Panda GateDefender Integra

Configurar DNAT para publicar los servicios internos hacia Internet

Casos de uso para configurar DNAT 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.

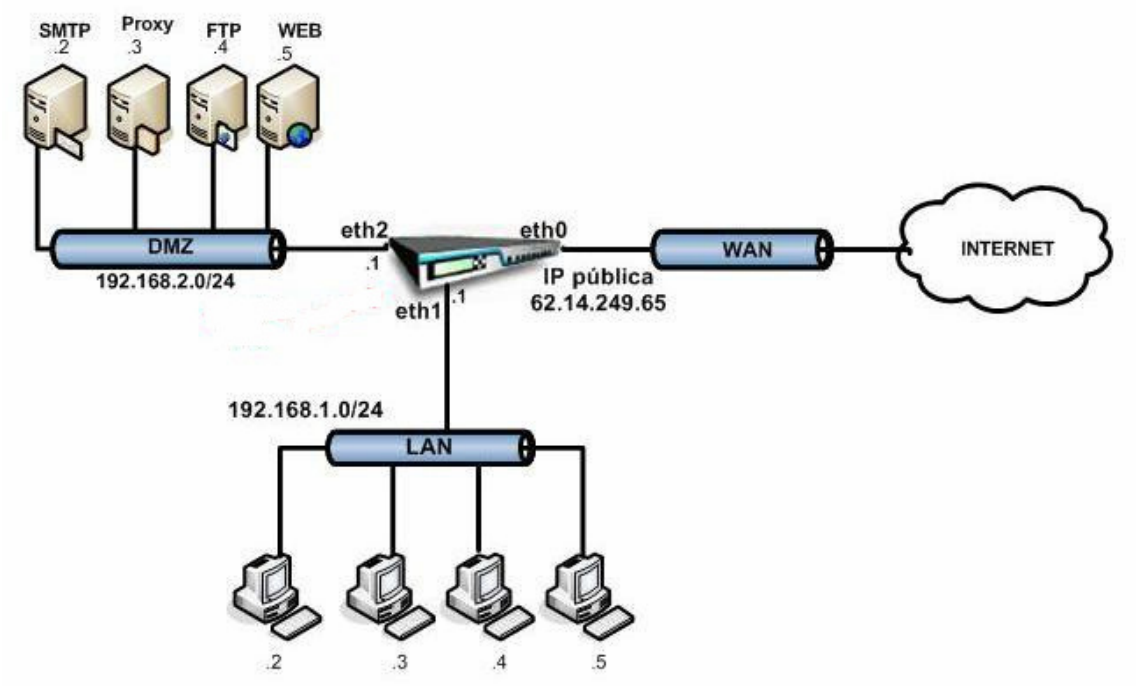
Tipos de letra utilizados en esta documentación:

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.

1 Introducción

A continuación se explica cómo se debe proceder en Panda GateDefender Integra para realizar una configuración correcta de DNAT y poder así publicar los servicios internos hacia Internet.

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 un Firewall corporativo (además del módulo Firewall podría estar activado también 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 con la dirección privada del interfaz WAN de Integra hacia Internet.

Esta aproximación se ha llevado a cabo para simplificar el caso de uso (how-to) y hacerlo más intuitivo.

Se da por supuesto que Integra ya ha sido configurado con reglas de SNAT, por lo que tanto la LAN como la DMZ son transparentes más allá del interfaz wan de Integra, cuya dirección IP es la única "representante" de la red que protege a Panda GateDefender Integra.

Es decir, la única forma de llegar tanto a Integra como a sus redes internas (LAN y DMZ en este caso) es a través de la dirección IP pública asignada a la máquina.

