Jose L. Muñoz, Juanjo Alins, Oscar Esparza, Jorge Mata

Firewalls & NAT Practices

Transport Control i Gestió a Internet (TCGI)
Universitat Politècnica de Catalunya (UPC)
Dp. Enginyeria Telemàtica (ENTEL)

Contents

0.1 Prácticas

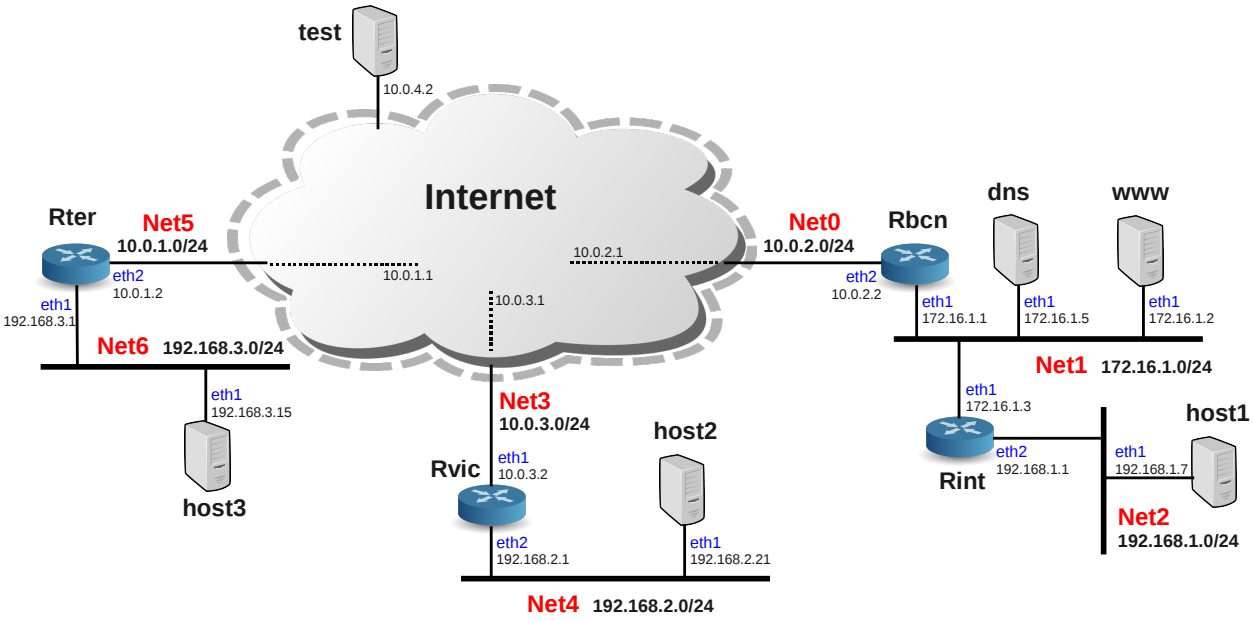


Figure 1: Escenario fwnat network

Exercise1– El objetivo de este ejercicio es que se familiarice con los conceptos básicos de filtrado de paquetes.

Para la realización de este ejercicio se utilizará el esquema de red mostrado en la figura 1. En primer lugar pondremos en marcha la simulación utilizando el comando:

```
host$ simctl fwnat start
```

Una vez que la simulación haya arrancado, se debe autoconfigurar la máquinas de las redes **Net0**, **Net1** y **Net2** ejecutando en el host de virtualización los siguientes comandos:

- Para la configuración de los interfaces de red ejecute

```
host$ simctl fwnat exec ifcfg
```

- Para la configuración de las rutas de encaminamiento indirectas ejecute:

```
host$ simctl fwnat exec routecfg
```

Verifique como han quedado configuradas las máquinas **Rbcn**, **www**, **Rint** y **host1** después de ejecutar los comandos anteriores. A continuación se realizarán diversas configuraciones de filtrado.

1. Configure las tablas de filtrado de la máquina **host1** de manera que no se permita ningún tipo de tráfico ICMP entrante a los procesos internos (locales) de dicha máquina.

   Con este filtrado responda a las siguientes preguntas:

   (a) Si desde **Rint** se ejecuta un `ping` con destino **host1** ¿se transmitirá el correspondiente mensaje ICMP *echo-request* por la red? ¿Es posible capturar el mensaje de respuesta ICMP *echo-reply*? Describa lo que ocurre en este caso.

   (b) Si en lugar de enviar el `ping` desde **Rint** hacia **host1**, lo hacemos en sentido contrario (ping desde **host1** hacia **Rint**) ¿se transmitirá el correspondiente mensaje ICMP *echo-request*? ¿y el *echo-reply*? Describa lo que ocurre en este caso.

2. Borre la configuración de filtrado anterior de **host1** y vuelva a configurar sus tablas de filtrado para obtener el siguiente comportamiento:

   (a) Desde **host1** se debe poder realizar correctamente un `ping` a una máquina remota (**Rint**).

   (b) **host1** no debe responder a ninguna petición de `ping` externa.

   En esta nueva situación, responda a las mismas preguntas del apartado anterior.

3. El problema de los esquemas de filtrado anteriores es que hay que configurar las tablas de filtrado en cada una de las máquinas, haciendo que la administración de la red sea compleja. La solución más utilizada es "confiar" la seguridad al router de la red, ya que todas las comunicaciones con el exterior fluyen a través de él y se puede aplicar un control centralizado a las mismas facilitando la administración. Cuando un *router* realiza funciones de filtrado o *firewall* se le conoce con el nombre de bastión de la red.
   En este punto, usted tiene que configurar el router **Rint** como bastión para protejer a los hosts internos (**host1**). Para ello prepare el escenario realizando las siguientes tareas:

   - Elimine las entradas de las tablas de filtrado de **host1**.
   - Verifique que las redes **Net1** y **Net2** están correctamente configuradas (direcciones IP y tablas de encaminamiento) de forma que exista conectividad entre ellas a nivel IP.

