IP Spoofing & BCP38

Ing. Mario Clep
MKE Solutions

15 y 16 de Noviembre de 2018

Buenos Aires

MKE solutions

Presentación Personal

- Nombre: Mario Clep
- Profesión: Ing. en Telecomunicaciones
- CTO - MKE Solutions
- Consultor y Entrenador MikroTik RouterOS
- Experiencia desde 2005

- marioclep@mkesolutions.net
- marioclep
- @marioclep

MUM

MKE Solutions

- Consultora en Telecomunicaciones
- Establecida en 2008
- Certificada en **ISO 9001:2015**
  - Soporte IT
  - Entrenamientos Oficiales

info@mkesolutions.net

@mkesolutions

/mkesolutions

/mkesolutions

www.MKESolutions.net

+54 9 358 4210029

MikroTik

MKE solutions

MUM

Academia de Entrenamientos

MikroTik MTCNA

MikroTik MTCWE

MikroTik MTCTCE

MikroTik MTCUME

MikroTik MTCIPv6E

MikroTik MTCRE

MikroTik MTCINE

- Entrenamientos Públicos y Privados.
- MikroTik Academy

Academia DE ENTRENAMIENTOS

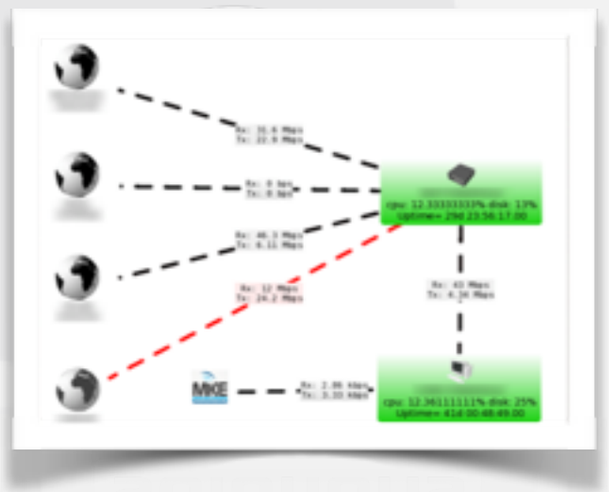
MikroTik

powered by MKE Solutions

MKE solutions

Soporte IT

- Diseño, desarrollo e implementación de soluciones.
- Incidencias puntuales.
- Soporte mensual (OutSourcing).
  - Revisión y Optimización
  - Actualización
  - Mantenimiento preventivo
  - Monitoreo
  - Asesoramiento
  - Soporte Prioritario
  - Guardia 24x7
  - Implementaciones Adicionales



MUM

Oráculo

oraculo monitoreo de redes

Status | Dashboard | Devices (226) | Maps | Syslog | Settings | Backups | Events (2) | ConfigHistory (1450) | Timeouts (4) | Account

NETWORK ONLINE
98.23%
Online 222 | Offline 4

TOTAL DEVICES
226
Warning 3 | Timeout 4 | No Login 0

TOTAL PORTS &
76419
Sensors 73147 | Ports 3230 | Add Options 42

EVENTS UNREAD
2
With Warning Status 2

CONFIG HISTORY
1450
Monitoring Devices 1

DISK USAGE
54%
Files Backups 21537 | Disk Backups 27G

Oraculo Server Status

Date	Uptime	License	Status	Bot Telegram	WebService
2018-04-11 14:30:28	14:30:28	OUTSOURCING	VALID_LICENSE	OK	OK
# CPU info	**CPU avr**	**Memory**	**Mem Used**	**Disk System**	**Disk Used**
3 Cores - Virtual a7769a6388d5	*2.61 1.92 1.91*	3.9 GiB	95%	59 GiB	56%

GeoMAPs Category

ZoomOut

Overview (1 Hour)

Device	AV 1h	RTT	PL	Downs	Alarms	Reboot	PF	Important
[redacted]	0%	0 ms	100%	0	0	0	0	4
[redacted]	0%	0 ms	99.97%	0	0	0	0	4
[redacted]	0%	0 ms	99.97%	0	0	0	0	4
[redacted]	0%	0 ms	98.21%	0	0	0	0	2
[redacted]	95.729%	331.52 ms	20.7%	15	0	0	0	2

Last Devices Timeout

Device	Category	Last Seen	Last Probe	Status
[redacted]	[redacted]	40 minutes ago	44 minutes ago	Timeout
[redacted]	[redacted]	20 hours ago	20 hours ago	Timeout
[redacted]	[redacted]	March 28	March 28	Timeout
[redacted]	[redacted]	March 27	March 27	Timeout

Last Events

When	Device	Event	Variable	Before	Actual
8 min	[redacted] 1.2.196 >	bgp	Change value for **peer** **Cache de Facebook BGP**	connect	active
13 min	[redacted] 1.2.196 >	bgp	Change value for **peer** **Cache de Facebook BGP**	active	connect
18 min	[redacted] 1.2.196 >	bgp	Change value for **peer** **Cache de Facebook BGP**	connect	active
23 min	[redacted] 1.2.196 >	bgp	Change value for **peer**	active	connect

MikroTik

oraculo.mkesolutions.net

MKE solutions

Introducción y Objetivos

Mas allá de proteger el router deshabilitando los servicios que no se utilizan e implementando reglas de Firewall, también es necesario (?) implementar reglas que controlen el tráfico desde/hacia sus clientes.

- **RFC2827 (BCP38).**
- RFC3704: RP-Filter.
- Puertos más comunes a proteger.
- IDS / IPS / mitigadores.
- BGP Blackholing.
- Buena comunicación (y predisposición) del proveedor.

El problema…

Torch (Running)

Basic

Interface: ether3

Entry Timeout: 00:00:03 s

Collect

- [x] Src. Address
- [x] Dst. Address
- [x] MAC Protocol
- [x] Protocol
- [ ] DSCP
- [ ] Src. Address6
- [ ] Dst. Address6
- [x] Port
- [ ] VLAN Id

Filters

Src. Address: 0.0.0.0/0

Dst. Address: [redacted]

