IP Spoofing & BCP38

Ing. Mario Clep
MKE Solutions

25 de Julio de 2017

Asunción - Paraguay

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

MKE Solutions

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

info@mkesolutions.net

@mkesolutions

/mkesolutions

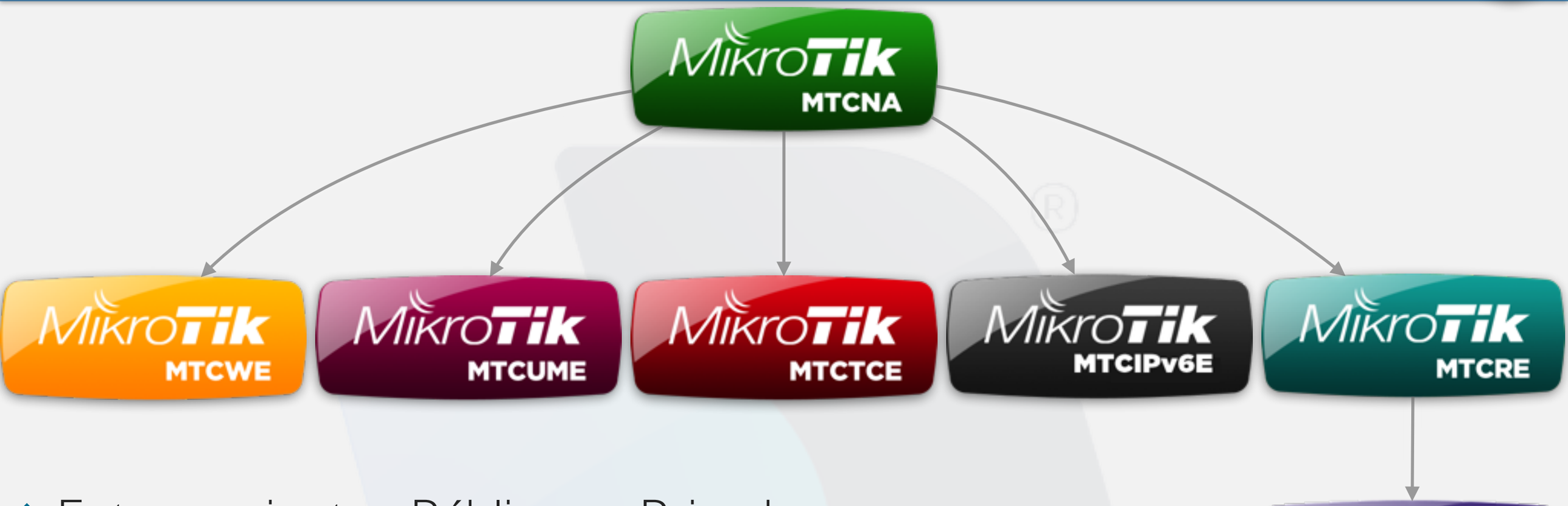
/mkesolutions

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

Academia de Entrenamientos



- Entrenamientos Públicos y Privados.
- ~300 alumnos por año, con un 75% de certificados.

Academia® DE ENTRENAMIENTOS

powered by MKE Solutions

MUM

MKE solutions

Felicitaciones!

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 (BCP86): RP-Filter.
- Puertos más comunes a proteger.
- IDS / IPS / mitigadores.
- BGP Blackholing.

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

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			[redacted]	[redacted]	[redacted]	[redacted]

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

Análisis

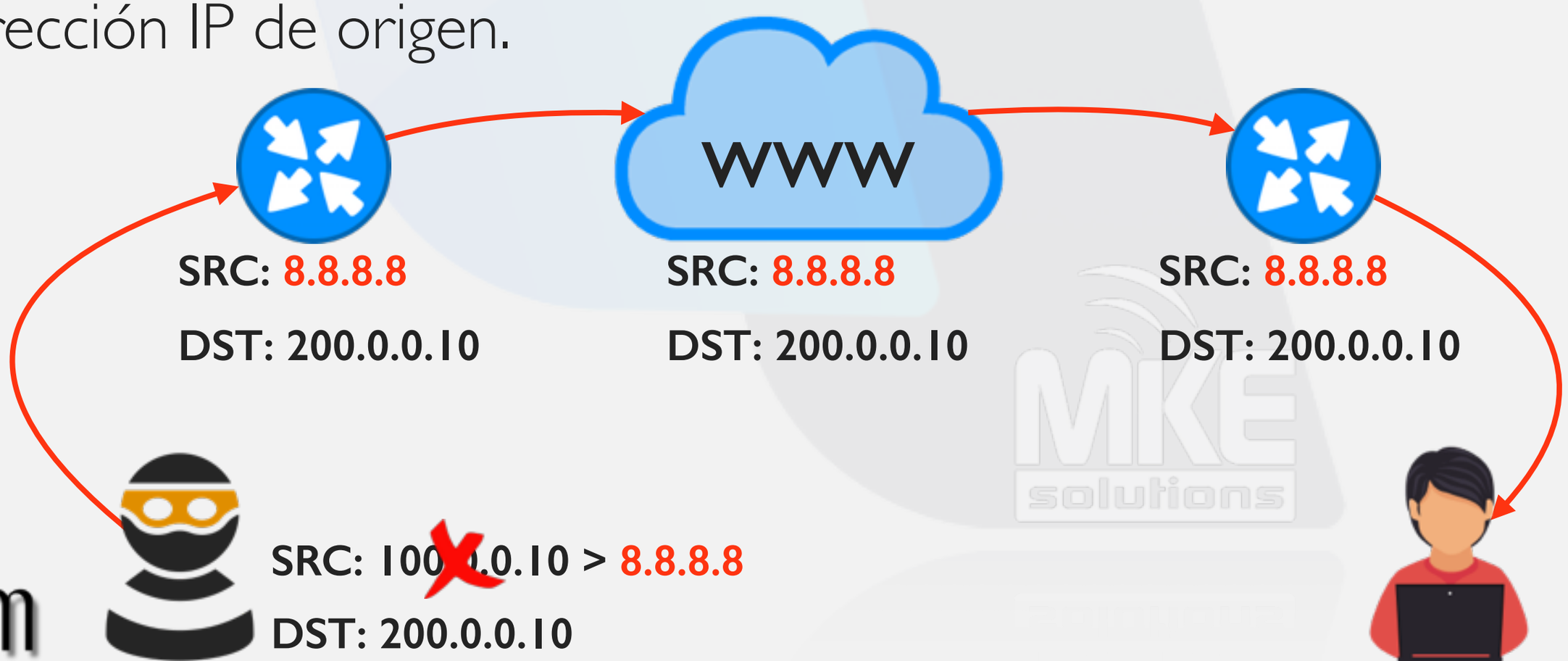
- Interfaz de entrada: WAN
- Todo el tráfico es UDP.
- **IP origen aleatoria.**
- **Puerto de origen aleatorio.**

- IP destino > Cliente atacado.
- **Puerto de destino aleatorio.**
- Paquetes recibidos: 26800.
- Paquetes enviados: 0.

¿Qué es el IP Spoofing?