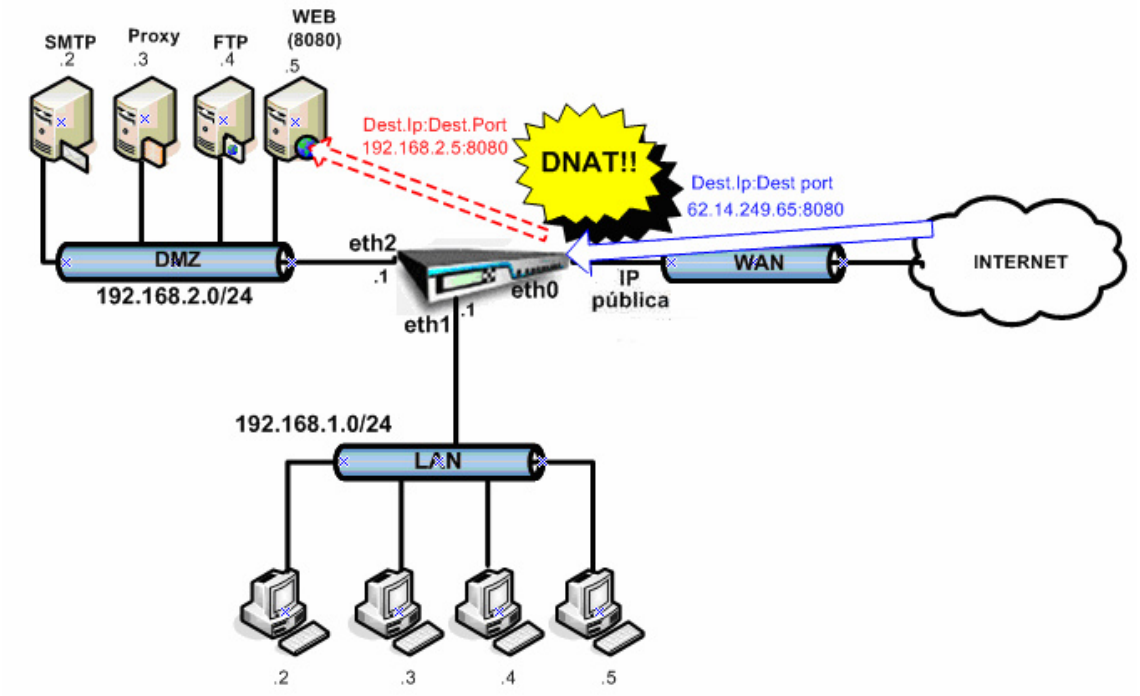
Como las redes internas están “ocultas”, para poder alcanzar los servidores de la DMZ en caso de querer hacer públicos sus servicios, es necesario realizar una configuración avanzada y añadir reglas DNAT; esta acción es denominada también como Port Forwarding.

A continuación se muestran varios escenarios diferentes y se explica cómo llevar a cabo las configuraciones necesarias para hacer públicos los servicios ofrecidos por los servidores de la DMZ.

2 Procedimiento

2.1 Ejemplo 1

Como se muestra en el siguiente escenario, el servidor web de la DMZ está ofreciendo sus servicios en el puerto 8080:



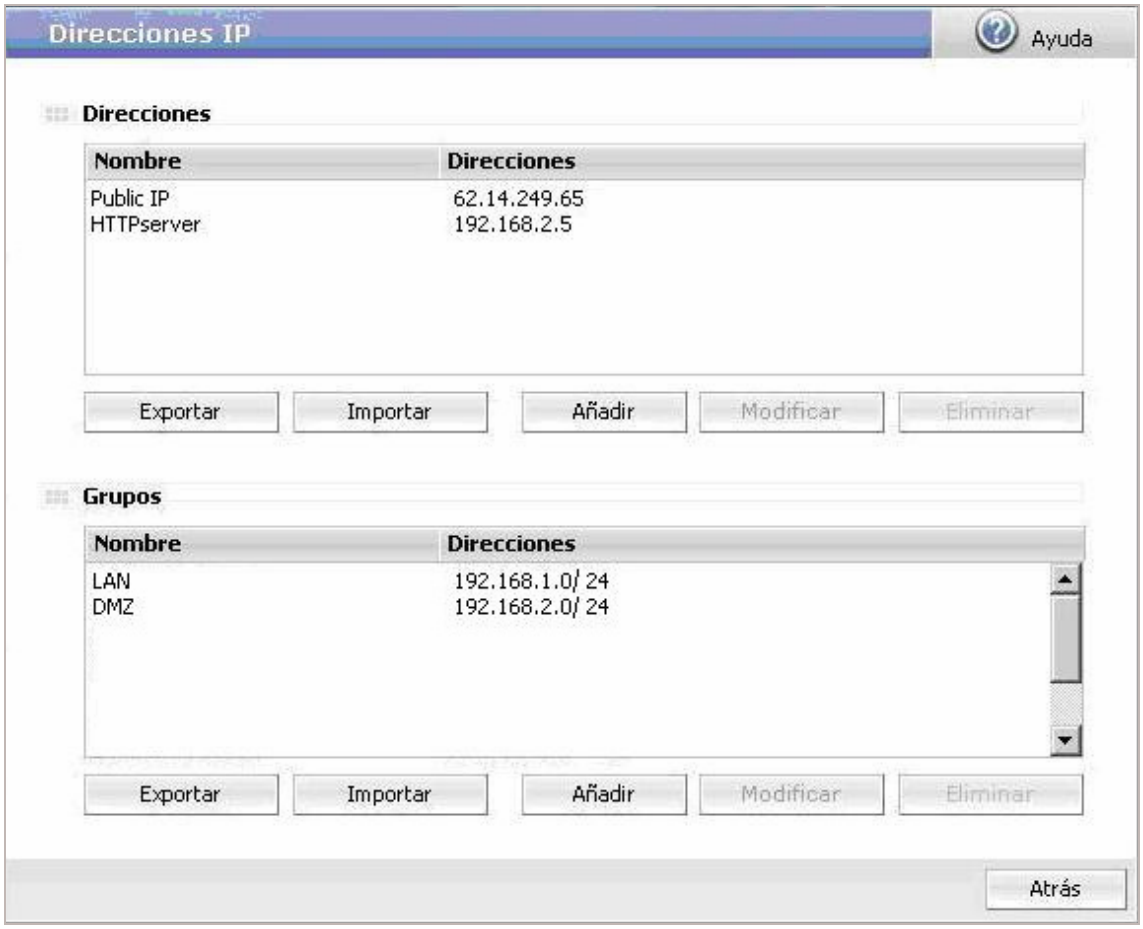
Para poder alcanzar desde Internet este servicio oculto tras el firewall de Integra, se puede hacer un mapeo estático de tal forma que el tráfico que llegue al puerto WAN de Integra por el puerto 8080 sea redirigido al servidor interno WEB en el mismo puerto.