Src. Address6: ::/0

Dst. Address6: ::/0

MAC Protocol: all

Protocol: any

Port: any

VLAN Id: any

DSCP: any

Eth. Pro...	Protocol	Src.	Dst.	VLAN Id	DSCP	Tx Rate	Rx Rate	Tx Pack...	Rx Pack...
800 (ip)	17 (udp)	31.76.153.223:35978	[redacted]:27610			0 bps	744 bps	0	1
800 (ip)	17 (udp)	32.19.202.196:39908	[redacted]:27147			0 bps	744 bps	0	1
800 (ip)	17 (udp)	32.37.142.48:61061	[redacted]:27201			0 bps	744 bps	0	1
800 (ip)	17 (udp)	31.83.117.100:17881	[redacted]:27041			0 bps	664 bps	0	1
800 (ip)	17 (udp)	31.56.178.81:27634	[redacted]:27767			0 bps	656 bps	0	1
800 (ip)	17 (udp)	31.102.163.139:44750	[redacted]:27558			0 bps	656 bps	0	1
800 (ip)	17 (udp)	31.193.74.77:10115	[redacted]:27868			0 bps	624 bps	0	1
800 (ip)	17 (udp)	31.196.149.127:19084	[redacted]:27912			0 bps	624 bps	0	1
800 (ip)	17 (udp)	31.200.180.117:52663	[redacted]:27638			0 bps	624 bps	0	1
800 (ip)	17 (udp)	30.211.242.93:50994	[redacted]:27398			0 bps	616 bps	0	1
800 (ip)	17 (udp)	31.6.180.183:50773	[redacted]:27126			0 bps	616 bps	0	1
800 (ip)	17 (udp)	31.73.198.161:17520	[redacted]:27649			0 bps	616 bps	0	1
800 (ip)	17 (udp)	31.92.41.152:18751	[redacted]:27107			0 bps	600 bps	0	1
800 (ip)	17 (udp)	31.103.203.105:38230	[redacted]:27232			0 bps	600 bps	0	1
800 (ip)	17 (udp)	31.164.165.10:28313	[redacted]:27204			0 bps	600 bps	0	1
800 (ip)	17 (udp)	31.175.155.111:11108	[redacted]:27476			0 bps	600 bps	0	1
800 (ip)	17 (udp)	32.18.148.207:55999	[redacted]:27964			0 bps	600 bps	0	1
800 (ip)	17 (udp)	30.204.198.217:27609	[redacted]:27628			0 bps	592 bps	0	1
800 (ip)	17 (udp)	31.11.133.75:39861	[redacted]:27848			0 bps	592 bps	0	1
800 (ip)	17 (udp)	31.33.125.24:46028	[redacted]:27493			0 bps	592 bps	0	1
800 (ip)	17 (udp)	31.77.218.138:16417	[redacted]:27743			0 bps	592 bps	0	1
800 (ip)	17 (udp)	31.88.132.122:50210	[redacted]:27391			0 bps	592 bps	0	1

900 items | Total Tx: 0 bps | Total Rx: 13.9 Mbps | Total Tx Packet: 0 | Total Rx Packet: 26 843

Análisis

Torch (Running)

Basic

Interface: ether3

Entry Timeout: 00:00:03 s

Collect

- [x] Src. Address
- [x] Dst. Address
- [x] MAC Protocol
- [x] Protocol
- [ ] DSCP
- [ ] Src. Address6
- [ ] Dst. Address6
- [x] Port
- [ ] VLAN Id

Filters

Src. Address: 0.0.0.0/0

Dst. Address: [redacted]

Src. Address6: ::/0

Dst. Address6: ::/0

MAC Protocol: all

Protocol: any

Port: any

VLAN Id: any

DSCP: any

Eth. Pro...	Protocol	Src.	Dst.	VLAN Id	DSCP	Tx Rate	Rx Rate	Tx Pack...	Rx Pack...
800 (ip)	17 (udp)	31.76.153.223:35978	[redacted]:27610			0 bps	744 bps	0	1
800 (ip)	17 (udp)	32.19.202.196:39908	[redacted]:27147			0 bps	744 bps	0	1
800 (ip)	17 (udp)	32.37.142.48:61061	[redacted]:27201			0 bps	744 bps	0	1
800 (ip)	17 (udp)	31.83.117.100:17881	[redacted]:27041			0 bps	664 bps	0	1
800 (ip)	17 (udp)	31.56.178.81:27634	[redacted]:27767			0 bps	656 bps	0	1
800 (ip)	17 (udp)	31.102.163.139:44750	[redacted]:27558			0 bps	656 bps	0	1
800 (ip)	17 (udp)	31.193.74.77:10115	[redacted]:27868			0 bps	624 bps	0	1
800 (ip)	17 (udp)	31.196.149.127:19084	[redacted]:27912			0 bps	624 bps	0	1
800 (ip)	17 (udp)	31.200.180.117:52663	[redacted]:27638			0 bps	624 bps	0	1
800 (ip)	17 (udp)	30.211.242.93:50994	[redacted]:27398			0 bps	616 bps	0	1
800 (ip)	17 (udp)	31.6.180.183:50773	[redacted]:27126			0 bps	616 bps	0	1
800 (ip)	17 (udp)	31.73.198.161:17520	[redacted]:27649			0 bps	616 bps	0	1
800 (ip)	17 (udp)	31.92.41.152:18751	[redacted]:27107			0 bps	600 bps	0	1
800 (ip)	17 (udp)	31.103.203.105:38230	[redacted]:27232			0 bps	600 bps	0	1
800 (ip)	17 (udp)	31.164.165.10:28313	[redacted]:27204			0 bps	600 bps	0	1
800 (ip)	17 (udp)	31.175.155.111:11108	[redacted]:27476			0 bps	600 bps	0	1
800 (ip)	17 (udp)	32.18.148.207:55999	[redacted]:27964			0 bps	600 bps	0	1
800 (ip)	17 (udp)	30.204.198.217:27609	[redacted]:27628			0 bps	592 bps	0	1
800 (ip)	17 (udp)	31.11.133.75:39861	[redacted]:27848			0 bps	592 bps	0	1
800 (ip)	17 (udp)	31.33.125.24:46028	[redacted]:27493			0 bps	592 bps	0	1
800 (ip)	17 (udp)	31.77.218.138:16417	[redacted]:27743			0 bps	592 bps	0	1
800 (ip)	17 (udp)	31.88.132.122:50210	[redacted]:27391			0 bps	592 bps	0	1

900 items | Total Tx: 0 bps | Total Rx: 13.9 Mbps | Total Tx Packet: 0 | Total Rx Packet: 26 843

