Mejora de red y espacio compartido

Solgata S.A.U. - Anexo Firewall

sòlgata
societat municipal
de gestió

Índice

1. Introducción

En el entorno empresarial actual, la seguridad de la red es una prioridad absoluta para proteger los datos sensibles y garantizar el funcionamiento ininterrumpido de las operaciones. La implementación de un firewall eficaz es crucial para defenderse contra amenazas externas y accesos no autorizados. Este anexo describe la configuración de un firewall en dispositivos MikroTik, centrándose en el uso de listas de direcciones (address lists) y listas de bloqueo (block lists) para mejorar la seguridad y el control del tráfico de red.

MikroTik ofrece potentes capacidades de firewall que permiten una configuración detallada y precisa para gestionar el tráfico de red. Una de las características clave de los firewalls de MikroTik es la capacidad de crear y utilizar listas de direcciones y listas de bloqueo. Estas herramientas permiten a los administradores de red definir y aplicar políticas de seguridad específicas, facilitando un control más granular y efectivo sobre el tráfico que atraviesa la red.

Las listas de direcciones en MikroTik permiten agrupar varias direcciones IP bajo un nombre común, simplificando la gestión y aplicación de reglas de firewall. Por ejemplo, se pueden crear listas de direcciones para categorizar IPs confiables, sospechosas o de ciertos rangos geográficos, facilitando la implementación de políticas de seguridad diferenciadas.

2. Configuración

Para la configuración del firewall, yo lo haré de manera rápida porque ya los tengo agregados en un archivo de configuración rsc. Este archivo lo que permite es que desde el terminal del sistema operativo del switch poder implementar cualquier archivo de configuración a base de comandos. En breve, explicaré cada comando y todas las líneas en general.

Lo implementaremos en el Switch Mikrotik, al cual entraremos mediante Winbox64, y configuraremos todos los parámetros para hacer que tenga una protección activa. Cabe recalcar que lo dividiremos en dos bloques según su uso, Reglas de filtrado y NAT. Dentro de las reglas de filtrado explicaremos un poco reglas generales para la LAN y luego mas en profundidad las reglas que hemos creado para la protección de las dos WAN.

2.1 Configuración de reglas de Filtrado

2.1.1 Configuración de reglas para la LAN

Empezaremos explicando la configuración de las reglas para la LAN (bridge1-LAN).

Ilustración 1: Reglas de filtrado de la LAN en el firewall de Mikrotik

En primer lugar, la primera línea indica que vamos a cambiar la configuración en IP>Firewall en el apartado de filter, que son reglas de filtrado.

-add action=accept chain=input src-address=192.168.30.0/24 \ comment="Aceptar trafic de la red 192.168.30.0 (LAN)"

En esta regla lo que indicamos es que acepte el tráfico de entrada de la subred 192.168.30.0/24 y además le añadimos un comentario para hacerlo mas visual.

-add action=accept chain=output protocol=1 out-interface=bridge1-LAN \ comment="Aceptar trafic ping per la interfaz bridge(LAN)"

-add action=accept chain=input protocol=1 in-interface=bridge1-LAN

En estas dos reglas, lo que hacemos es permitir el tráfico de entrada y saliente por la interfaz bridge1-LAN de el protocolo ICMP (puerto 1) que es sinónimo a ping.

2.1.2 Configuración de las reglas para la WAN

En este punto, vamos a explicar la configuración para la address list WAN1 que creamos en el apartado de interfaces del switch mikrotik, esta lista de interfaces, como no queremos repetir todas las reglas dos veces para cada una de las WAN, nos iremos a interfaces>address lists y en listas veremos las dos listas que creamos, WAN1 con eth1-WAN y WAN2 con eth2-WAN. Ahora lo que haremos, será hacer que la lista WAN1, también contenga la lista WAN2, es decir, que con solo aplicar la configuración a WAN1 también la aplicaríamos para WAN2.

