

MODULO 17

Firewall

1. Configuraciones de Firewall.

1.1. Filter Rules

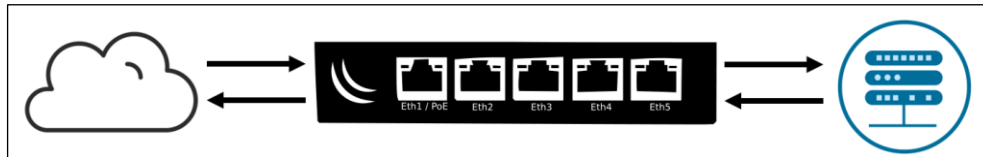
En IP -> Firewall -> Filter Rules, Podemos encontrar el filtro para todas las reglas del firewall de MikroTik

El firewall de MikroTik se basa en Linux, lo que quiere decir es que las reglas que encontremos se van a ejecutar en orden.

En MikroTik existen 3 formas para operar el firewall.

- FORWARD

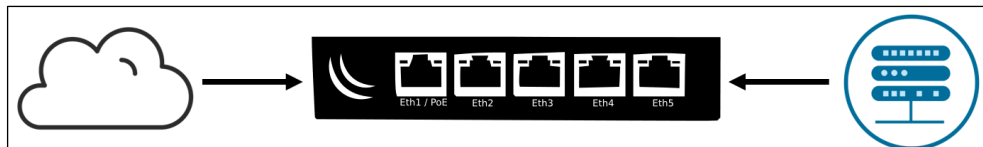
El modo Forward de MikroTik se aplica a todo el tráfico que intente atravesar el router ya sea de LAN hacia INTERNET o de INTERNET hacia LAN



Ej. Crearíamos reglas forward para aceptar o negar acceso a diferentes sitios

- INPUT

El modo Input en MikroTik se aplica a todo el tráfico que se dirige al router ya sea de LAN hacia el router o de INTERNET hacia el router.

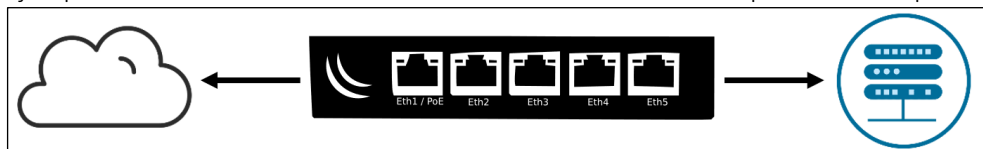


Este modo de operación captura el tráfico que va contra el router (tráfico que intenta acceder al router)

Ej. Crearíamos reglas de tipo Input para configurar el Hardening (protección del router) logramos proteger el router con reglas Input.

- OUTPUT

El modo Output en MikroTik se aplica a todo el tráfico saliente del router como por ejemplo cuando el router realiza consultas DNS o tráfico con el protocolo icmp.



- Seis reglas que siempre deberían estar presentes en FilterRules.
 - En modo Forward aceptar todas las conexiones establecidas y relacionadas.

Con esto logramos que las conexiones seguras sean persistentes.

- En modo Forward denegar todas las conexiones invalidas.

De esta forma solo nos quedamos con las conexiones validas y descartamos las conexiones Invalidas.

- En modo Input aceptar todas las conexiones establecidas y relacionadas.

- En modo Input denegar todas las conexiones invalidas.

The left screenshot shows the 'Firewall Rule' configuration window in WinBox. The 'General' tab is active. 'Chain' is set to 'input'. 'Src. Address' and 'Dst. Address' are empty. 'Protocol' is set to 'any'. 'Src. Port' and 'Dst. Port' are empty. 'Any. Port' is checked. 'In. Interface' and 'Out. Interface' are empty. 'In. Interface List' and 'Out. Interface List' are empty. 'Packet Mark', 'Connection Mark', 'Routing Mark', and 'Routing Table' are empty. 'Connection Type' is set to 'any'. 'Connection State' has 'invalid' checked, and 'established', 'related', 'new', and 'untracked' are unchecked. 'Connection NAT State' is empty. The 'Action' tab is visible on the right, showing 'Action' set to 'drop'.

The right screenshot shows the 'Action' tab of the 'Firewall Rule' configuration window. 'Action' is set to 'drop'. 'Log' is unchecked. 'Log Prefix' is empty. The 'General' tab is visible on the left, showing 'Chain' set to 'input'.

