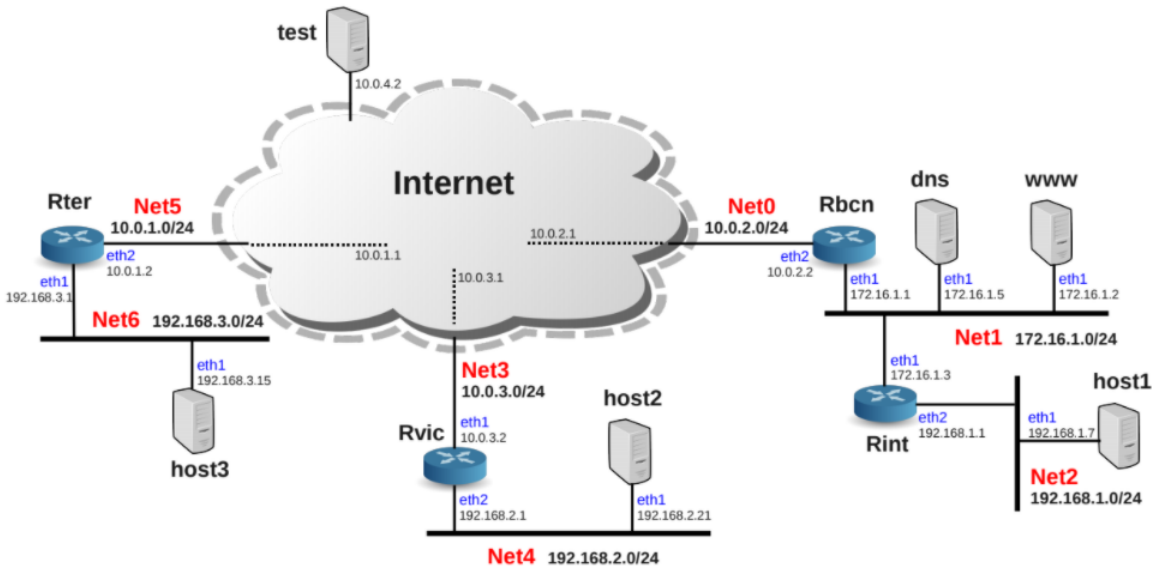


Exercise 1

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 cómo 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:

   `host1#: iptables -t filter -A INPUT -d 192.168.1.7 -p icmp -j DROP`

   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.

   Un echo-request des de Rint es transmetrà per la xarxa, ja que el firewall no atura l'enviament de pings, però el host1 NO acceptarà missatges d'aquest tipus degut a la configuració anterior, per tant rep el echo-request, però no envia cap echo-reply.

   `Rint#: ping -c 1 192.168.1.7`

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.
Quan enviem un echo-request des de Host1 a Rint, s'envia correctament, ja que només hem bloquejat els missatges entrants, i no els sortints.
L'echo-reply des de Rint s'enviarà i es podrà capturar a la SimNet2, però no arribarà al host1.

2. Borre la configuración de filtrado anterior de host1 y vuelva a configurar sus tablas de filtrado para obtener el siguiente comportamiento:
`host1# iptables -t filter -D INPUT -d 192.168.1.7 -p icmp -j DROP`
`host1# iptables -t filter -A INPUT -d 192.168.1.7 -p icmp --icmp-type echo-request -j DROP` --> Veiem que només cal descartar els echo-request ja que per sí mateix ja arriba a tots els altres al fer un ping.

a) Desde host1 se debe poder realizar correctamente un ping a una máquina remota (Rint).
`host1#: ping -c 1 192.168.1.1`

b) host1 no debe responder a ninguna petición de ping externa. En esta nueva situación, responda a las mismas preguntas del apartado anterior.
`Rint#: ping -c 1 192.168.1.7`

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 proteger 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.
`Rint# iptables -A FORWARD -d 192.128.1.0/24 -p icmp --icmp-type echo-request -j DROP`
`host1# ping -c 1 172.16.1.2` -> OK
`www# ping -c 1 192.168.1.7` -> El paquet echo-reply no s’enviarà perquè la Net2 no accepta mssg de ICMP echo-request.

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.

```
Rint# iptables -A FORWARD -d 192.128.1.0/24 -p tcp --tcp-flags
ALL SYN -j DROP
```

`host1# ssh 172.16.1.2` -> OK

`www1# ssh 192.168.1.7` -> NOT ACCEPTED

Observem com NO es pot connectar, i només la Net1 veu els paquets. En canvi, fer telnet des de host1 fins a www si que es pot.

