# NAT Y FIREWALLS

## NATP

El Funcionamiento del NAT (Network Address Translation) es esencialmente un proceso mediante el cual los dispositivos de red modifican la información de direccionamiento en los paquetes IP mientras se transmiten a través de una interfaz de red. El NAT se utiliza comúnmente en enrutadores y cortafuegos para permitir que múltiples dispositivos en una red privada utilicen una sola dirección IP pública para acceder a Internet.

El NAT es una herramienta clave para permitir la comunicación entre la red interna y la red externa (Internet) utilizando una única dirección IP pública. El proceso de NAT se lleva a cabo en el enrutador o cortafuegos que conecta la red interna con Internet. A continuación, se detalla el funcionamiento del NAT:

1. Determinación de la interfaz de origen y destino: Cuando un paquete sale de la red interna hacia Internet, el enrutador identifica la interfaz de salida (interna) y la interfaz de entrada (externa) del paquete.

2. Traducción de direcciones IP: El enrutador reemplaza la dirección IP de origen del paquete con su propia dirección IP pública asignada por el ISP. Esto oculta las direcciones IP internas de los dispositivos de la red interna y evita que se expongan a Internet.

3. Mapeo de puertos (Port Address Translation - PAT): Además de traducir las direcciones IP, el enrutador también asigna un número de puerto único a cada conexión saliente. Esto permite que múltiples dispositivos en la red interna compartan la misma dirección IP pública, ya que el enrutador puede identificar el dispositivo correcto en función del número de puerto asignado.

4. Seguimiento de la tabla de traducción: El enrutador mantiene una tabla de traducción NAT que asocia las direcciones IP y los números de puerto internos con las direcciones IP y los números de puerto externos.

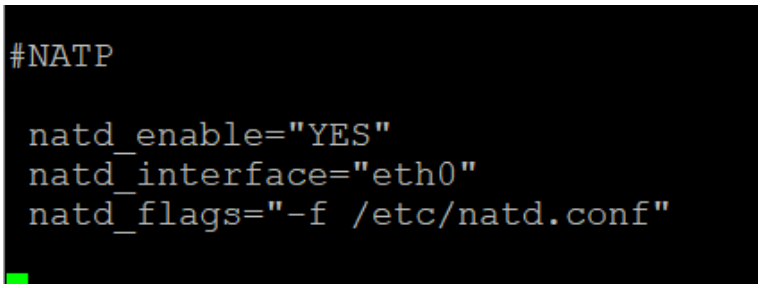
5. Envío del paquete hacia Internet: Una vez que se ha traducido la dirección IP y el número de puerto, el paquete se envía a través de la interfaz externa hacia Internet.

6. Recepción de la respuesta: Cuando llega una respuesta desde Internet, el enrutador utiliza la tabla de traducción NAT para determinar a qué dispositivo de la red interna debe enviar la respuesta. Luego, realiza la traducción inversa de la dirección IP y el número de puerto para que la respuesta pueda ser entregada al dispositivo correcto en la red interna.

**Tareas**

**Tarea 1**

1. Crear el archivo de configuración /etc/natd.conf (actualmente vacío).
2. En /etc/rc.conf




3. service natd restart

**Tarea 2:**

1. Abre o crea el archivo de reglas de firewall /usr/local/etc/ipfw.conf **:**

add divert natd all from any to any

2. Guarda y cierra el archivo **/etc/ipfw.rules**.

service natd restart

**Tarea 3:**

1. Abre y añade en el archivo de reglas de firewall /usr/local/etc/ipfw.conf **:**

add divert natd tcp from any to any 22005 via interfaz_pública
add divert natd tcp from any to any 22006 via interfaz_pública
add divert natd tcp from any to any 22007 via interfaz_pública
add divert natd tcp from any to any 22008 via interfaz_pública
add divert natd tcp from any to any 22009 via interfaz_pública

2. service ipfw restart

Con estos pasos, habrás configurado correctamente **natd** para la traducción de direcciones y puertos, preparado **ipfw** en una configuración básica y realizado redirecciones de puertos según las especificaciones de las tareas.

```
add allow tcp from 10.48.0.0/23 to 172.23.18.0/24 53 setup keep-state
add allow tcp from 10.48.0.0/23 to 172.23.18.0/24 80 setup keep-state
add allow tcp from 10.48.0.0/23 to 172.23.18.0/24 443 setup keep-state

#Permitir trafico ICMP
add allow icmp from any to any

#Permitir acceso ssh desde la red punlica y el propio cortafuegos a maquina de >
add allow tcp from 10.48.0.0/23 to 172.23.18.0/24 22 setup keep-stat #SSH
add allow tcp from any to 172.23.18.0/24 123 setup keep-state #SSh desde cortaf>

#Activar NAT
add divert 8668 ip from any to any via eth0

# Log del trafico relevante
add allow tcp from 172.23.18.0/24 to 10.48.0.0/23 22 setup keep-state
add log tcp from 10.48.0.0/23 to 172.23.18.0/24 22 setup keep-state
```

**Preguntas de examen**

**NAT**

Sobre NAPT:

a) ¿Debe tener lugar en la interfaz de salida, de entrada, o en ambas? (NOTA: esta se anuló debido a cierta ambigüedad: aunque generalmente lo denominamos “salida” a Internet --desde el punto de vista de la organización--, sería más adecuado indicar interfaz externa, interna o ambas. Toda la puntuación va a la cuestión 2, pues incluye en cierta forma ésta.)

b) En el tráfico saliente, ¿afecta a las direcciones y puertos origen, destino o ambos?