- En modo Output aceptar todas las conexiones establecidas y relacionadas.

The left screenshot shows the 'Firewall Rule' configuration window in WinBox. The 'General' tab is active. 'Chain' is set to 'output'. 'Src. Address' and 'Dst. Address' are empty. 'Protocol' is set to 'any'. 'Src. Port' and 'Dst. Port' are empty. 'Any. Port' is checked. 'In. Interface' and 'Out. Interface' are empty. 'In. Interface List' and 'Out. Interface List' are empty. 'Packet Mark', 'Connection Mark', 'Routing Mark', and 'Routing Table' are empty. 'Connection Type' is set to 'any'. 'Connection State' has 'established' and 'related' checked, and 'invalid', 'new', and 'untracked' are unchecked. 'Connection NAT State' is empty. The 'Action' tab is visible on the right, showing 'Action' set to 'accept'.

The right screenshot shows the 'Action' tab of the 'Firewall Rule' configuration window. 'Action' is set to 'accept'. 'Log' is unchecked. 'Log Prefix' is empty. The 'General' tab is visible on the left, showing 'Chain' set to 'output'.

- En modo Output denegar todas las conexiones invalidas.

The left screenshot shows the 'New Firewall Rule' configuration window in WinBox. The 'General' tab is active. 'Chain' is set to 'output'. 'Src. Address' and 'Dst. Address' are empty. 'Protocol' is set to 'any'. 'Src. Port' and 'Dst. Port' are empty. 'Any. Port' is checked. 'In. Interface' and 'Out. Interface' are empty. 'In. Interface List' and 'Out. Interface List' are empty. 'Packet Mark', 'Connection Mark', 'Routing Mark', and 'Routing Table' are empty. 'Connection Type' is set to 'any'. 'Connection State' has 'invalid' checked, and 'established', 'related', 'new', and 'untracked' are unchecked. 'Connection NAT State' is empty. The 'Action' tab is visible on the right, showing 'Action' set to 'drop'.

The right screenshot shows the 'Action' tab of the 'New Firewall Rule' configuration window. 'Action' is set to 'drop'. 'Log' is unchecked. 'Log Prefix' is empty. The 'General' tab is visible on the left, showing 'Chain' set to 'output'.

Quedando de la siguiente forma

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out...
... Aceptar trafico establecido y relacionado									
0	✓ acc...	forward							
... Negar Trafico invalido									
1	✗ drop	forward							
... Aceptar Entrada establecida y relacionada									
2	✓ acc...	input							
... Negar entradas invalidas									
3	✗ drop	input							
... Aceptar salidas establecidas y relacionadas									
4	✓ acc...	output							
... Negar salidas invalidas									
5	✗ drop	output							

1.2. NAT (Network Address Traslation)

En IP -> **Firewall**, aquí podemos encontrar a NAT (Network Address Translation)

En primera instancia Podemos ver que NAT trabaja en 2 modos de operación:

SRCNAT = Es la regla NAT para cambiar el origen cuando queremos hacer una salida a INTERNET tomando en cuenta una acción (esconde la IP origen-privada para enmascararla con la IP destino-publica)

DSTNAT = Es la regla NAT para cambiar el destino (usada generalmente para el portforwarding), (podemos habilitar o inhabilitar el acceso desde INTERNET hacia nuestra LAN) haciendo uso de srcAddress y dstAddress

1.3. Mangle

En IP -> **Firewall**, Aquí podemos encontrar a Mangle

Marcado de paquetes, conexiones o tablas (aquí no se toman acciones, solo marcado de paquetes)

En primera instancia vemos que tiene 5 modos de trabajo, 3 que ya vimos anteriormente y 2 principales con las cuales destaca MANGLE.

POSTROUTING = Trafico procesado saliente del router.

PREROUTING = Trafico procesado antes del ingreso al router.

1.4. RAW

En IP -> **Firewall**, aquí podemos encontrar a RAW

RAW es como FilterRules, sirve para identificar tráfico y realizar alguna acción

Las reglas RAW se aplican antes de que alguna conexión sea establecida en Connection Tracking, de esta manera podemos bloquear tráfico no deseado ahorrando recursos de procesamiento de manera significativa.

