Ejercicios de Routerboard de MikroTik: permitir y bloquear la conexión SSH en el Firewall de MikroTik

Ayuda

Firewall con ejemplos

Connection tracking: permite visualizar las conexiones en las que interviene nuestro equipo.

[crayon-6a9d679ddda7d843217988/]

Reglas generales

Escritura de firewall: siempre conviene empezar con las reglas de estado, para ahorrar procesamiento y acelerar las conexiones ya establecidas y las relativas.

[crayon-6a9d679ddda84600583176/]

Aceptar conexiones VPN:

```
[admin@MikroTik] > ip firewall filter add protocol=gre action=accept chain=input
[admin@MikroTik] > ip firewall filter add protocol=tcp dst-port=1723 action=accept chain=input comment="ACEPTO CONEXIONES VPN"
```

Denegar ping y loguear los intentos de ping:

```
[admin@MikroTik] > ip firewall filter add protocol=icmp chain=input action=log log-prefix="PING DENEGADO"
[admin@MikroTik] > ip firewall filter add protocol=icmp action=accept chain=input comment="DENIEGO ICMP"
```

```
[admin@MikroTik] > log print
23:34:12 firewall,info PING DENEGADO input: in:ether1
out:(none), src-mac 00:21:70:fd:e3:25, proto ICMP (type 8,
code 0), 192.168.4.254->192.168.4.1, len 64
```

Uso de listas

Las listas contienen direcciones IP para las que podemos tomar determinadas acciones. De esta manera, mantenemos una única lista de direcciones y la invocamos en el firewall.

Crear una lista especificando desde dónde permitimos conexiones SSH

```
[admin@MikroTik] > ip firewall address-list add list=ssh-
permitido address=192.168.1.2/32 comment="MAQUINA DEL
ADMINISTRADOR"
[admin@MikroTik] > ip firewall filter add src-address-
list=!ssh-permitido protocol=tcp dst-port=22 action=drop
chain=input comment="ACEPTO SSH DESDE LAS MAQUINAS EN LA LISTA
ssh-permitido"
```