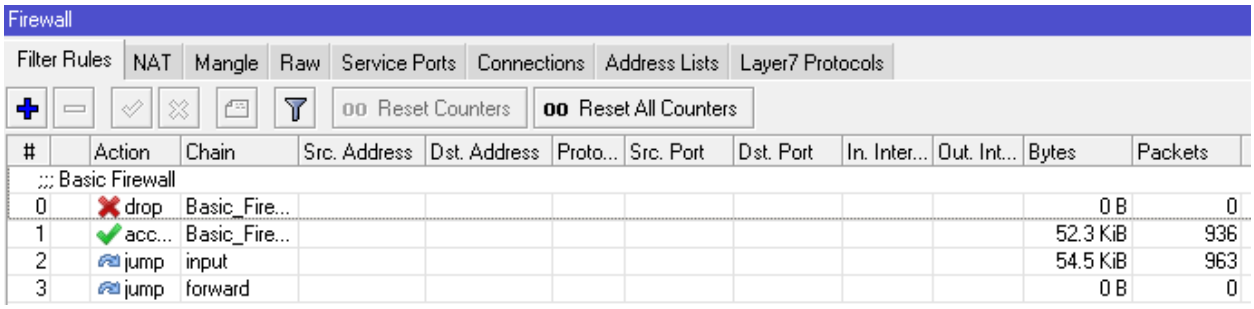
Laboratorio especial: Configuración de Firewall Filter MikroTik

Objetivo: Configurar conjunte de reglas de firewall para proteger su MikroTik de ataques externos.

Paso 1: siempre conviene empezar con las reglas de estado, para ahorrar procesamiento y acelerar las conexiones

Comandos:

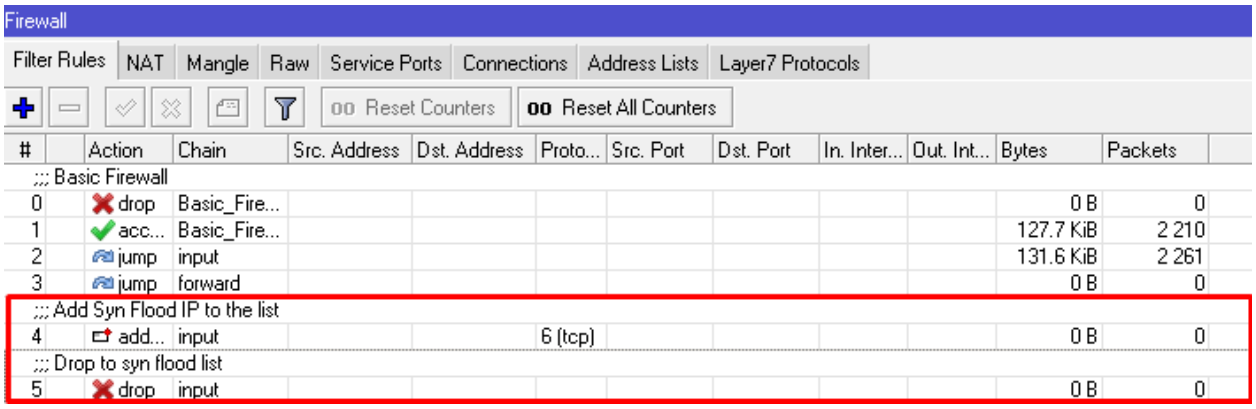
```
ip firewall filter
  add action=drop chain=Basic_Firewall comment="Basic Firewall" \
    connection-state=invalid
     add action=accept chain=Basic_Firewall connection-state=established,related
        add action=jump chain=input jump-target=Basic_Firewall
           add action=jump chain=forward jump-target=Basic_Firewall
```



Paso 2: Protección contra SynFlood: Es una forma de ataque de denegación de servicio en el que un atacante envía una sucesión de solicitudes al sistema del objetivo en un intento de consumir suficientes recursos del servidor para que el sistema no responda al tráfico legítimo. Copiar y pegar script tal cual esta**.**

Comandos:

```
/ip firewall filter
  add action=add-src-to-address-list address-list=Syn_Flooder \
    address-list-timeout=30m chain=input comment=\
      "Add Syn Flood IP to the list" connection-limit=30,32 protocol=tcp \
        tcp-flags=syn
          add action=drop chain=input comment="Drop to syn flood list" \
            src-address-list=Syn_Flooder
```



Paso 3: En esta ocasión agregaremos las siguientes reglas: **Port scan** o escaneo de puertos fuera de mi red, Dos attack o ataque de denegación de servicio, y por ultimo DNS relay.

