Panda GateDefender Integra

Configurar SNAT

Casos de uso para configurar SNAT con GateDefender Integra

Panda Software 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 www.pandasoftware.es/productos y www.pandasoftware.es/soporte para más información.

D.L. BI-3269-05

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.

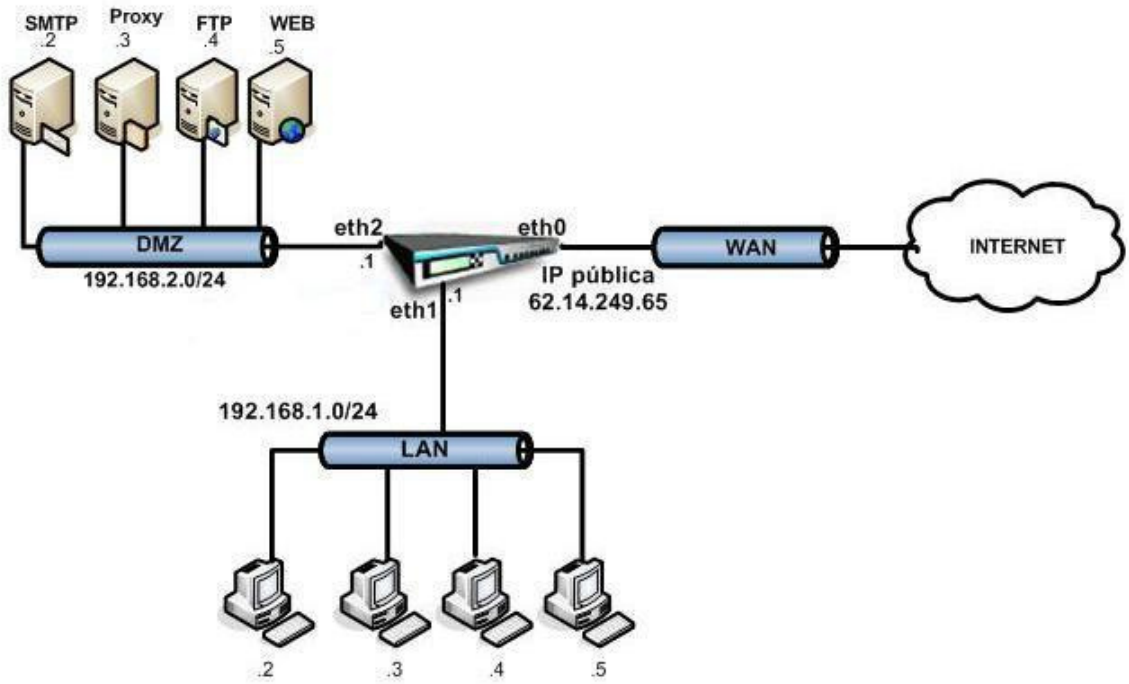
Tipos de letra utilizados en esta documentación:

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.

Introducción

A continuación se explica cómo se debe proceder en Panda GateDefender Integra para configurar SNAT correctamente.

En todo el documento, se tomará como referencia la red que se muestra a continuación:



En esta simulación se ha colocado una unidad de Panda GateDefender Integra en el perímetro de la red para realizar las funciones de Firewall corporativo (además del módulo Firewall podría estar activado cualquier otro módulo).

En este contexto, Integra se ha configurado con 3 interfaces: Eth0 para la zona WAN, Eth1 para la LAN, y Eth2 para la DMZ.

En la DMZ se han colocado los servidores corporativos.

