Seguridad Perimetral con MikroTik

José Miguel Ojeda Flores – CEO Home Capacity LATAM

MUM ECUADOR 2019 Home Capacity LATAM

JOSÉ MIGUEL OJEDA FLORES

- Ingeniero en Sistemas con mención en Telemática.
- Magister en Administración de Empresas con especialidad en Gestión de Proyectos.
- Fundador y CEO de Home Capacity LATAM
- Experiencia con MikroTik desde 2009
- Instructor Certificado MikroTik desde 2011
- Certificaciones MikroTik: MTCNA, MTCTCE, MTCWE, MTCUME, MTCRE, MTCINE, MTCIPv6E, MTCSE.

MUM ECUADOR 2019 Home Capacity LATAM

HOME CAPACITY LATINOAMÉRICA

- Establecida en el 2013 – Guayaquil – Ecuador
- Asesorías y Consultorías en Telecomunicaciones.
- Soporte Técnico Especializado.
  - Soporte por Horas.
  - Soporte Mensual – 8x5 y 24x7.
  - Revisión y Mejoras en tu red.
  - Implementaciones bajo requerimientos.
- Entrenamientos Oficiales en MikroTik y otras marcas

HOMECAPACITY S.A.
Training & Consulting

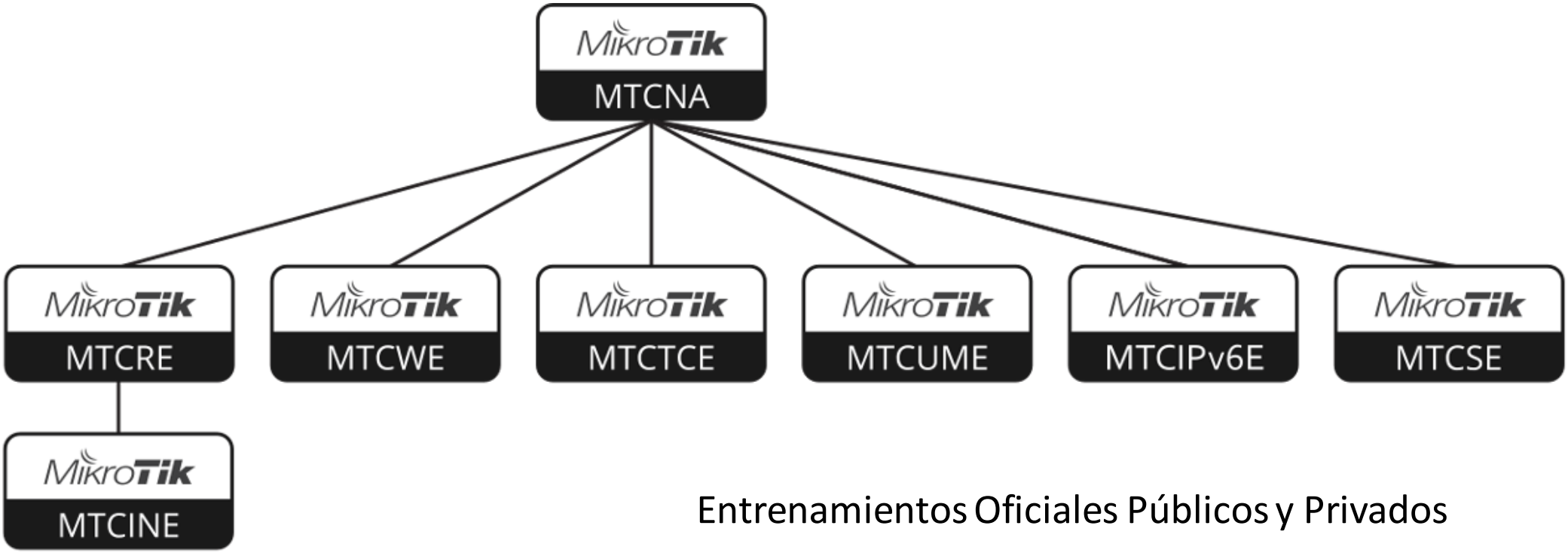
soporte@home-capacity.com

curssos@home-capacity.com

/HomeCapacity/

MUM ECUADOR 2019

Home Capacity LATAM

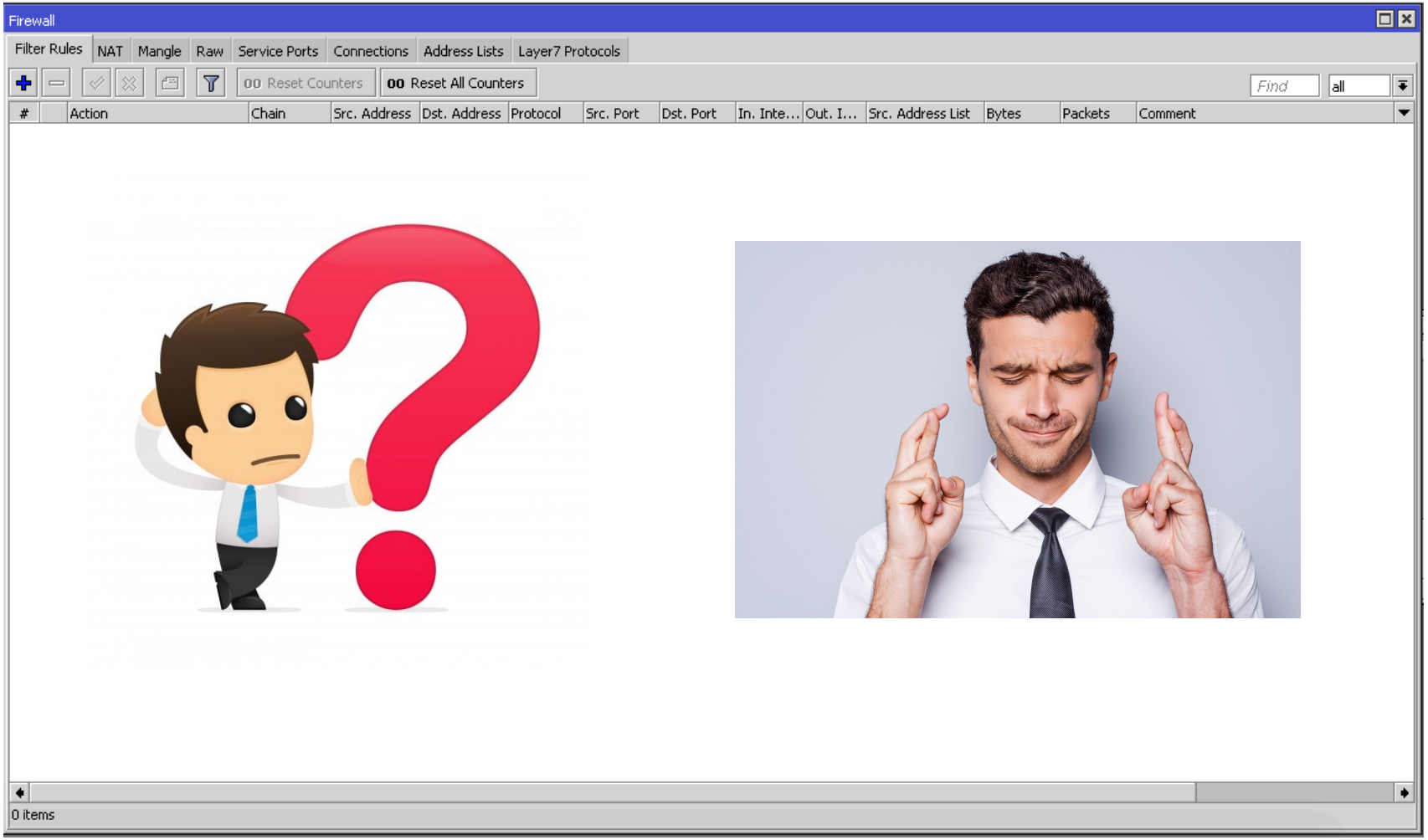


Entrenamientos Oficiales Públicos y Privados

Contáctanos: miguel.ojeda@home-capacity.com

MUM ECUADOR 2019

Home Capacity LATAM



MUM ECUADOR 2019 Home Capacity LATAM

Firewall

Filter Rules | NAT | Mangle | Raw | Service Ports | Connections | Address Lists | Layer7 Protocols