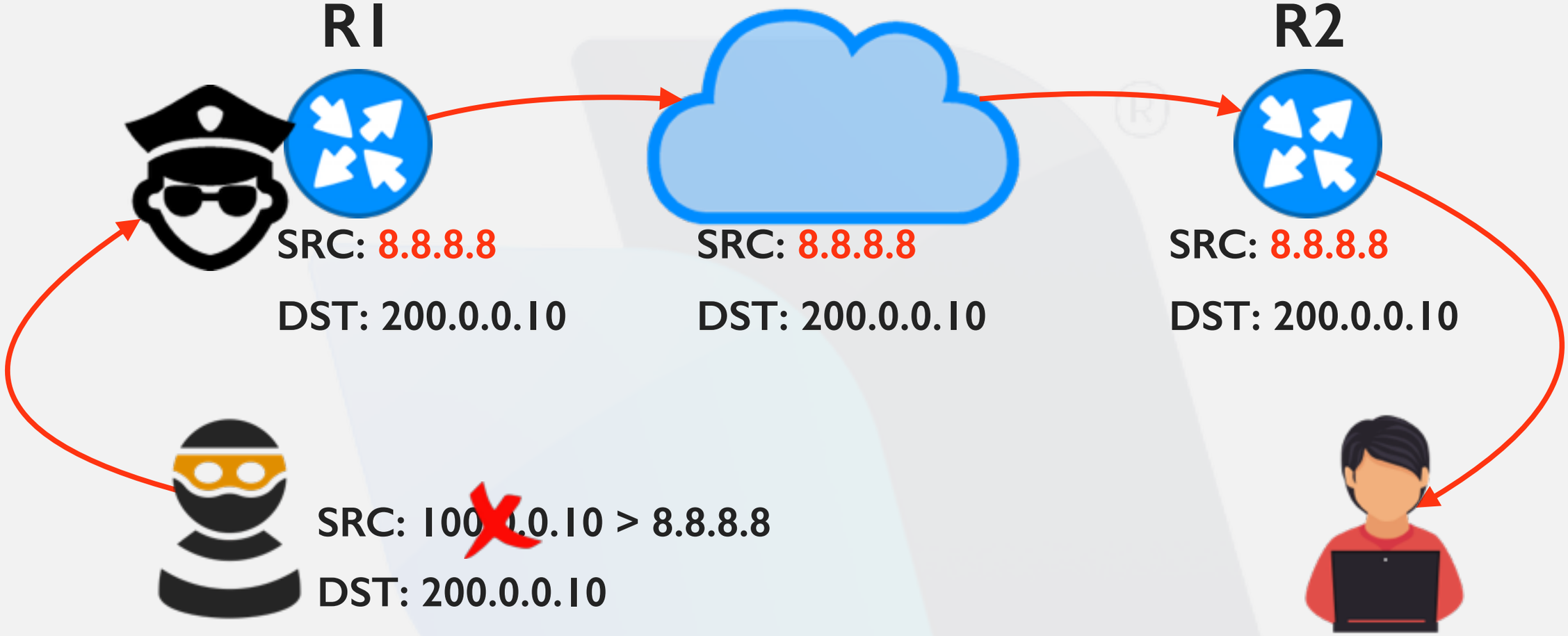
- Sustitución de la dirección IP de origen de un paquete IP por otra totalmente falsa.

- 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!**



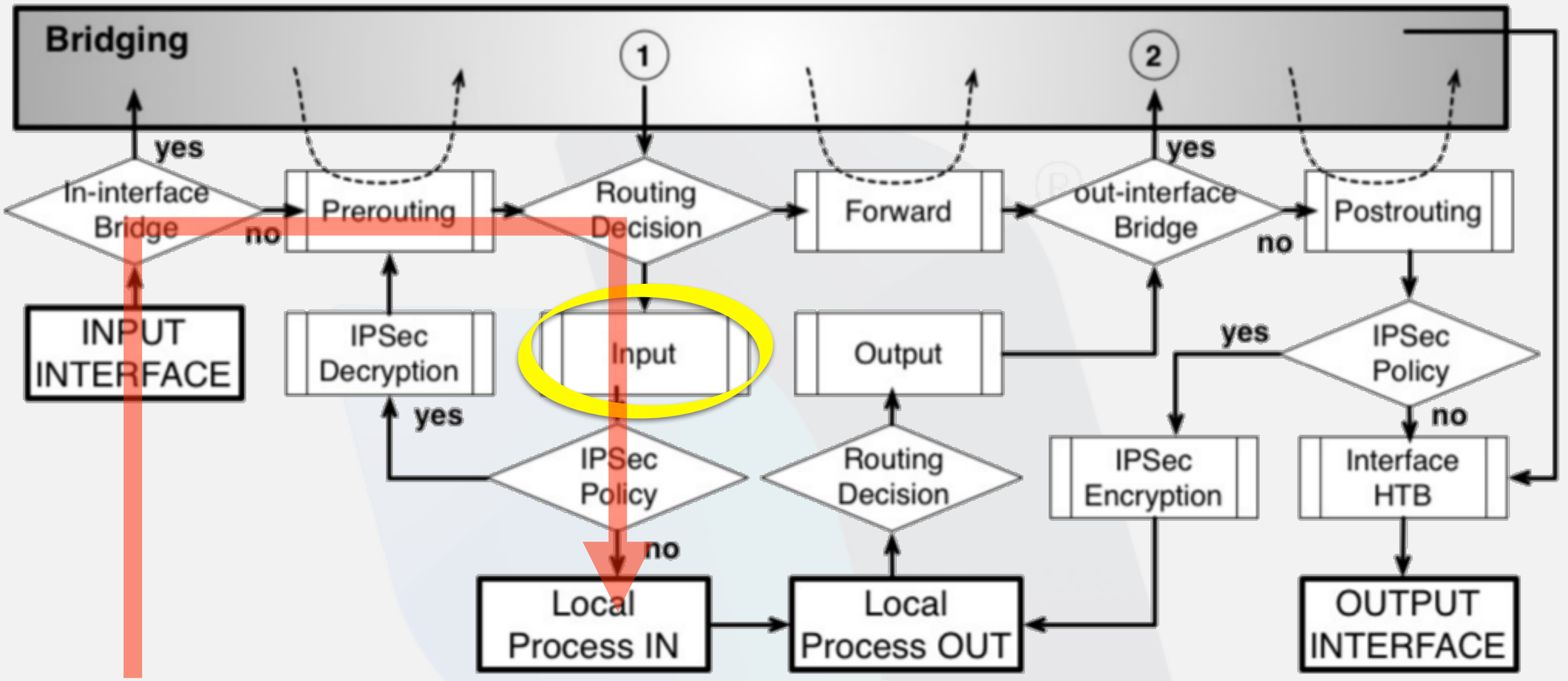
- **R2** no tiene manera de reconocer si el nuevo origen **8.8.8.8** es verdadero o falso.

- Implementar BCP38 ó uRPF.