Con esta configuración, las peticiones a la dirección IP pública de Integra por el puerto 8080 pasarán a través de Integra, que cambiará la dirección IP destino por la dirección IP privada del servidor web en la DMZ.

Para ello, será necesario añadir una regla DNAT en el firewall.

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

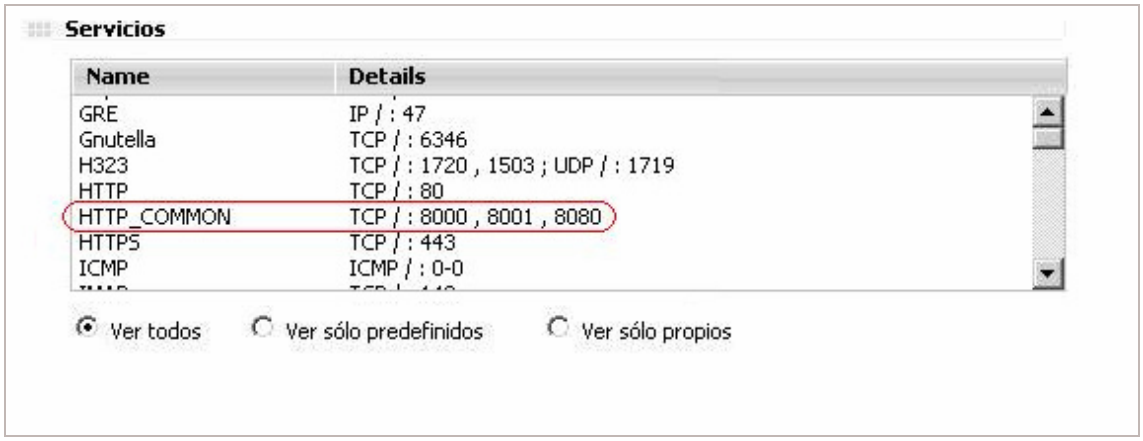
1. Se introducen algunas definiciones de redes que pueden ser útiles a la hora de configurar las reglas.



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 simplifica el trabajo a la hora de introducir gran cantidad de reglas.

2. Se define el servicio que se va a mapear. En este caso no sería necesario añadir uno nuevo, ya que HTTP en el puerto 8080 ya existe en los servicios predefinidos por defecto:



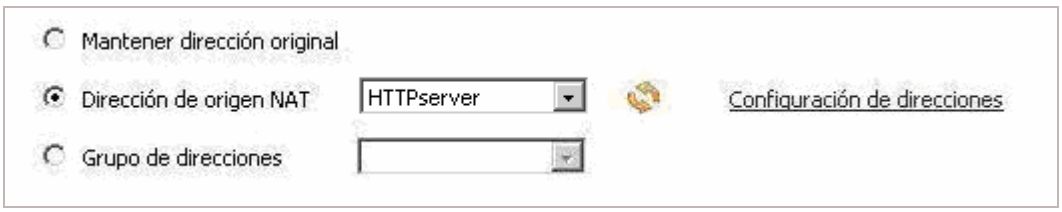
3. Se añade la regla DNAT que mapee al servidor web interno el tráfico HTTP por el puerto 8080 que se reciba:

   Se elige la acción como DNAT, la cual crea la regla DNAT:

   Se le asigna un nombre, y se definen las características del tráfico que va a estar afectado por esta regla:

   - Se va a aplicar al tráfico cuyo origen sea cualquiera, ya que se desconoce el origen de las peticiones que vengan de Internet.
   - Como destino se debe colocar la dirección IP del interfaz que va a recoger el tráfico, en este caso el interfaz web que tiene asignada la dirección IP pública.
   - El servicio para el que se va a aplicar esta regla en este caso es HTTP_COMMON, definido por defecto y que incluye tráfico HTTP por el puerto 8080.

4. Se definen los parámetros del destino final del mapeo estático:



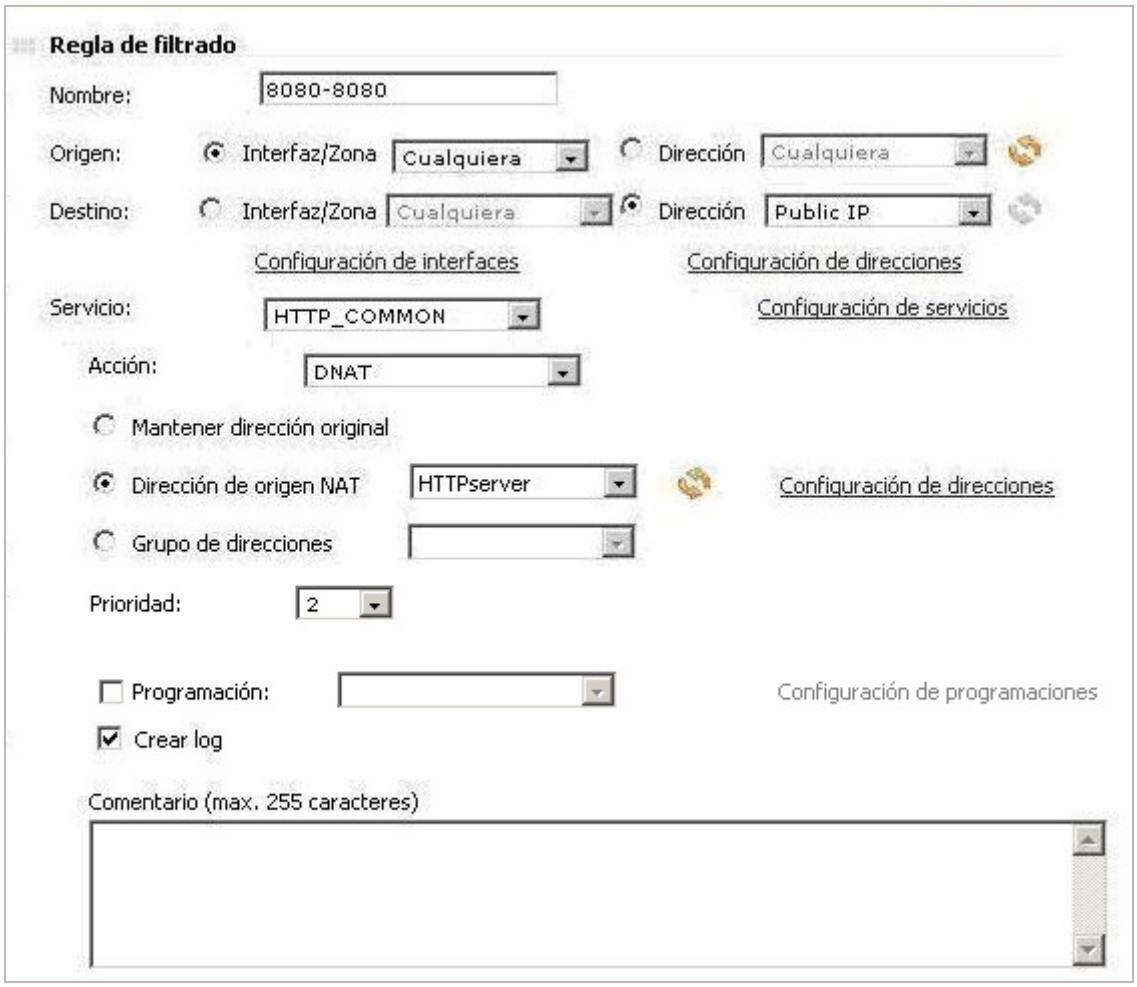
   En el campo NAT target address, se debe introducir el servidor destino de la petición HTTP. En este caso, se puede hacer caso de la definición que se ha introducido para el servidor web de la DMZ, en vez de introducir la dirección IP directamente.