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)

Sabem que TOTES LES COMUNICACIONS AMB EL DNS UTILITZEN UDP PEL PORT 53. Per tant, hem d'impedir que entri tot tràfic UDP, menys el que surti d'algun host des del port 53.

```
Rint#: iptables -A FORWARD -p udp --sport 53 -d 192.168.1.0/24
-j ACCEPT
Rint#: iptables -A FORWARD -p udp --dport 53 -s 192.168.1.0/24
-j ACCEPT
Rint#: iptables -A FORWARD -p udp -j DROP
```

**Obs: Les comandes amb iptable es llegeixen en ordre, per tant si un paquet compleix la primera norma, les altres ja no es miren*

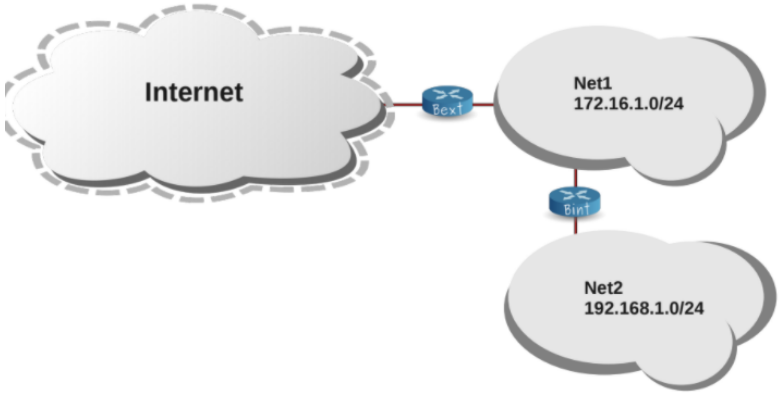
`host1# ping -c1 172.16.1.2` -> Tráfico a servidor DNS OK

`host1# nc 172.16.1.2 53` -> Tráfico UDP saliente de Net2 rechazado

`www:~# nc 192.168.1.7 53` -> Tráfico UDP entrante a Net2 rechazado

Exercise 2

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

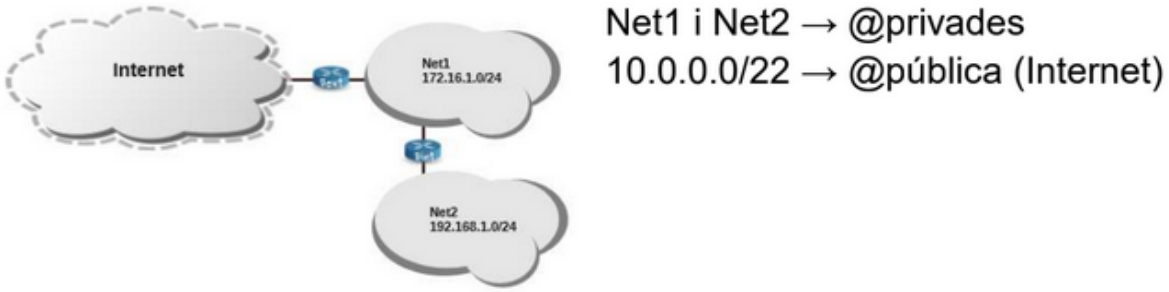
```
host$ simctl fwnat exec ifcfg
```

- 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?
   `www:~# ping -c1 10.0.4.2` -> No funciona ja que la IP de www és privada.

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.
   `Rbcn#: iptables -t nat -A POSTROUTING -o eth2 -j SNAT --to 10.0.2.2`
   - -o eth2: output interace
   - -j SNAT: t'indica l'acció que realitzarà
   - --to: @IP de destí
   - POSTROUTING: la traducció de la IP d'origen (la qual les xarxes públiques no entenen) es fa un cop el paquet ja s'ha encaminat.

   `www#: ping -c1 10.0.4.2` -> OK
3. La figura muestra el típico esquema de firewall con doble bastión (bastión 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 qué está sucediendo en la red.

```
Rbcn#: iptables -t nat -A PREROUTING -i eth2 -d 10.0.2.2 -j DNAT --to
172.16.1.2
```

- -i: input, ens indica que el destí del paquet és el host des d'on fem la comanda.
- -j DNAT: el router tradueix l'adreça de destí abans del routing (PREROUTING), ja que des d'internet no podem posar IPs privades.