

“Una red empieza a ser segura, cuando conociendo usuario y contraseña, no podemos acceder a ella”

Partiendo de esta primicia, detallamos la seguridad propia de un dispositivo Mikrotik.

Servicios

Mikrotik dispone de varios servicios que, en caso de no ser utilizados, deberían estar **DESHABILITADOS**.

Proxy http – Menú IP -> WebProxy

The image shows the 'Web Proxy Settings' dialog box in Mikrotik WinBox. The 'General' tab is selected. The 'Enabled' checkbox is checked and highlighted in yellow. The 'Src. Address' is set to '::'. The 'Port' is set to '8080'. The 'Anonymous' checkbox is unchecked. The 'Parent Proxy' and 'Parent Proxy Port' fields are empty. The 'Cache Administrator' is set to 'webmaster'. The 'Max. Cache Size' is set to 'unlimited' KiB. The 'Max Cache Object Size' is set to '2048' KiB. The 'Cache On Disk' checkbox is unchecked. The 'Max. Client Connections' is set to '600'. The 'Max. Server Connections' is set to '600'. The 'Max Fresh Time' is set to '3d 00:00:00'. The 'Serialize Connections' and 'Always From Cache' checkboxes are unchecked. The 'Cache Hit DSCP (TOS)' is set to '4'. The 'Cache Path' is set to 'web-proxy'. The status bar at the bottom indicates 'stopped'.

Field	Value
Enabled	<input checked="" type="checkbox"/>
Src. Address	::
Port	8080
Anonymous	<input type="checkbox"/>
Parent Proxy	
Parent Proxy Port	
Cache Administrator	webmaster
Max. Cache Size	unlimited KiB
Max Cache Object Size	2048 KiB
Cache On Disk	<input type="checkbox"/>
Max. Client Connections	600
Max. Server Connections	600
Max Fresh Time	3d 00:00:00
Serialize Connections	<input type="checkbox"/>
Always From Cache	<input type="checkbox"/>
Cache Hit DSCP (TOS)	4
Cache Path	web-proxy

DNS Caché – Menú: IP -> DNS

The screenshot shows the 'DNS Settings' window with the following fields and controls:

- Servers: [Dropdown menu]
- Dynamic Servers: 8.8.8.8, 9.9.9.9, 8.8.4.4
- Allow Remote Requests (highlighted in yellow)
- Max UDP Packet Size: 4096
- Query Server Timeout: 2.000 s
- Query Total Timeout: 10.000 s
- Max. Concurrent Queries: 100
- Max. Concurrent TCP Sessions: 20
- Cache Size: 2048 KiB
- Cache Max TTL: 7d 00:00:00
- Cache Used: 17 KiB

Buttons on the right: OK, Cancel, Apply, Static, Cache.

Samba (compartición de archivos) – Menú: IP -> SMB

The screenshot shows the 'SMB Settings' window with the following fields and controls:

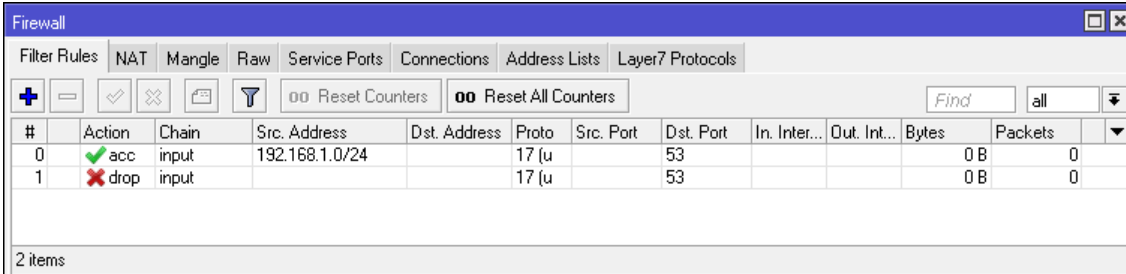
- Enabled (highlighted in yellow)
- Domain: MSHOME
- Comment: MikrotikSMB
- Allow Guests
- Interfaces: all

Buttons on the right: OK, Cancel, Apply, Shares, Users.