Direcciones y puertos origen.

a) ¿Debe tener lugar en la interfaz externa, interna o en ambas?

En el contexto de NAPT, la traducción de direcciones y puertos generalmente ocurre en la interfaz externa del firewall o del dispositivo que realiza la traducción. Esto significa que las direcciones IP y los puertos de los dispositivos en la red interna se traducen a una dirección IP y puerto únicos en la interfaz externa cuando se comunican con recursos en Internet. Por lo tanto, la traducción de direcciones y puertos debe tener lugar en la interfaz externa.

b) En el tráfico entrante (procedente de la red Internet), ¿afecta a las direcciones y puertos origen, destino o ambos?

En el tráfico entrante desde Internet, la traducción de direcciones y puertos afecta a las direcciones y puertos de destino. Cuando un paquete entra desde Internet hacia la red interna, la dirección IP y el puerto de destino del paquete se traducen de la dirección IP pública y el puerto asignado a una dirección IP privada y puerto correspondiente en la red interna. Esto permite que múltiples dispositivos internos compartan una única dirección IP pública. Por lo tanto, la traducción de direcciones y puertos en el tráfico entrante afecta al destino del paquete.

**Cortafuegos**

Sea un cortafuegos como el que se ha configurado en el laboratorio. Indique si las siguientes afirmaciones son ciertas o falsas, justificando la respuesta.

-Todos los paquetes que no sean de la interfaz local pasan por el proceso de NAT

Falso. Los paquetes que van al cortafuegos por la interfaz interna no pasan por NAT.

-Cuando un paquete no es aceptado por el cortafuegos (deny), se envía un rechazo al remitente.

Falso. Se descarta sin más.

- No todas las reglas que aceptan un paquete (allow) generan una regla dinámica.

Cierto. Por ejemplo, las de ICMP.

-Si un paquete viaja de una red a otra, pasa dos veces por el cortafuegos ipfw.

Cierto. Pasa una vez por cada interfaz

Sea un cortafuegos como el que se ha configurado en el laboratorio. Indique si las siguientes afirmaciones son ciertas o falsas. Imprescindible justificar la respuesta

**a):** ¿Todos los datagramas IP que no sean de la interfaz local son analizados por el proceso de NAPT?

Falsa: No todos los datagramas IP que no son de la interfaz local son analizados por el proceso de NAPT. En la configuración del laboratorio, se aplica NAPT solo al tráfico saliente, es decir, el tráfico que sale de la red interna hacia la red externa. Los datagramas IP que no son de la interfaz local pueden ser filtrados por otras reglas del firewall antes de que se realice la traducción de direcciones y puertos por el proceso de NAPT.

**b):** ¿Cuándo un datagrama IP no es aceptado por el cortafuegos (deny), este genera y envía un datagrama IP al remitente para informar de dicho rechazo?

Falsa: El cortafuegos IPFW en FreeBSD, como se ha configurado en el laboratorio, no genera y envía un datagrama IP al remitente para informar de un rechazo. Cuando un datagrama IP es denegado (deny) por una regla del cortafuegos, simplemente se descarta y no se envía ningún mensaje de rechazo al remitente.

**c):** ¿Todas las reglas que aceptan un paquete (allow) generan una regla dinámica (estado)?

Falsa: En el cortafuegos IPFW, solo las reglas que utilizan la opción **keep-state** o **established** generan reglas dinámicas de estado. Estas reglas se utilizan para realizar un seguimiento del estado de las conexiones y permitir el tráfico de retorno asociado con esas conexiones.

**d):** ¿Si un datagrama IP viaja de una red a otra (p.ej. desde la red externa a la interna), ambas conectadas directamente al cortafuegos ipfw y activado el cortafuegos como rúter IP, se procesarán dos veces todas las reglas del cortafuegos ipfw?

Falsa: Las reglas del cortafuegos IPFW no se procesarán dos veces. El procesamiento de las reglas del cortafuegos ocurre una sola vez, ya sea que el paquete entre o salga de la red interna o externa. El cortafuegos examina los paquetes basándose en las reglas definidas y decide si permitir o denegar el paso del paquete según corresponda, independientemente de si el paquete entra o sale de la red interna o externa.