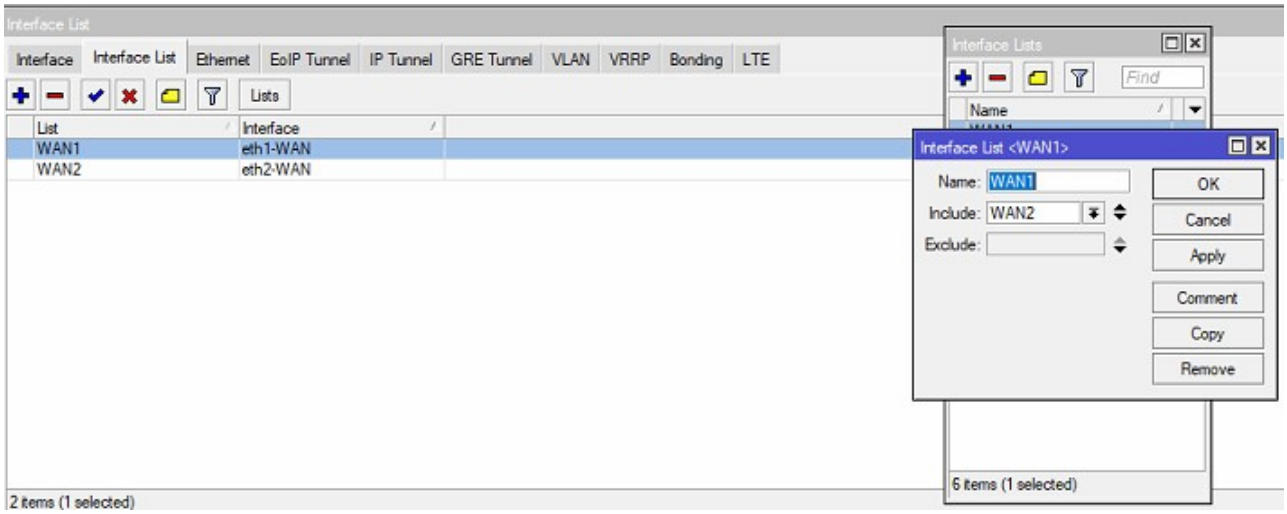


Ilustración 2: Lista de direcciones WAN1, la cual contiene WAN2 para la configuración del Firewall en Mikrotik

Ahora, explicaremos las reglas de configuración de esta address list.

Bloqueo TELNET

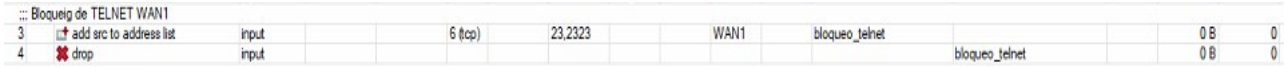


Ilustración 3: Reglas de bloqueo de telnet para las conexiones entrantes de la WAN en el firewall de Mikrotik

-add action=add-src-to-address-list address-list=bloqueo_telnet address-list-timeout=2w chain=input \ comment="Bloqueig de TELNET WAN1" dst-port=23,2323 in-interface-list=WAN1 protocol=tcp

-add action=drop chain=input src-address-list=bloqueo_telnet

Primera regla: Cada vez que alguien intenta conectarse a los puertos Telnet (23 o 2323) a través de la interfaz WAN1, la dirección IP de origen de esta solicitud se agrega a la lista de direcciones bloqueo_telnet por un periodo de 2 semanas.

Segunda regla: Luego, cualquier paquete entrante cuyo origen esté en la lista bloqueo_telnet se descarta automáticamente.

Bloqueo SSH

Ilustración 4: Reglas de bloqueo de SSH para las conexiones entrantes de la WAN en el firewall de Mikrotik

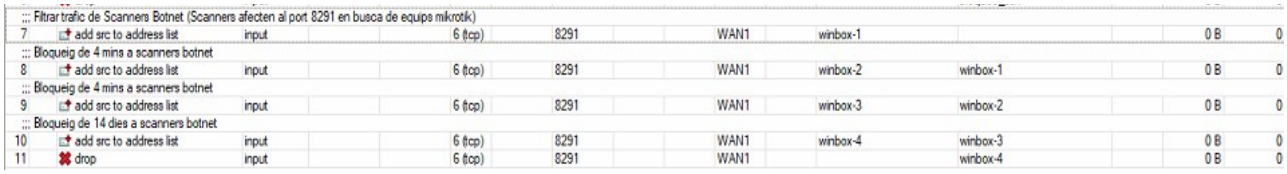
-add action=add-src-to-address-list address-list=bloqueo_ssh address-list-timeout=2w chain=input / comment="Bloqueig de SSH WAN1" dst-port=22 in-interface-list=WAN1 protocol=tcp

-add action=drop chain=input src-address-list=bloqueo_ssh

Primera regla: Cada vez que alguien intenta conectarse al puerto SSH (22) a través de la interfaz WAN1, la dirección IP de origen de esta solicitud se agrega a la lista de direcciones bloqueo_ssh por un periodo de 2 semanas.