En caso de requerir poner en producción alguno de ellos, debemos restringir su acceso por firewall, es decir, **¿desde donde deben ser accesibles estos servicios?** Por ejemplo:

- Queremos habilitar el DNS Caché para nuestra red interna 192.168.1.0/24

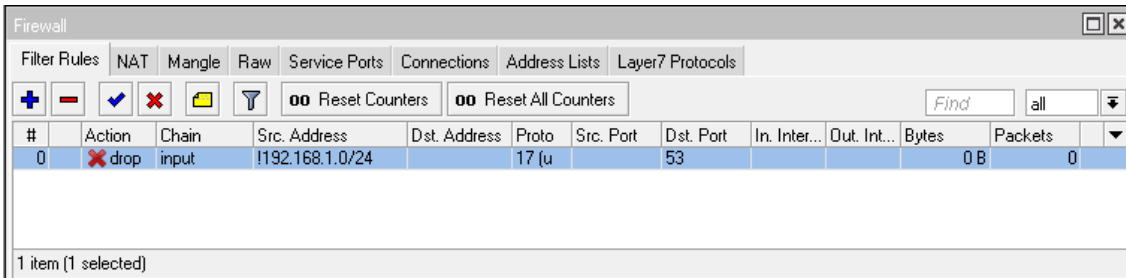
Permitimos el acceso en el chain input (conexión entrante al propio Mikrotik) al puerto UDP/53 desde el origen 192.168.1.0/24, y el resto lo descartamos:



#	Action	Chain	Src. Address	Dst. Address	Proto	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
0	✓ acc	input	192.168.1.0/24		17 (u)		53			0 B	0
1	✗ drop	input			17 (u)		53			0 B	0

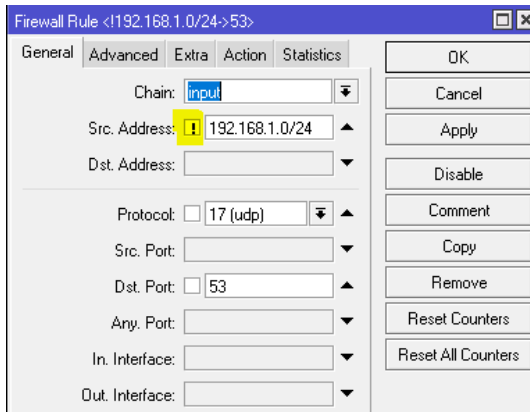
2 items

Un poco más elegante: Todo lo que NO sea 192.168.1.0/24, lo descartamos:



#	Action	Chain	Src. Address	Dst. Address	Proto	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
0	✗ drop	input	!192.168.1.0/24		17 (u)		53			0 B	0

1 item (1 selected)



Firewall Rule <192.168.1.0/24>53

General | Advanced | Extra | Action | Statistics

Chain: input

Src. Address: ! 192.168.1.0/24

Dst. Address:

Protocol: 17 (udp)

Src. Port:

Dst. Port: 53

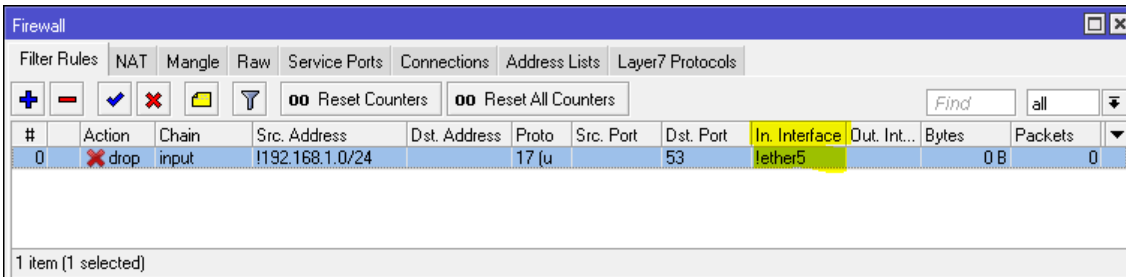
Any. Port:

In. Interface:

Out. Interface:

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, Reset All Counters

También podemos especificar interfaces, siempre recomendamos que las reglas sean lo más específicas posible. (todo lo que no sea 192.168.1.0/24 y acceda por ether5, donde ether5 es la interfaz del rango 192.168.1.0/24):



#	Action	Chain	Src. Address	Dst. Address	Proto	Src. Port	Dst. Port	In. Interface	Out. Int...	Bytes	Packets
0	✗ drop	input	!192.168.1.0/24		17 (u)		53	ether5		0 B	0

1 item (1 selected)

SNMP – Menú IP -> SNMP

SNMP Settings

Enabled

Contact Info:

Location:

Engine ID:

Trap Target:

Trap Community: public

Trap Version: 1

Trap Generators:

Trap Interfaces:

Src. Address:

OK
Cancel
Apply
Communities

En caso de que el dispositivo no se vaya a monitorizar, se recomienda deshabilitar el servicio.

Si queremos monitorizar el dispositivo, deberemos especificar la IP del agente SNMP desde la cual accederemos a ellos:

SNMP Settings

Enabled

Contact Info:

Location:

Engine ID:

Communities

SNMP Communities

Name	Addresses	Security	Read Ac...	Write Acc
public	::/0	none	yes	no

SNMP Community <public>

Name: public

Addresses: 10.254.32.4

Security: none

Read Access

Write Access

Authentication Protocol: MD5

Encryption Protocol: DES

Authentication Password:

Encryption Password:

OK
Cancel
Apply
Copy
Remove

Únicamente deberíamos permitir el acceso de lectura.

