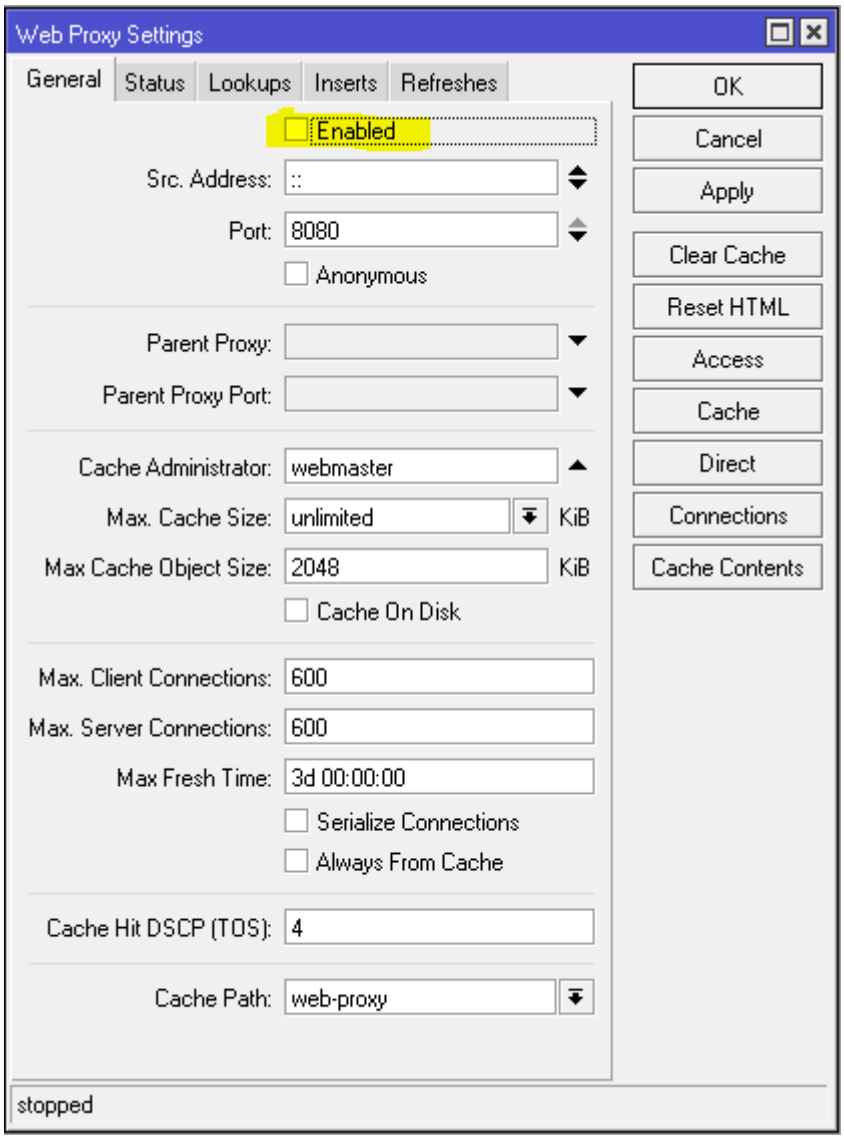
“Una red empieza a ser segura, cuando conociendo usuario y contraseña, no podemos acceder a ella”