MikroTik

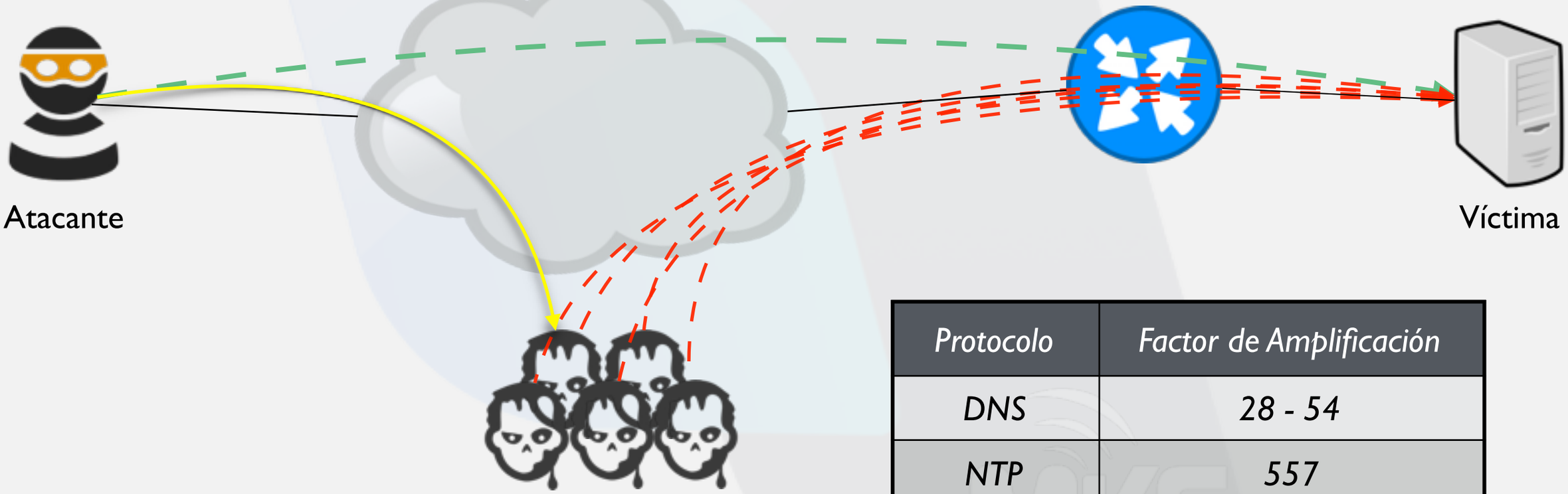
MKE solutions

Análisis

- Interfaz de entrada: WAN
- Todo el tráfico es UDP.
- **IP origen aleatoria.**
- **Puerto de origen aleatorio.**
- IP destino > Cliente atacado.
- **Puerto de destino aleatorio.**
- Paquetes recibidos: 26800.
- Paquetes enviados: 0.

¿Qué es DoS / DDoS?

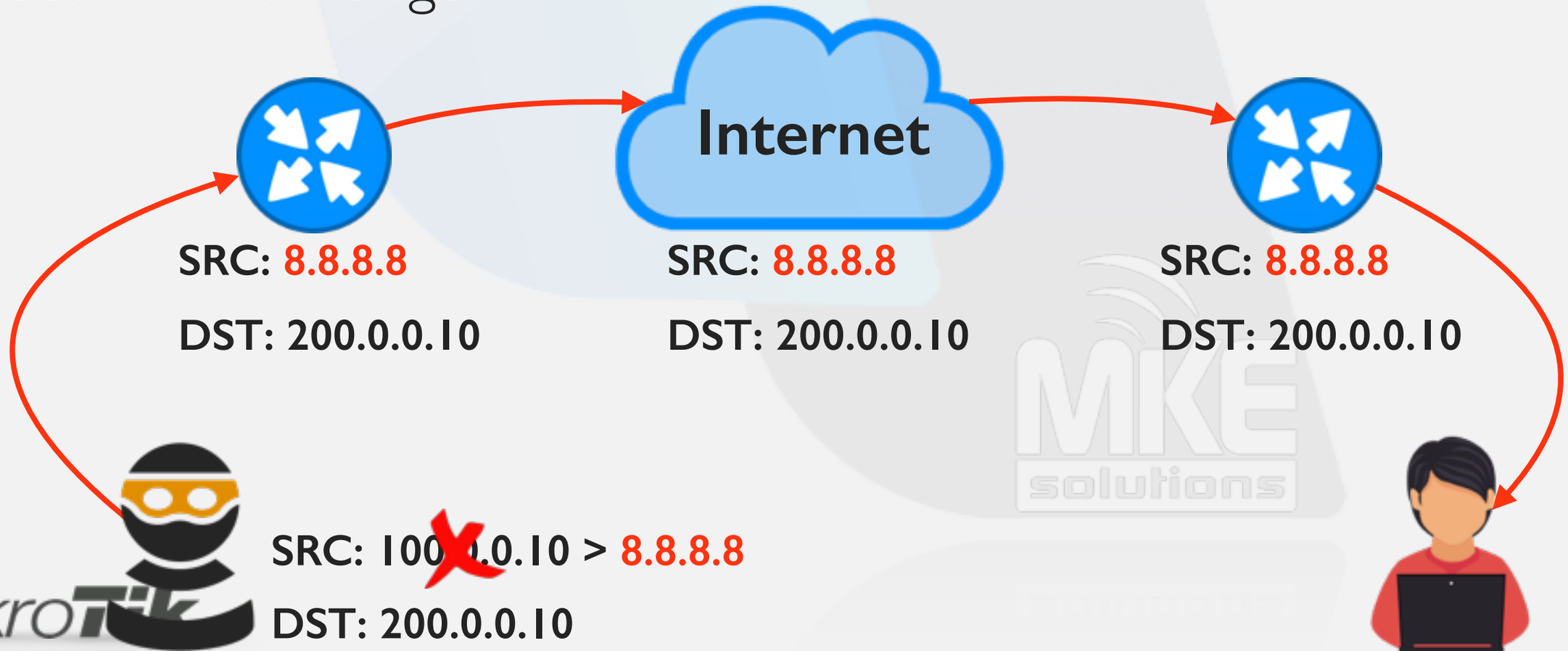
- Los ataques de denegación de servicio tienen como principal objetivo atacar el vínculo más débil para provocar una caída del servicio: capacidad contratada, capacidad de procesamiento, enlaces troncales, distribuciones, AB del cliente, etc.