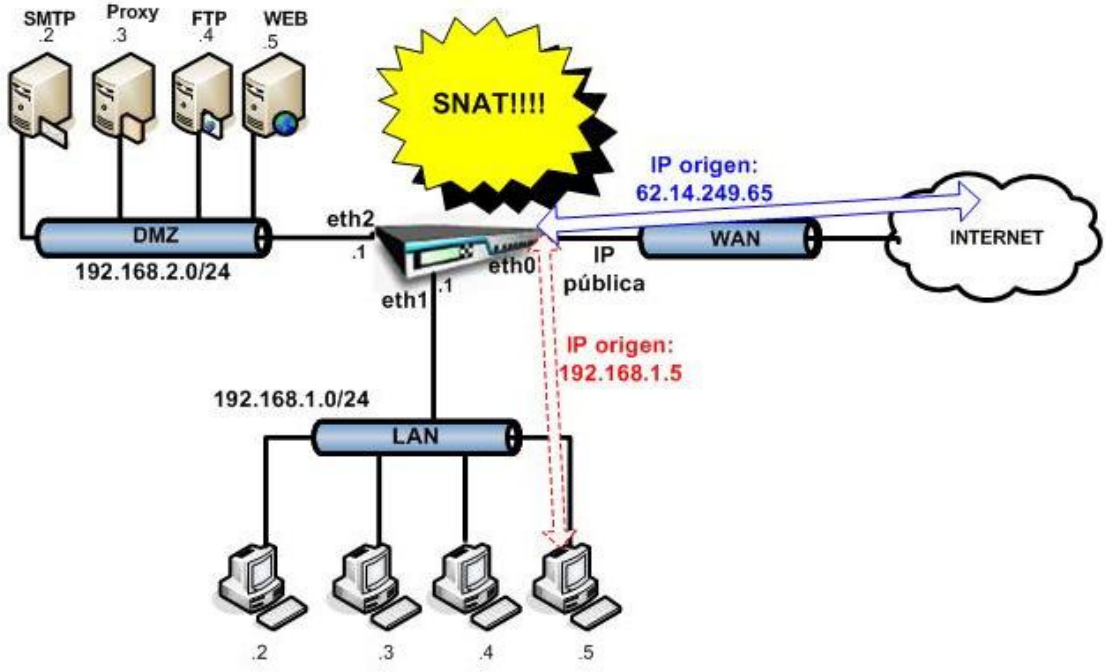
En la figura se aprecia como al interfaz Eth0 se le ha asignado una dirección IP pública. Habitualmente, en las configuraciones reales más comunes, el interfaz WAN tendrá asignada una dirección IP privada, y será otro dispositivo adicional el que le proporcione los servicios WAN, como por ejemplo un router ADSL, un cable módem, etc, el cual dispondrá de una dirección IP pública (dinámica o estática) que normalmente* hará NAT *automáticamente la dirección privada del interfaz WAN de Integra hacia Internet.

Esta aproximación se ha llevado a cabo para que el procedimiento se simplifique y sea más intuitivo.

En caso de que la unidad de Panda GateDefender Integra se dedique únicamente a enrutar tráfico (modo de funcionamiento Router), sin realizar ninguna configuración adicional, todo el tráfico que pase desde la LAN o desde la DMZ a la zona WAN que sea permitido por las políticas del firewall en caso de estar activado, tendrá asignado en el campo IP origen, una dirección IP privada perteneciente a estas zonas, y no podrá llegar a Internet al no usar una dirección IP pública válida.

Para que los dispositivos situados en la red interna (LAN o DMZ) de esta compañía puedan salir a Internet, se puede usar la función SNAT incorporada en el módulo Firewall.

A continuación se muestra cómo introducir una regla SNAT que permita a los usuarios de la LAN salir a Internet usando la dirección IP pública asignada al interfaz WAN:



Con la regla que se va a introducir, el host 192.168.1.5 de la LAN saldrá a Internet llevando en el encabezado de sus paquetes la dirección 62.14.249.65, dirección IP pública asignada al interfaz WAN, y válida en Internet.

1 Procedimiento

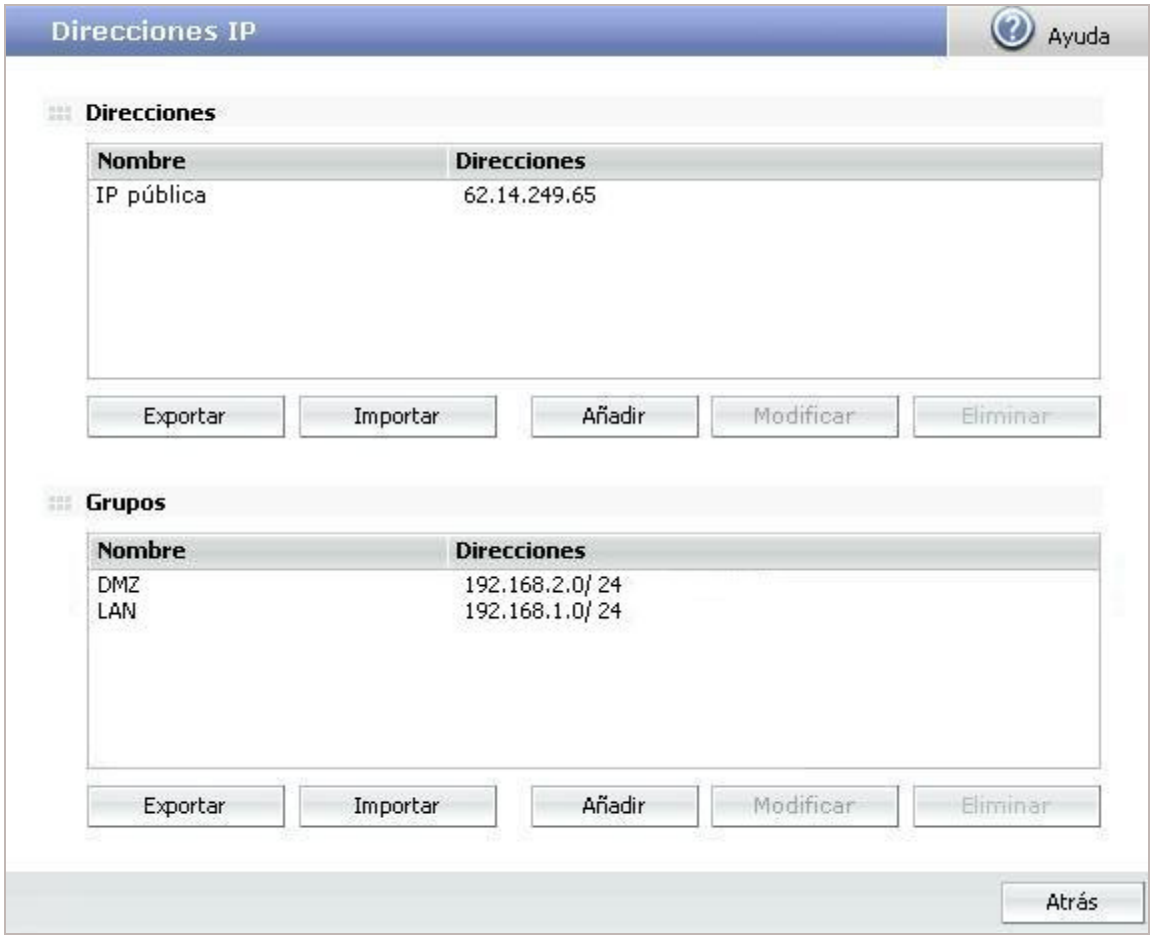
El primer factor a tener en cuenta es que NAT (SNAT/DNAT) no se activa por defecto cuando Integra funciona en modo Router. En este modo de funcionamiento, Integra simplemente enruta tráfico.

