SOPORTES QUE EVIDENCIEN LA IMPLEMENTACION DE SISTEMAS INTERNOS DE SEGURIDAD PARA SU RED ENCAMINADOS A EVITAR EL ACCESO NO AUTORIZADO A SU RED, LA REALIZACION DE SPAMMING, O QUE DESDE SISTEMAS PUBLICOS SE TENGA ACCESO A SU RED CON EL FIN DE DIFUNDIR EN ELLA CONTENIDO RELACIONADO CON PORNOGRAFIA INFANTIL (INTERNET).

CONTROL DE CAMBIOS

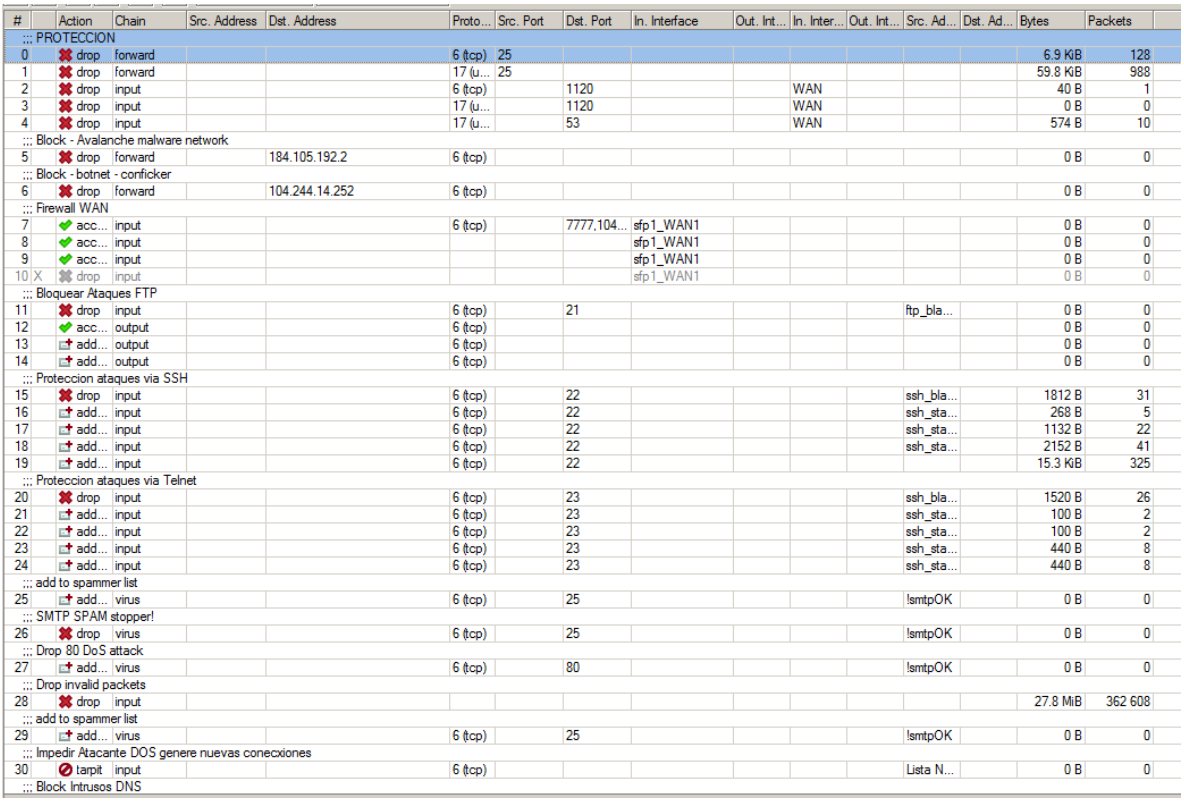
Versión	Fecha	Sección Modificada	Descripción cambios	Responsable(s)
0.1	01/02/2024	Todo	Creación del documento	Dirección de tecnologías de las comunicaciones