Protocolo	*Factor de Amplificación*
DNS	*28 - 54*
NTP	*557*
SNMPv2	*6.3*
NetBIOS	*3.8*
CharGEN	*358*

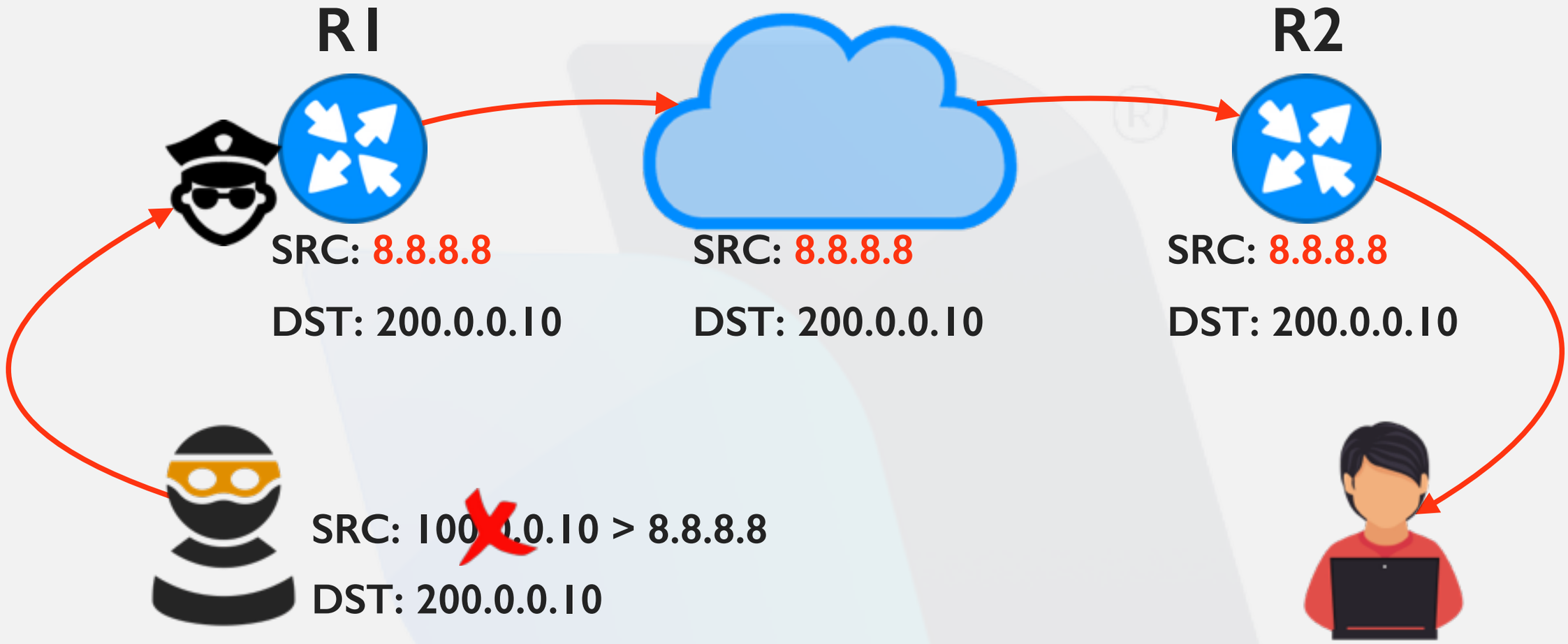
¿Qué es el IP Spoofing?

- Sustitución de la dirección IP de origen de un paquete IP por otra totalmente falsa.
- Un router **normalmente** inspecciona la cabecera IP, busca la dirección IP de destino y la compara con su tabla de enrutamiento para determinar cual es el próximo salto, pero no hace nada con la dirección IP de origen.



¿Se puede hacer algo?

- **Filtrar el tráfico válido antes que sea demasiado tarde!**

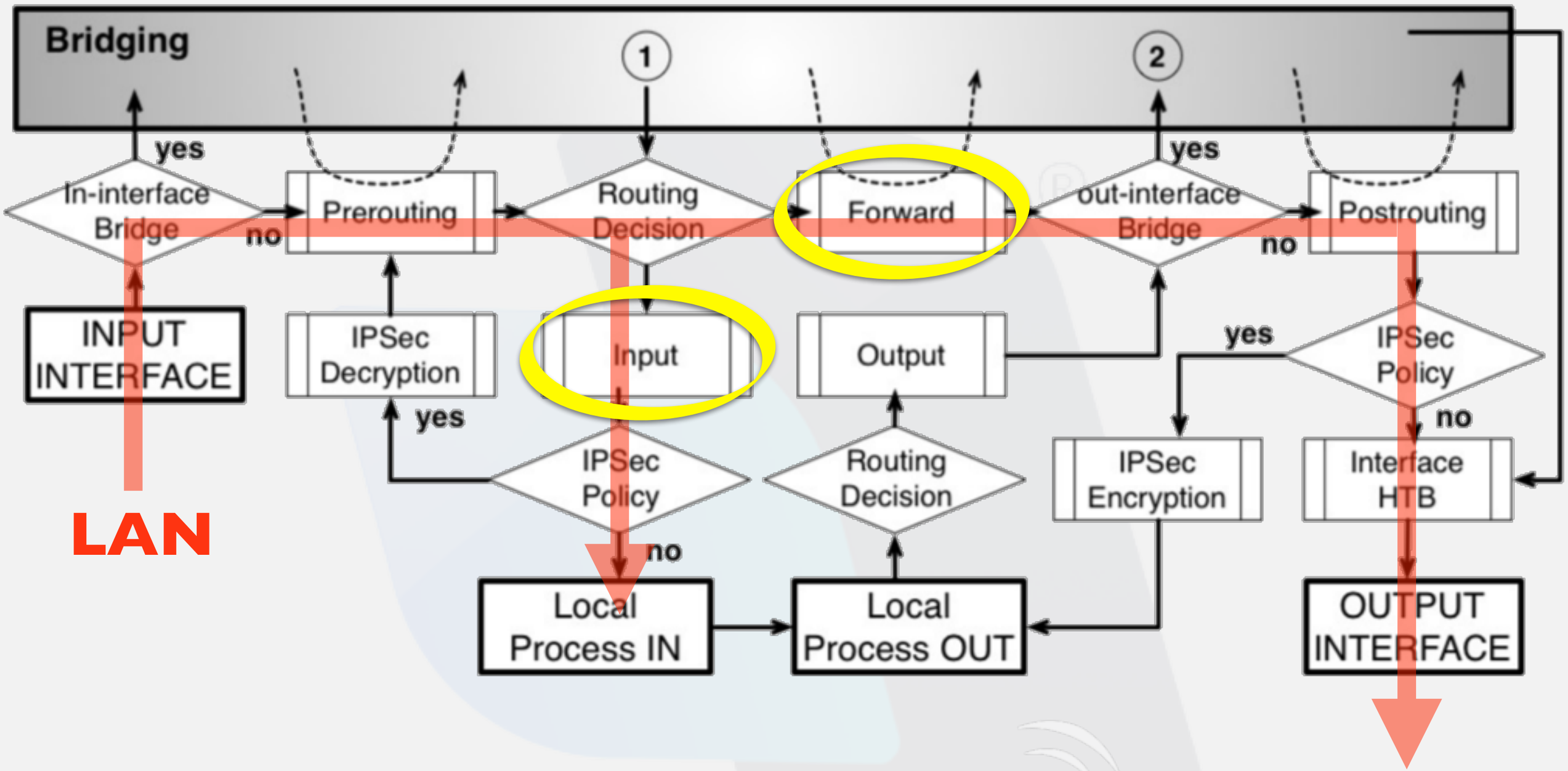


- **R2** no tiene manera de reconocer si el nuevo origen **8.8.8.8** es verdadero o falso.
- Implementar BCP38 ó uRPF.