Para activar SNAT, se debe configurar el firewall con reglas SNAT, que son reglas diferentes de las reglas de filtrado.

Al igual que si se introdujeran reglas de filtrado, se puede llevar a cabo una configuración previa de direcciones IP y redes desde el menú **Definiciones de direcciones IP** para simplificar la gestión de las reglas.

Por lo tanto, como primer paso, y siguiendo el esquema marcado:

1. Se introducen definiciones de redes que pueden ser útiles a la hora de configurar las reglas.



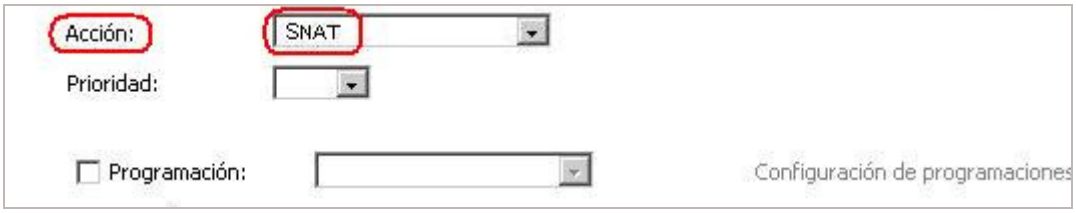
.

En este caso, se definen los rangos de redes LAN y DMZ así como la dirección IP pública asignada al interfaz WAN.

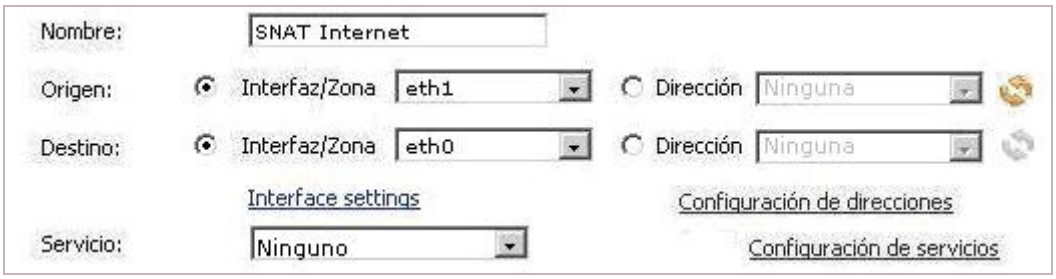
Nota: Este paso no es obligatorio - se pueden introducir las direcciones sin haberlas definido previamente, aunque en caso de introducir muchas reglas, se simplifica el trabajo.

2. Se añade una nueva regla:

La acción que se debe seleccionar es SNAT:



3. A continuación se configuran el resto de los parámetros:



- Se asigna un nombre cualquiera a la regla.
- Se eligen las propiedades origen y destino de los paquetes que se vayan a hacer NAT. Esta elección se puede hacer de diferentes formas: por interfaz, por zona o por dirección IP. En este caso, se quiere hacer NAT el tráfico que venga de la LAN (interfaz eth1) y vaya destinado a Internet (interfaz eth0).
- Se eligen los servicios a los que se quiere aplicar la regla SNAT. En este caso se quiere hacer SNAT de cualquier tipo de tráfico.

