Tienes que tres máquinas en la misma red. Las 3 tienen que tener ssh instalado: A (10.5.2.10), B (10.5.2.11) y C (10.5.2.12). Vamos a jugar con el firewall de la máquina A.

*Lo primero, vamos a aceptar todos los paquetes con estado ESTABLISHED o RELATED:*

**iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT**

**iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT**

**iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT**

En una máquina (A) con GNU/Linux:

1. Vacía todas las cadenas de las tablas INPUT y OUTPUT.

**iptables -F**

**iptables -t filter -F**

Comprueba que desde B y C puedes hacer PING a A.

Comprueba que desde B y C puedes conectarte por ssh a A.

1. Pon DROP como política por defecto de la cadena INPUT.

**iptables -P INPUT DROP**

Comprueba que ni desde B ni desde C puedes hacer PING a la máquina A.

Comprueba que ni desde B ni desde C puedes conectarte por ssh a A.

1. Permite los PINGs hacia la máquina A desde B.

**iptables -A INPUT -p icmp -s 10.5.2.11 -m state --state NEW -j ACCEPT**

Comprueba que desde B puedes hacer PING a la máquina A.

Comprueba que desde B no puedes conectarte a A por ssh.

Comprueba que desde C no puedes conectarte a A por SSH ni hacer PING.

1. Permite las conexiones ssh hacia A desde C.

**iptables -A INPUT -p tcp --dport 22 -s 10.5.2.12 -m state --state NEW -j ACCEPT**

**Si no hubiéramos añadido las líneas para aceptar todos los paquetes en estado**

**ESTABLISHED y RELATED:**

**iptables -A INPUT -p tcp --dport 22 -s 10.5.2.12 -j ACCEPT**

**iptables -A OUTPUT -p tcp --sport 22 -d 10.5.2.15 -j ACCEPT (no es necesario)**

Comprueba que desde B puedes hacer PING a la máquina A.

Comprueba que desde B no puedes conectarte a A por ssh.

Comprueba que desde C puedes conectarte a A por SSH.

Comprueba que desde C no puedes hacer PING a la máquina A.

Comprueba que desde A puedes hacer PING a B y C.

1. Pon DROP como política por defecto de la cadena OUTPUT.

**iptables -P OUTPUT DROP**

Comprueba que desde A no puedes hacer PING ni a A ni a C.

Comprueba que desde A no puedes conectarte por ssh ni a B ni a C.

1. Permite los PINGs hacia B.

**iptables -A OUTPUT -p icmp -d 10.5.2.12 -m state --state NEW -j ACCEPT**

**Si no hubiéramos añadido las líneas para aceptar todos los paquetes en estado**

**ESTABLISHED y RELATED:**

**iptables -A OUTPUT -p icmp -d 10.5.2.12 -j ACCEPT**

**iptables -A INPUT -p icmp -s 10.5.2.12 -j ACCEPT**

Comprueba que desde A puedes hacer PING a B.

Comprueba que desde A no puedes hacer PING a C.

Comprueba que desde A no puedes conectarte por ssh a B ni a C.

1. Permite las conexiones ssh desde A hacia C.

**iptables -A OUTPUT -p tcp --dport 22 -d 10.5.2.12 -m state --state NEW -j ACCEPT**

**Si no hubiéramos añadido las líneas para aceptar todos los paquetes en estado**

**ESTABLISHED y RELATED:**

**iptables -A OUTPUT -p tcp --dport 22 -d 10.5.2.12 -j ACCEPT**

**iptables -A INPUT -p tcp --sport 22 -s 10.5.2.12 -j ACCEPT**

Comprueba que desde A puedes conectarte a A por SSH.

Ahora vamos a configurar el firewall para controlar el tráfico entre la red int y la red ext. Abre en NETinVM las máquinas fw (eth0:10.5.0.254 y eth2:10.5.2.254), inta (10.5.2.10), intb (10.5.2.11), exta (10.5.0.10) y extb (10.5.0.11).

Primero, pon ACCEPT como política por defecto de todas las cadenas de la máquina intb c

Ahora, en los siguientes ejercicios nos centraremos en la máquina *fw*.

1. Vacía todas las cadenas de las tablas nat y filter Pon las políticas por defecto de las cadenas de la tabla filter en DROP.

**iptables -F**

**iptables -t nat -F**

**iptables -P INPUT DROP**

**iptables -P OUTPUT DROP**

**iptables -P FORWARD DROP**

Comprueba que desde inta no se puede acceder por ssh ni hacer PING hacia exta.

Comprueba que desde exta no se puede hacer PING a fw.

1. Permite (con todo lo que ello conlleva) el tráfico ssh desde la máquina inta hacia la red ext.

**iptables -A FORWARD -p tcp --dport 22 -s 10.5.2.10 -i eth2 -m state --state NEW -j ACCEPT**

**PREGUNTA; ¿por qué funciona sin tener que haber hecho el MASQUERADE?**

Comprueba que desde inta puedes acceder por ssh a exta y extb.

**ssh exta**

**ssh extb**

Comprueba que desde intb no puedes acceder por ssh a exta ni a extb.

**ssh exta**

**ssh extb**

1. Permite (con todo lo que ello conlleva) el tráfico ssh desde la máquina extb hacia la red int.

**iptables -t nat -A PREROUTING -p tcp --dport 2567 -i etho -j DNAT --to-destination 10.5.2.10:22**

**iptables -t nat -A PREROUTING -p tcp --dport 7652 -i etho -j DNAT --to-destination 10.5.2.11:22**

**iptables -A FORWARD -p tcp --dport 22 -s 10.5.0.11 -i eth0 -m state --state NEW -j ACCEPT**

Comprueba que desde extb puedes acceder por ssh a inta e intb.

**Dependiendo de la máquina cuyo control quieras tomar, deberás poner una de estas dos instrucciones:**

**Para inta: ssh -p 2567 10.5.0.254**

**Para intb: ssh -p 7652 10.5.0.254**

Comprueba que desde exta no puedes acceder por ssh a inta ni a intb.

**Dependiendo de la máquina cuyo control quieras tomar, deberás poner una de estas dos instrucciones:**

**Para inta: ssh -p 2567 10.5.0.254**

**Para intb: ssh -p 7652 10.5.0.254**