BCP38

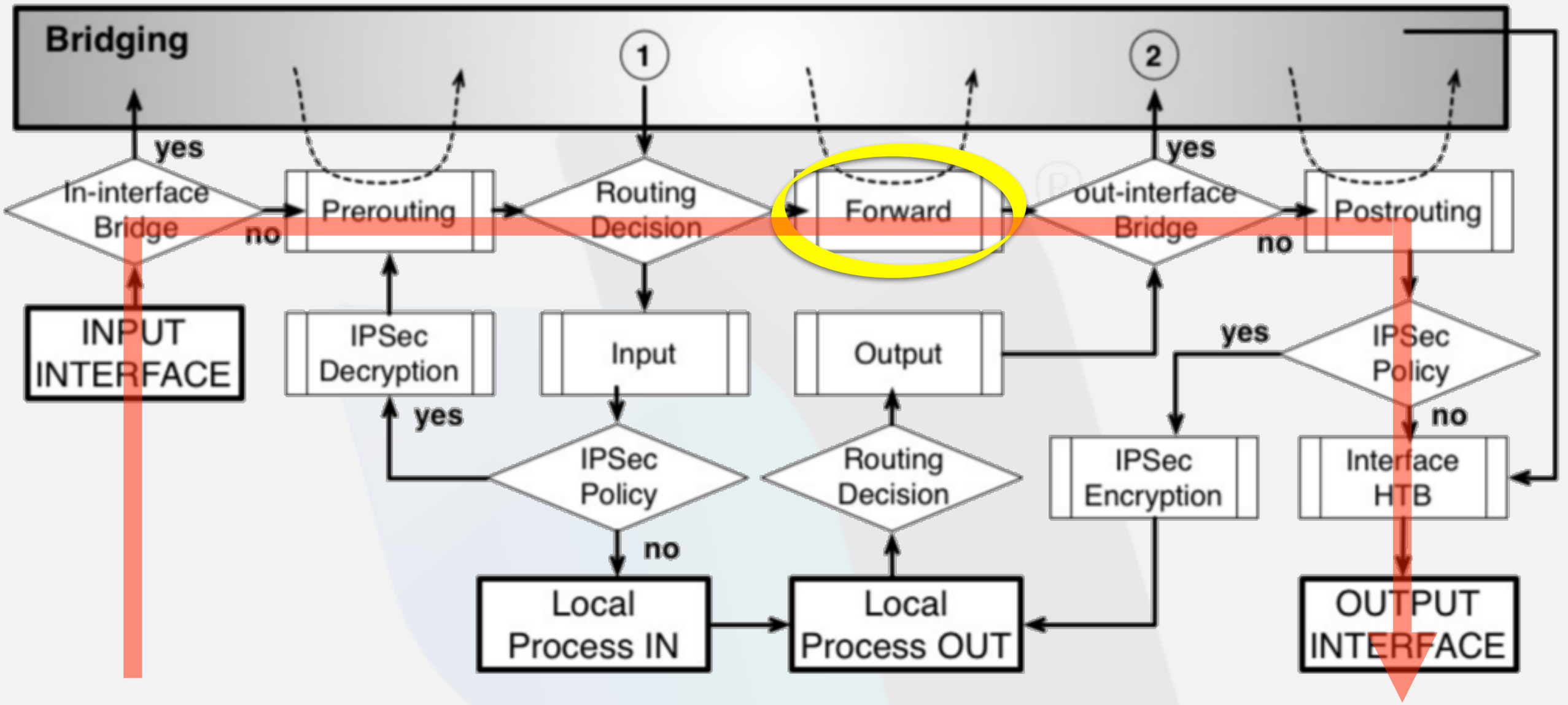
- **Que?** BCP38: Best Current Practice 38 > RFC2827
- **Cuando?** Mayo de 2000.
- **Porqué?** Eliminar los ataques DoS provocados por IP Spoofing y detectar el verdadero origen del ataque.
- **Cómo?** Bloqueando el tráfico que ingrese al router con *direcciones IP de origen diferentes a nuestras propias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