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

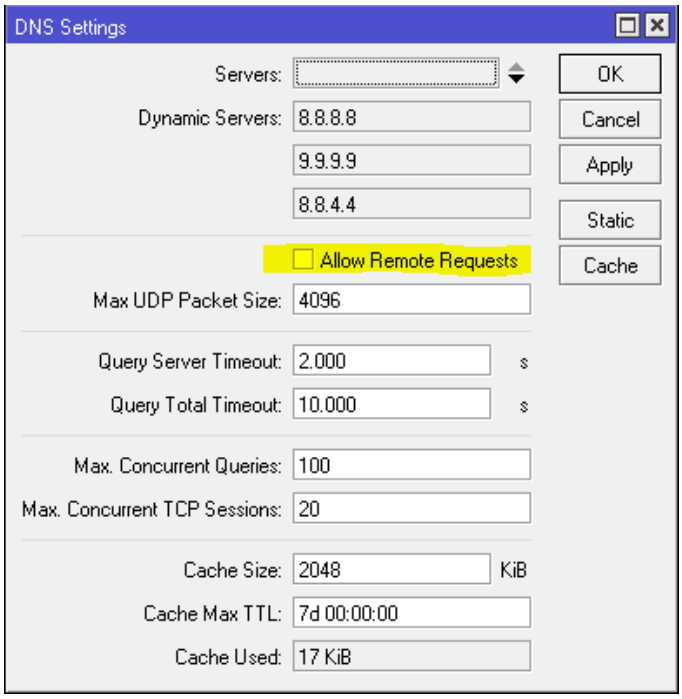
Servicios

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

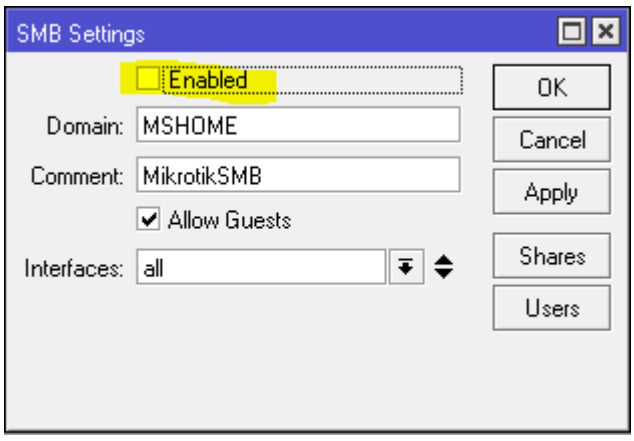
Proxy http – Menú IP -> WebProxy



DNS Caché – Menú: IP -> DNS



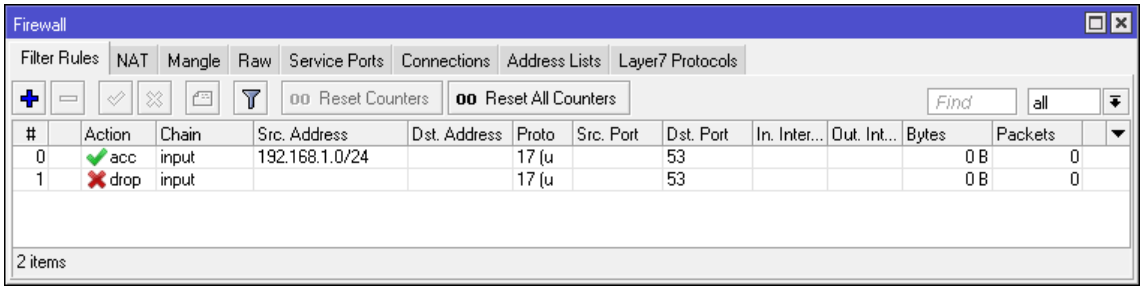
Samba (compartición de archivos) – Menú: IP -> SMB



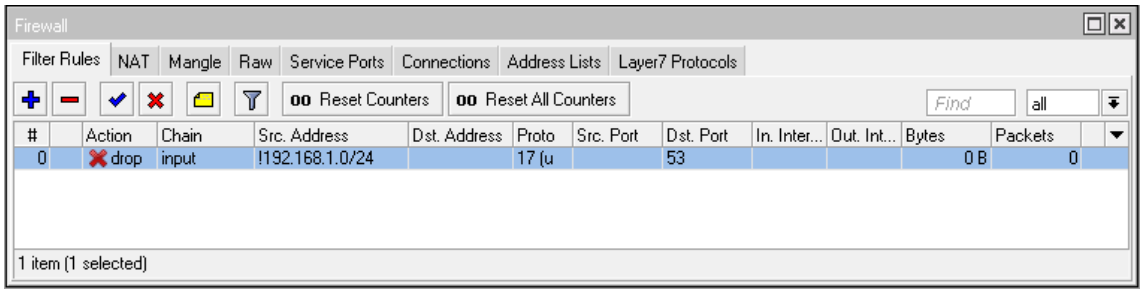
En caso de requerir poner en producción alguno de ellos, debemos restringir su acceso por firewall, es decir, **¿desde donde deben ser accesibles estos servicios?** Por ejemplo:

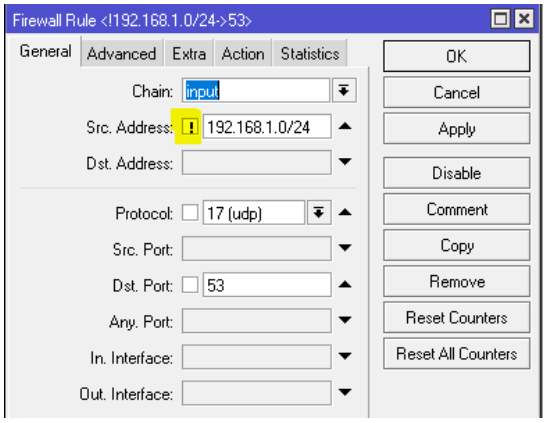
- Queremos habilitar el DNS Caché para muestra red interna 192.168.1.0/24

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:

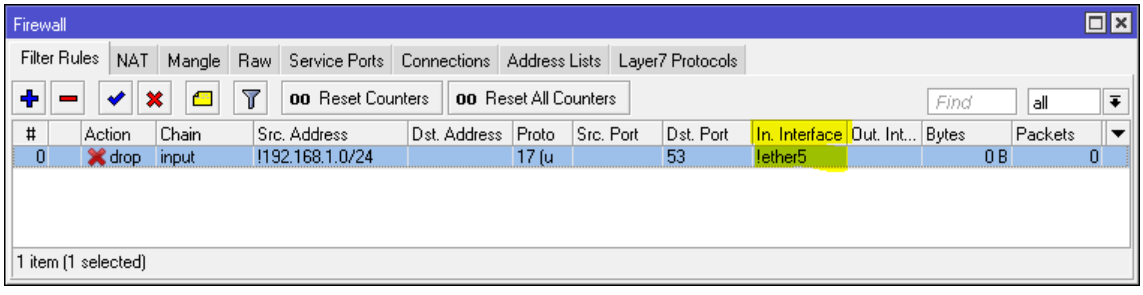


Un poco más elegante: Todo lo que NO sea 192.168.1.0/24, lo descartamos:

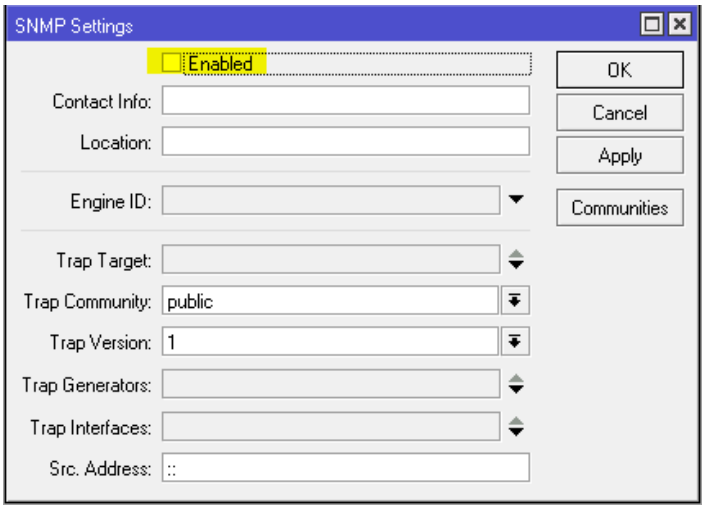




También podemos especificar interfaces, siempre recomendamos que las reglas sean lo más específicas posible. (todo lo que no sea 192.168.1.0/24 y acceda por ether5, donde ether5 es la interfaz del rango 192.168.1.0/24):