00 Reset Counters | 00 Reset All Counters | Find | all

#	Action	Chain	Src...	Dst. ...	Protocol	Sr...	Dst. Port	In. Int...	...	In. Int...	...	Src. A...	Dst. A...	Bytes	Packets	Comment
0	drop	input			6 (tcp)									842.7 KiB	21 569	IN - DEESCARTA PORT SCAN
1	drop	input			6 (tcp)		2222					Ataqu...		18.6 KiB	335	IN - DESCARTA LISTA DE ATAQUE SSH
2	add src to address list	input			6 (tcp)		2222					SSH_I...		444 B	9	IN - AGREGA IP A LISTA DE ATAQUE SSH
3	add src to address list	input			6 (tcp)		2222					SSH_I...		948 B	19	IN - SSH INTENTO 3
4	add src to address list	input			6 (tcp)		2222					SSH_I...		2012 B	40	IN - SSH INTENTO 2
5	add src to address list	input			6 (tcp)		2222							13.9 KiB	286	IN - SSH INTENTO 1
6	accept	input			1 (icmp)									3099.6 KiB	50 520	IN - REVISION ICMP FLOOD
7	accept	input												39.0 MiB	543 766	IN - PERMITE CONEXIONES ESTABLECIDAS Y RELACIONADA
8	accept	input			89 (ospf)									5.9 MiB	56 353	IN - PERMITE OSPF
9	accept	input			6 (tcp)		179							6.4 KiB	155	IN - PERMITE BGP
10	accept	input			47 (gre)									9.9 MiB	116 266	IN - PERMITE GRE Y EOIP
11	accept	input			6 (tcp)		1723							1004 B	25	IN - PERMITE PPTP
12	accept	input			6 (tcp)		8728							18.5 KiB	317	IN - PERMITE API SONAR
13	accept	input			6 (tcp)		8291							660 B	12	IN - PERMITE WINBOX ADMIN
14	log	input												12.3 KiB	111	IN - LOG DE TODO LO DEMAS
15	drop	input												12.0 KiB	108	IN - DESCARTA TODO LO DEMAS
16	accept	forward												870.7 GiB	1252 97...	FW - PERMITE CONEXIONES ESTABLECIDAS Y RELACIONAD
17	accept	forward			6 (tcp)									653.0 MiB	13 427 964	FW - PERMITE TRAFICO TCP
18	accept	forward			6 (tcp)									0 B	0	FW - PERMITE TRAFICO BGP
19	accept	forward			47 (gre)									4614.9 KiB	53 680	FW - PERMITE TRAFICO GRE
20	accept	forward			50 (ipsec-esp)									407.5 KiB	3 213	FW - PERMITE TRAFICO IPSEC
21	accept	forward			17 (udp)									7.1 GiB	38 544 360	FW - PERMITE TRAFICO UDP
22	accept	forward			1 (icmp)									163.6 MiB	2 668 819	FW - PERMITE TRAFICO ICMP
23	log	forward												0 B	0	IN - LOG DE TODO LO DEMAS
24	drop	forward												0 B	0	IN - DESCARTA TODO LO DEMAS
25	accept	ICMP			1 (icmp)									0 B	0	ICMP - PERMITE 8:0
26	accept	ICMP			1 (icmp)									0 B	0	ICMP - PERMITE 0:0
27	accept	ICMP			1 (icmp)									0 B	0	ICMP - PERMITE 11:0
28	accept	ICMP			1 (icmp)									0 B	0	ICMP - PERMITE 3:3
29	accept	ICMP			1 (icmp)									0 B	0	ICMP - PERMITE 3:4
30	drop	ICMP			1 (icmp)									0 B	0	ICMP - DESCARTE RESTO ICMP

Sabías que…

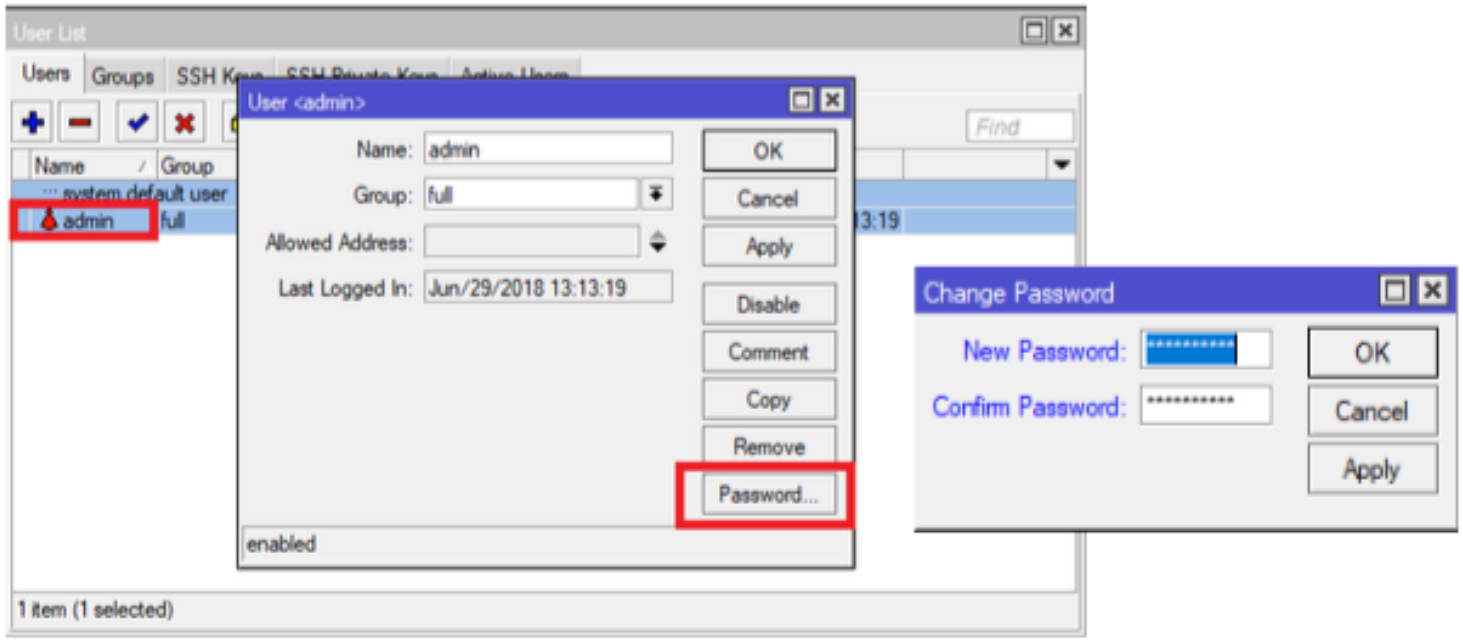
El origen de los riesgos de seguridad pueden ser:

- **Internos:** Cerca del 70% de ataques reportados provienen de las redes locales.
- **Externos:** Seguridad Perimetral (Prevenir accesos no autorizados desde el Internet).