Segunda regla: Luego, cualquier paquete entrante cuyo origen esté en la lista bloqueo_ssh se descarta automáticamente.

Bloqueo Winbox



;;; Filtrar trafic de Scanners Botnet (Scanners afecten al port 8291 en busca de equips mikrotik)											
7	add src to address list	input		6 (tcp)	8291		WAN1	winbox-1			0 B	0
;;; Bloqueig de 4 mins a scanners botnet											
8	add src to address list	input		6 (tcp)	8291		WAN1	winbox-2	winbox-1		0 B	0
;;; Bloqueig de 4 mins a scanners botnet											
9	add src to address list	input		6 (tcp)	8291		WAN1	winbox-3	winbox-2		0 B	0
;;; Bloqueig de 14 dies a scanners botnet											
10	add src to address list	input		6 (tcp)	8291		WAN1	winbox-4	winbox-3		0 B	0
11	drop	input		6 (tcp)	8291		WAN1		winbox-4		0 B	0

Ilustración 5: Reglas de bloqueo de Winbox para las conexiones entrantes de la WAN en el firewall de Mikrotik

-add chain=input protocol=tcp dst-port=8291 src-address-list=winbox-4 action=drop \ in-interface-list=WAN1 comment="Filtrar trafic de Scanners Botnet (Scanners afecten al port 8291 en busca de equips mikrotik)"

-add chain=input protocol=tcp dst-port=8291 action=add-src-to-address-list \ address-list=winbox-1 address-list-timeout=00:04:00 \ in-interface-list=WAN1

-add chain=input protocol=tcp dst-port=8291 src-address-list=winbox-1 action=add-src-to-address-list \ address-list=winbox-2 address-list-timeout=00:04:00 \ in-interface-list=WAN1

-add chain=input protocol=tcp dst-port=8291 src-address-list=winbox-2 action=add-src-to-address-list \ address-list=winbox-3 address-list-timeout=00:04:00 \ in-interface-list=WAN1

-add chain=input protocol=tcp dst-port=8291 src-address-list=winbox-3 action=add-src-to-address-list \ address-list=winbox-4 address-list-timeout=2w \ in-interface-list=WAN1 comment="Bloqueig de 14 dies a scanners botnet"

Primera Regla: Añade la dirección IP de origen a la lista winbox-1 si intenta conectarse al puerto 8291, con un tiempo de permanencia de 4 minutos.

Segunda Regla: Si la IP de origen ya está en la lista winbox-1 y vuelve a intentar conectarse al puerto 8291 dentro de esos 4 minutos, se añade a la lista winbox-2, también por 4 minutos.

Tercera Regla: Si la IP de origen ya está en la lista winbox-2 y vuelve a intentar conectarse al puerto 8291 dentro de esos 4 minutos, se añade a la lista winbox-3, también por 4 minutos.

Cuarta Regla: Si la IP de origen ya está en la lista winbox-3 y vuelve a intentar conectarse al puerto 8291 dentro de esos 4 minutos, se añade a la lista winbox-4 por 2 semanas. Esto indica que la IP ha realizado múltiples intentos de conexión, probablemente de forma maliciosa, y se bloquea durante 14 días.

Quinta Regla: Bloquea inmediatamente el tráfico entrante al puerto 8291 si la IP de origen está en la lista winbox-4, que es una lista de direcciones de origen bloqueadas.

Bloqueo DNS

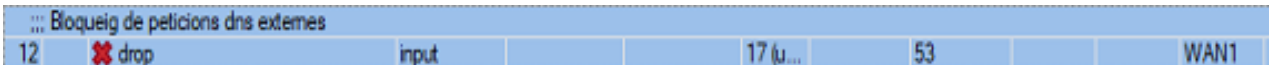


Ilustración 6: Reglas de bloqueo de peticiones DNS para las conexiones entrantes de la WAN en el firewall de Mikrotik

-add action=drop chain=input comment="Bloqueig de peticions dns externes" dst-port=53 \ in-interface-list=WAN1 protocol=udp

La regla tiene como objetivo principal bloquear cualquier solicitud DNS entrante desde redes externas hacia el router. Esto ayuda a proteger el router y la red interna de posibles abusos y ataques externos.

