinados servicios, una vez que haya establecido el túnel VPN con el servidor VPN PPTP, es necesario configurar las políticas de seguridad en Integra como se muestra a continuación:

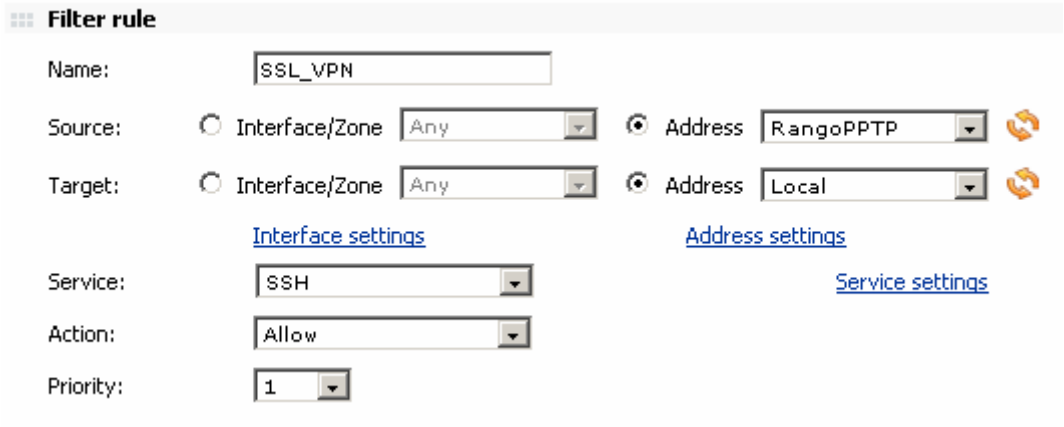
> Integra: **Permitir** el tráfico desde el **origen** *roadwarrior* al **destino** *Lan* para aquellos servicios que se desee.

Nota: No es necesario habilitar una regla explícita en el firewall para permitir las respuestas a las sesiones ya establecidas con las reglas de filtrado inversas ya que Integra ya dispone de la opción interna de seguimiento de conexiones (Connection tracking) que se encarga de ello.

Ejemplo: ¿Qué reglas será necesario añadir en el firewall de Integra para que el roadwarrior pueda acceder por SSH (TCP 22) a la red local de Integra?

Solución:

Firewall de Integra:



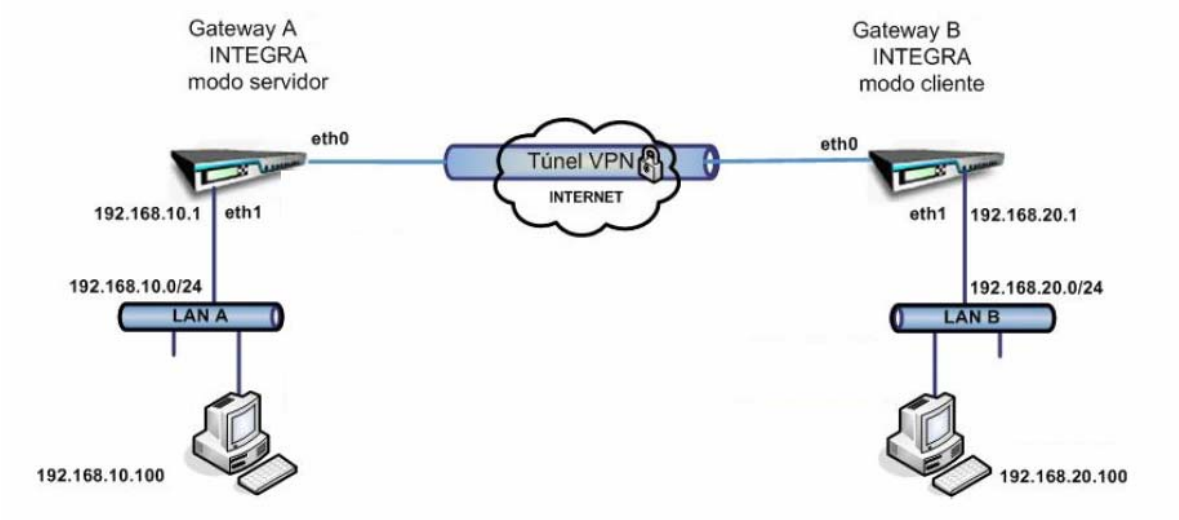
Índice

2.4 VPN SSL

Panda GateDefender Integra permite implementar dos arquitecturas diferentes para este protocolo:

Gateway (oficina)-to-gateway (oficina), y Gateway (oficina)-Roadwarrior:

2.4.1 Gateway-to-gateway



Sea el escenario de la figura, en el que hay dos dispositivos de Panda GateDefender Integra entre los que se acaba de establecer un túnel SSL.