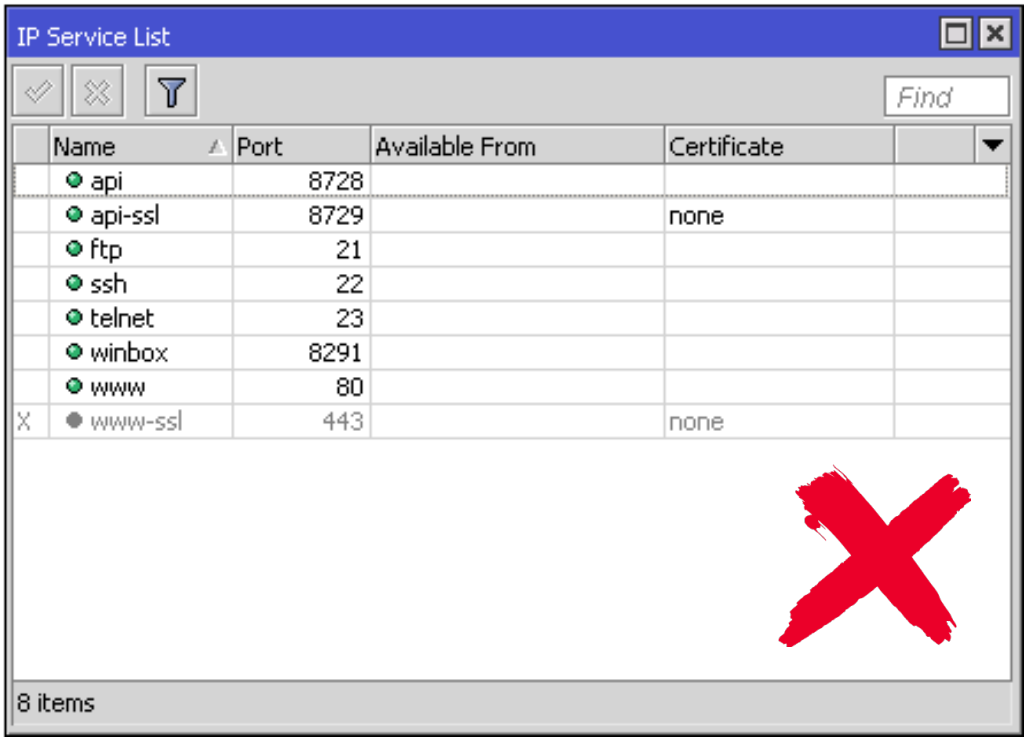
Las vulnerabilidades atacadas son…

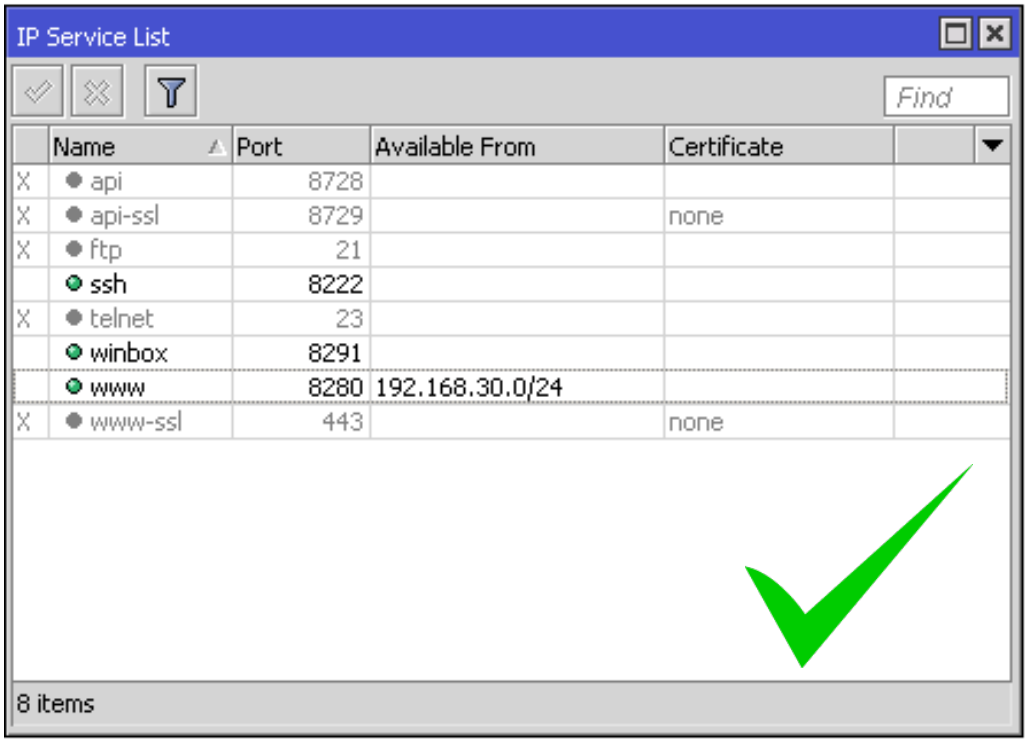
- Protocolos
- Software
- Configuración

Credenciales por defecto - RouterOS



Servicios por defecto - RouterOS





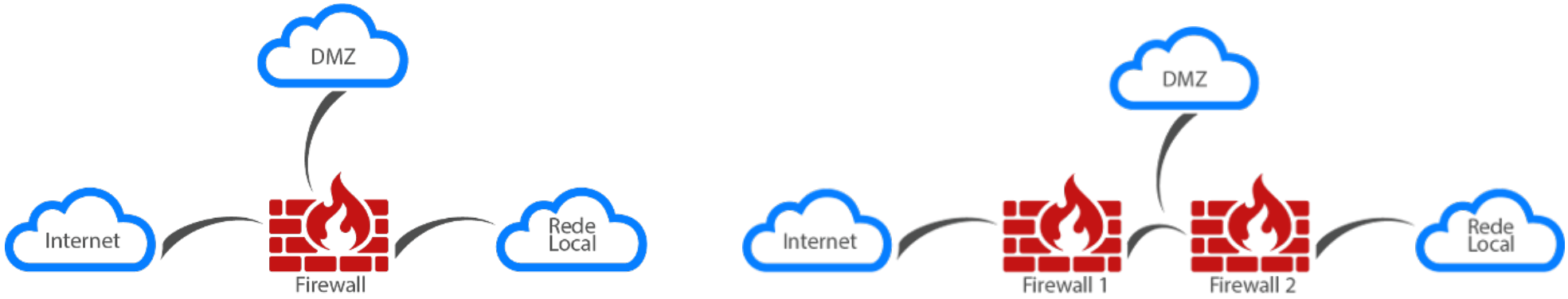
Implementación Común

A pesar de ser extremadamente simple, es posible ver que para que el tráfico entre o salga de la red protegida, es obligatorio pasar por el firewall. Esta topología ofrece nada más que una capa de seguridad real, por lo que es necesario evaluar con atención los escenarios donde se recomienda el uso de esta topología.

Una vez que el firewall se ha comprometido, no hay ningún impedimento para que atacante pueda acceder a la red protegida

Seguridad Perimetral

La seguridad perimetral es un método de defensa de la red, que se basa en el establecimiento de recursos de seguridad en el perímetro de la red y en diferentes niveles, permitiendo definir niveles de confianza, el acceso a usuarios internos o externos a determinados servicios y denegando cualquier tipo de acceso a otros.

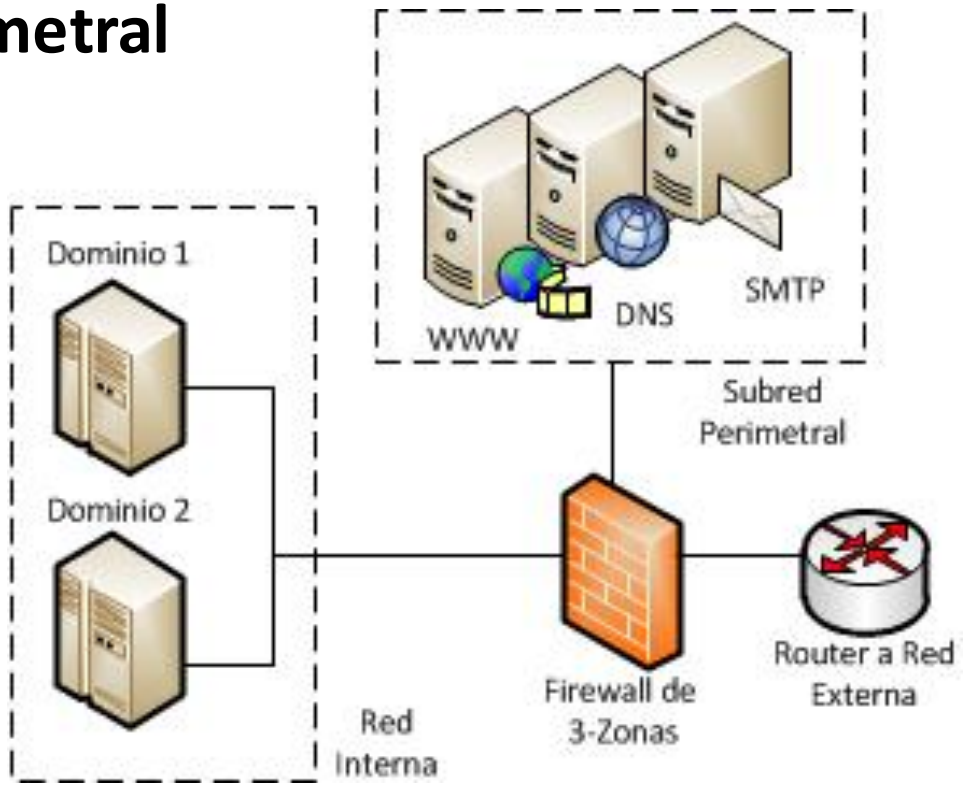


Objetivos

- ✓ Rechazar conexiones a servicios comprometidos.
- ✓ Permitir sólo ciertos tipos de tráfico.
- ✓ Proporcionar un único punto de conexión al exterior.
- ✓ Ocultar servicios vulnerables que no son fáciles de proteger.
- ✓ Auditar el tráfico entre el exterior y el interior de la red.