BCP38 - Ingress Filtering

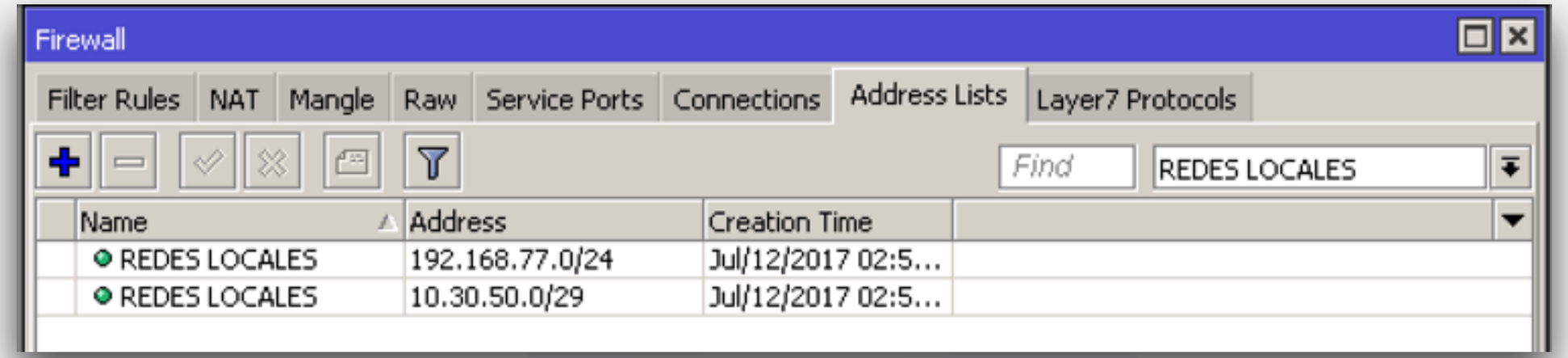
- **Que?** BCP38: Best Current Practice 38 > RFC2827
- **Cuando?** Mayo de 2000.
- **Porqué?** Eliminar los ataques DoS provocados por IP Spoofing y detectar el verdadero origen del ataque.
- **Cómo?** Bloqueando el tráfico que ingrese al router con *direcciones IP de origen diferentes a nuestras propias direcciones*.
- **Donde?** En las interfaces locales de nuestros routers.