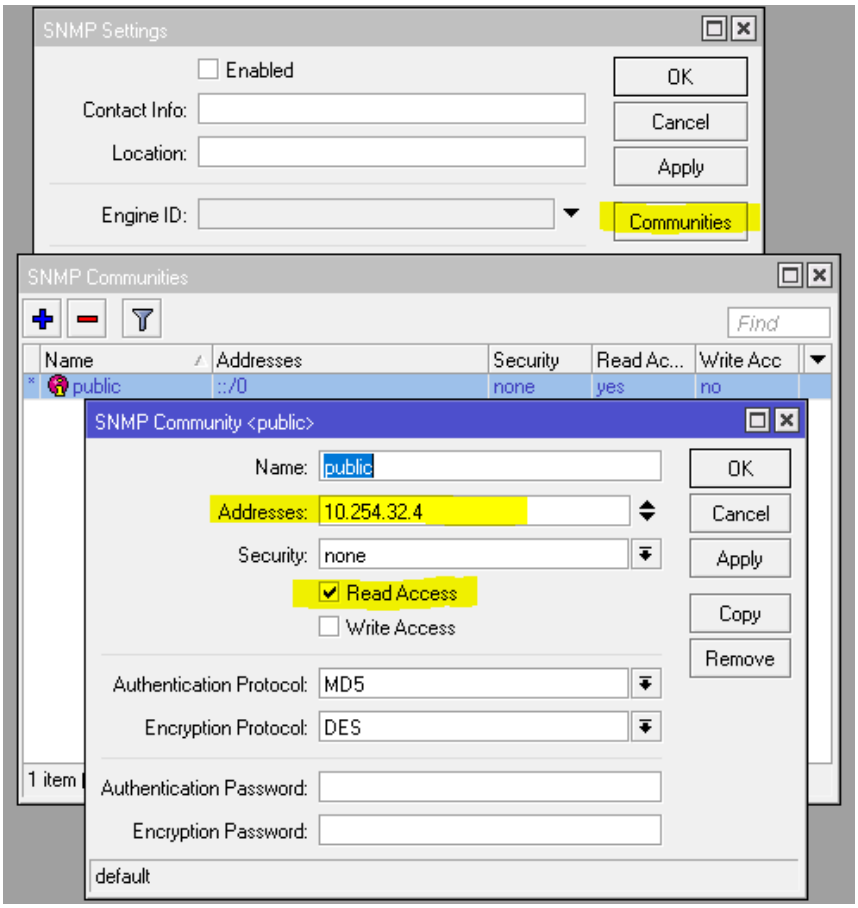


SNMP – Menú IP -> SNMP



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

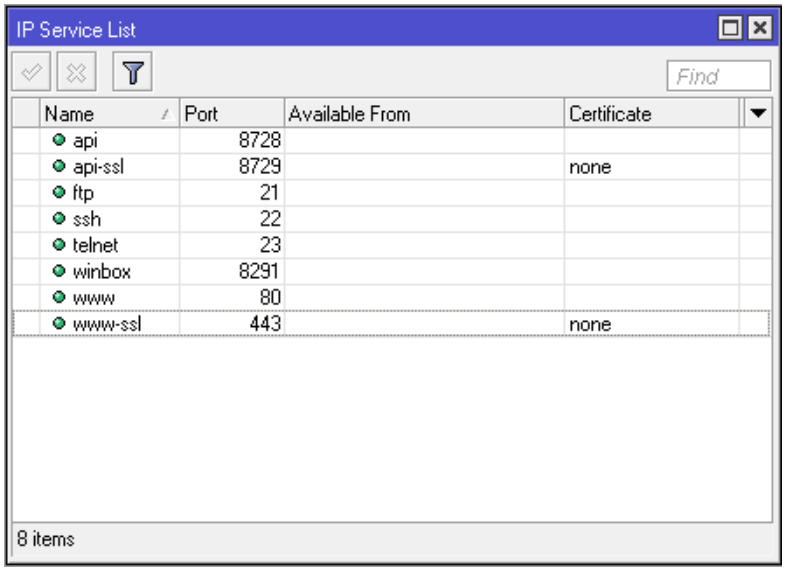
Si queremos monitorizar el dispositivo, deberemos especificar la IP del agente SNMP desde la cual accederemos a ellos:



Únicamente deberíamos permitir el acceso de lectura.