Elementos de Seguridad Perimetral

- ✓ Routers de Frontera
- ✓ Firewalls
- ✓ IDS.
- ✓ Zonas Desmilitarizadas
- ✓ Redes Privadas Virtuales

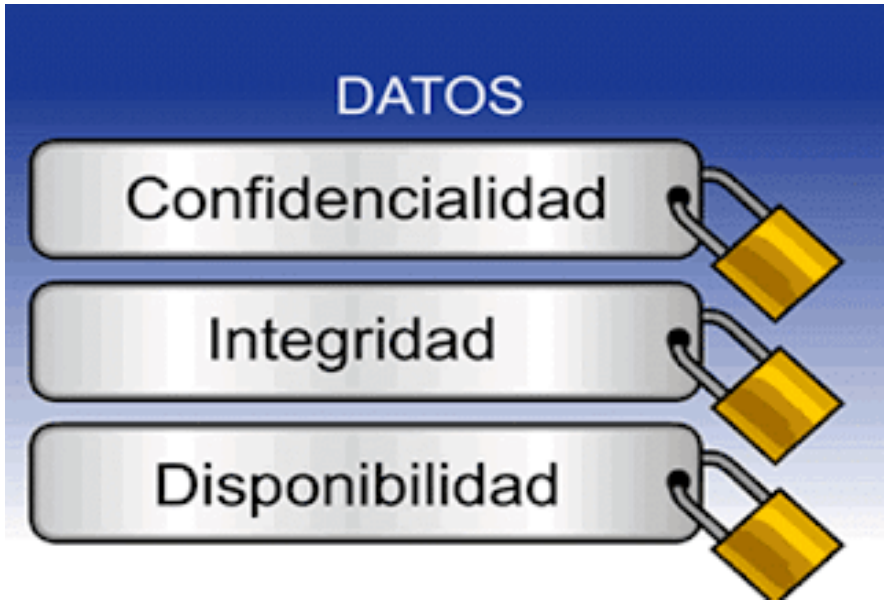


Qué debemos proteger? …. Cuál es el activo más importante?

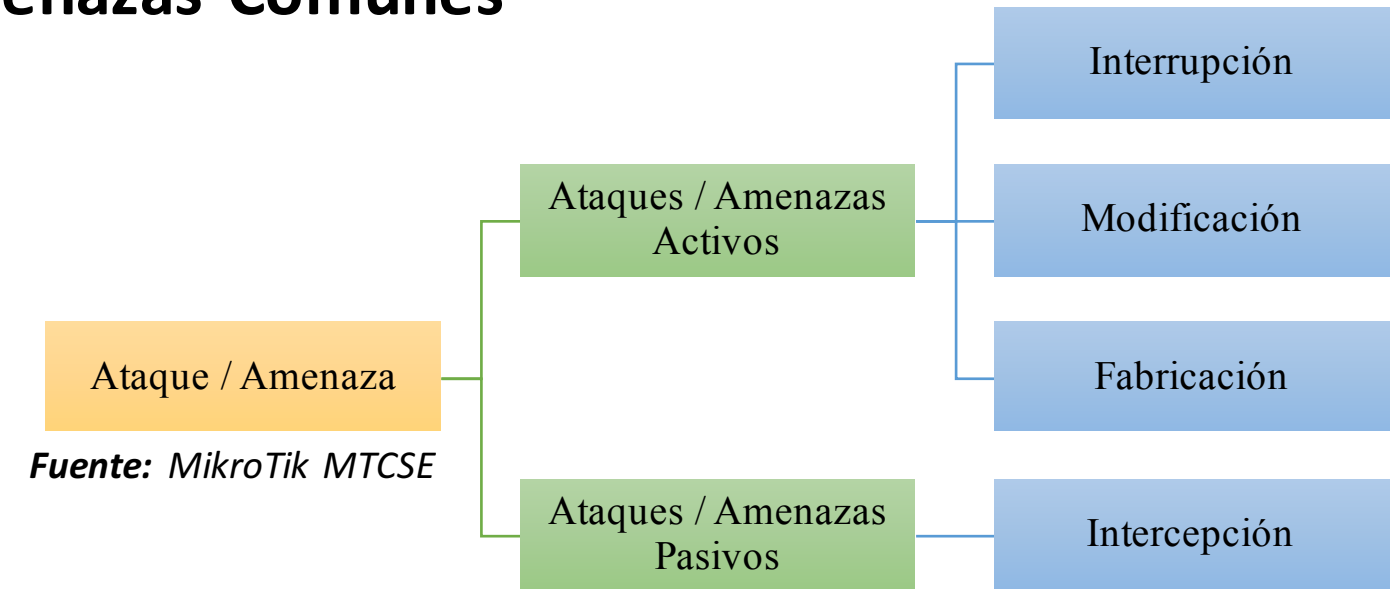
Confidencialidad: asegurar que la información no es divulgada a personas no autorizadas, procesos o dispositivos.

Integridad: asegurar la autenticidad de la información (que no haya sido alterada).

Disponibilidad: refiriéndonos al acceso oportuno y confiable a datos y servicios de información para usuarios autorizados.



Amenazas Comunes



Fuente: *MikroTik MTCSE*

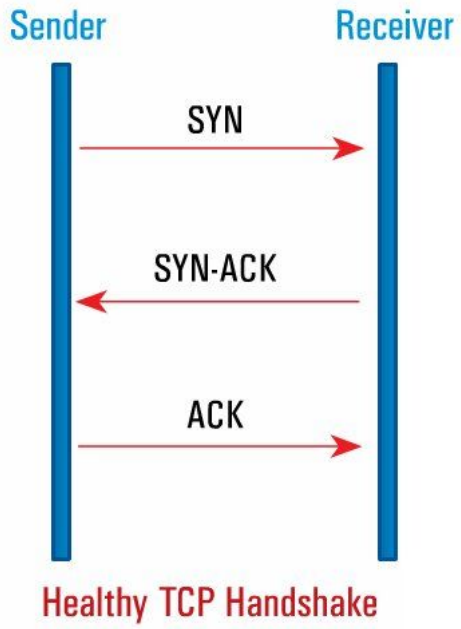
Los ataques de red pueden ser tan variados como los sistemas a los que intentan penetrar. Algunos ataques son complejos mientras que otros son realizados por el desconocimiento de los usuarios.

Ataques DoS

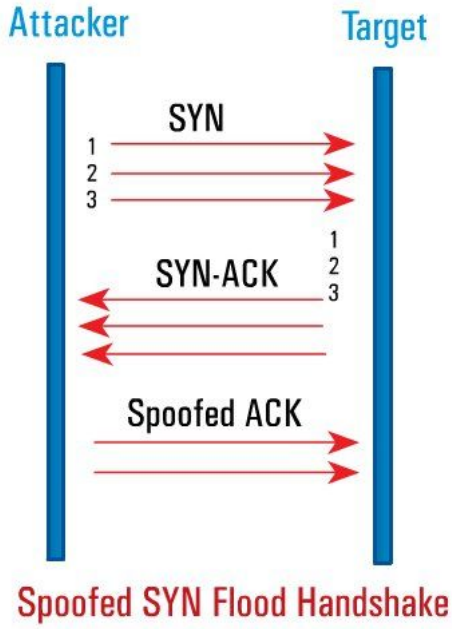
Es el más conocido de los ataques y a su vez el más difícil de eliminar completamente. Son fáciles de realizar. No intentan acceder a nuestra red sino lograr que uno o más servicios no este disponible.

TCY SYN FLOOD

La técnica fundamental detrás de un ataque DoS es hacer que el sistema objetivo esté ocupado, este tipo de ataque aprovecha el "three-way handshake" para establecer la comunicación TCP.