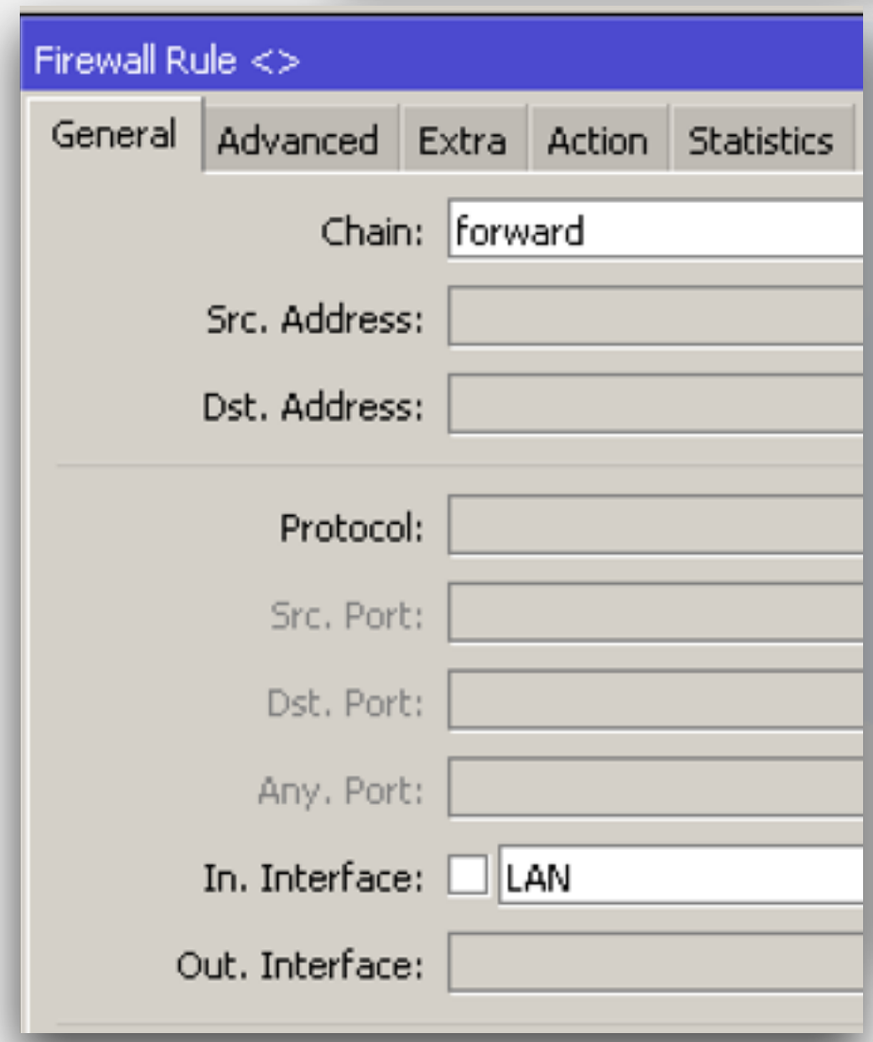
MUM Diagrama de Flujo en RouterOS

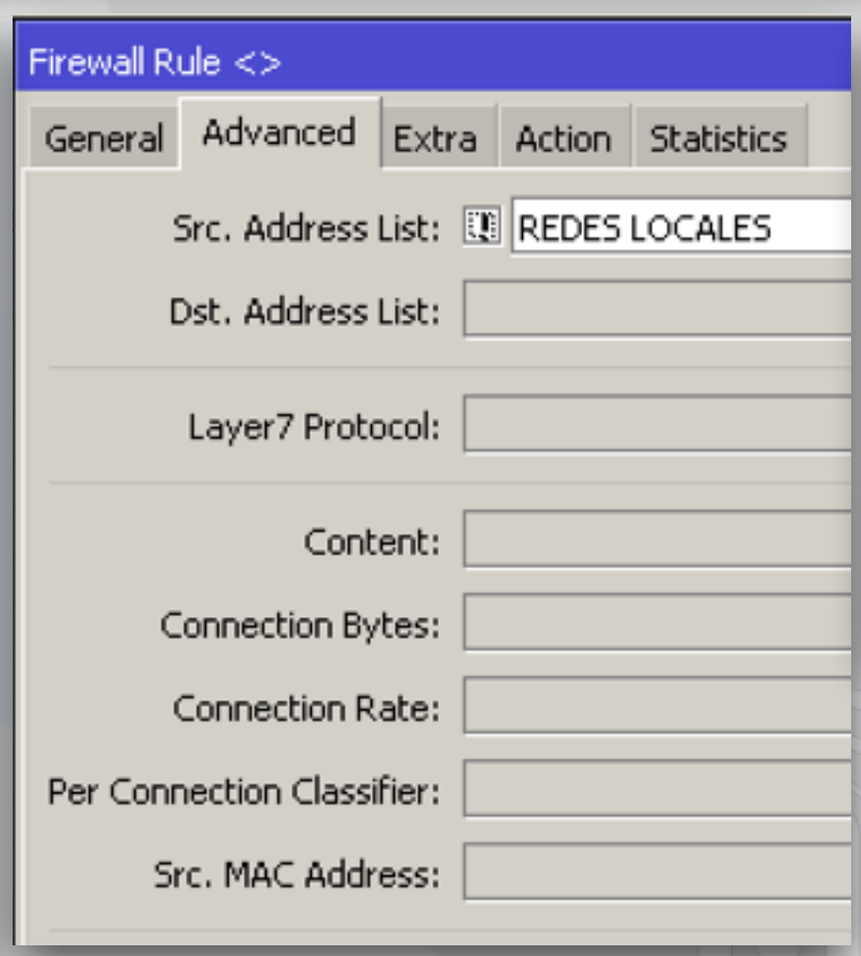


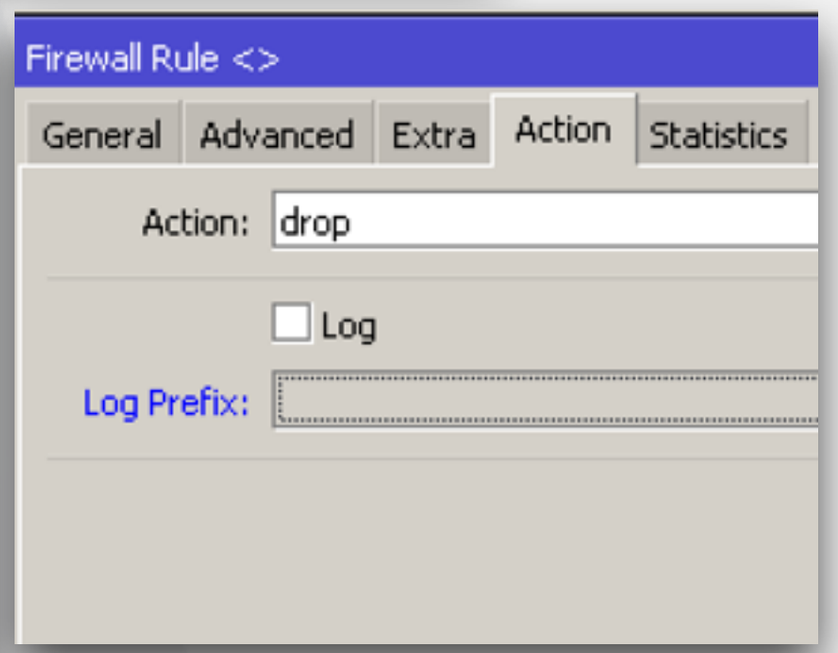
- */ip firewall filter add* ***chain=forward / chain=input…***

Reglas de Firewall









MikroTik

MKE solutions

Reglas de Firewall

```
/ ip firewall address-list
add address=192.168.78.0/24 list="REDES LOCALES"
add address=10.30.50.0/29 list="REDES LOCALES"

/ ip firewall filter
add chain=forward in-interface=LAN src-address-list=!"REDES LOCALES"  \
action=drop comment=BCP38

add chain=input in-interface=LAN src-address-list=!"REDES LOCALES"  \
action=drop comment=BCP38
```

DDoS en acción

Torch (Running)

Basic

Interface: Locales

Entry Timeout: 00:00:03 s

Collect

- [x] Src. Address
- [ ] Src. Address6
- [x] Dst. Address
- [ ] Dst. Address6
- [x] MAC Protocol
- [x] Port
- [x] Protocol
- [ ] VLAN Id
- [ ] DSCP