En ambas unidades, se ha definido previamente desde el menú **Definiciones** varios grupos de direcciones que recogen el rango de direcciones locales y remotas respectivamente:

Integra A:
Local_A= 192.168.10.0/24
Remota_B= 192.168.20.0/24
Integra B:
Local_B= 192.168.20.0/24
Remota_A= 192.168.10.0/24

Para que desde la LAN A se pueda alcanzar la LAN B, no basta únicamente con establecer el túnel que las comunica a través de Internet de forma segura, sino que habrá que configurar el firewall con las reglas adecuadas.

- Caso 1: Desde la LAN A se quiere acceder a la LAN B

Las siguientes políticas de filtrado deben ser configuradas:

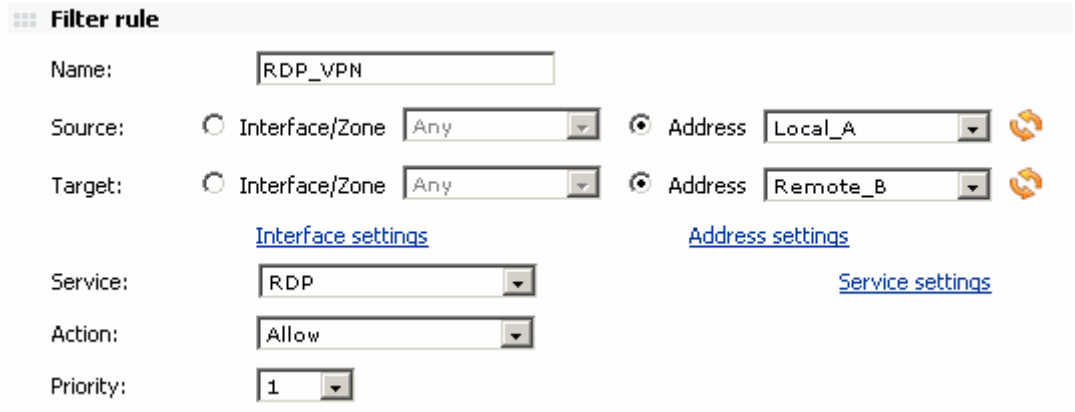
Integra A: **Permitir** el tráfico desde el **origen** *LANA* al **destino** *LANB* para aquellos servicios que se desee.
Integra B: **Permitir** el tráfico desde el **origen** *LANA* al **destino** *LANB* para aquellos servicios que se desee.

Nota: No es necesario habilitar una regla explícita en el firewall para permitir las respuestas a las sesiones ya establecidas con las reglas de filtrado inversas ya que Integra ya dispone de la opción interna de seguimiento de conexiones (Connection tracking) que se encarga de ello.

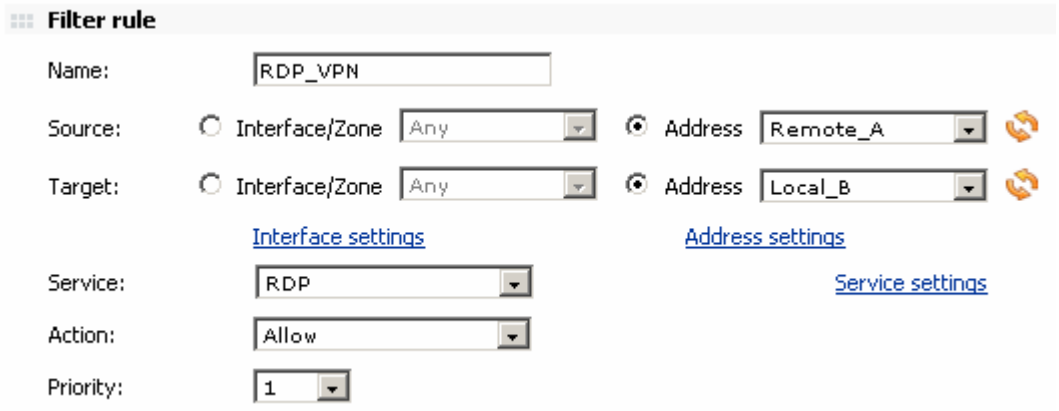
Ejemplo: ¿Qué reglas habría que añadir en los firewalls de ambos dispositivos de Integra para que el host de la red A (192.168.10.100) pueda llegar por RDP (TCP 3389) al host de la red B (192.168.20.100)?