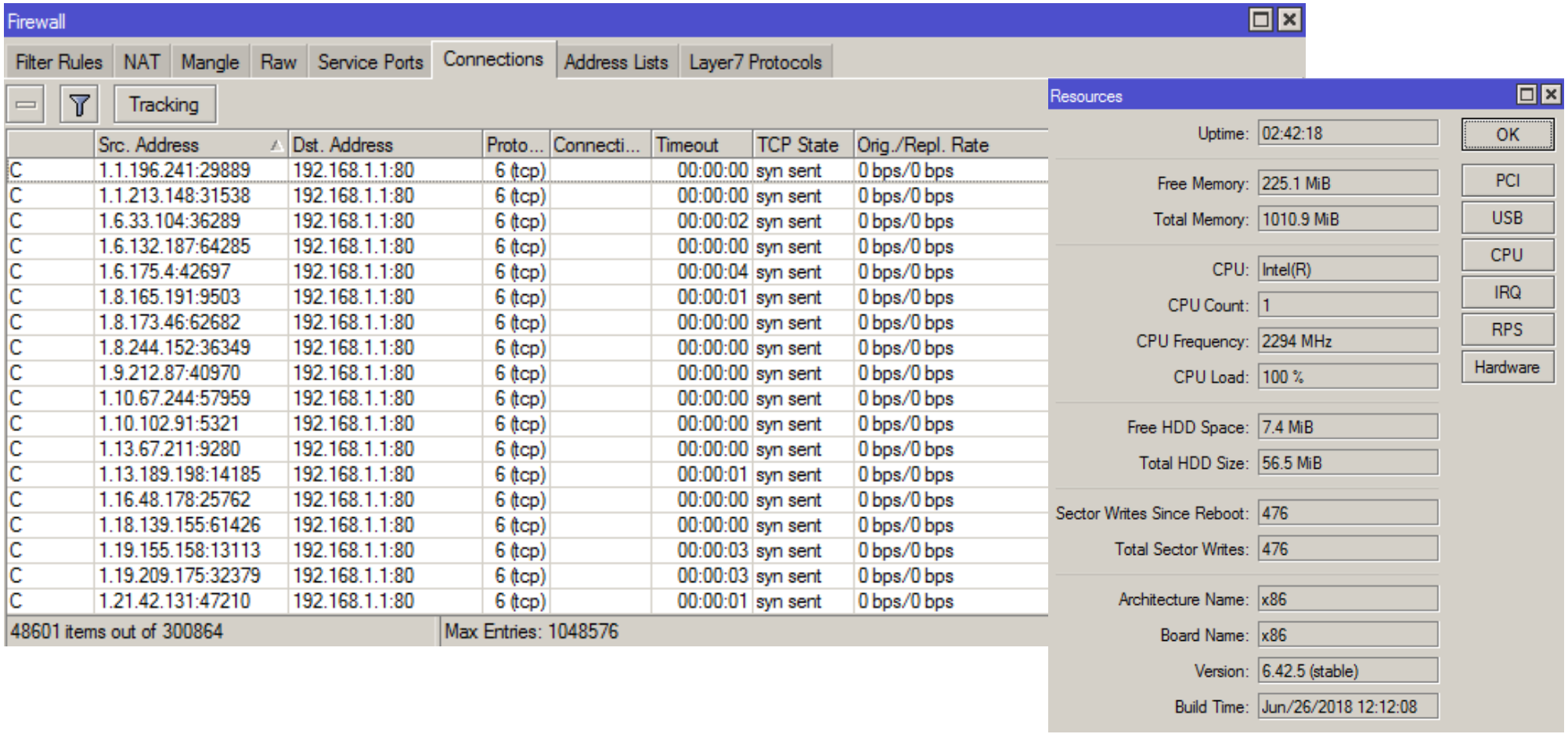
Healthy TCP Handshake

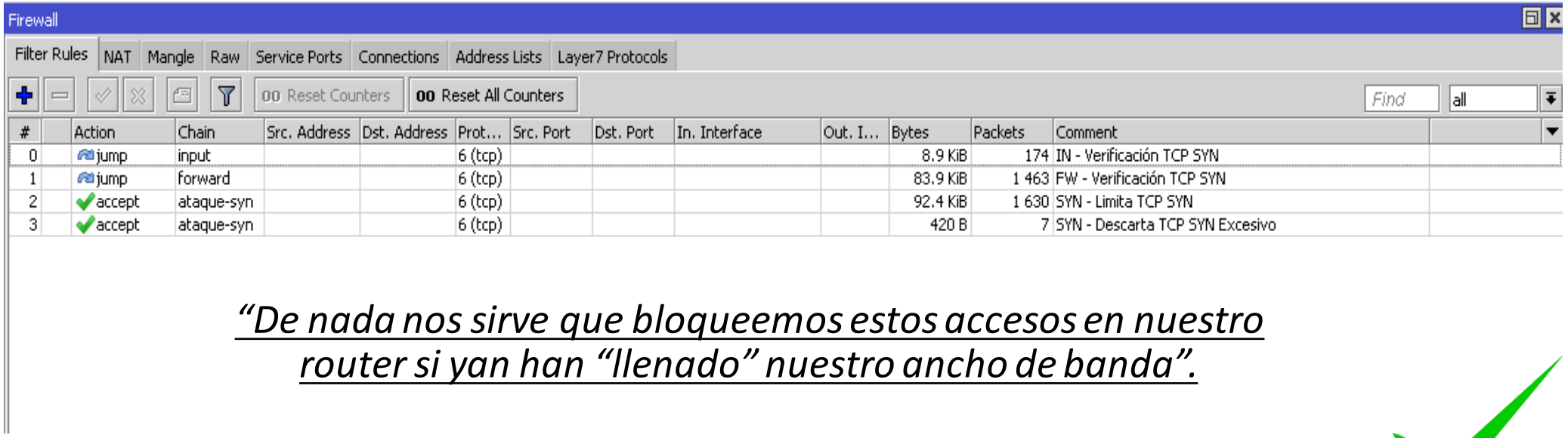


Spoofed SYN Flood Handshake

MUM ECUADOR 2019

Home Capacity LATAM





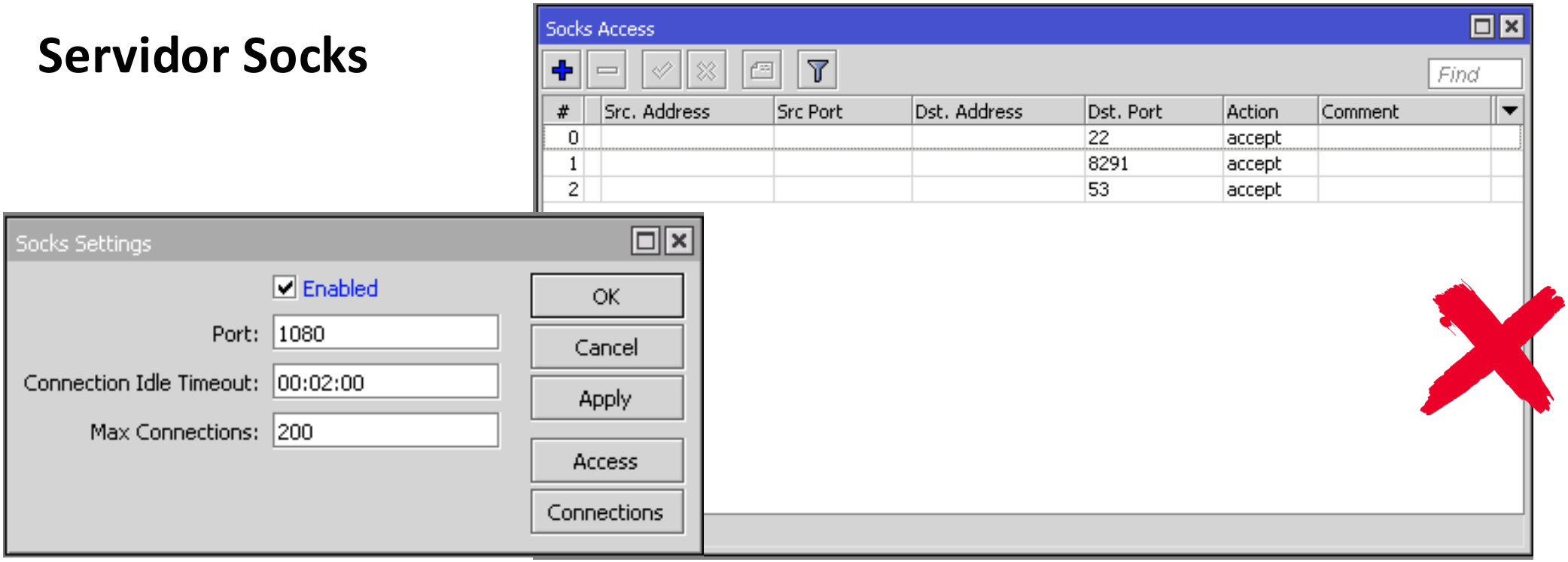
#	Action	Chain	Src. Address	Dst. Address	Prot...	Src. Port	Dst. Port	In. Interface	Out. I...	Bytes	Packets	Comment
0	jump	input			6 (tcp)					8.9 KiB	174	IN - Verificación TCP SYN
1	jump	forward			6 (tcp)					83.9 KiB	1 463	FW - Verificación TCP SYN
2	accept	ataque-syn			6 (tcp)					92.4 KiB	1 630	SYN - Limita TCP SYN
3	accept	ataque-syn			6 (tcp)					420 B	7	SYN - Descarta TCP SYN Excesivo

"De nada nos sirve que bloqueemos estos accesos en nuestro router si yan han "llenado" nuestro ancho de banda".

Medida Anti-DoS:

Configurar los FW y routers para que limiten el máximo de conexiones que un sistema puede tener abiertas al mismo tiempo.

Servidor Socks



SOCKS es un servidor proxy que permite que los datos de las aplicaciones basadas en TCP se transmitan a través del firewall, incluso si el firewall bloqueara los paquetes.