MUM Diagrama de Flujo en RouterOS



- Ataque dirigidos al router.
- */ip firewall filter add* ***chain=input…***

MUM Diagrama de Flujo en RouterOS

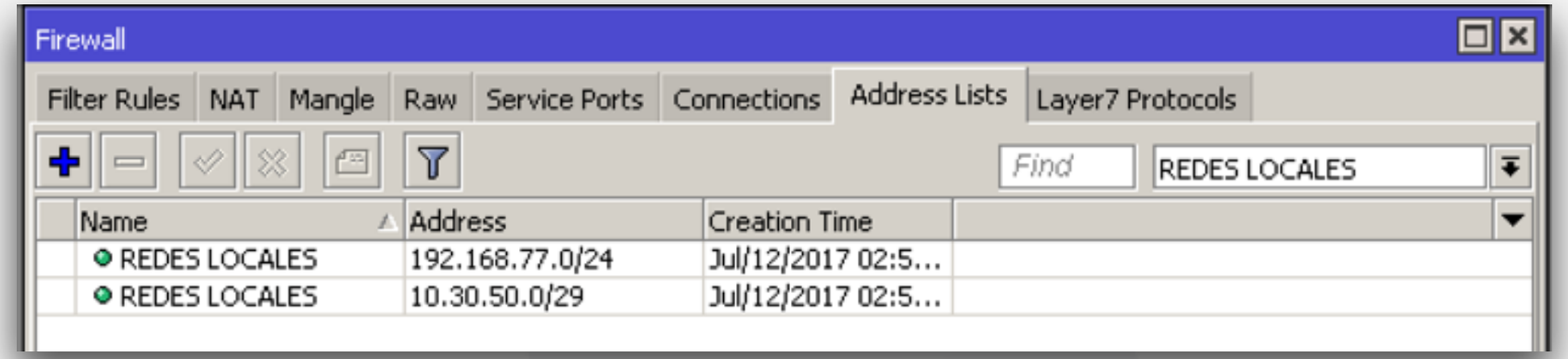


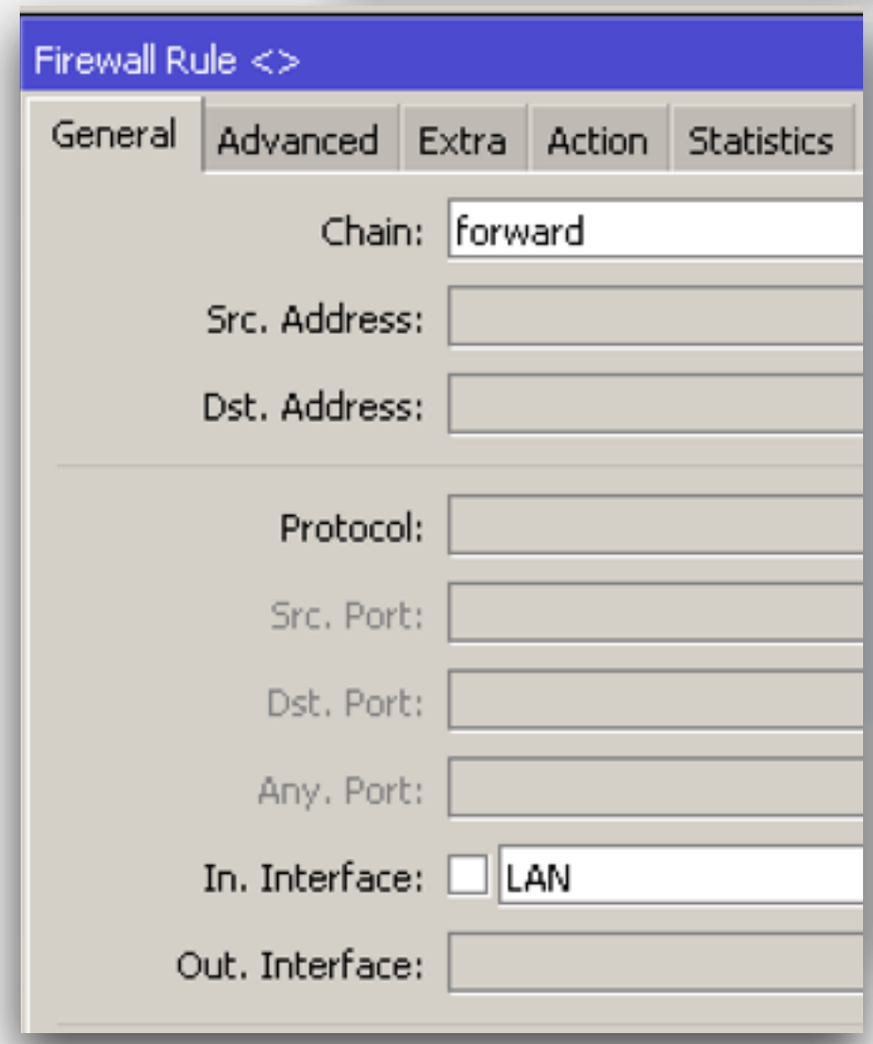
- Ataques que no son dirigidos al router.
- *Ip firewall filter add* ***chain=forward…***