   Si se marca el campo **Keep original address**, el encabezado destino no se cambiaría. Este caso puede ser usado en situaciones especiales.

   La opción Target port en este caso no es necesaria ya que el puerto destino no va a cambiar.

5. Se definen el resto de los parámetros opcionales de registro de información, planificación de la regla, etc.

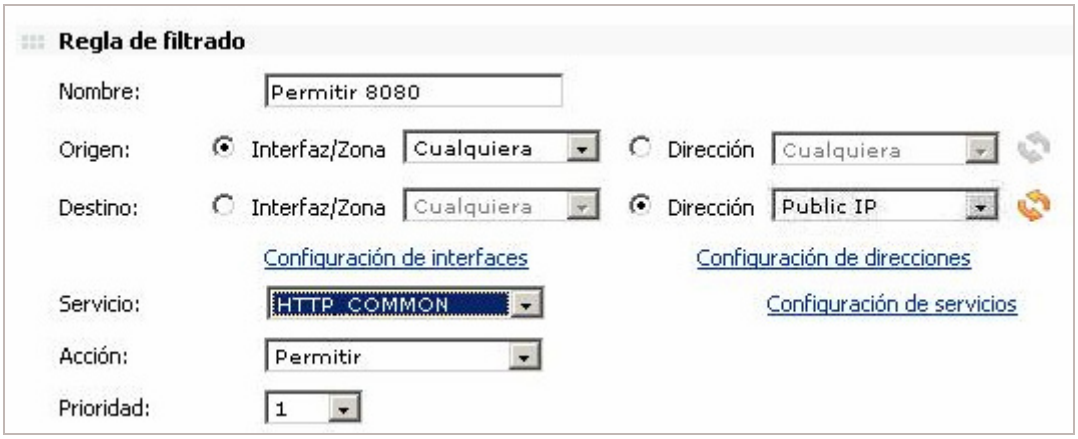
   Una vez definidos todos los parámetros, la regla quedaría como se muestra a continuación:



Una vez introducida la regla DNAT, es necesario que el tráfico que va a ser redirigido no sea bloqueado por las reglas de filtrado del Firewall.

En este caso, las reglas por defecto bloquearían la entrada de este tráfico HTTP por el puerto 8080, por lo que será necesaria una regla que permita este tráfico.

Para ello, se debe crear una regla de filtrado como la que se muestra a continuación:



Esta regla permite el tráfico que venga de cualquier origen, destinado a la dirección IP pública asignada en el interfaz web, y cuyos puertos destino sean aquellos incluidos en el servicio definido como HTTP_common, entre los que se incluye el 8080.