Solución:

Firewall de Integra A:



Firewall de Integra B:



Estas reglas permitirán que el host de la red local A acceda por RDP al host de la red B.

- **Caso 2: Desde la LAN B se quiere acceder a la LAN A**

Las siguientes políticas de filtrado deben ser configuradas:

Integra B: **Permitir** el tráfico desde el **origen** *lanB* al **destino** *LanA* para aquellos servicios que se desee.

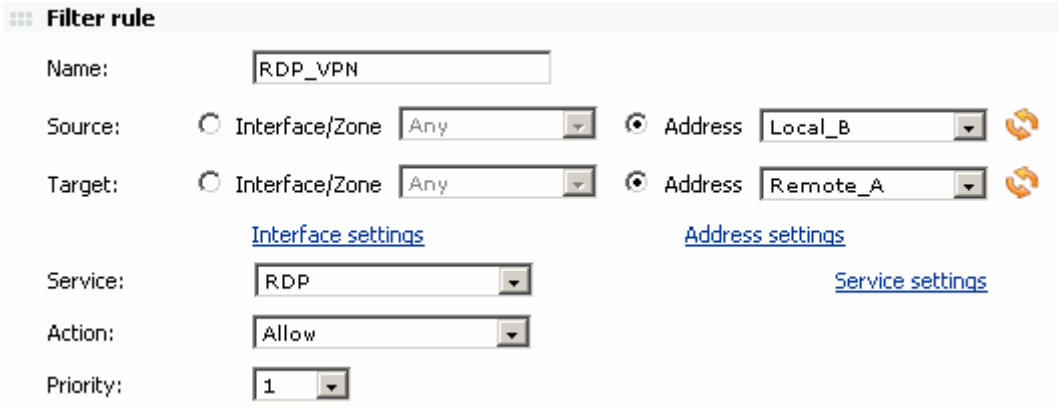
Integra A: **Permitir** el tráfico desde el **origen** *lanB* al **destino** *LanA* para aquellos servicios que se desee.

Ejemplo:

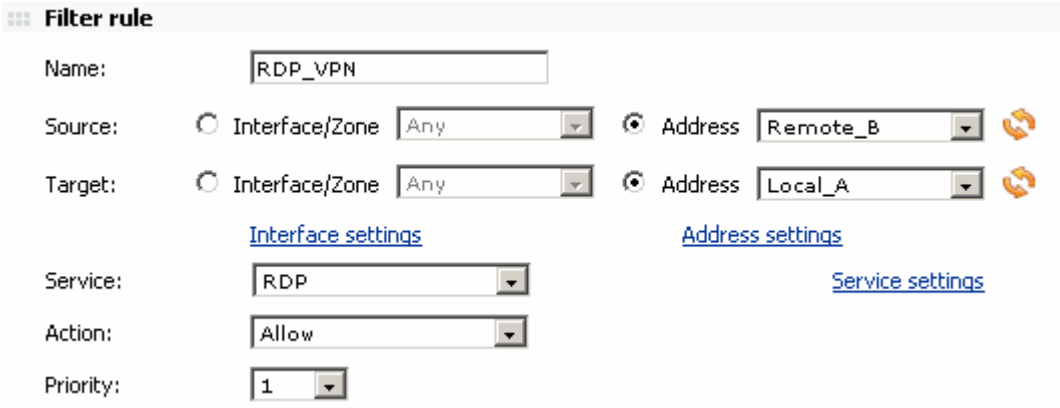
Si se desea acceder vía RDP del host de la red B al host de la red A, habría que cambiar el origen y el destino de los paquetes respecto del caso anterior:

Solución:

Firewall de Integra B:

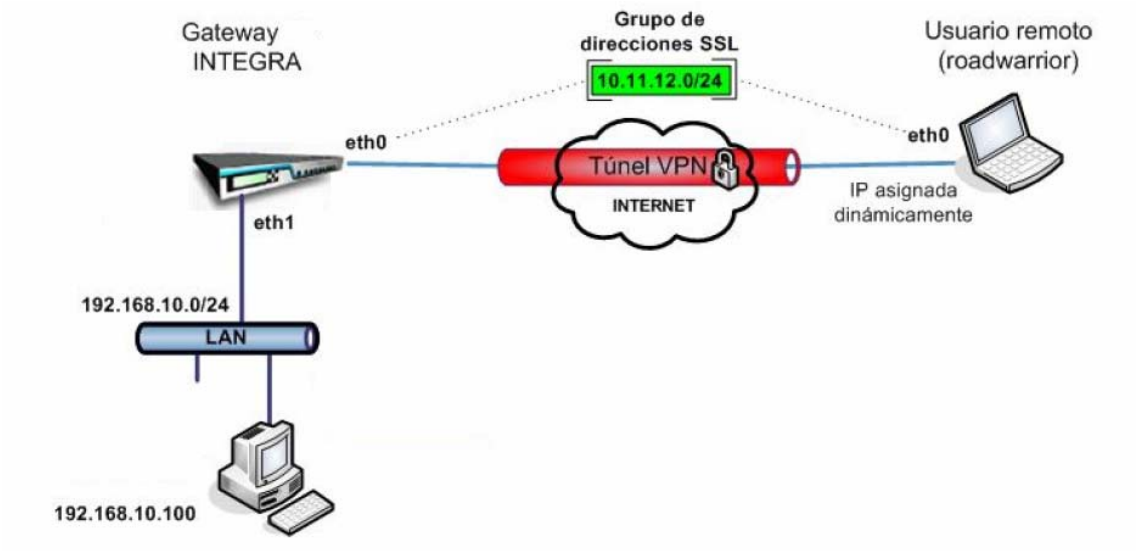


Firewall de Integra A:



Índice

2.4.2 Gateway-to-Roadwarrior



Sea el escenario de la figura, en el que hay una unidad de Panda GateDefender Integra que actúa como servidor VPN para clientes remotos (roadwarriors) entre los que se acaba de establecer un túnel SSL.

El grupo de direcciones SSL (ver la figura) se utilizará para asignar direcciones IP virtuales a los diferentes roadwarriors que se conecten al servidor. Estas direcciones IP, serán las que utilicen en la LAN local del servidor VPN.

Nota: Para verificar qué dirección IP se le ha asignado a cada roadwarrior se puede acceder al **submenú Monitor VPN** desde el **menú VPN** de la consola web.

Para simplificar la gestión de las reglas del firewall, desde el **menú Definiciones** de Integra se definen los siguientes grupos de direcciones:

- Virtual_SSL= 10.11.12.0/24
- Local=192.168.10.0/24

Si se quiere permitir que el roadwarrior una vez que haya establecido el túnel VPN con el servidor VPN SSL, pueda acceder a la red local con determinados servicios, es necesario configurar las políticas de seguridad en Integra como se muestra a continuación:

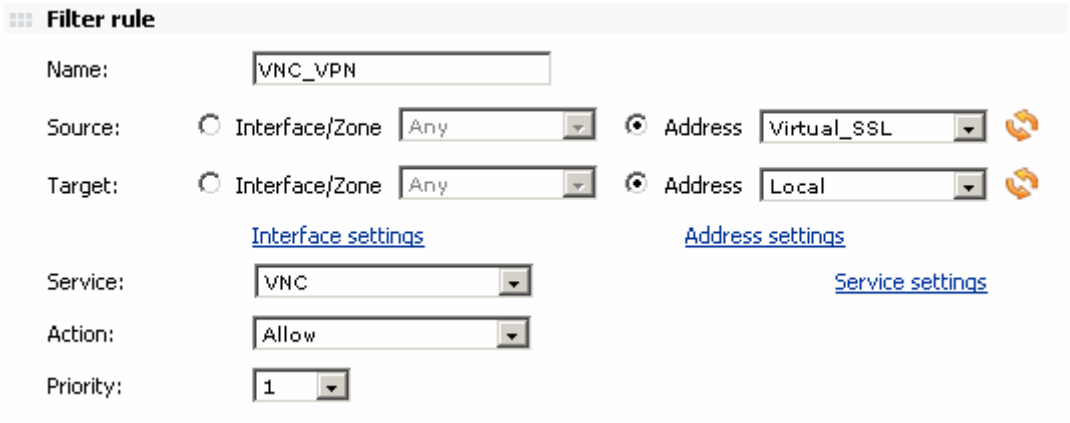
> Integra: **Permitir** el tráfico desde el **origen** *roadwarrior* al **destino** *Lan* para aquellos servicios que se desee.

Nota: No es necesario habilitar una regla explícita en el firewall para permitir las respuestas a las sesiones ya establecidas con las reglas de filtrado inversas ya que Integra ya dispone de la opción interna de seguimiento de conexiones (Connection tracking) que se encarga de ello.

Ejemplo: ¿Qué reglas habría que añadir en el firewall de Integra para que el roadwarrior pueda acceder por VNC (TCP 5900) a la red local de Integra?

Solución:

Firewall de Integra:



Índice