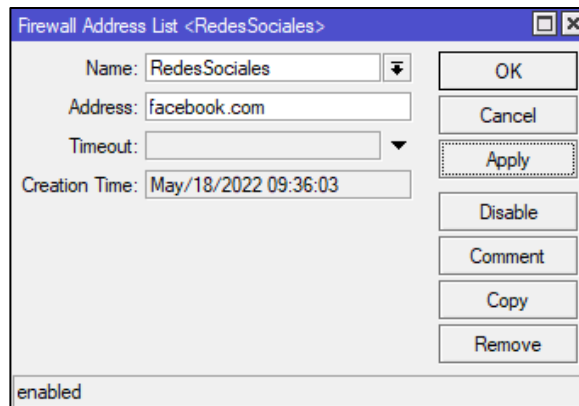
1.5. Connections

En IP -> **Firewall**, aquí Podemos encontrar el **ConectionTracking (Seguimiento de conexión)**

1.6. Address List

En IP -> **Firewall**, Aquí Podemos encontrar a AddressList (lista de direcciones)

Podemos crear listas de direcciones para en algún momento realizar alguna acción



1.7. Layer 7 Protocol

En IP -> **Firewall**, Aquí podemos encontrar a L7P

Nos sirve crear expresiones regulares para identificar tráfico en base al contenido

MODULO 18

NetWatch

2. NetWatch de MikroTik

1.1. Que es NetWatch

NetWatch es una de las herramientas más poderosas que tiene MikroTik, con esta funcionalidad podemos saber cuándo una red local o la conexión a internet ha dejado de estar en línea y de esa forma podemos automatizar acciones.

El funcionamiento de NetWatch básicamente es hacer ping a diferentes redes y el programado se trata en que si el ping no responde en un determinado tiempo se realiza una acción automatizada mediante scripts.

1.2. Cuando utilizarlo

El uso de NetWatch es ilimitado a la creatividad del administrador

1.3. Ejemplo de uso de NetWatch

Vamos a programar una tarea en la que se verificara la conexión a internet de nuestro router MikroTik, induciremos una regla firewall en la que bloqueamos las salidas o las peticiones hacia internet al mismo tiempo programaremos una regla NetWatch para que tome acciones de acuerdo a la respuesta que obtenga, si tiene conectividad no se hará nada o se podría tomar alguna acción, si no tiene conectividad vamos a iniciar un proceso de automatización mediante un script que deshabilite la falla de salida a internet que nosotros mismos provocamos.

PRIMERO:

Vamos a crear una regla que bloquea hacer ping al 8.8.8.8 por el protocolo icmp y lo verificaremos.

GENERAL

ACTION

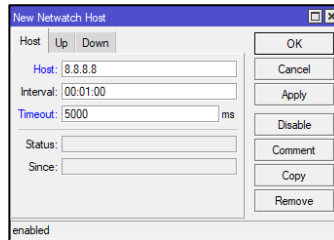
```
[admin@MikroTik1] > ping 8.8.8.8
```

SEQ	HOST	SIZE	TTL	TIME	STATUS
0					packet rejected
1					packet rejected
2					packet rejected

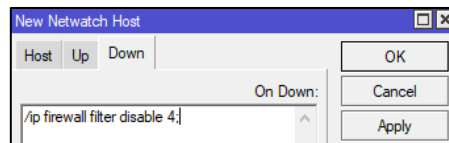
SEGUNDO:

En Tools -> **NetWatch**, vamos a configurar lo siguiente

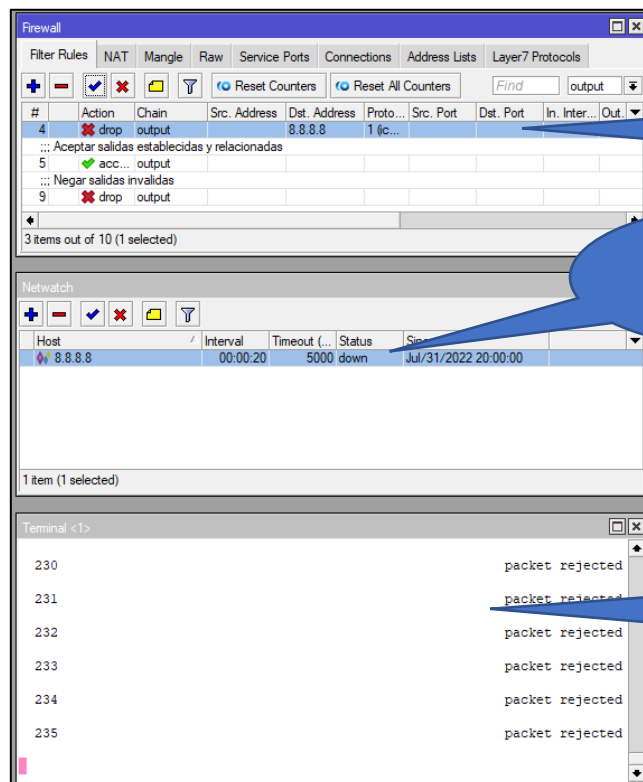
Host : 8.8.8.8
Interval : Es el tiempo intervalo en que NetWatch realizara el ping
Timeout : Tiempo en el que NetWatch usara para saber si el estado de conexión esta UP o DOWN. En milisegundos



De acuerdo a la respuesta de NetWatch el mismo determinara si la conexión está en estado DOWN o está en estado UP, ahora de acuerdo al estado obtenido debemos programar un script Dentro de las pestañas de Up o Down, que será script que se ejecutará de acuerdo al estado Obtenido, para este ejemplo usaremos un script que inhabilite la regla firewall que nosotros Programamos en firewall. Que en este caso vendría siendo la regla 4.



Momento cuando NetWatch está haciendo el análisis de tráfico hacia 8.8.8.8



Regla de firewall activa

NetWatch marca el estado en

Verificación de conexión

Ahora luego de aplicarse el script de NetWatch

The screenshot displays three windows from the MikroTik WinBox interface:

- Firewall:** Shows a list of rules. Rule 4 is selected and disabled (indicated by a red 'X' icon). The rule is named 'drop' and has an action of 'drop' on the 'output' chain. A blue callout bubble points to the disabled icon with the text "Inhabilita la regla".
- Netwatch:** Shows a single entry for host '8.8.8.8' with an interval of '00:00:20', a timeout of '5000', and a status of 'up'. A blue callout bubble points to the 'up' status with the text "NetWatch marca el estado en UP".
- Terminal <1>:** Displays a list of ping results for host '8.8.8.8'. The results show a sequence of '56 114' followed by response times (e.g., 51ms, 52ms, 51ms, 54ms, 51ms, etc.). A blue callout bubble points to the response times with the text "Verificacion de conexion".

MODULO 19

Hardening

3. HARDENING

3.1. Que es Hardening.

Endurecimiento, en seguridad informática es el proceso de asegurar un sistema mediante la reducción de vulnerabilidades en el mismo ya sea cerrando puerto, eliminando usuarios por defecto, etc. Con el fin de volver más robusto la seguridad de una red.

Para resolver un problema el primer paso es identificar las vulnerabilidades.

3.2. Configuraciones de hardening

3.2.1. Firewall

NOTA: trabajar en SafeMode para evitar posibles problemas de desconexión

- 1er Hardening, de tipo INPUT => Trafico dirigido hacia nuestro router.

ANTES DE EMPEZAR DEBE ESTAR CONFIGURADA LAS 6 REGLAS BASICAS DE FIREWALL.

REGLA QUE PERMITA LA ADMINISTRACION DEL MIKROTIK SOLAMENTE DESDE WAN y NEGAMOS TODOS OTROS INTENTOS DE ADMINISTRACION

GENERAL

Chain : input
Protocol : (6) tcp
Dst. Port : Puertos permitidos en IP->Services

<input checked="" type="checkbox"/>	ssh	22
<input checked="" type="checkbox"/>	telnet	23
<input checked="" type="checkbox"/>	winbox	8291

In. Interface : ether1 o la interface ethernet por donde vamos a realizar administración

ACTION

Action : accept
Marcar log : ☒ Log

- 2do Hardening, de tipo INPUT => Trafico dirigido hacia nuestro router
REGLA QUE PERMITA TODAS LAS CONSULTAS DNS DESDE LA LAN

GENERAL

Chain : input
Protocol : (17)udp
Dst. Port : 53 -> puerto de consultas DNS
In. Interface : ether3 -> Interface donde establecimos LAN