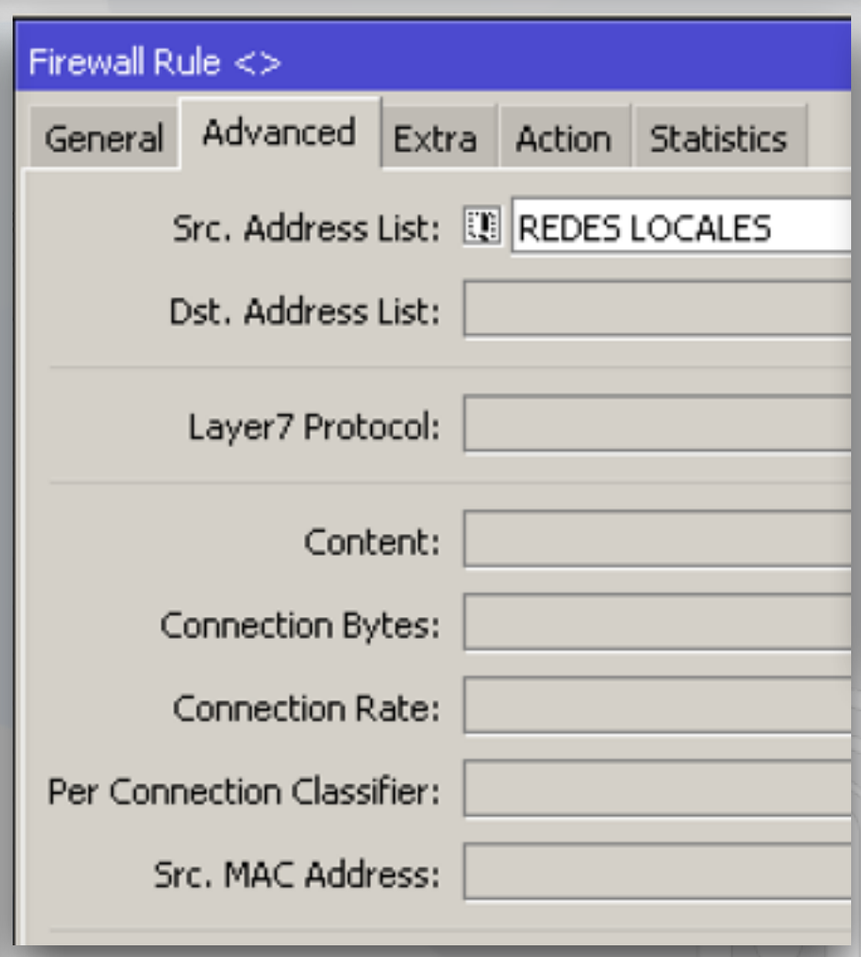
MUM

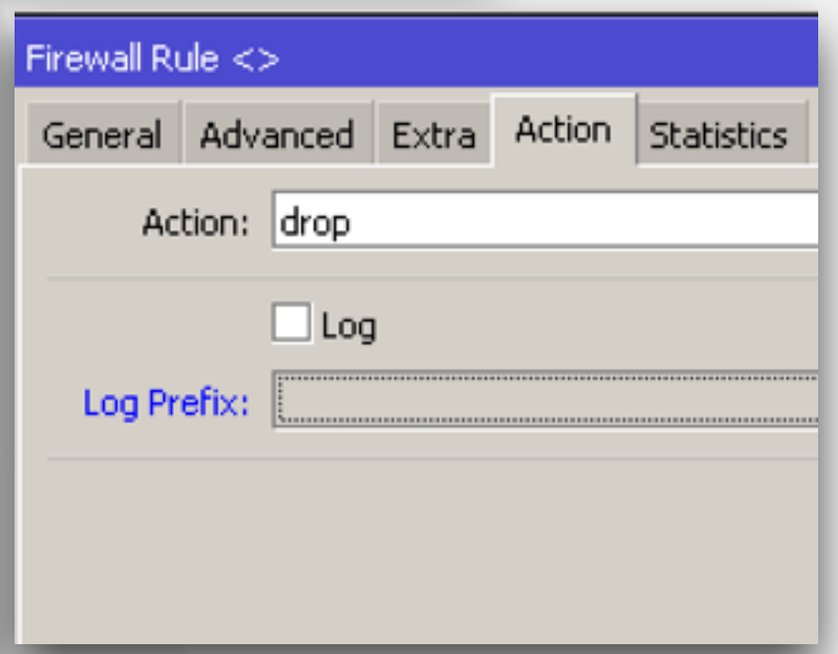
MKE solutions

Reglas de Firewall









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
```

DoS en acción sin BCP38

Session: 192.168.77.1 Uptime: 02:21:08 CPU: 100%

Torch (Running)

Basic
- Interface: LAN
- 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: 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

Eth. Pr...	Protocol	Src.	Dst.	VLAN Id	DSCP	Tx Rate	Rx Rate	Tx Pack...	Rx Pack...
800 (ip)	6 (tcp)	192.168.77.209:52817	192.168.77.1:8291 (winb...			127.3 k...	11.1 kbps	14	16
800 (ip)	6 (tcp)	192.168.77.209:52836	64.233.190.189:443 (htt...			1000 bps	528 bps	1	1
800 (ip)	6 (tcp)	3.223.162.77:1833	200.200.200.1:80 (http)			0 bps	432 bps	0	1
800 (ip)	6 (tcp)	2.211.77.33:1925	200.200.200.1:80 (http)			0 bps	432 bps	0	1
800 (ip)	6 (tcp)	4.9.70.207:1976	200.200.200.1:80 (http)			0 bps	432 bps	0	1
800 (ip)	6 (tcp)	3.53.25.223:2022	200.200.200.1:80 (http)			0 bps	432 bps	0	1
800 (ip)	6 (tcp)	3.251.102.150:2042	200.200.200.1:80 (http)			0 bps	432 bps	0	1
800 (ip)	6 (tcp)	4.25.36.115:2050	200.200.200.1:80 (http)			0 bps	432 bps	0	1
800 (ip)	6 (tcp)	2.178.211.238:2108	200.200.200.1:80 (http)			0 bps	432 bps	0	1
800 (ip)	6 (tcp)	2.133.100.79:2187	200.200.200.1:80 (http)			0 bps	432 bps	0	1
800 (ip)	6 (tcp)	2.90.233.152:2217	200.200.200.1:80 (http)			0 bps	432 bps	0	1
800 (ip)	6 (tcp)	2.20.213.173:2221	200.200.200.1:80 (http)			0 bps	432 bps	0	1
800 (ip)	6 (tcp)	3.218.95.117:2265	200.200.200.1:80 (http)			0 bps	432 bps	0	1
800 (ip)	6 (tcp)	3.255.252.167:2417	200.200.200.1:80 (http)			0 bps	432 bps	0	1
800 (ip)	6 (tcp)	4.28.4.205:2438	200.200.200.1:80 (http)			0 bps	432 bps	0	1
800 (ip)	6 (tcp)	3.33.28.145:2494	200.200.200.1:80 (http)			0 bps	432 bps	0	1
800 (ip)	6 (tcp)	4.48.252.183:2522	200.200.200.1:80 (http)			0 bps	432 bps	0	1
800 (ip)	6 (tcp)	4.28.49.205:2677	200.200.200.1:80 (http)			0 bps	432 bps	0	1
800 (ip)	6 (tcp)	2.167.114.104:2753	200.200.200.1:80 (http)			0 bps	432 bps	0	1
800 (ip)	6 (tcp)	4.17.176.232:2780	200.200.200.1:80 (http)			0 bps	432 bps	0	1
800 (ip)	6 (tcp)	2.99.240.208:2797	200.200.200.1:80 (http)			0 bps	432 bps	0	1
800 (ip)	6 (tcp)	3.139.233.130:2839	200.200.200.1:80 (http)			0 bps	432 bps	0	1
800 (ip)	6 (tcp)	4.59.193.44:2923	200.200.200.1:80 (http)			0 bps	432 bps	0	1
800 (ip)	6 (tcp)	3.2.233.118:2959	200.200.200.1:80 (http)			0 bps	432 bps	0	1
800 (ip)	6 (tcp)	3.244.151.76:3024	200.200.200.1:80 (http)			0 bps	432 bps	0	1