Filters

Src. Address: 0.0.0.0/0

Dst. Address: 0.0.0.0/0

Src. Address6: ::/0

Dst. Address6: ::/0

MAC Protocol: all

Protocol: any

Port: any

VLAN Id: any

DSCP: any

Start

Stop

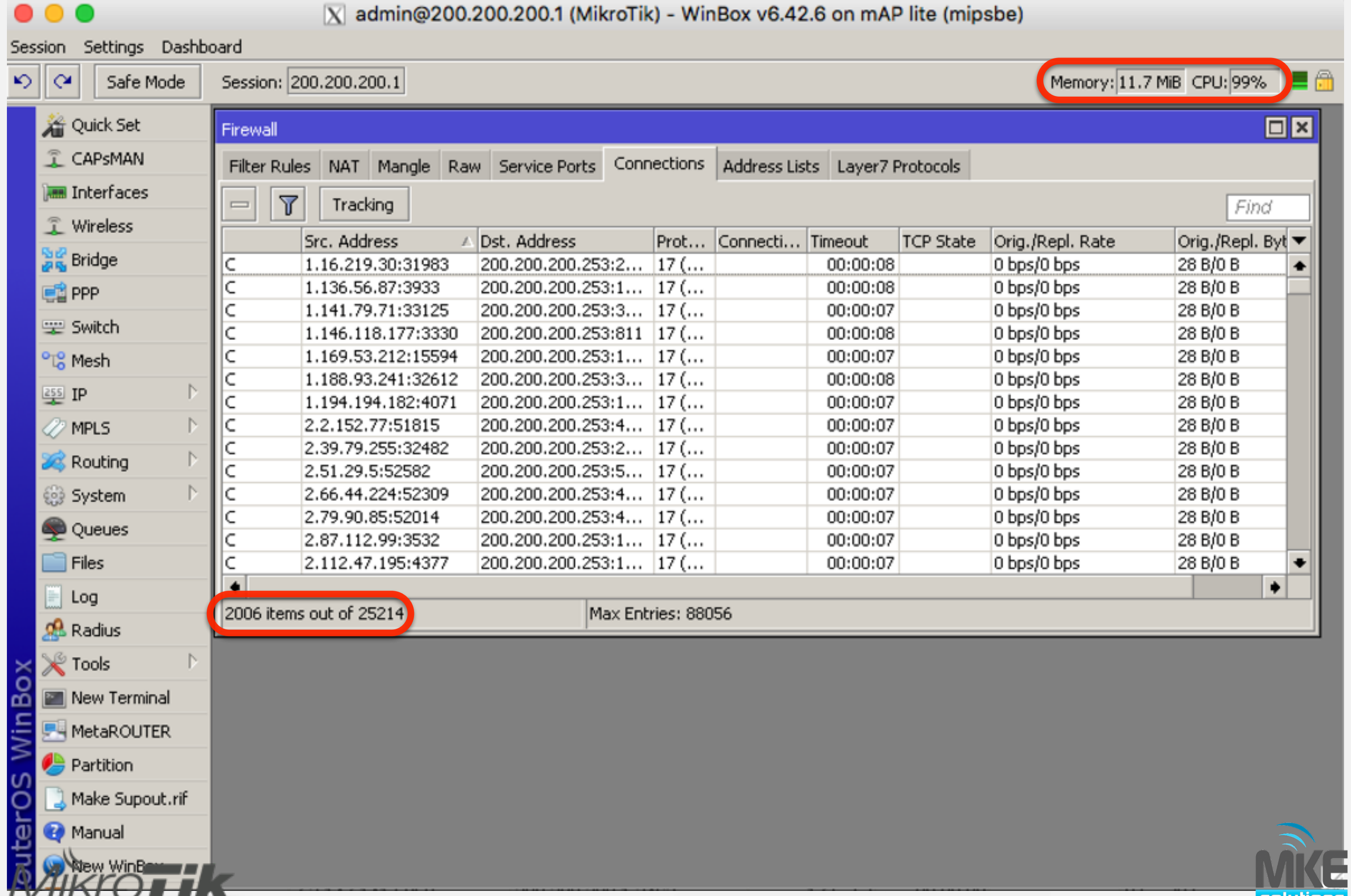
Close

New Window

Et...	Pro...	Src.	Dst.	VLAN Id	DSCP	Tx Rate	Rx Rate	Tx Pack...	Rx Pack...
800 ...	17 ...	40.248.77.163:10588	200.200.200.253:8334			0 bps	0 bps	0	0
800 ...	17 ...	35.178.1.126:10591	200.200.200.253:8337			0 bps	0 bps	0	0
800 ...	17 ...	28.60.94.218:10601	200.200.200.253:8347			0 bps	0 bps	0	0
800 ...	17 ...	7.202.239.92:10603	200.200.200.253:8349			0 bps	336 bps	0	1
800 ...	17 ...	5.91.31.75:10625	200.200.200.253:8371			0 bps	336 bps	0	1
800 ...	17 ...	18.112.41.1:10627	200.200.200.253:8373			0 bps	336 bps	0	1
800 ...	17 ...	1.217.246.210:10636	200.200.200.253:8382			0 bps	336 bps	0	1
800 ...	17 ...	29.155.75.91:10642	200.200.200.253:8388			0 bps	0 bps	0	0
800 ...	17 ...	32.222.50.18:10644	200.200.200.253:8390			0 bps	0 bps	0	0
800 ...	17 ...	17.61.129.60:10647	200.200.200.253:8393			0 bps	336 bps	0	1
800 ...	17 ...	18.18.192.94:10648	200.200.200.253:8394			0 bps	336 bps	0	1
800 ...	17 ...	5.213.112.199:10657	200.200.200.253:8403			0 bps	336 bps	0	1
800 ...	17 ...	17.83.140.228:10660	200.200.200.253:8406			0 bps	336 bps	0	1
800 ...	17 ...	17.168.51.106:10665	200.200.200.253:8411			0 bps	336 bps	0	1

7900 items | Total Tx: 4.2 kbps | Total Rx: 3.2 Mbps | Total Tx Packet: 5 | Total Rx Packet: 9 509

DDoS en acción



DDoS en acción

admin@200.200.200.1 (MikroTik) - WinBox v6.42.6 on mAP lite (mipsbe)

Session Settings Dashboard

Safe Mode Session: 200.200.200.1 Memory: 41.9 MiB CPU: 49%

Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
MetaROUTER
Partition
Make Supout.rif

RouterOS WinBox

Firewall

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

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

#		Action	Chain	Prot...	Src. Port	In. Int...	Out. I...	Src. Address List	Bytes	Packets
0		drop	forward			Locales		!REDES LOCALES	8.5 MiB	318 387

1 item (1 selected)