ACTION

Action : accept
Marcar log : ☒ Log

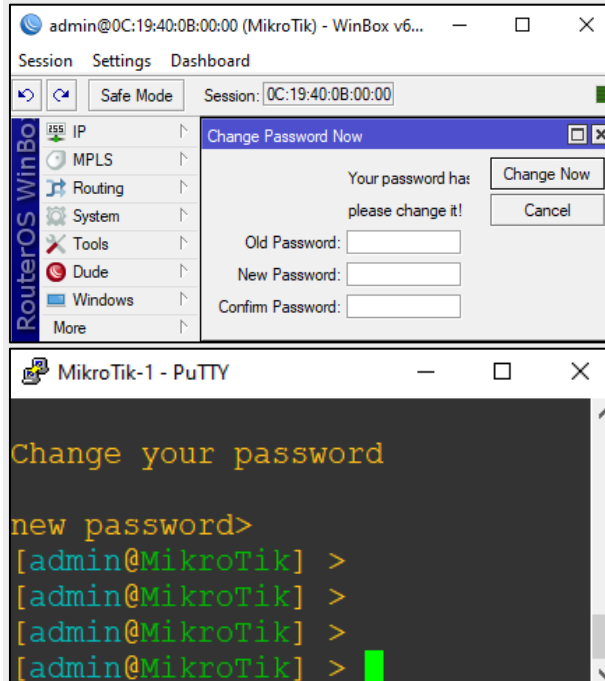
- 3er Hardening, de tipo input => Trafico dirigido hacia nuestro router.
DENEGAR TODO TRAFICO ENTRANTE

Quedando de la siguiente forma

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out...
0	acc...	forward							
1	drop	forward							
2	acc...	input							
3	drop	input							
4	acc...	output							
5	drop	output							
6	acc...	input			6 (tcp)		22,8291	ether1	
7	acc...	input			17 (u...		53	ether2	
8	drop	input							

Inicio de pruebas del funcionamiento

Acceso WinBox y SSH desde PC Admin del LAB (Aceptado)



Acceso SSH desde Ubuntu en LAN de MikroTik (Denegado)

```
root@osboxes:/home/osboxes# ssh admin@20.20.20.1
ssh: connect to host 20.20.20.1 port 22: Connection timed out
```

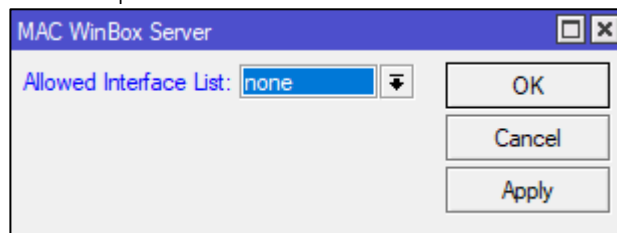
Con estas pocas reglas le sumamos mucha seguridad a nuestro router MikroTik

3.2.2. Mac telnet server

Sirve para esconder las identidades MAC de nuestro router MikroTik con el fin de que ningún dispositivo conectado pueda ver las direcciones MAC de nuestro router MikroTik agregando una capa de seguridad para nuestro router.

Esconder todas las direcciones MAC de nuestro router.

En Tools -> MAC_Seaver -> MAC WinBox Server, none, con el fin de que ninguna interface ethernet pueda conectar mediante WinBox a nuestro MikroTik.



Habilitar la visibilidad MAC solamente de una lista de interfaces Ethernet.

En **Interfaces -> Interface list -> List**, Creamos una lista de interfaces a la cual llamamos **MAC TELNET**

Ahora en **Interfaces -> Interface list**, con el nombre de lista que ya creamos agregamos una interface ethernet para que sea la única por donde se podrán acceder mediante WinBox.

Ahora en **Tools -> Mac Server -> WinBox MAC Server**, seleccionamos la lista de interfaces que creamos

De esta forma agregamos más seguridad a nuestro router.

3.2.3. IP Service List

Se recomienda deshabilitar todo lo que no se utiliza y solo dejar habilitado SSH y WinBox para que sean los únicos métodos de administración de nuestro router.

