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

En una máquina (A) con GNU/Linux:

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

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.

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.

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.

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.

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.

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.

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 fx, inta, intb, exta y extb

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.

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.

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

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

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

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

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