DECLARACIÓN DE CONFIDENCIALIDAD

La presente documentación es propiedad intelectual de **VISIÓN SATELITAL COMUNICACIONES**, tiene carácter confidencial y no podrá ser objeto de reproducción total o parcial, tratamiento informático ni transmisión de ninguna forma o por cualquier medio, ya sea electrónico, mecánico, por fotocopia, registro o cualquiera otro, sin expresa autorización. Asimismo, tampoco podrá ser objeto de préstamo, alquiler o cualquier forma de cesión de uso sin el permiso previo y escrito de **VISIÓN SATELITAL COMUNICACIONES,** titular de la propiedad intelectual. El incumplimiento de las limitaciones señaladas por cualquier persona que tenga acceso a la documentación será perseguido conforme a la ley.

Teniendo en cuenta que **VISIÓN SATELITAL COMUNICACIONES**, tiene en su red CORE un router Cloud Core Mikroitk, se han configurado reglas den el Filtro del Firewall, encargado de analizar los paquetes y conexiones desde y hacia la red interna y externa, enfocada a bloquear y enviar a listas negras las conexiones detectadas como ataques, impedir ataques SPAM, además la regla para direccionar el acceso a las paginas restringidas como pornografías infantil, el cual se carga la lista descargada del MINTIC.