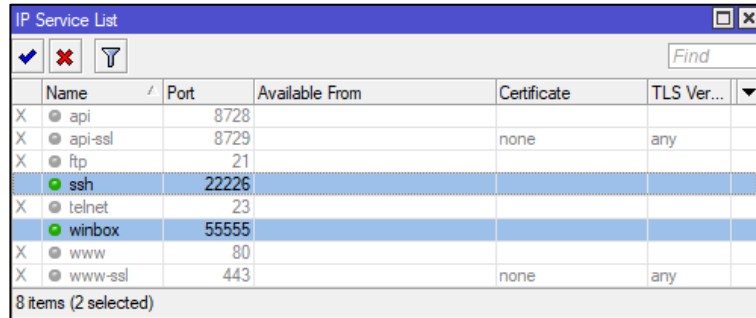
	Name	Port	Available From	Certificate	TLS Ver...
X	api	8728			
X	api-ssl	8729		none	any
X	ftp	21			
	ssh	22			
X	telnet	23			
	winbox	8291			
X	www	80			
X	www-ssl	443		none	any

8 items

3.2.4. Default ports

Para agregar una capa de seguridad más se recomienda cambiar los puertos de administración por defecto ya que si hacemos todo lo anterior en WinBox no deberíamos tener acceso desde otras interfaces ethernet si lo intentamos por la dirección MAC del router

pero si intentamos ingresar por la dirección IP del router tendremos acceso sin restricciones, es por eso que se debe cambiar los puertos de administración por defecto.



	Name	Port	Available From	Certificate	TLS Ver...
X	api	8728			
X	api-ssl	8729		none	any
X	ftp	21			
	ssh	22226			
X	telnet	23			
	winbox	55555			
X	www	80			
X	www-ssl	443		none	any

8 items (2 selected)

Con esto cumplimos gran parte del hardening incrementamos la seguridad de nuestro router en gran medida

MODULO 20
FIREWALL Y WEB FILTER.

4. Que es web filter?

Es el bloqueo de páginas para los usuarios no puedan navegar en ciertas paginas

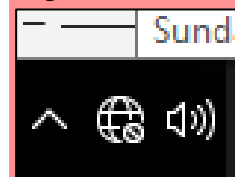
4.1. Modos de operación del firewall

4.1.1. Bloquear todo – permitir solo tráfico específico (NO RECOMENDABLE)

- En IP -> **Firewall** -> **FilterRules**, vamos a bloquear todo tráfico en el modo FORWARD. Agregamos una nueva regla en modo FORWARD sin especificar lo demás. Par indicarle al MikroTik la operación ANY = TODO, en action negamos todo con la opción DROP.

Firewall						
Filter Rules						
#	Action	Chain	Src. Address	Dst. Address	Proto.	
...	Negar toda navegacion					
0	✖ drop	forward				

La configuración realizada provocara la siguiente acción, debido a que estamos negando todo tráfico.



- Ahora vamos a configurar que solo podamos acceder a ciertas páginas.
En IP -> Firewall -> AddressList, vamos a crear una regla de páginas permitidas.

En FilterRules agregamos una nueva regla FORWARD

EN GENERAL – indicamos la interface que intentara acceder al internet

Con esto indicamos al router que esta configuración aplica solo a Eth-3 de LAN que intente atravesar el router hacia internet

EN ADVANCED – indicamos que el destino va ser solo las páginas permitidas.

EN ACTION – Aceptamos la conexión.

Ahora debemos posicionar la regla de aceptar antes que la regla de denegar, porque el router lee cada regla de arriba hacia abajo, primero acepta la conexión hacia las páginas permitidas y niega todo lo demás.

#	Action	Chain	Src. Address	Dst. Address
0	accept	forward		
1	drop	forward		

4.1.2. Permitir todo – Bloquear solo tráfico específico (CONFIGURACION RECOMENDABLE)

En IP -> Firewall -> AddressList

primero agregamos una Lista de direcciones donde vamos a especificar las páginas prohibidas de acceso

Ahora En IP -> Firewall -> FilterRules vamos a configurar en denegado de acceso a las páginas prohibidas.

EN GENERAL – en modo FORWARD especificando la interface de aplicación

EN ADVANCED – Especificamos el destino de tráfico (Paginas prohibidas)

EN ACTION

Ahora en IP -> Firewall -> FilterRules, vamos a configurar una regla para permitir acceso a todo lado

#	Action	Chain
0	drop	forward
1	accept	forward