800 (ip)	6 (tcp)	2.15.130.244:3031 (eppc)	200.200.200.1:80 (http)			0 bps	432 bps	0	1

607 items | Total Tx: 318.7 kbps | Total Rx: 3.0 Mbps | Total Tx Packet: 37 | Total Rx Packet: 7 106

DoS en acción sin BCP38

Session: 192.168.77.1 — Uptime: 02:28:4 — CPU: 100%

Firewall

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

Tracking — Find

	Src. Address	Dst. Address	Prot...	Connecti...	Timeout	TCP State	Orig./Repl. Rate
SC	1.1.1.1	1.1.1.3	1 (ic...		00:00:00		0 bps/0 bps
Cs	1.18.43.89:19793	200.200.200.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps
Cs	1.23.79.95:19394	200.200.200.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps
Cs	1.43.117.108:19342	200.200.200.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps
Cs	1.51.79.90:12843	200.200.200.1:80	6 (tcp)		00:00:01	syn sent	0 bps/0 bps
Cs	1.57.185.192:19264	200.200.200.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps
Cs	1.66.171.147:27191	200.200.200.1:80	6 (tcp)		00:00:01	syn sent	0 bps/0 bps
Cs	1.73.170.172:5108	200.200.200.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps
Cs	1.79.76.23:31804	200.200.200.1:80	6 (tcp)		00:00:02	syn sent	0 bps/0 bps
Cs	1.79.197.40:46534	200.200.200.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps
Cs	1.109.105.116:36111	200.200.200.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps
Cs	1.114.232.18:3345	200.200.200.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps
Cs	1.123.18.179:3369	200.200.200.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps
Cs	1.152.3.79:2575	200.200.200.1:80	6 (tcp)		00:00:01	syn sent	0 bps/0 bps
Cs	1.154.73.159:46582	200.200.200.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps
Cs	1.154.180.110:3246	200.200.200.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps
Cs	1.167.115.253:3415	200.200.200.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps
Cs	1.168.254.183:19082	200.200.200.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps
Cs	1.177.60.236:30762	200.200.200.1:80	6 (tcp)		00:00:01	syn sent	0 bps/0 bps
Cs	1.177.90.211:19675	200.200.200.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps
Cs	1.177.179.183:4032	200.200.200.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps
Cs	1.180.89.23:41707	200.200.200.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps

3789 items out of 35308 (1 selected) | Max Entries: 218008

Start | Stop | Close | ew Window

DoS en acción con BCP38

Session: 192.168.77.1 Uptime: 02:35:59 CPU: 66%