Bloqueo de Solicitudes DNS (DNS DoS)

Firewall

Filter Rules | NAT | Mangle | Raw | Service Ports | Connections | Address Lists | Layer7 Protocols

00 Reset Counters | 00 Reset All Counters | Find | all

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Interface	Out. I...	Bytes	Packets	Comment
0	drop	input			6 (tcp)		53	ether1		0 B	0	
1	drop	input			17 (udp)		53	ether1		0 B	0	

Firewall

Filter Rules | NAT | Mangle | Raw | Service Ports | Connections | Address Lists | Layer7 Protocols

00 Reset Counters | 00 Reset All Counters | Find | all

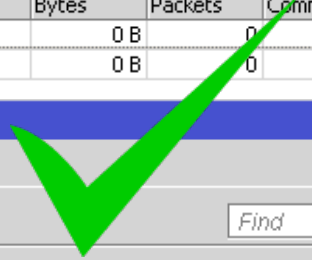
#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Inte...	Out. I...	Src. Address List	Limit/Rate	Bytes	Packets	Comment
0	accept	input			6 (tcp)		53	!ether1			100/sec	0 B	0	
1	accept	input			17 (udp)		53	!ether1			100/sec	0 B	0	

Firewall

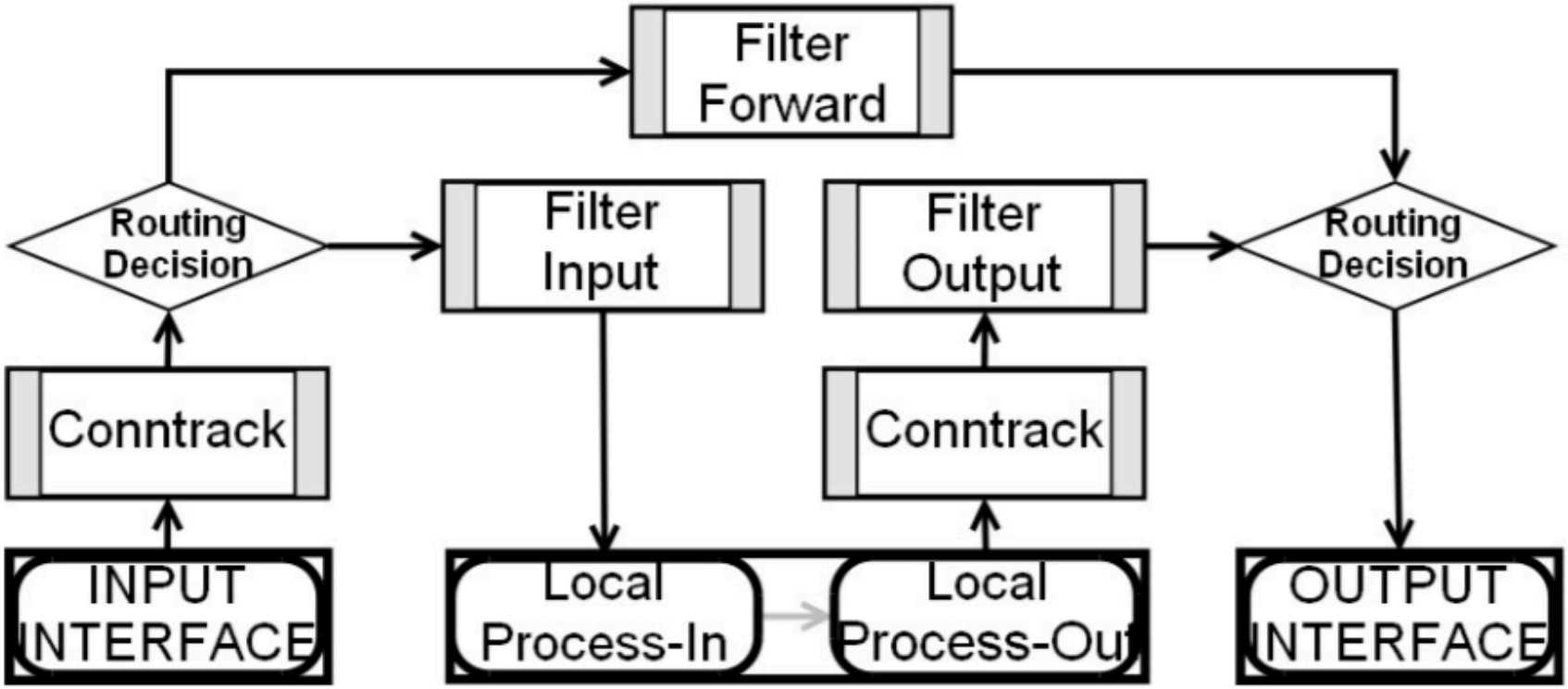
Filter Rules | NAT | Mangle | Raw | Service Ports | Connections | Address Lists | Layer7 Protocols

00 Reset Counters | 00 Reset All Counters | Find | all

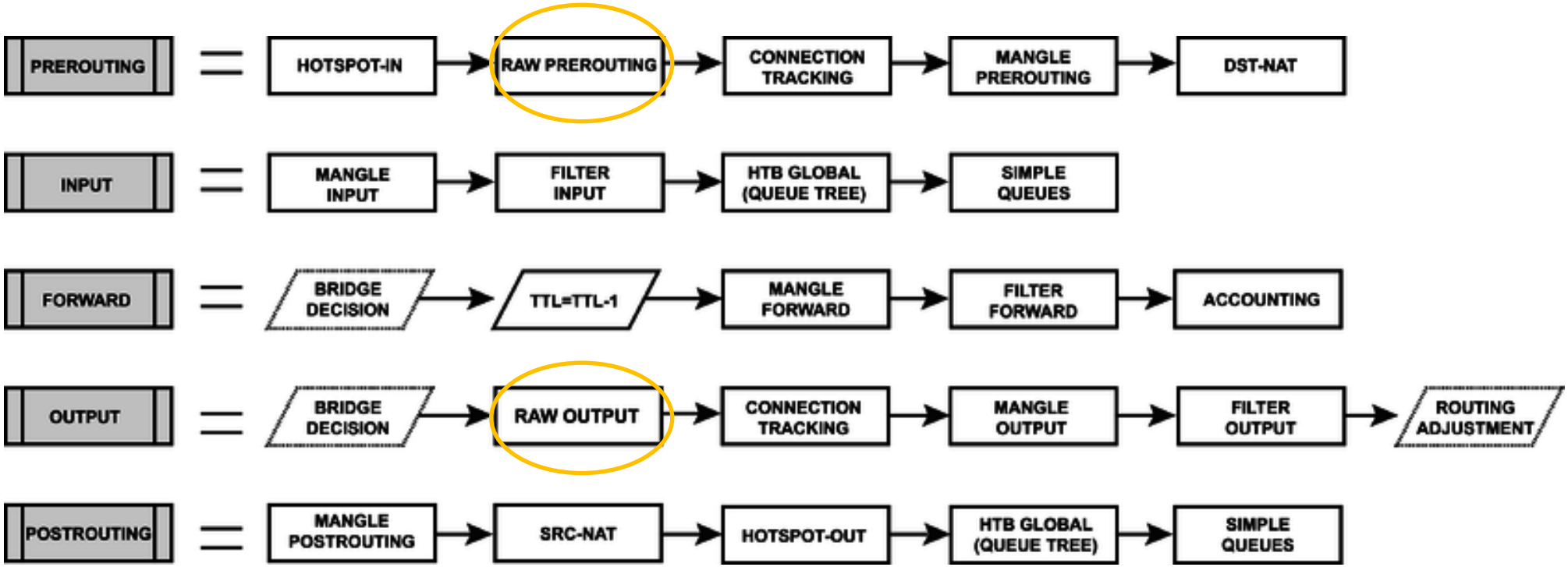
#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Int...	Out. I...	Bytes	Packets	Comment
0	drop	prerouting			6 (tcp)		53	ether1		0 B	0	RAW - Descarta DNS TCP
1	drop	prerouting			17 (udp)		53	ether1		0 B	0	RAW - Descarta DNS UDP