Firewall Rule <>

General | Advanced | Extra | Action | Statistics

Bytes: 8.5 MiB
Packets: 318 387
Rate: 1654.9 kbps
Packet Rate: 7 388 p/s

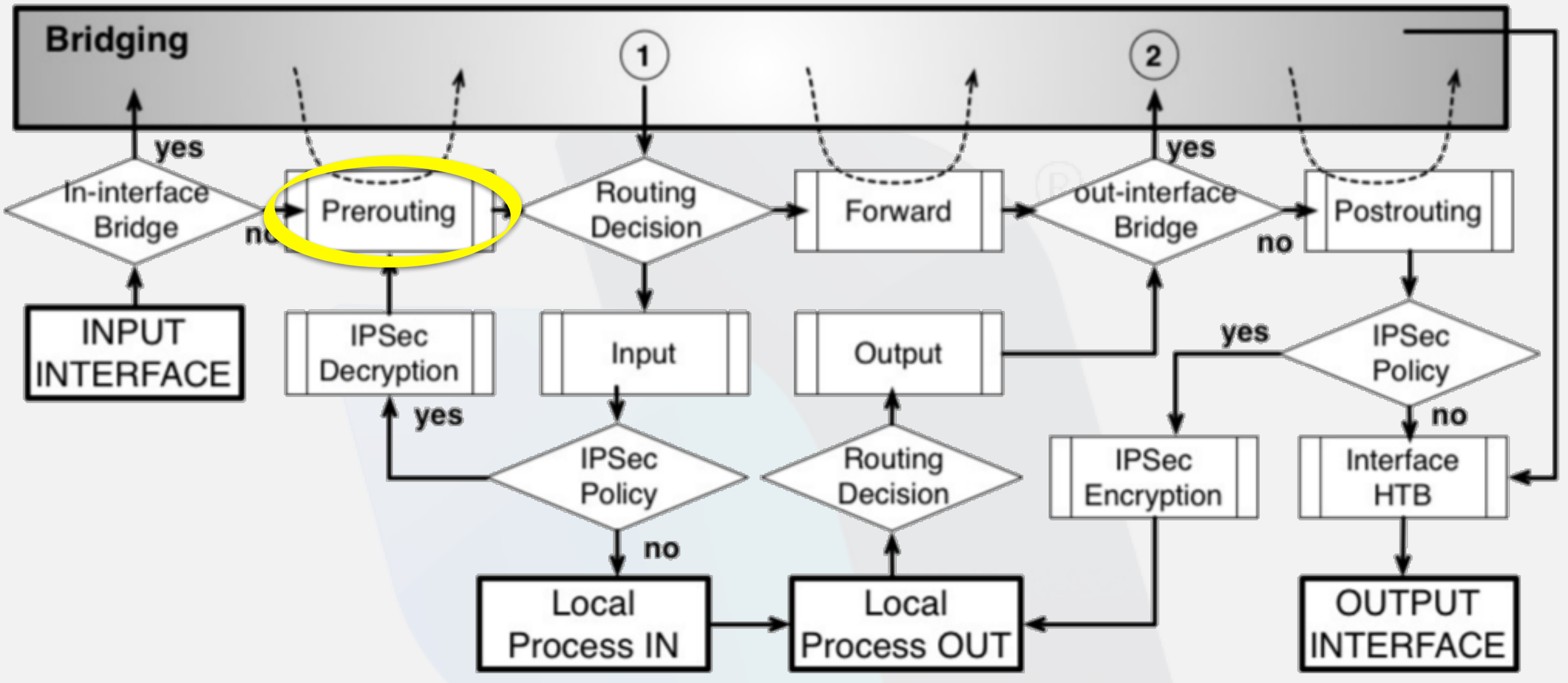
Rate: 1654.9 kbps

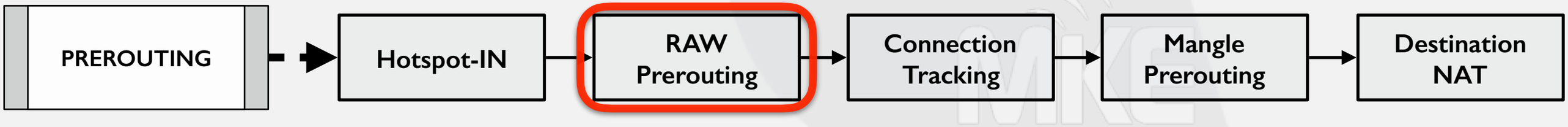
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters

MikroTik

MKE solutions

RAW en RouterOS v6





Resultados Finales (RAW)

admin@200.200.200.1 (MikroTik) - WinBox v6.42.6 on mAP lite (mipsbe)

Session Settings Dashboard

Safe Mode Session: 200.200.200.1 Memory: 34.3 MiB CPU: 18%

- Quick Set
- CAPsMAN
- Interfaces
- Wireless
- Bridge
- PPP
- Switch
- Mesh
- IP
- MPLS
- Routing
- System
- Queues
- Files
- Log
- Radius
- Tools
- New Terminal
- MetaROUTER
- Partition
- Make Supout.rif
- Manual
- New WinBox

RouterOS WinBox

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	Prot...	Src. Port	Dst. Port	In. Int...	Out. I...	Bytes	Packets
0		acc...	prerouting			17 (...	68				7.3 KiB	49
1		drop	prerouting						Locales		50.8 MiB	1 903 142

Raw Rule <>

General | Advanced | Extra | Action | Statistic

Chain: prerouting
Src. Address:
Dst. Address:
Protocol:
Src. Port:
Dst. Port:
Any. Port:
In. Interface: Locales
Out. Interface:
In. Interface List:
Out. Interface List:

New Raw Rule

General | Advanced | Extra | Action | Statistics

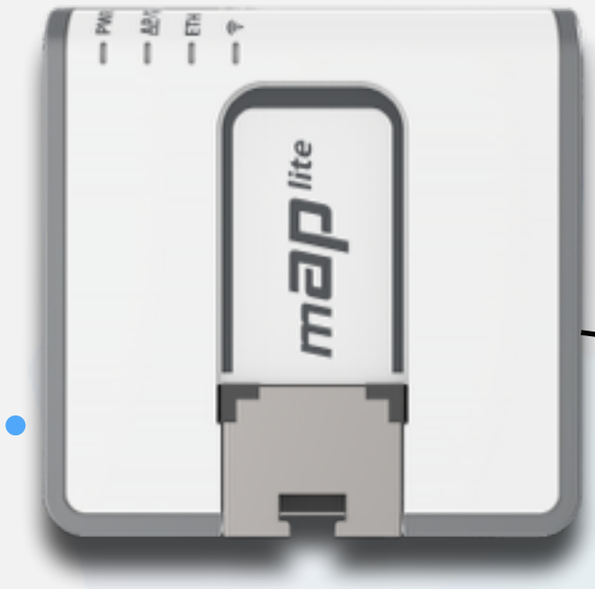
Src. Address List: ! REDES LOCALES
Dst. Address List:
Content:
Per Connection Classifier:
Src. MAC Address:
IPsec Policy:
TLS Host:
Ingress Priority:
Priority:
DSCP (TOS):
TCP MSS:

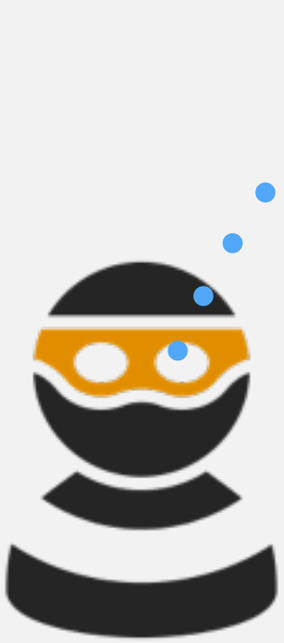
New Raw Rule

General | Advanced | Extra | Action | Statistics

Action: drop
Log
Log Prefix:

DEMO!!





192.168.88.x

200.200.200.254

Conclusión

- **BCP38** no evita que se generen ataques de DoS, cuando se originan desde redes validas, ni impide que se reciban estos ataques desde la interfaz pública.

- La implementación de estas reglas significan un **aumento insignificante del CPU** de un router cuando el tráfico es normal.

- El no disponer de dichas reglas implica un **aumento considerable del CPU** cuando se produce este ataque, provocando **inconsistencias en la red, mayores latencias y reinicios del equipo.**

- ***Si todos los ISP implementaran BCP38, no existiría IP Spoofing.***

Bibliografía

- *https://www.ietf.org/rfc/rfc2827.txt*
- *https://en.wikipedia.org/wiki/IP_address_spoofing*
- *https://en.wikipedia.org/wiki/Ingress_filtering*
- *https://wiki.mikrotik.com/wiki/Manual:IP/Firewall/Raw*
- *https://wiki.mikrotik.com/wiki/Manual:Packet_Flow_v6*
- *https://en.wikipedia.org/wiki/Best_current_practice*

¿Preguntas?

MUCHAS GRACIAS!

Ing. Mario Clep

MKE Solutions

- marioclep@mkesolutions.net

- marioclep

- @marioclep

+54 9 358 4210029