Comandos:

/ip firewall filter

add action=drop chain=input comment="Portscan drop" src-address-list=\

Port_scan

add action=add-src-to-address-list address-list=Port_scan \

address-list-timeout=12w6d chain=input comment="Port scan detection" \

protocol=tcp psd=21,3s,3,1

add action=tarpit chain=input comment="Dos attack drop" connection-limit=3,32 \

protocol=tcp src-address-list=Black_list

add action=add-src-to-address-list address-list=DDoS_Blacklist \

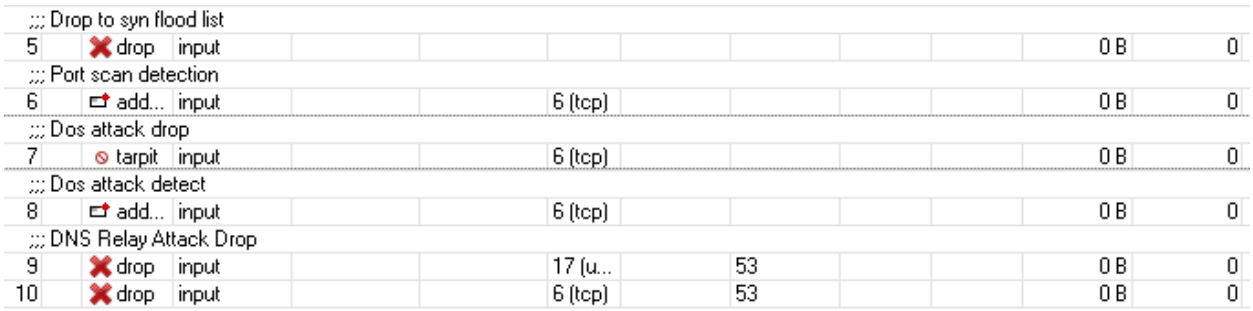
address-list-timeout=12w6d chain=input comment="Dos attack detect" \

connection-limit=10,32 log=yes protocol=tcp

add action=drop chain=input comment="DNS Relay Attack Drop" connection-state=\

new dst-port=53 protocol=udp

add action=drop chain=input connection-state=new dst-port=53 protocol=tcp

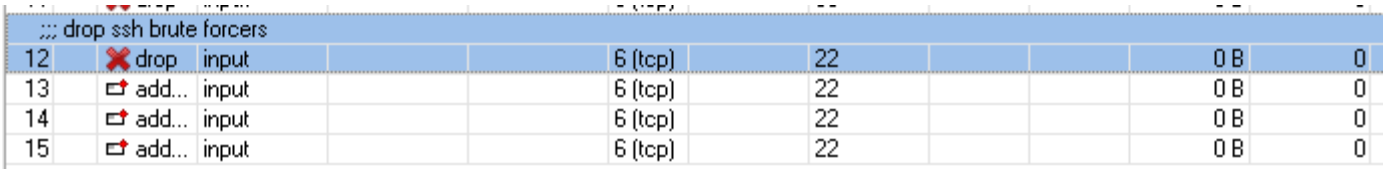


;;; Drop to syn flood list										
5		drop	input						0 B	0
;;; Port scan detection										
6		add...	input			6 (tcp)			0 B	0
;;; Dos attack drop										
7		tarpit	input			6 (tcp)			0 B	0
;;; Dos attack detect										
8		add...	input			6 (tcp)			0 B	0
;;; DNS Relay Attack Drop										
9		drop	input			17 (u...	53		0 B	0
10		drop	input			6 (tcp)	53		0 B	0

Paso 4: Regla **SSH brute force login prevention** a los 3 intentos de ssh fallidos banear ips por 10 dias.