La seguridad se realiza a nivel CORE tanto para red WAN como para redes LAN

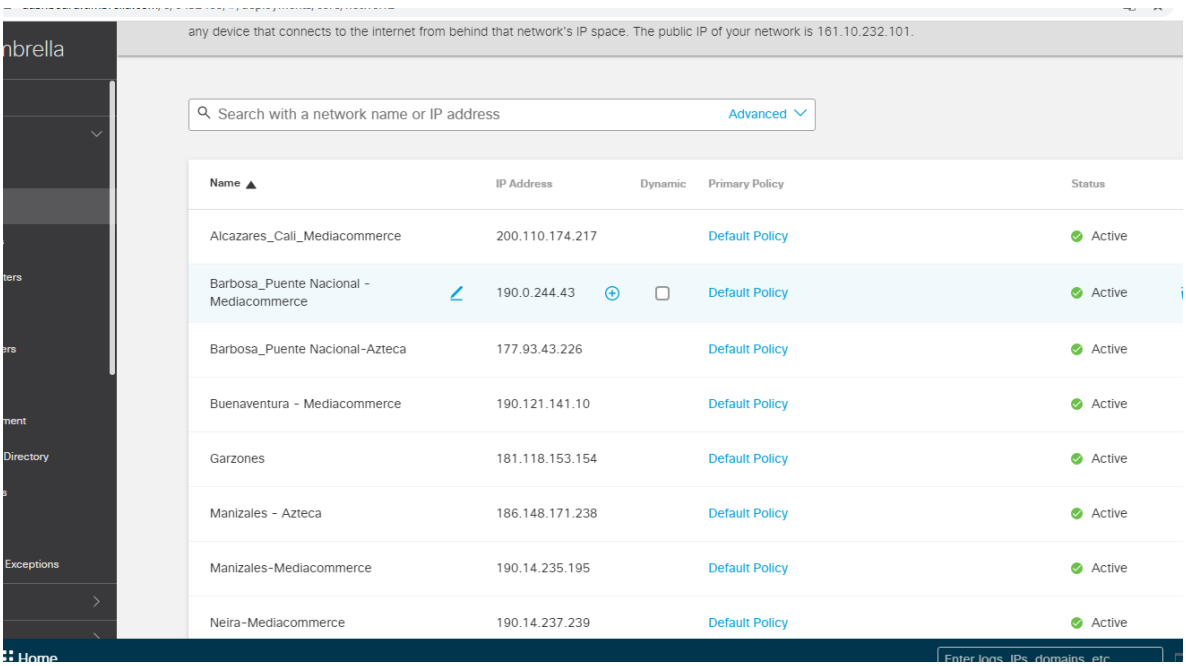


#		Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Interface	Out. Int...	In. Inter...	Out. Int...	Src. Ad...	Dst. Ad...	Bytes	Packets
;;; PROTECCION																
0		drop	forward			6 (tcp)	25								6.9 KiB	128
1		drop	forward			17 (u...	25								59.8 KiB	988
2		drop	input			6 (tcp)		1120			WAN				40 B	1
3		drop	input			17 (u...		1120			WAN				0 B	0
4		drop	input			17 (u...		53			WAN				574 B	10
;;; Block - Avalanche malware network																
5		drop	forward		184.105.192.2	6 (tcp)									0 B	0
;;; Block - botnet - conficker																
6		drop	forward		104.244.14.252	6 (tcp)									0 B	0
;;; Firewall WAN																
7		acc...	input			6 (tcp)		7777,104...	sfp1_WAN1						0 B	0
8		acc...	input						sfp1_WAN1						0 B	0
9		acc...	input						sfp1_WAN1						0 B	0
10	X	drop	input						sfp1_WAN1						0 B	0
;;; Bloquear Ataques FTP																
11		drop	input			6 (tcp)		21					ftp_bla...		0 B	0
12		acc...	output			6 (tcp)									0 B	0
13		add...	output			6 (tcp)									0 B	0
14		add...	output			6 (tcp)									0 B	0
;;; Proteccion ataques via SSH																
15		drop	input			6 (tcp)		22					ssh_bla...		1812 B	31
16		add...	input			6 (tcp)		22					ssh_sta...		268 B	5
17		add...	input			6 (tcp)		22					ssh_sta...		1132 B	22
18		add...	input			6 (tcp)		22					ssh_sta...		2152 B	41
19		add...	input			6 (tcp)		22							15.3 KiB	325
;;; Proteccion ataques via Telnet																
20		drop	input			6 (tcp)		23					ssh_bla...		1520 B	26
21		add...	input			6 (tcp)		23					ssh_sta...		100 B	2
22		add...	input			6 (tcp)		23					ssh_sta...		100 B	2
23		add...	input			6 (tcp)		23					ssh_sta...		440 B	8
24		add...	input			6 (tcp)		23					ssh_sta...		440 B	8
;;; add to spammer list																
25		add...	virus			6 (tcp)		25					!smtpOK		0 B	0
;;; SMTP SPAM stopper!																
26		drop	virus			6 (tcp)		25					!smtpOK		0 B	0
;;; Drop 80 DoS attack																
27		add...	virus			6 (tcp)		80					!smtpOK		0 B	0
;;; Drop invalid packets																
28		drop	input												27.8 MiB	362 608
;;; add to spammer list																
29		add...	virus			6 (tcp)		25					!smtpOK		0 B	0
;;; Impedir Atacante DOS genere nuevas conecxiones																
30		tarpit	input			6 (tcp)							Lista N...		0 B	0
;;; Block Intrusos DNS																

;;; Impedir Atacante DOS genere nuevas conecxiones													
30	tarpit	input			6 (tcp)						Lista N...	0 B	0
;;; Block Intrusos DNS													
31	drop	input			17 (u...		53	ether1				0 B	0
;;; Block Intrusos WebProxy													
32	drop	input			6 (tcp)		3128	ether1				0 B	0
;;; Detect and add-list SMTP virus or spammers													
33	add...	forward			6 (tcp)		25					0 B	0
;;; VIRUS DE WINDOWS													
34	drop	virus			6 (tcp)		135-139,...					0 B	0
;;; Accept established connection packets													
35	acc...	input										736.7 MiB	10 066 669
;;; Accept related connection packets													
36	acc...	input										60.6 MiB	672 210

Grafica de protección Firewall Mikrotik CCR

Adicionalmente contamos con un firewall a nivel de DNS el cual se encarga de analizar la navegación y poder detectar posibles fallas de seguridad en la red, gestionando de manera global la navegación y bloquear algún servicio, página o APP en toda la red