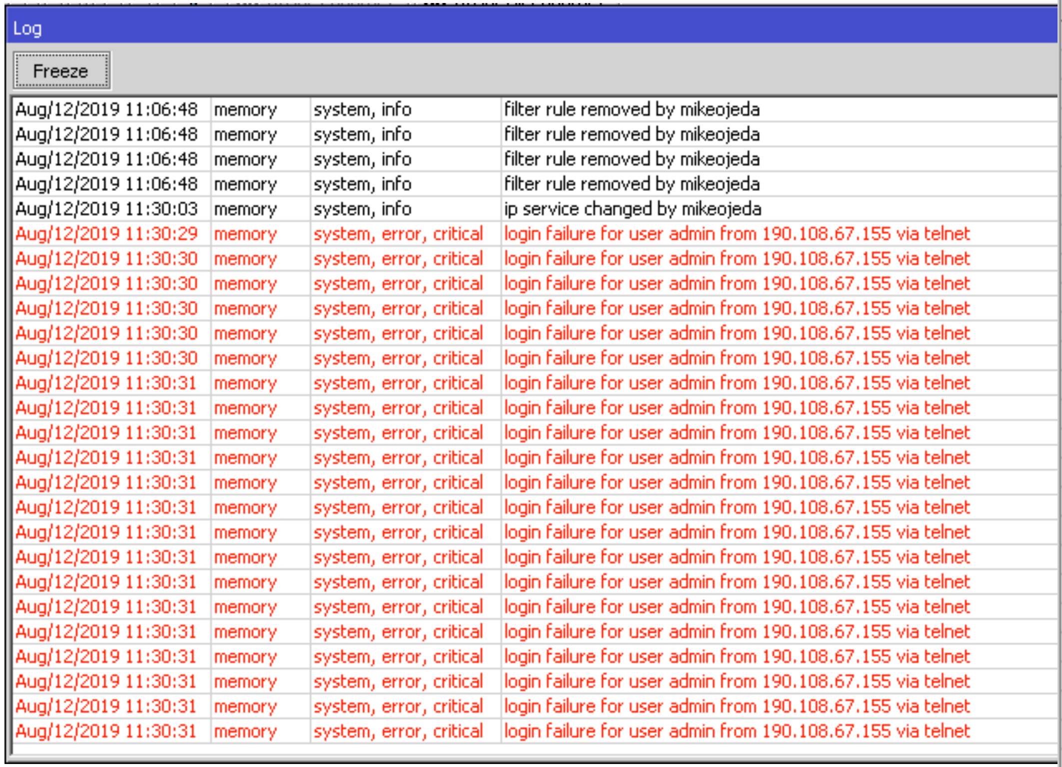
Flujo Básico de Firewall



Por qué RAW TABLE



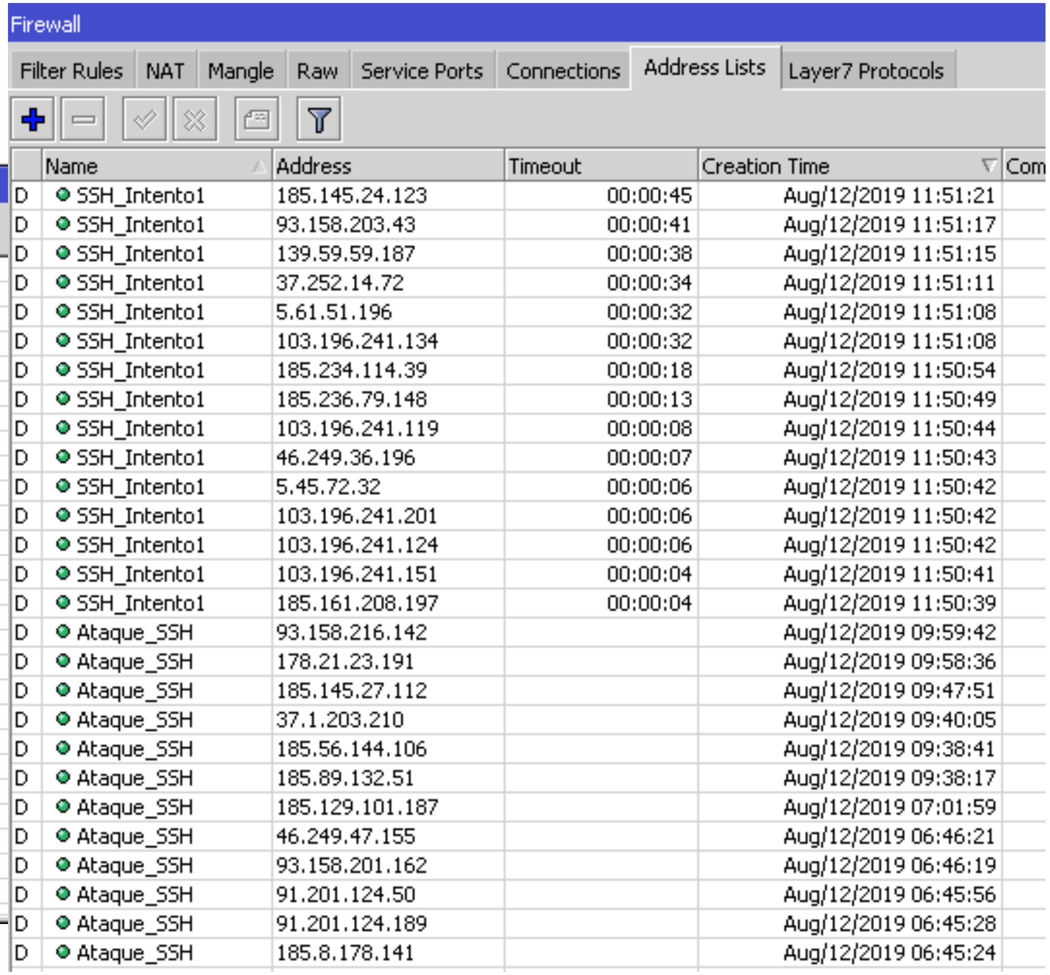
Ataques de Fuerza Bruta



Log

Freeze

Aug/12/2019 11:06:48	memory	system, info	filter rule removed by mikeojeda
Aug/12/2019 11:06:48	memory	system, info	filter rule removed by mikeojeda
Aug/12/2019 11:06:48	memory	system, info	filter rule removed by mikeojeda
Aug/12/2019 11:06:48	memory	system, info	filter rule removed by mikeojeda
Aug/12/2019 11:30:03	memory	system, info	ip service changed by mikeojeda
Aug/12/2019 11:30:29	memory	system, error, critical	login failure for user admin from 190.108.67.155 via telnet
Aug/12/2019 11:30:30	memory	system, error, critical	login failure for user admin from 190.108.67.155 via telnet
Aug/12/2019 11:30:30	memory	system, error, critical	login failure for user admin from 190.108.67.155 via telnet
Aug/12/2019 11:30:30	memory	system, error, critical	login failure for user admin from 190.108.67.155 via telnet
Aug/12/2019 11:30:30	memory	system, error, critical	login failure for user admin from 190.108.67.155 via telnet
Aug/12/2019 11:30:30	memory	system, error, critical	login failure for user admin from 190.108.67.155 via telnet
Aug/12/2019 11:30:31	memory	system, error, critical	login failure for user admin from 190.108.67.155 via telnet
Aug/12/2019 11:30:31	memory	system, error, critical	login failure for user admin from 190.108.67.155 via telnet
Aug/12/2019 11:30:31	memory	system, error, critical	login failure for user admin from 190.108.67.155 via telnet
Aug/12/2019 11:30:31	memory	system, error, critical	login failure for user admin from 190.108.67.155 via telnet
Aug/12/2019 11:30:31	memory	system, error, critical	login failure for user admin from 190.108.67.155 via telnet
Aug/12/2019 11:30:31	memory	system, error, critical	login failure for user admin from 190.108.67.155 via telnet
Aug/12/2019 11:30:31	memory	system, error, critical	login failure for user admin from 190.108.67.155 via telnet
Aug/12/2019 11:30:31	memory	system, error, critical	login failure for user admin from 190.108.67.155 via telnet
Aug/12/2019 11:30:31	memory	system, error, critical	login failure for user admin from 190.108.67.155 via telnet
Aug/12/2019 11:30:31	memory	system, error, critical	login failure for user admin from 190.108.67.155 via telnet
Aug/12/2019 11:30:31	memory	system, error, critical	login failure for user admin from 190.108.67.155 via telnet
Aug/12/2019 11:30:31	memory	system, error, critical	login failure for user admin from 190.108.67.155 via telnet
Aug/12/2019 11:30:31	memory	system, error, critical	login failure for user admin from 190.108.67.155 via telnet
Aug/12/2019 11:30:31	memory	system, error, critical	login failure for user admin from 190.108.67.155 via telnet
Aug/12/2019 11:30:31	memory	system, error, critical	login failure for user admin from 190.108.67.155 via telnet



Firewall

Filter Rules | NAT | Mangle | Raw | Service Ports | Connections | Address Lists | Layer7 Protocols