Puertos de gestión – Menú IP -> Services

Por defecto:

The screenshot shows the 'IP Service List' window with a table of services. The 'Available From' column is empty for all services, and the 'Certificate' column shows 'none' for 'api-ssl' and 'www-ssl'. The status icons for all services are green circles with a dot.

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

8 items

Recomendado:

Salvo casos puntuales de software de terceros (uso de API), skins de instaladores o similares, lo común es usar los servicios de ssh y winbox para gestionar dispositivos Mikrotik. Todos aquellos servicios que no se utilicen deben de estar DESHABILITADOS.

The screenshot shows the 'IP Service List' window with the same table of services. In this configuration, the status icons for 'api', 'api-ssl', 'telnet', 'www', and 'www-ssl' are red 'X' marks, indicating they are disabled. The status icons for 'ftp', 'ssh', and 'winbox' are green circles with a dot, indicating they are enabled. The 'Available From' and 'Certificate' columns remain the same as in the previous screenshot.

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

8 items

Y ahora la pregunta, **¿desde DONDE debe ser accesible el uso de estos servicios?**

Imaginemos que nuestra red de gestión donde disponemos de distintos servicios que deben tener acceso a los dispositivos Mikrotik tiene el rango 172.16.0.0/25, y cómo hemos hecho un buen diseño, el pool de VPN es el rango 172.16.0.128/25.

Así pues, sumalizando podemos decir que nuestra “red segura” es el rango: 172.16.0.0/24

Si no especificamos el parámetro “Available From”, por defecto RouterOS usa 0.0.0.0/0, es decir, desde cualquier dirección IP origen. Para restringir el acceso únicamente a nuestra “red segura” (en el ejemplo: 172.16.0.0/24), especificamos dicho parámetro:

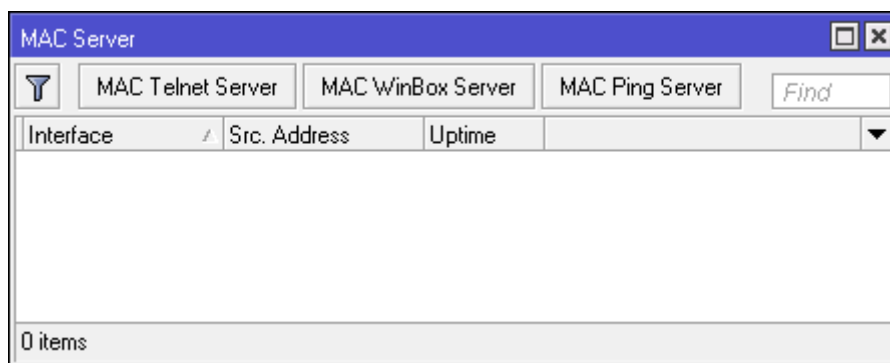
	Name	Port	Available From	Certificate
X	api	8728		
X	api-ssl	8729		none
X	ftp	21		
	ssh	22	172.16.0.0/24	
X	telnet	23		
	winbox	8291	172.16.0.0/24	
X	www	80		
X	www-ssl	443		none

8 items (1 selected)

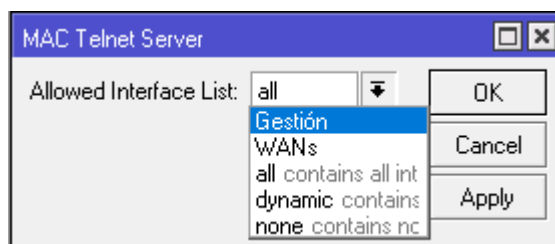
Otras funcionalidades

MAC- Server – Menú: Tools → MAC Server

RouterOS dispone de servicios en capa 2 como MAC-Winbox o MAC-Telnet.



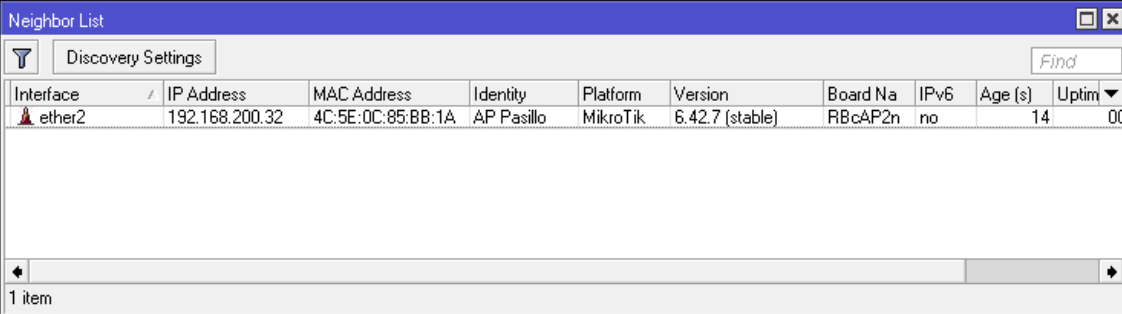
Estos servicios funcionan con “Interface List” (recordemos que son servicios de capa 2, por lo que pasamos de IP a interface):