Comandos:

```
ip firewall filter
  add action=drop chain=input connection-state=new dst-port=53 protocol=tcp
   add action=drop chain=input comment="drop ssh brute forcers" dst-port=22 \
     protocol=tcp src-address-list=ssh_blacklist
       add action=add-src-to-address-list address-list=ssh_blacklist \
        address-list-timeout=1w3d chain=input connection-state=new dst-port=22 \
           protocol=tcp src-address-list=ssh_stage2
            add action=add-src-to-address-list address-list=ssh_stage2 \
        address-list-timeout=1m chain=input connection-state=new dst-port=22 \
   protocol=tcp src-address-list=ssh_stage2
add action=add-src-to-address-list address-list=ssh_stage1 \
address-list-timeout=1m chain=input connection-state=new dst-port=22 \
 protocol=tcp
```

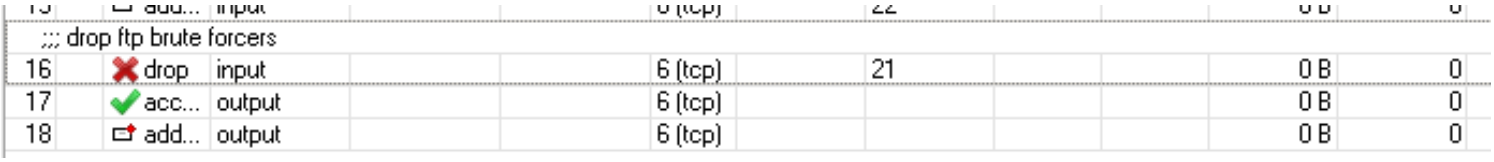


;;; drop ssh brute forcers										
12		drop	input			6 (tcp)		22			0 B	0
13		add...	input			6 (tcp)		22			0 B	0
14		add...	input			6 (tcp)		22			0 B	0
15		add...	input			6 (tcp)		22			0 B	0

Paso 5: FTP brute forcers, port 21**.**

Comandos:

```
 ip firewall filter
add action=drop chain=input comment="drop ftp brute forcers" dst-port=21 \
    protocol=tcp src-address-list=ftp_blacklist
      add action=accept chain=output content="530 Login incorrect" dst-limit=\
         1/1m,9,dst-address/1m protocol=tcp
           add action=add-dst-to-address-list address-list=ftp_blacklist \
              address-list-timeout=3h chain=output content="530 Login incorrect" \
                 protocol=tcp
```



	;;; drop ftp brute forcers								
16	drop	input			6 (tcp)	21		0 B	0
17	acc...	output			6 (tcp)			0 B	0
18	add...	output			6 (tcp)			0 B	0

Paso 6: Winbox brute force login prevention, port :8291 a los 3 intentos fallidos banear ips por 15 dias.

Comandos:

/ip firewall filter

add action=drop chain=input comment=\

"Bruteforce login prevention(Winbox brute forcers)" dst-port=8291 \

protocol=tcp src-address-list=winbox_blacklist

add action=add-src-to-address-list address-list=winbox_blacklist \

address-list-timeout=2w1d chain=input comment=\

"Bruteforce login prevention(Winbox: stage3)" connection-state=new \

dst-port=8291 protocol=tcp src-address-list=winbox_stage_2

add action=add-src-to-address-list address-list=winbox_stage_2 \

address-list-timeout=6h chain=input comment=\

"Bruteforce login prevention(Winbox: stage2)" connection-state=new \

dst-port=8291 protocol=tcp src-address-list=winbox_stage_1

add action=add-src-to-address-list address-list=winbox_stage_1 \

address-list-timeout=12h chain=input comment=\

"Bruteforce login prevention(Winbox: stage1)" connection-state=new \

dst-port=8291 protocol=tcp

add action=accept chain=input comment="Winbox acces from WAN" dst-port=8291 \ log=yes protocol=tcp

	;;; Bruteforce login prevention(Winbox brute forcers)									
19	drop	input			6 (tcp)	8291			0 B	0
	;;; Bruteforce login prevention(Winbox: stage3)									
20	add...	input			6 (tcp)	8291			0 B	0
	;;; Bruteforce login prevention(Winbox: stage2)									
21	add...	input			6 (tcp)	8291			0 B	0
	;;; Bruteforce login prevention(Winbox: stage1)									
22	add...	input			6 (tcp)	8291			0 B	0
	;;; Winbox acces from WAN									
23	acc...	input			6 (tcp)	8291			0 B	0

Paso 7: Aceptar trafico input y forward que usted desee que entre o pase por su router mikrotik en mi caso dejare estos campos vacios, y por ultimo para cerrar nuestro contenedor de reglas un Drop imput para todo lo que no cumpla con mis reglas de entrada Dropearlo**.**

Comandos:

/ip firewall filter

add action=accept chain=input

add action=accept chain=forward

add action=drop chain=input comment="Drop Others" connection-nat-state=\

!dstnat