	Name	Address	Timeout	Creation Time	Com
D	SSH_Intento1	185.145.24.123	00:00:45	Aug/12/2019 11:51:21	
D	SSH_Intento1	93.158.203.43	00:00:41	Aug/12/2019 11:51:17	
D	SSH_Intento1	139.59.59.187	00:00:38	Aug/12/2019 11:51:15	
D	SSH_Intento1	37.252.14.72	00:00:34	Aug/12/2019 11:51:11	
D	SSH_Intento1	5.61.51.196	00:00:32	Aug/12/2019 11:51:08	
D	SSH_Intento1	103.196.241.134	00:00:32	Aug/12/2019 11:51:08	
D	SSH_Intento1	185.234.114.39	00:00:18	Aug/12/2019 11:50:54	
D	SSH_Intento1	185.236.79.148	00:00:13	Aug/12/2019 11:50:49	
D	SSH_Intento1	103.196.241.119	00:00:08	Aug/12/2019 11:50:44	
D	SSH_Intento1	46.249.36.196	00:00:07	Aug/12/2019 11:50:43	
D	SSH_Intento1	5.45.72.32	00:00:06	Aug/12/2019 11:50:42	
D	SSH_Intento1	103.196.241.201	00:00:06	Aug/12/2019 11:50:42	
D	SSH_Intento1	103.196.241.124	00:00:06	Aug/12/2019 11:50:42	
D	SSH_Intento1	103.196.241.151	00:00:04	Aug/12/2019 11:50:41	
D	SSH_Intento1	185.161.208.197	00:00:04	Aug/12/2019 11:50:39	
D	Ataque_SSH	93.158.216.142		Aug/12/2019 09:59:42	
D	Ataque_SSH	178.21.23.191		Aug/12/2019 09:58:36	
D	Ataque_SSH	185.145.27.112		Aug/12/2019 09:47:51	
D	Ataque_SSH	37.1.203.210		Aug/12/2019 09:40:05	
D	Ataque_SSH	185.56.144.106		Aug/12/2019 09:38:41	
D	Ataque_SSH	185.89.132.51		Aug/12/2019 09:38:17	
D	Ataque_SSH	185.129.101.187		Aug/12/2019 07:01:59	
D	Ataque_SSH	46.249.47.155		Aug/12/2019 06:46:21	
D	Ataque_SSH	93.158.201.162		Aug/12/2019 06:46:19	
D	Ataque_SSH	91.201.124.50		Aug/12/2019 06:45:56	
D	Ataque_SSH	91.201.124.189		Aug/12/2019 06:45:28	
D	Ataque_SSH	185.8.178.141		Aug/12/2019 06:45:24	

Limitar intentos de conexión SSH

Firewall

Filter Rules | NAT | Mangle | Raw | Service Ports | Connections | Address Lists | Layer7 Protocols

00 Reset Counters | 00 Reset All Counters | Find | all

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Interface	Out. I...	Bytes	Packets	Comment
0	add src to address list	input			6 (tcp)		22			0 B	0	IN - SSH Intento 1
1	add src to address list	input			6 (tcp)		22			0 B	0	IN - SSH Intento 2
2	add src to address list	input			6 (tcp)		22			0 B	0	IN - SSH Intento 3
3	add src to address list	input			6 (tcp)		22			0 B	0	IN - Lista Negra SSH
4	drop	input			6 (tcp)		22			0 B	0	IN - Descartar Lista Negra SSH

Firewall

Filter Rules | NAT | Mangle | Raw | Service Ports | Connections | Address Lists | Layer7 Protocols

00 Reset Counters | 00 Reset All Counters | Find | all

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Interface	Out. I...	Bytes	Packets	Comment
0	drop	input			6 (tcp)		22			0 B	0	IN - Descartar Lista Negra SSH
1	add src to address list	input			6 (tcp)		22			0 B	0	IN - Lista Negra SSH
2	add src to address list	input			6 (tcp)		22			0 B	0	IN - SSH Intento 3
3	add src to address list	input			6 (tcp)		22			0 B	0	IN - SSH Intento 2
4	add src to address list	input			6 (tcp)		22			0 B	0	IN - SSH Intento 1

Port Knocking

Firewall

Filter Rules | NAT | Mangle | Raw | Service Ports | Connections | Address Lists | Layer7 Protocols

00 Reset Counters | 00 Reset All Counters | Find | all

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Inte...	Out. I...	Src. Address List	Bytes	Packets	Comment
0	accept	input			6 (tcp)		22,8291			IP-Permitidas	0 B	0	IN - Conexión SSH y Winbox IP-Permitidas

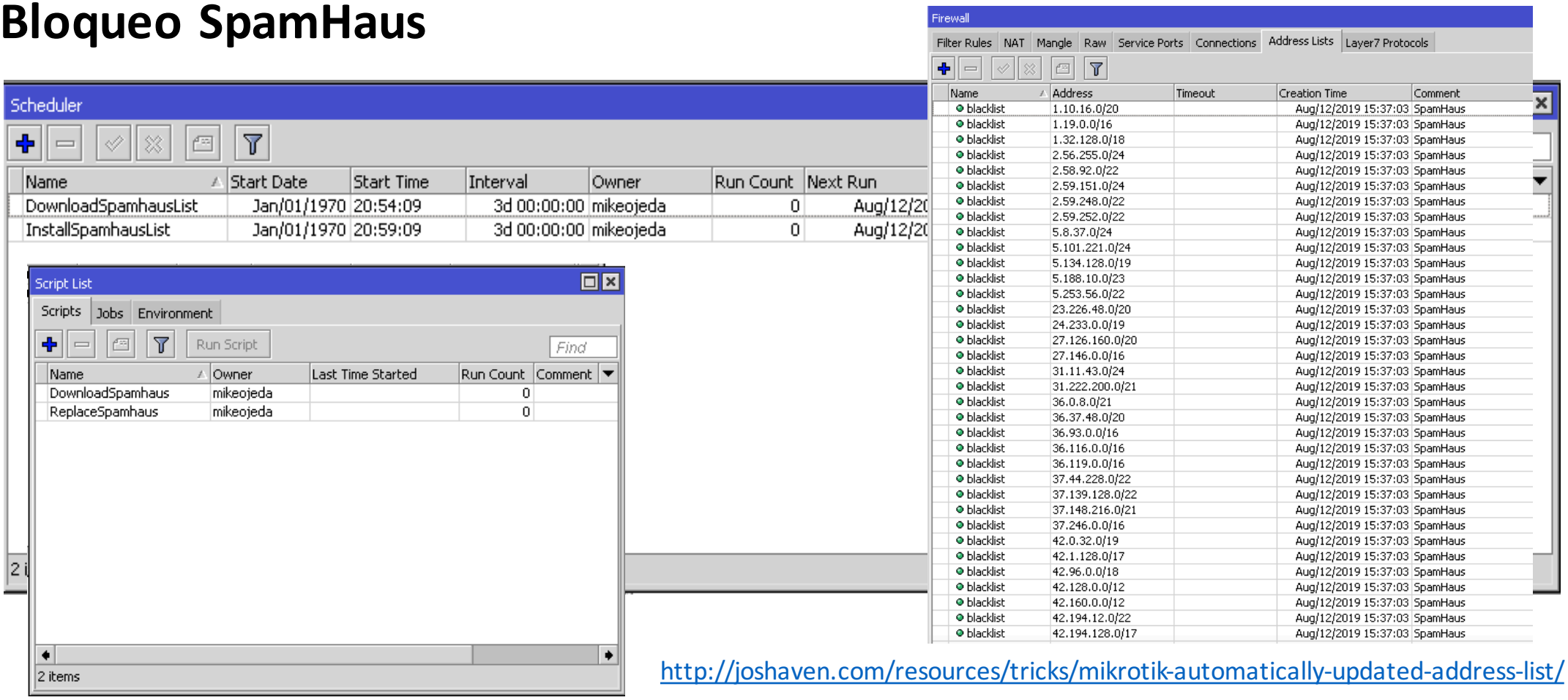
Firewall

Filter Rules | NAT | Mangle | Raw | Service Ports | Connections | Address Lists | Layer7 Protocols

00 Reset Counters | 00 Reset All Counters | Find | all

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Inte...	Out. I...	Src. Address List	Bytes	Packets	Comment
0	accept	input			6 (tcp)		22,8291			IP-Permitidas	0 B	0	IN - Descartar Lista Negra SSH
1	add src to address list	input			6 (tcp)		3000			Knock2	0 B	0	IN - Knocking 3
2	add src to address list	input			6 (tcp)		2000			Knock1	0 B	0	IN - Knocking 2
3	add src to address list	input			6 (tcp)		1000				0 B	0	IN - Knocking 1

Bloqueo SpamHaus



http://joshaven.com/resources/tricks/mikrotik-automatically-updated-address-list/

Preguntas?

Muchas Gracias !!!

José Miguel Ojeda Flores
miguel.ojeda@home-capacity.com
miguel.ojeda@mikrotiksolutions.com
(+593)992629181
Skype: ojedamiguel