Los parámetros que vienen a continuación, le indican a Panda GateDefender Integra cual es la dirección IP o direcciones IP que tiene que usar en la traslación de direcciones:

En este caso, sólo se dispone de una dirección IP en la pata WAN que se ha definido como Public IP (dirección IP pública), y que se utilizará para hacer NAT de todas las peticiones que lleguen desde cualquier dispositivo de la LAN.

Si se selecciona la opción **Keep original address**, se aplicará una regla de SNAT, pero no se le modificará la dirección IP origen del paquete. Esto puede ser útil en algunas situaciones especiales, como por ejemplo a la hora de configurar una VPN IPSEC en un entorno de NAT.

El campo **Address group** se utilizará en caso de tener varias direcciones para hacer el cambio de encabezado origen en vez de una sola.

Desde aquí, también se puede introducir directamente la prioridad que se va a asignar a la nueva regla introducida y que además refleja la prioridad de la regla dentro del conjunto de reglas SNAT.
Si no se modifica este campo, la regla se colocará al final de la última regla SNAT existente.

Por último, sólo quedarían parámetros opcionales en los que se puede configurar la regla para que funcione a unas horas determinadas, o la opción de logear todo paquete sobre el que se realice el SNAT con las características de esta regla.

Una vez se haya añadido la regla, se refleja en consola, en el grupo de reglas SNAT (después de las reglas de filtrado):

Reglas de filtrado

Activa	Nombre	Fuente	Destino	Programación	Servicio	Acción
☑	PING	Todas	Todas	Ninguna	PING	Permitir
☑	TELNETegress	Todas	WAN	Ninguna	Telnet	Permitir
☑	FTPegress	Todas	WAN	Ninguna	FTP	Permitir
☑	HTTPegress	Todas	WAN	Ninguna	HTTP	Permitir
☑	HTTPSegress	Todas	WAN	Ninguna	HTTPS	Permitir
☑	SMTPegress	Todas	WAN	Ninguna	SMTP	Permitir
☑	DNSegress	Todas	WAN	Ninguna	DNS	Permitir
☑	POP3egress	Todas	WAN	Ninguna	POP3	Permitir
☑	IMAPegress	Todas	WAN	Ninguna	IMAP	Permitir
☑	EgressProh...	Todas	WAN	Ninguna	Todas	Denegar
☑	DENY	Todas	Todas	Ninguna	Todas	Denegar
☑	SNAT Internet	eth1	eth0	Ninguna	Todas	SNAT

2 Problemas más comunes

Uno de los problemas más comunes que se pueden presentar a la hora de configurar SNAT es el bloqueo del tráfico SNAT por las propias reglas de filtrado del firewall. Por lo tanto, además de la regla de SNAT, será necesario asegurarse de que las reglas del firewall permiten la salida de ese tráfico.

Por ejemplo, en el conjunto de reglas que se muestran a continuación, existe una regla de SNAT que se va a aplicar a todo el tráfico que va de la LAN a la WAN:

Activa	Nombre	Fuente	Destino	Programación	Servicio	Acción
☑	PING	Todas	Todas	Ninguna	PING	Permitir
☑	TELNETegress	Todas	WAN	Ninguna	Telnet	Permitir
☑	FTPegress	Todas	WAN	Ninguna	FTP	Denegar
☑	HTTPegress	Todas	WAN	Ninguna	HTTP	Permitir
☑	HTTPSegress	Todas	WAN	Ninguna	HTTPS	Permitir
☑	SMTPegress	Todas	WAN	Ninguna	SMTP	Permitir
☑	DNSegress	Todas	WAN	Ninguna	DNS	Permitir
☑	POP3egress	Todas	WAN	Ninguna	POP3	Permitir
☑	IMAPegress	Todas	WAN	Ninguna	IMAP	Permitir
☑	EgressProh...	Todas	WAN	Ninguna	Todas	Denegar
☑	DENY	Todas	Todas	Ninguna	Todas	Denegar
☑	SNAT Internet	eth1	eth0	Ninguna	Todas	SNAT

En este caso, aquellos equipos que van a hacer uso del servicio SNAT desde la LAN, podrán acceder a Internet sin problemas usando sus navegadores en el protocolo HTTP, pero sin embargo, a pesar de la regla SNAT, no podrán usar tráfico FTP hacia Internet ya que hay una regla de filtrado que lo está impidiendo.

Una configuración que se debe evitar, ya que puede generar problemas de tráfico mal "nateado" consiste en utilizar, tanto en el campo origen como en el campo destino, la opción **Cualquiera** a la hora de crear una regla de SNAT.

0906-PGDIHT02-01-SP