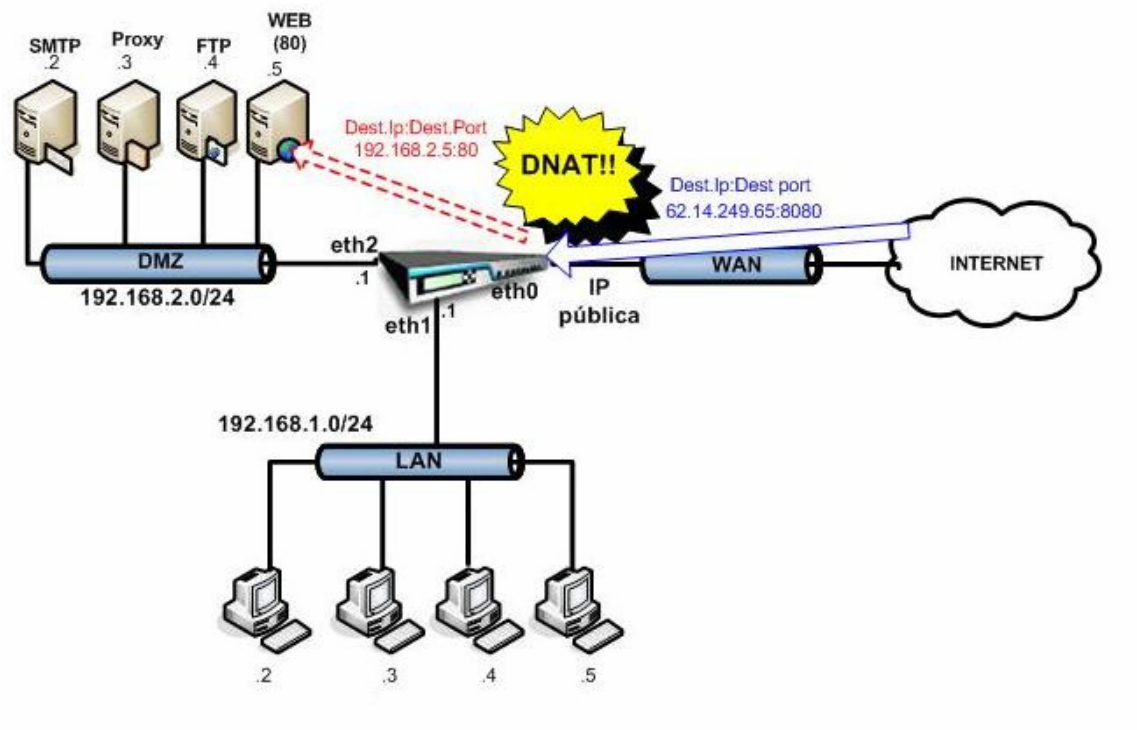
Estas reglas de filtrado, junto con la regla DNAT definida, se encargarán de re-direccionar el tráfico por el puerto 8080 que llegue a Integra por su interfaz WAN hacia el servidor Web en la DMZ:

Reglas de filtrado

Activa	Nombre	Fuente	Destino	Programación	Servicio	Acción
☑	8080-8080	Todas	Public IP	Ninguna	HTTP_C...	DNAT
☑	Permitir 8080	Todas	Public IP	Ninguna	HTTP_C...	Permitir
☑	FTPegress	Todas	Todas	Ninguna	FTP	Permitir
☑	SSH	Todas	Todas	Ninguna	Todas	Permitir
☑	HTTPegress	Todas	WAN	Ninguna	HTTP	Permitir
☑	Syslog	LAN	WAN	Ninguna	Syslog	Permitir
☑	HTTPSegress	Todas	WAN	Ninguna	HTTPS	Permitir
☑	SMTPegress	Todas	WAN	Ninguna	SMTP	Permitir
☑	DNSegress	Todas	Todas	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

2.2 Ejemplo 2

En este caso se va a proceder como en el ejemplo 1, con la diferencia de que el servidor web ofrece sus servicios por el puerto 80, aunque públicamente se siguen ofreciendo en el 8080. En este caso, además de cambiar la dirección IP destino, habrá que cambiar el puerto destino del 8080 al 80.

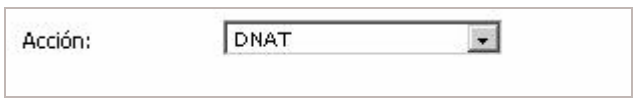


Para ello será necesario añadir una regla DNAT en el firewall.

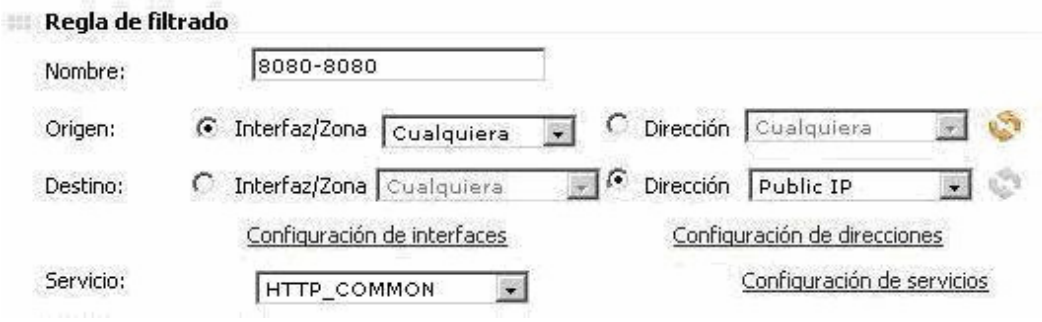
Por lo tanto, como primer paso, y siguiendo el esquema marcado:

1. Se introducen las mismas definiciones de redes y servicios que en el ejemplo 1.
2. Se añade la regla DNAT que mapee al servidor web interno el tráfico HTTP por el puerto 8080 que se reciba:

   Se elige la acción como DNAT, la cual crea la regla DNAT:

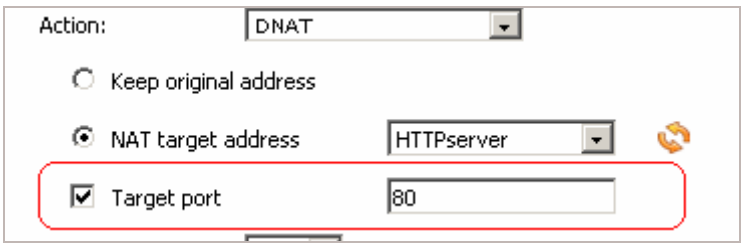


   Se le asigna un nombre, y se definen las características del tráfico que va a estar afectado por esta regla:



- Se va a aplicar al tráfico cuyo origen sea cualquiera, ya que se desconoce el origen de las peticiones que vengan de Internet.
- Como destino se debe colocar la dirección IP del interfaz que va a recoger el tráfico, en este caso el interfaz web que tiene asignada la dirección IP pública.
- El servicio para el que se va a aplicar esta regla es en este caso HTTP_COMMON, definido por defecto y que incluye tráfico HTTP por el puerto 8080.

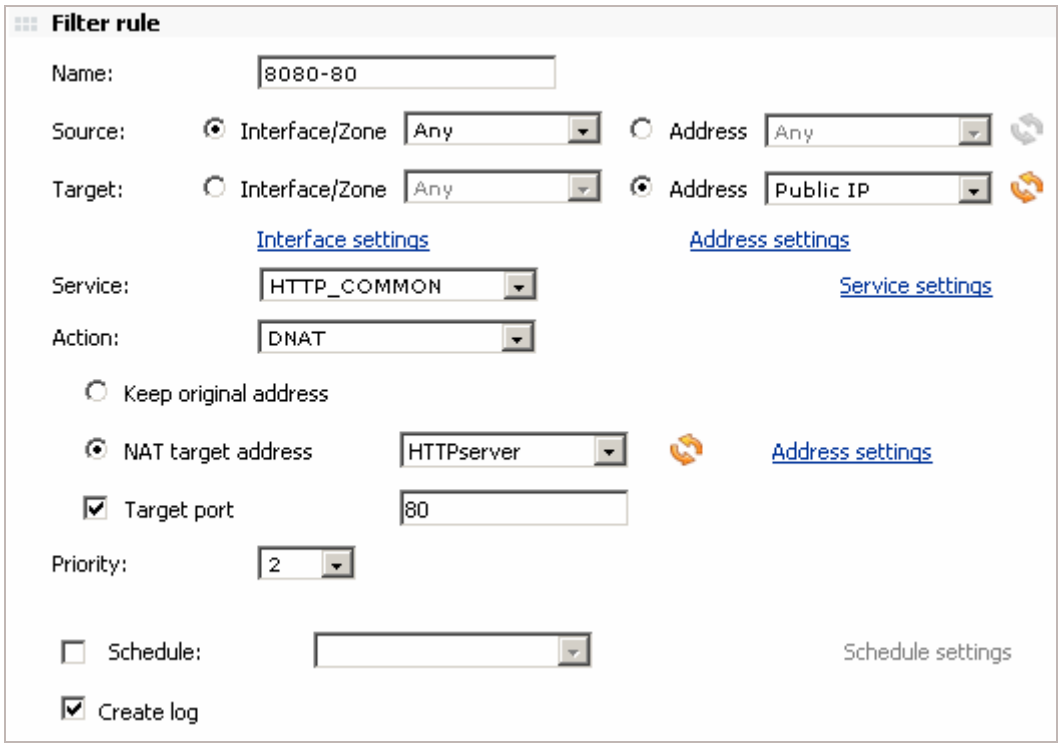
3. Se definen los parámetros del destino final del mapeo estático:



En este caso, como también se desea cambiar el puerto destino, se debe activar **Target port** e incluir el puerto destino real en el que está escuchando el servidor, en este caso el 80.