Bloqueo de proxys web externos

Ilustración 7: Reglas de bloqueo de peticiones web para las conexiones entrantes de la WAN en el firewall de Mikrotik

-add action=drop chain=input comment="Bloqueig de proxys web externs" \ dst-port=8080 in-interface-list=WAN1 protocol=tcp

Esta regla de firewall es una medida de seguridad importante para cualquier red que utilice un router MikroTik. Al bloquear el tráfico entrante destinado a proxys web a través del puerto 8080 desde interfaces conectadas a redes externas, se protege el router contra posibles abusos y ataques, y se optimiza su rendimiento, asegurando que solo el tráfico legítimo y autorizado sea procesado.

Bloqueo de Spamware

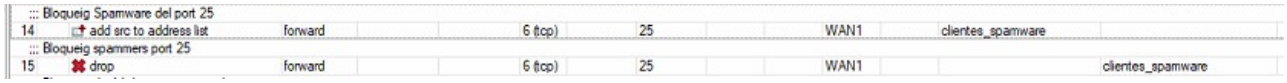


Ilustración 8: Reglas de bloqueo de spamware para las conexiones entrantes de la WAN en el firewall Mikrotik

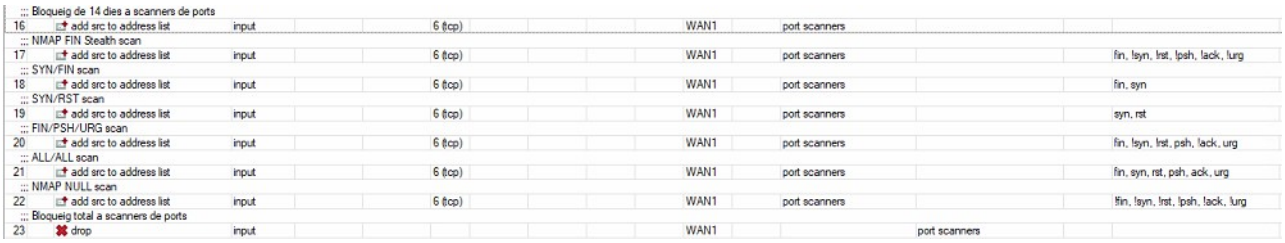
-add chain=forward protocol=tcp dst-port=25 connection-limit=30,32 limit=50,5 \ action=add-src-to-address-list address-list=clientes_spamware address-list-timeout=1d \ comment="Bloqueig Spamware del port 25" in-interface-list=WAN1

-add chain=forward protocol=tcp dst-port=25 src-address-list=clientes_spamware \ action=drop comment="Bloqueig spammers port 25" in-interface-list=WAN1

La primera regla detecta direcciones IP que intentan establecer un número excesivo de conexiones al puerto 25 en un corto periodo de tiempo, lo cual es un comportamiento típico de spamware. Cuando se detecta tal comportamiento, la dirección IP de origen se añade a la lista clientes_spamware durante un día.

La segunda regla descarta automáticamente cualquier tráfico TCP destinado al puerto 25 si la dirección IP de origen está en la lista clientes_spamware. Esto previene que IPs detectadas como posibles spammers puedan enviar más correos electrónicos a través del router.

Bloqueo a escáneres de puertos



	;;; Bloqueig de 14 dies a scanners de ports									
16	add src to address list	input		6 (tcp)			WAN1	port scanners		
	;;; NMAP FIN Stealth scan									
17	add src to address list	input		6 (tcp)			WAN1	port scanners		fin, !syn, !rst, !psh, !ack, !urg
	;;; SYN/FIN scan									
18	add src to address list	input		6 (tcp)			WAN1	port scanners		fin, syn
	;;; SYN/RST scan									
19	add src to address list	input		6 (tcp)			WAN1	port scanners		syn, rst
	;;; FIN/PSH/URG scan									
20	add src to address list	input		6 (tcp)			WAN1	port scanners		fin, !syn, !rst, psh, !ack, urg
	;;; ALL/ALL scan									
21	add src to address list	input		6 (tcp)			WAN1	port scanners		fin, syn, rst, psh, ack, urg
	;;; NMAP NULL scan									
22	add src to address list	input		6 (tcp)			WAN1	port scanners		!fin, !syn, !rst, !psh, !ack, !urg
	;;; Bloqueig total a scanners de ports									
23	drop	input					WAN1		port scanners	