Código Fuente reglas mikrotik

```
/ip firewall filter

add action=drop chain=forward comment=PROTECCION protocol=tcp src-port=25

add action=drop chain=forward protocol=udp src-port=25

add action=drop chain=input dst-port=1120 in-interface-list=WAN
protocol=tcp

add action=drop chain=input dst-port=1120 in-interface-list=WAN
protocol=udp

add action=drop chain=input dst-port=53 in-interface-list=WAN
protocol=udp

add action=drop chain=forward comment="Block - Avalanche malware network"
dst-address=184.105.192.2 protocol=tcp

add action=drop chain=forward comment="Block - botnet - conficker" dst-
address=104.244.14.252 port=80 protocol=tcp

add action=accept chain=input comment="Firewall WAN" dst-port=7777,10445
in-interface=sfp1_WAN1 protocol=tcp

add action=accept chain=input connection-state=established in-
interface=sfp1_WAN1

add action=accept chain=input connection-state=related in-
interface=sfp1_WAN1

add action=drop chain=input disabled=yes in-interface=sfp1_WAN1

add action=drop chain=input comment="Bloquear Ataques FTP" 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

add action=add-dst-to-address-list address-list=ftp_blacklist address-
list-timeout=12h chain=output content="530 Login incorrect" protocol=tcp
```

```
add action=drop chain=input comment="Proteccion ataques via SSH" 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_stage3

add action=add-src-to-address-list address-list=ssh_stage3 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_stage2 address-list-timeout=1m chain=input connection-state=new dst-port=22 protocol=tcp src-address-list=ssh_stage1

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

add action=drop chain=input comment="Proteccion ataques via Telnet" dst-port=23 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=23 protocol=tcp src-address-list=ssh_stage3

add action=add-src-to-address-list address-list=ssh_stage3 address-list-timeout=1m chain=input connection-state=new dst-port=23 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=23 protocol=tcp src-address-list=ssh_stage1

add action=add-src-to-address-list address-list=ssh_stage1 address-list-timeout=1m chain=input connection-state=new dst-port=23 protocol=tcp src-address-list=ssh_stage1

add action=add-src-to-address-list address-list=spammer address-list-timeout=1d chain=virus comment="add to spammer list" connection-limit=30,32 dst-port=25 limit=10,5 protocol=tcp src-address-list=\

    !smtpOK

add action=drop chain=virus comment="SMTP SPAM stopper!" dst-port=25 protocol=tcp src-address-list=!smtpOK
```

```
add action=add-src-to-address-list address-list=spammer address-list-timeout=2d chain=virus comment="Drop 80 DoS attack" connection-limit=40,32 dst-port=80 limit=20,5 protocol=tcp src-address-list=\
    !smtpOK
add action=drop chain=input comment="Drop invalid packets" connection-state=invalid
add action=add-src-to-address-list address-list=spammer address-list-timeout=1d chain=virus comment="add to spammer list" connection-limit=30,32 dst-port=25 limit=10,5:packet protocol=tcp \
    src-address-list=!smtpOK
add action=tarpit chain=input comment="Impedir Atacante DOS genere nuevas conecxiones" protocol=tcp src-address-list="Lista Negra"
add action=drop chain=input comment="Block Intrusos DNS" dst-port=53 in-interface=ether1 protocol=udp
add action=drop chain=input comment="Block Intrusos WebProxy" dst-port=3128 in-interface=ether1 protocol=tcp
add action=add-src-to-address-list address-list=spammer address-list-timeout=1d chain=forward comment="Detect and add-list SMTP virus or spammers" connection-limit=30,32 dst-port=25 limit=50,5:packet \
    protocol=tcp
add action=drop chain=virus comment="VIRUS DE WINDOWS" dst-port=135-139,445 protocol=tcp
add action=accept chain=input comment="Accept established connection packets" connection-state=established
add action=accept chain=input comment="Accept related connection packets" connection-state=related
```