   En este momento, debe ser posible realizar con éxito un ping desde **www** o **Rbcn** a cualquiera de las máquinas de la **Net2** y viceversa.

   Ahora, añada las entradas necesarias en su bastión (**Rint**) para obtener el siguiente comportamiento:

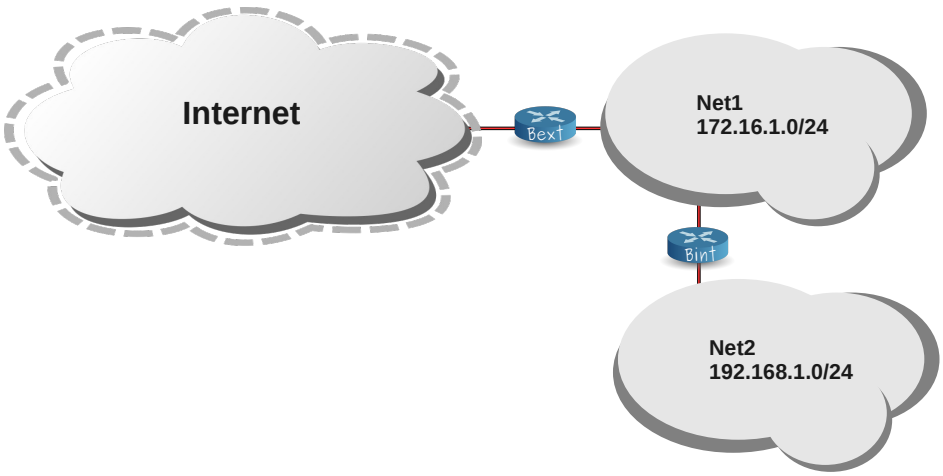
   (a) Un ping realizado desde una máquina externa a **Net2** hacia una máquina perteneciente a **Net2** no debe ser respondido, pero en el caso contrario, es decir un ping iniciado desde una máquina de **Net2** hacia una máquina externa, sí que debe funcionar correctamente. Verifique el funcionamiento de este filtro.

   (b) Si una máquina de una red externa a **Net2**, realiza un intento de conexión a un servicio TCP de un servidor alojado en **Net2**, este intento de conexión debe ser rechazado, pero en el caso contrario sí que debe funcionar correctamente. Verifique el funcionamiento de este filtro utilizando las máquinas de **Net1** como red externa de pruebas.

(c) Finalmente, filtre todo el tráfico UDP que entre o salga de **Net2**, excepto el tráfico UDP que vaya dirigido a un servidor DNS (que se supone externo a **Net2**)

Exercise2–

El objetivo de este ejercicio es que usted se familiarice con las técnicas de NAT. Se utilizará el mismo escenario mostrado en la figura 1. Si usted se centra en la redes formadas por **Net0**, **Net1** y **Net2**, puede observar que desde un punto de vista administrativo respecto al espacio de direcciones IP, la red de la figura anterior se puede ver de la siguiente manera:



En este caso se ha considerado que los rangos de direcciones 192.168.0.0/22 y 172.16.1.0/24 se corresponden con direcciones privadas. Por otro lado, se ha considerado que los rangos de direcciones 10.0.0.0/22 hacen referencia a un sistema de direccionamiento público (en la figura se ha considerado que Internet hace uso del rango 10.0.0.0/22)

Arranque la simulación ejecutando desde el host de virtualización el comando:

```
host$ simctl fwnat start
```

Una vez que la simulación haya arrancado, se debe autoconfigurar la máquinas de las redes **Net0**, **Net1** y **Net2** ejecutando en el host de virtualización los siguientes comandos:

- Para la configuración de los interfaces de red ejecute

```
host$ simctl fwnat exec ifcfg
```

- Para la configuración de las rutas de encaminamiento indirectas ejecute:

```
host$ simctl fwnat exec routecfg
```

- Para realizar la configuración de las tablas de filtrado de **Rint** ejecute:

```
host$ simctl fwnat exec fwcfg
```

1. Desde el host **www** de **Net1**, realice un `ping` a 10.0.4.2 (**test**) ¿funciona? ¿Es un problema de filtrado o de direccionamiento?

2. Para solucionar el problema anterior configure el router externo **Rbcn** para que realice SNAT para sus redes internas. Una vez configurado pruebe a realizar el `ping` a 10.0.4.2 ¿funciona ahora? Utilice las herramientas de análisis de tráfico que conoce para ver que está sucediendo en la red.

3. La figura muestra el típico esquema de *firewall* con doble bastión (bastion externo –Rbcn– y bastión interno –Rint–), zona desmilitarizada (**Net1**) o DMZ (*DeMilitarized Zone*) para los servidores con acceso externo, y red interna (**Net2**). En este esquema las máquinas de la red interna pueden establecer conexiones a los servidores de la DMZ y a servidores externos (Internet), tal y como se ha configurado en el ejercicio anterior. En este esquema de doble bastión, se debe poder acceder a los servidores de la DMZ desde el exterior pero no a los *hosts* de la red interna.
   Configure el bastión externo (**Rbcn**) para dar acceso al servidor web de **www** desde Internet y haga uso de la máquina externa (**test**) para verificar la configuración. Utilice las herramientas de análisis de tráfico que conoce para ver que está sucediendo en la red.