Ilustración 9: Reglas de bloqueo a escáneres de puertos para las conexiones entrantes de la WAN en el firewall Mikrotik

-add action=add-src-to-address-list address-list="port scanners" \ address-list-timeout=2w chain=input comment="Bloqueig de 14 dies a scanners de ports" \ in-interface-list=WAN1 protocol=tcp psd=21,3s,3,1

-add action=add-src-to-address-list address-list="port scanners" \ address-list-timeout=2w chain=input comment="NMAP FIN Stealth scan" \ in-interface-list=WAN1 protocol=tcp tcp-flags=fin,!syn,!rst,!psh,!ack,!urg

-add action=add-src-to-address-list address-list="port scanners" \ address-list-timeout=2w chain=input comment="SYN/FIN scan" \ in-interface-list=WAN1 protocol=tcp tcp-flags=fin,syn

-add action=add-src-to-address-list in-interface-list=WAN1 \ address-list="port scanners" address-list-timeout=2w chain=input \ comment="SYN/RST scan" disabled=no protocol=tcp tcp-flags=syn,rst

-add action=add-src-to-address-list in-interface-list=WAN1 address-list="port scanners" \ address-list-timeout=2w chain=input comment="FIN/PSH/URG scan" disabled=no protocol=tcp \ tcp-flags=fin,psh,urg,!syn,!rst,!ack

-add action=add-src-to-address-list in-interface-list=WAN1 address-list="port scanners" \ address-list-timeout=2w chain=input comment="ALL/ALL scan" disabled=no protocol=tcp \ tcp-flags=fin,syn,rst,psh,ack,urg

-add action=add-src-to-address-list in-interface-list=WAN1 address-list="port scanners" \ address-list-timeout=2w chain=input comment="NMAP NULL scan" disabled=no protocol=tcp \ tcp-flags=!fin,!syn,!rst,!psh,!ack,!urg

-add action=drop chain=input in-interface-list=WAN1 comment="Bloqueig total a scanners de ports" \ disabled=no src-address-list="port scanners"

La primera regla detecta escaneos de puertos mediante el detector PSD (sus reglas son:

-Acumule un peso de 21 dentro de un período de 3 segundos.

-Considere un escaneo si se intentan acceder al menos 3 puertos diferentes.

-Tenga en cuenta intentos de escaneo en un único puerto alto para su detección.) y añade la IP origen a la lista "port scanners" por 14 días.

La segunda regla detecta paquetes con el flag FIN y sin los flags SYN, RST, PSH, ACK, URG. En resumidas cuentas, detecta escaneos de puertos tipo NMAP FIN Stealth y añade la IP origen a la lista "port scanners" por 14 días.

La tercera regla detecta escaneos SYN/FIN y añade la IP origen a la lista "port scanners" por 14 días.

La cuarta regla detecta escaneos SYN/RST y añade la IP origen a la lista "port scanners" por 14 días.

La quinta regla detecta paquetes con los flags FIN, PSH y URG sin los flags SYN, RST, ACK. Básicamente detecta escaneos FIN/PSH/URG y añade la IP origen a la lista "port scanners" por 14 días.

La sexta regla detecta escaneos ALL/ALL y añade la IP origen a la lista "port scanners" por 14 días.

La séptima regla detecta paquetes sin ningún flag activado. Sobre la práctica esta regla detecta escaneos NMAP NULL y añade la IP origen a la lista "port scanners" por 14 días.

La octava regla bloquea todo el tráfico entrante desde direcciones IP que han sido identificadas como scanners de puertos y están en la lista "port scanners".

2.2 Configuración de reglas NAT

En la configuración no hay que crear muchas reglas, simplemente hay que enmascarar el tráfico saliente por la interfaz WAN para que pueda tener conexión a internet.

Ilustración 10: Reglas para enmascarar el tráfico saliente por la interfaz WAN para tener acceso a internet configurado en el firewall de MikroTik