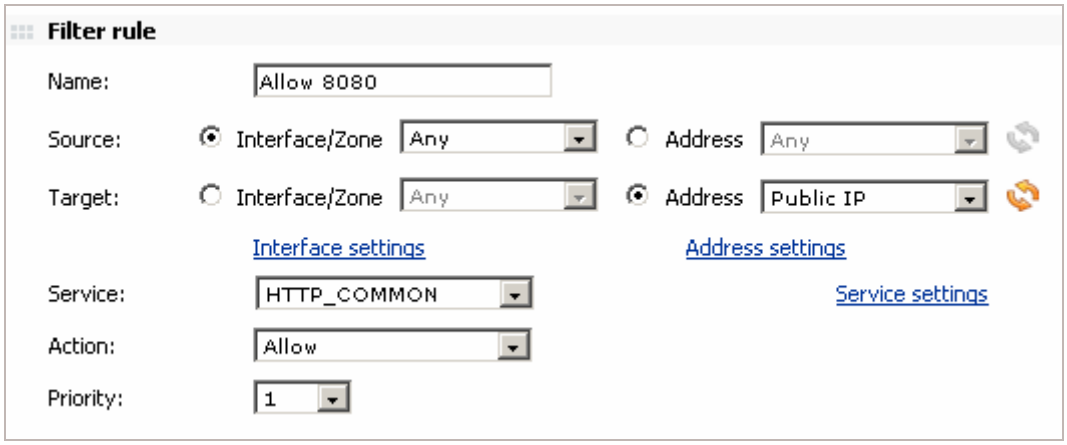
4. Se definen el resto de los parámetros opcionales de registro de información, planificación de la regla, etc.

Una vez definidos todos los parámetros, la regla quedaría como se muestra a continuación:



Al igual que en el caso anterior, las reglas de filtrado no deben bloquear el tráfico que vaya a ser redirigido.

Para ello, se debe crear una regla de filtrado como la que se muestra a continuación:



Esta regla permite el tráfico que venga de cualquier origen, destinado a la dirección IP pública asignada en el interfaz web, y cuyos puertos destino sean aquellos incluidos en el servicio definido como HTTP_common, entre los que se incluye el 8080.

Estas reglas de filtrado, junto con la regla DNAT definida, se encargarán de re-direccionar el tráfico por el puerto 8080 que llegue a Integra por su interfaz WAN hacia el servidor Web en la DMZ en el puerto 80.

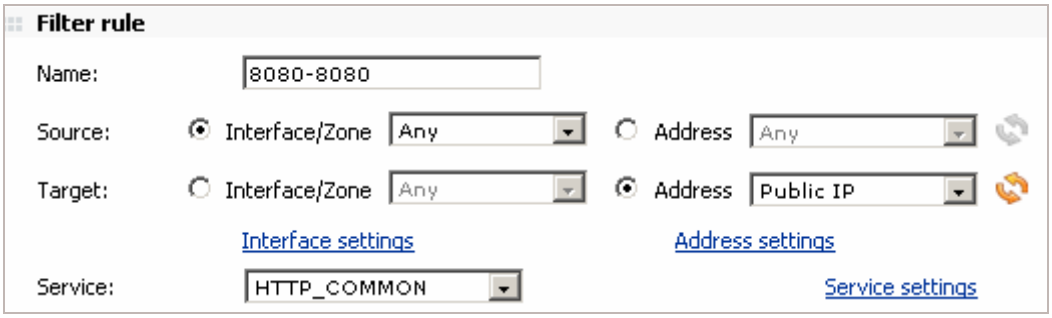
Filtering rules

Active	Name	Source	Target	Schedule	Service	Action
☑	8080-80	All	Public IP	None	HTTP_C...	DNAT
☑	Allow 8080	All	Public IP	None	HTTP_C...	Allow
☑	PING	All	All	None	ICMP	Allow
☑	TELNETegress	All	WAN	None	Telnet	Allow
☑	FTPegress	All	WAN	None	FTP	Allow
☑	HTTPegress	All	WAN	None	HTTP	Allow
☑	HTTPSegress	All	WAN	None	HTTPS	Allow
☑	SMTPegress	All	WAN	None	SMTP	Allow
☑	DNSegress	All	WAN	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

3 Problemas más comunes

Uno de los problemas más comunes que se pueden dar a la hora de configurar DNAT es el bloqueo del tráfico que vaya a ser redirigido hacia dentro por las propias reglas de filtrado del firewall. Por lo tanto, además de la regla de DNAT, será necesario asegurarse de que las reglas del firewall permiten la recepción y tratamiento de ese tráfico.

Otro de los problemas habituales que se pueden encontrar es la definición errónea de los parámetros que definen el tráfico sobre el que va a aplicar la regla DNAT. Es necesario asegurarse que en el campo IP destino, se hace referencia al interfaz sobre el que se va a recoger el tráfico a redireccionar; en los ejemplos anteriores la dirección IP pública de Integra que hace referencia al interfaz es eth0.



0906-PGDIHT03-01-SP