Torch

Basic

Interface: LAN

Entry Timeout: 00:00:03 s

Collect

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

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

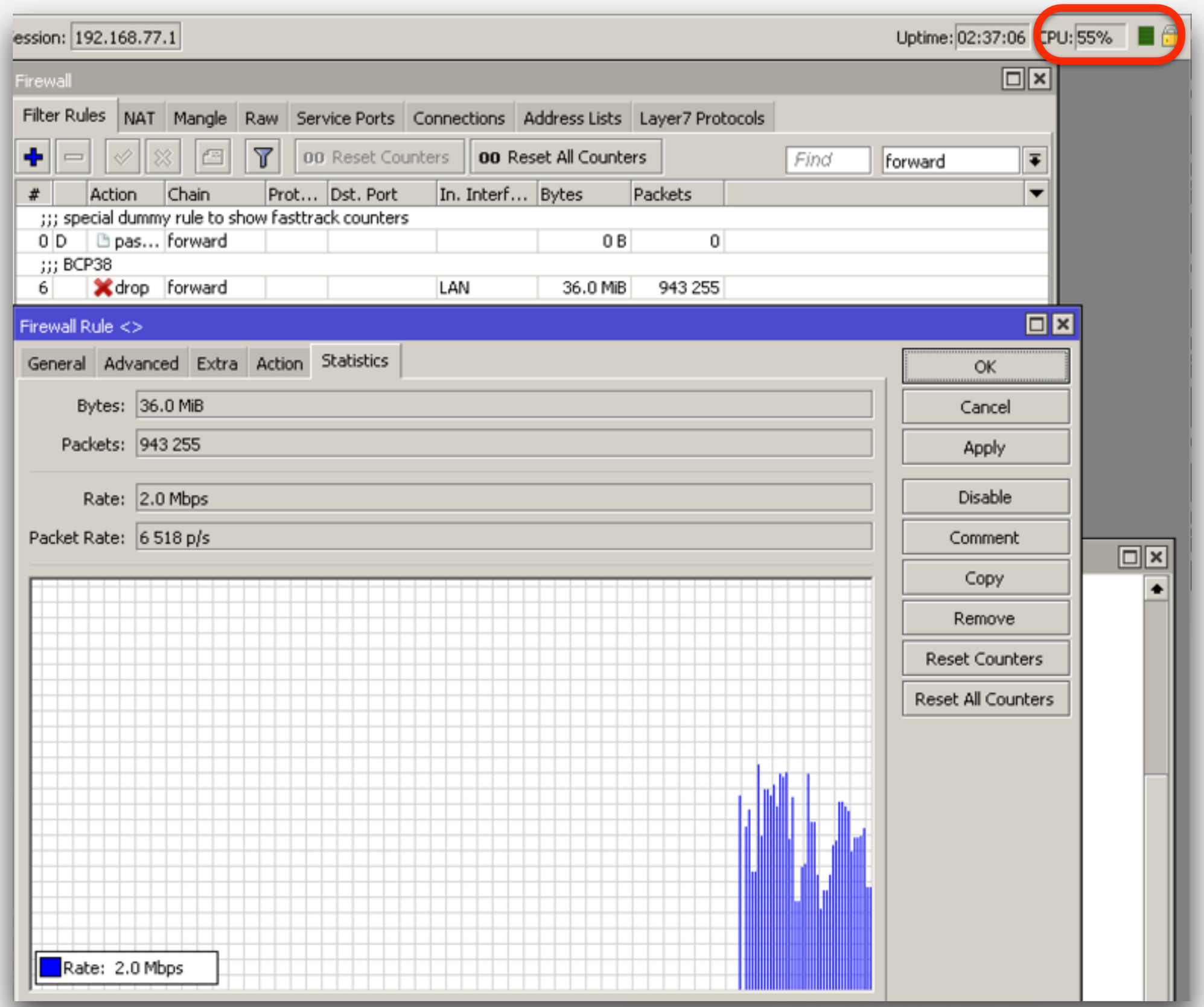
DSCP: any

Start | Stop | Close | New Window

Eth. Pr...	Protocol	Src.	Dst.	VLAN Id	DSCP	Tx Rate	Rx Rate	Tx Pack...	Rx Pack...
800 (ip)		14.190.192.90	200.200.200.1			0 bps	432 bps	0	1
800 (ip)		15.223.90.7	200.200.200.1			0 bps	432 bps	0	1
800 (ip)		13.254.172.25	200.200.200.1			0 bps	432 bps	0	1
800 (ip)		17.74.22.214	200.200.200.1			0 bps	432 bps	0	1
800 (ip)		17.46.84.165	200.200.200.1			0 bps	432 bps	0	1
800 (ip)		14.161.100.17	200.200.200.1			0 bps	432 bps	0	1
800 (ip)		13.91.103.213	200.200.200.1			0 bps	432 bps	0	1
800 (ip)		14.14.227.159	200.200.200.1			0 bps	432 bps	0	1
800 (ip)		14.115.18.69	200.200.200.1			0 bps	432 bps	0	1
800 (ip)		15.16.156.66	200.200.200.1			0 bps	432 bps	0	1
800 (ip)		14.74.140.250	200.200.200.1			0 bps	432 bps	0	1
800 (ip)		14.248.156.6	200.200.200.1			0 bps	432 bps	0	1
800 (ip)		14.106.133.162	200.200.200.1			0 bps	432 bps	0	1
800 (ip)		17.20.6.30	200.200.200.1			0 bps	432 bps	0	1
800 (ip)		17.100.194.248	200.200.200.1			0 bps	432 bps	0	1
800 (ip)		14.69.170.103	200.200.200.1			0 bps	432 bps	0	1
800 (ip)		15.167.179.128	200.200.200.1			0 bps	432 bps	0	1
800 (ip)		13.179.111.212	200.200.200.1			0 bps	432 bps	0	1
800 (ip)		15.17.29.248	200.200.200.1			0 bps	432 bps	0	1
800 (ip)		17.15.237.62	200.200.200.1			0 bps	432 bps	0	1
800 (ip)		15.216.62.7	200.200.200.1			0 bps	432 bps	0	1
800 (ip)		16.28.167.131	200.200.200.1			0 bps	432 bps	0	1
800 (ip)		14.115.16.237	200.200.200.1			0 bps	432 bps	0	1
800 (ip)		16.149.237.17	200.200.200.1			0 bps	432 bps	0	1
800 (ip)		17.104.146.3	200.200.200.1			0 bps	432 bps	0	1
800 (ip)		13.250.196.28	200.200.200.1			0 bps	432 bps	0	1

3600 items | Total Tx: 119.6 kbps | Total Rx: 3.4 Mbps | Total Tx Packet: 19 | Total Rx Packet: 7 932

DoS en acción con BCP38



MUM Resultados del ataque con BCP38

Session: 192.168.77.1 Uptime: 02:37:22 CPU: 55%

Firewall

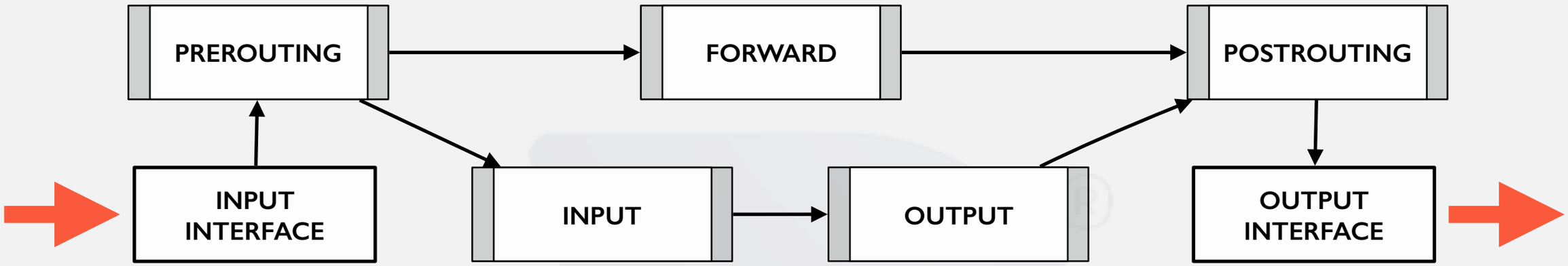
Filter Rules | NAT | Mangle | Raw | Service Ports | Connections | Address Lists | Layer7 Protocols

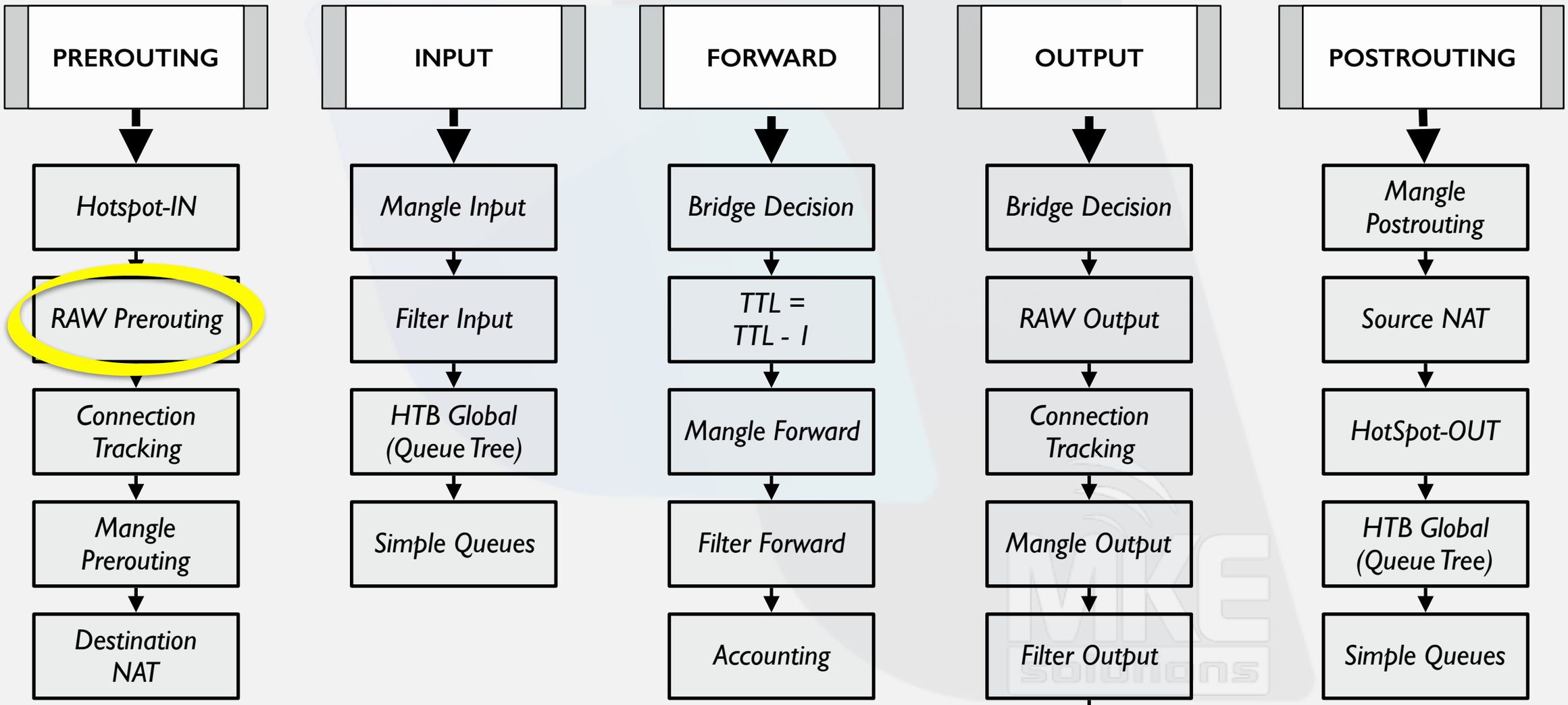
Tracking | Find

	Src. Address	Dst. Address	Prot...	Connecti...	Timeout	TCP State	Orig./Repl. Rate
SC	1.1.1.1	1.1.1.3	1 (ic...		00:00:03		0 bps/0 bps
C	10.30.50.1:44344	255.255.255.255:5...	17 (...		00:00:06		0 bps/0 bps