Recomendamos que estos servicios únicamente sean accesibles (en su caso) por interfaces de gestión.

Neighbors – Menú: IP -> Neighbors

Del mismo modo, cuando menos información pueda tener un “vecino” no seguro de nosotros, mejor. Recomendamos deshabilitar el “discovery” en todas las interfaces no seguras.

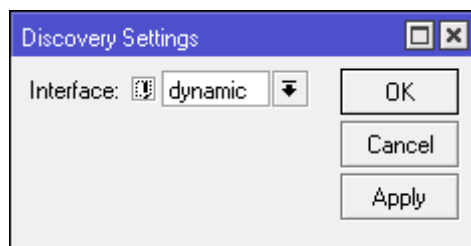


The screenshot shows a window titled "Neighbor List" with a "Discovery Settings" tab. It contains a table with the following data:

Interface	IP Address	MAC Address	Identity	Platform	Version	Board Na	IPv6	Age (s)	Uptime
ether2	192.168.200.32	4C:5E:0C:85:BB:1A	AP Pasillo	MikroTik	6.42.7 (stable)	RBcAP2n	no	14	00

At the bottom of the window, it indicates "1 item".

En las nuevas versiones disponemos de un parámetro llamado “dynamic” (por ejemplo, conexiones pppoe), por lo que podemos especificar que esté habilitado en todas las interfaces NO dinámicas (así viene por defecto).



Servicio VPN

Geo-IP filter.

Existen herramientas para obtener listas de direcciones (address-list) de direccionamiento público de cada país:

<https://mikrotikconfig.com/firewall/>

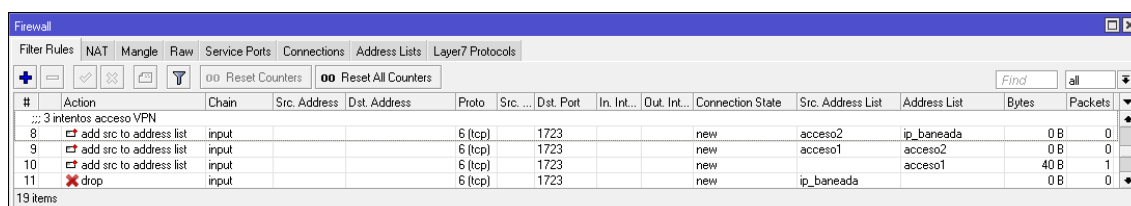
Podemos especificar, por ejemplo, que el acceso VPN sólo esté permitido desde una IP perteneciente a España. Estas listas de direccionamiento público deberán ser actualizadas cada cierto tiempo. (tres meses, por ejemplo).

#	Action	Chain	Src. Address	Dst. Address	Proto	Src. ...	Dst. Port	In. Int...	Out. Int...	Connection State	Src. Address List	Address List	Bytes	Packets
... Acceso VPN sólo Spain														
0	✖ drop	input			6 (tcp)		1723			new	Spain		0 B	0

La regla descarta la conexión si el origen NO (exclamación antes del argumento) pertenece al "address-list" de direcciones IP españolas.

Restricción de accesos.

Paralelamente, también es recomendable restringir el número de intentos de conexión al servicio VPN. Por ejemplo, podemos crear una serie de reglas, tales que tras tres intentos de conexión erróneos nos "banea" la dirección IP de origen durante 4 horas (por ejemplo).



#	Action	Chain	Src. Address	Dst. Address	Proto	Src. ...	Dst. Port	In. Int...	Out. Int...	Connection State	Src. Address List	Address List	Bytes	Packets
... 3 intentos acceso VPN														
8	➕ add src to address list	input			6 (tcp)		1723			new	acceso2	ip_baneada	0 B	0
9	➕ add src to address list	input			6 (tcp)		1723			new	acceso1	acceso2	0 B	0
10	➕ add src to address list	input			6 (tcp)		1723			new		acceso1	40 B	1
11	✖ drop	input			6 (tcp)		1723			new	ip_baneada		0 B	0

En este caso no especificamos la dirección de destino, ya que queremos que la regla aplique a cualquiera de las direcciones IP del propio dispositivo.