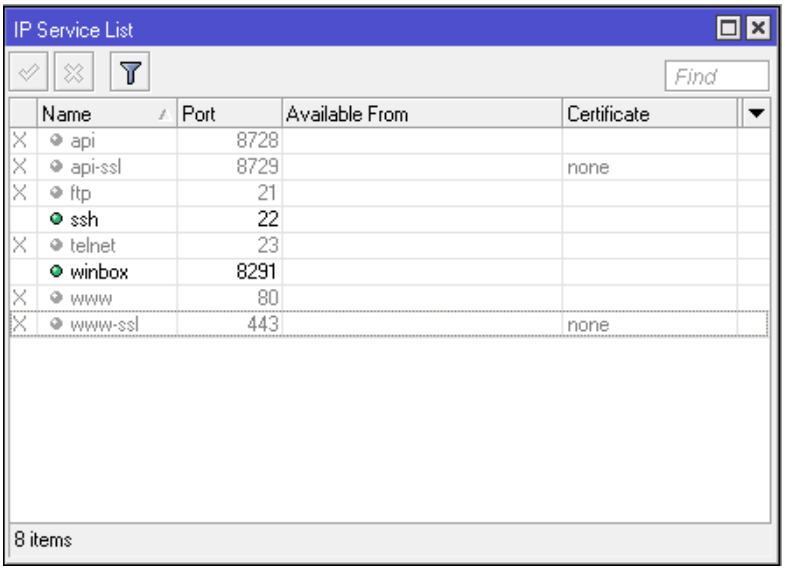
Puertos de gestión – Menú IP -> Services

Por defecto:



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.

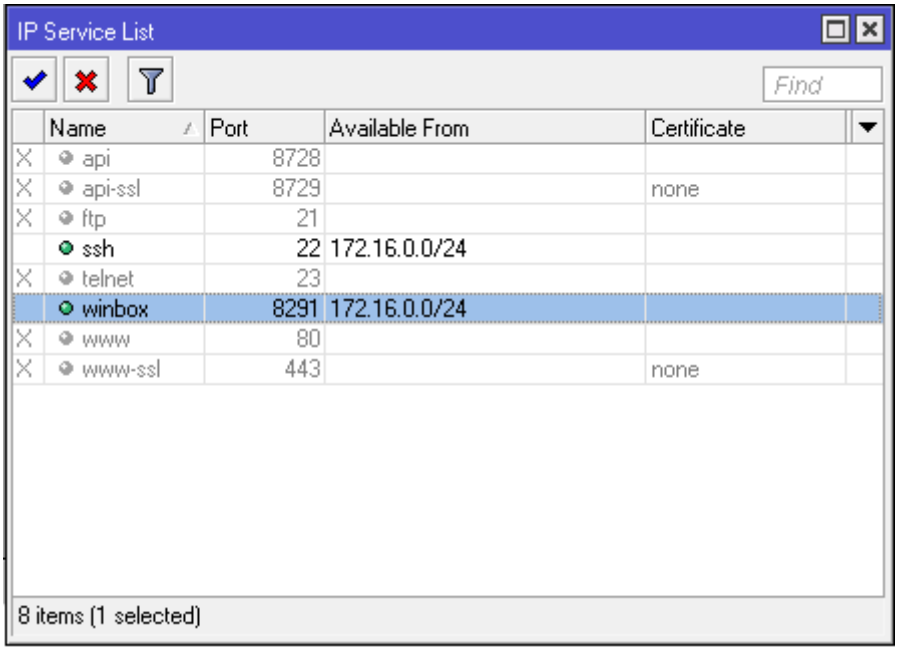


Y ahora la pregunta, **¿desde DONDE debe ser accesible el uso de estos servicios?**

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, sumarizando podemos decir que nuestra "red segura" es el rango: 172.16.0.0/24

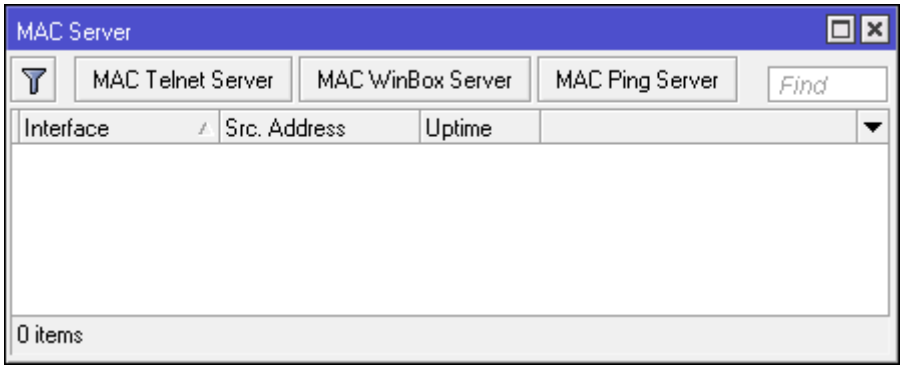
Si no especificamos el parámetro "Available From", por defecto RouterOS usa 0.0.0.0/0, es decir, desde cualquier dirección IP origen. Para restringir el acceso únicamente a nuestra "red segura" (en el ejemplo: 172.16.0.0/24), especificamos dicho parámetro:



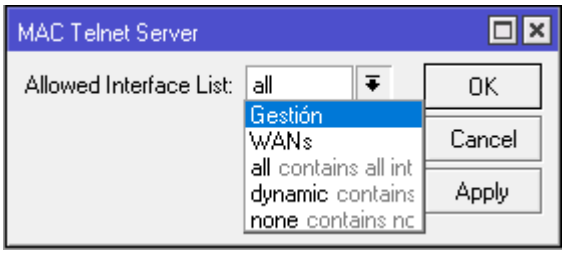
Otras funcionalidades

MAC- Server – Menú: Tools –> MAC Server

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



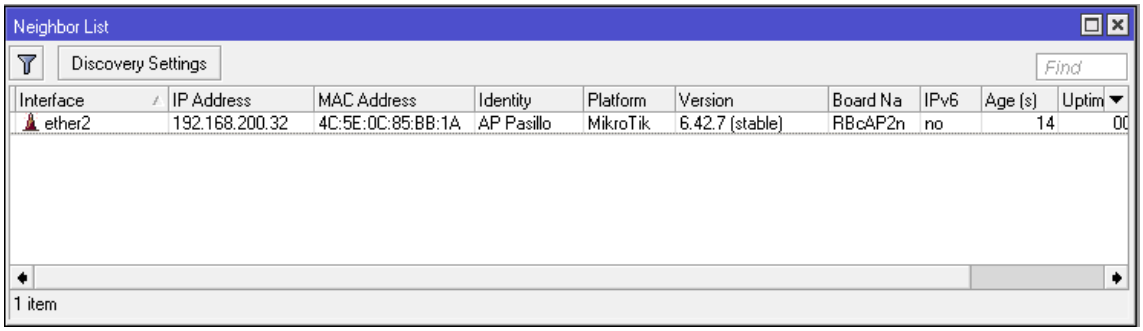
Estos servicios funcionan con "Interface List" (recordemos que son servicios de capa 2, por lo que pasamos de IP a interface):



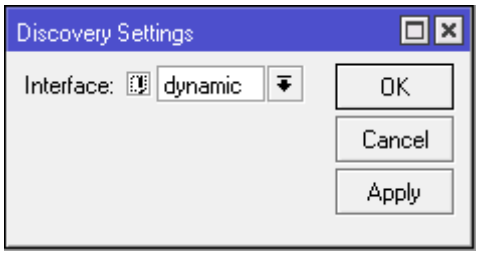
Recomendamos que estos servicios únicamente sean accesibles (en su caso) por interfaces de gestión.

Neighboors – 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.



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/

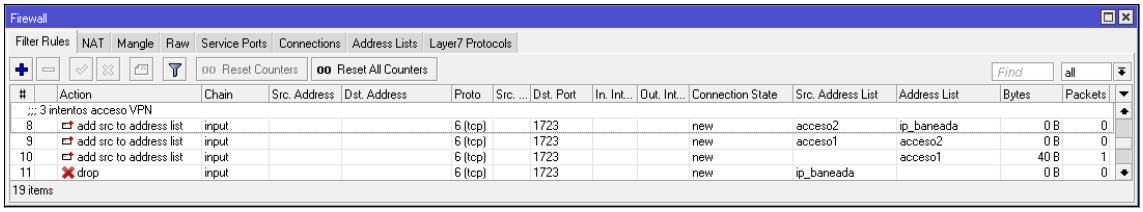
Podemos especificar, por ejemplo, que el acceso VPN sólo esté permitido desde una IP perteneciente a España. Estas listas de direccionamiento público deberán ser actualizadas cada cierto tiempo. (tres meses, por ejemplo).

#	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 "banee" la dirección IP de origen durante 4 horas (por ejemplo).



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.