SACs	10.30.50.2:5060	190.11.152.82:3478	17 (...		00:02:09		0 bps/0 bps
SACs	10.30.50.2:5060	190.226.45.39:5060	17 (...		00:59:09		0 bps/0 bps
SC	186.137.27.104	8.8.8.8	1 (ic...		00:00:04		0 bps/0 bps
EC	186.137.27.104	186.137.26.132	47 (...		00:09:56		0 bps/0 bps
ESAC	186.137.27.104	186.137.26.132	47 (...		04:59:53		0 bps/0 bps
SAC	186.137.27.104:34989	186.137.26.132:1723	6 (tcp)		04:59:53	time wait	0 bps/0 bps
SAC	186.137.27.104:34990	186.137.26.132:1723	6 (tcp)		23:59:44	established	0 bps/0 bps
C	192.168.77.1:47363	255.255.255.255:5...	17 (...		00:00:06		0 bps/0 bps
SACs	192.168.77.200:41710	74.125.204.188:5228	6 (tcp)		23:44:51	established	0 bps/0 bps
SACs	192.168.77.200:42419	64.233.190.188:5228	6 (tcp)		22:18:28	established	0 bps/0 bps
SACs	192.168.77.200:42427	64.233.190.188:5228	6 (tcp)		22:18:48	established	0 bps/0 bps
SACs	192.168.77.200:42429	64.233.190.188:5228	6 (tcp)		22:28:36	established	0 bps/0 bps
SACs	192.168.77.200:44291	169.47.5.236:5222	6 (tcp)		23:58:53	established	0 bps/0 bps
SACs	192.168.77.200:46811	64.233.186.188:5228	6 (tcp)		22:18:15	established	0 bps/0 bps
SACs	192.168.77.200:46918	64.233.186.188:5228	6 (tcp)		23:33:11	established	0 bps/0 bps
SACs	192.168.77.200:47101	64.233.186.188:5228	6 (tcp)		23:38:02	established	0 bps/0 bps
SACs	192.168.77.201:54069	17.188.164.87:5223	6 (tcp)		23:54:10	established	0 bps/0 bps
C	192.168.77.209:17500	192.168.77.255:17...	17 (...		00:00:08		0 bps/0 bps
C	192.168.77.209:17500	255.255.255.255:1...	17 (...		00:00:08		0 bps/0 bps
SACs	192.168.77.209:51745	169.55.74.36:443	6 (tcp)		23:59:49	established	0 bps/0 bps

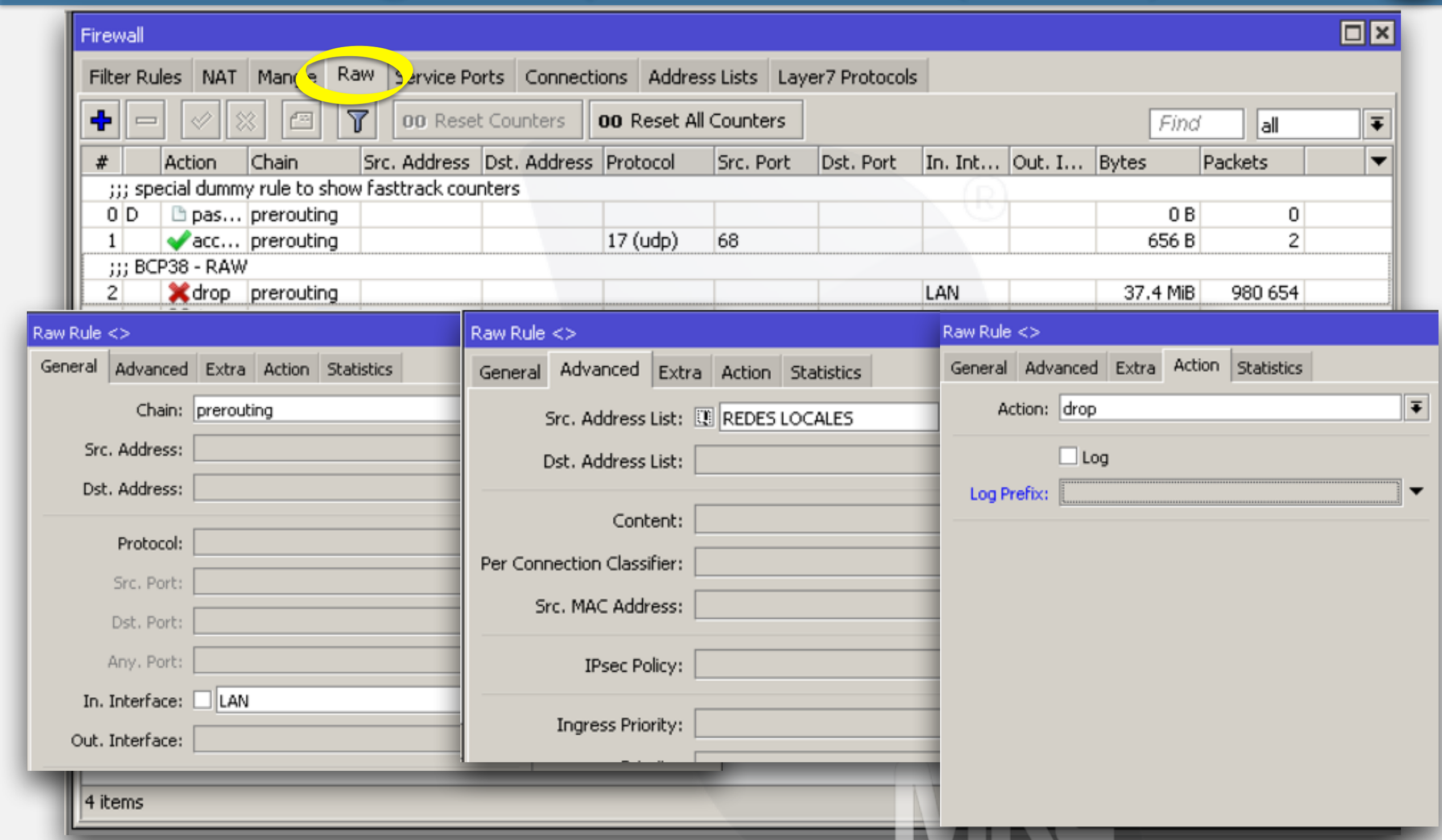
48 items | Max Entries: 218008

RAW en RouterOS v6





Reglas Optimizadas (RAW)



- Regla simplificada!!!

Resultados Finales (RAW)

Session: 192.168.77.1 — Uptime: 03:02:18 — CPU: 27%

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
;;; special dummy rule to show fasttrack counters												
0	D	pas...	prerouting								0 B	0
1		acc...	prerouting			17 (udp)	68				656 B	2
;;; BCP38 - RAW												
2		drop	prerouting						LAN		22.5 MiB	589 218
3	X	drop	prerouting						ether5		0 B	0

Raw Rule <>

General | Advanced | Extra | Action | Statistics

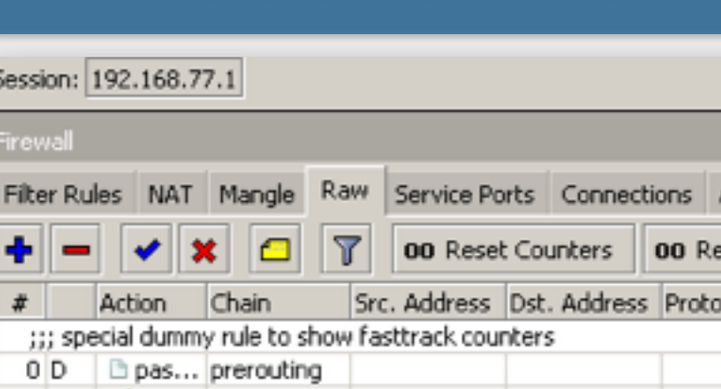
OK

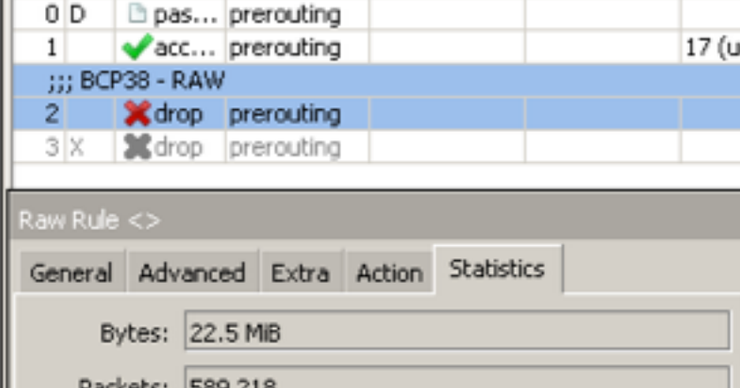
Bytes: 22.5 MiB

Packets: 589 218

Rate: 3.6 Mbps

Packet Rate: 11 424 p/s





enabled

Profile (Running)

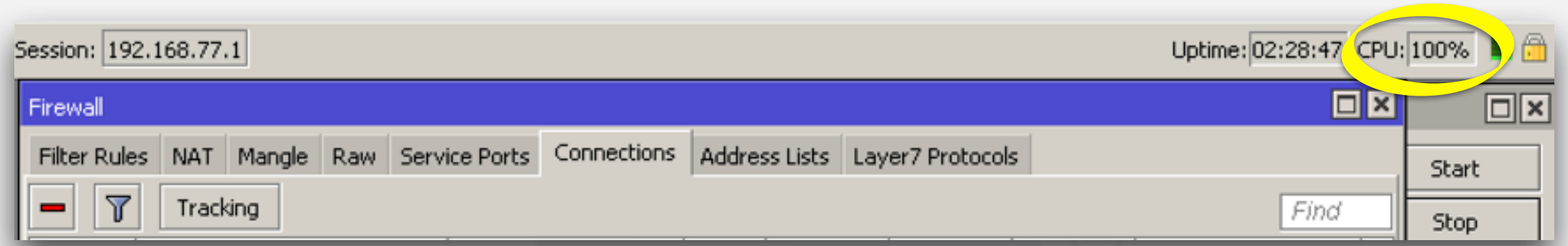
CPU: all

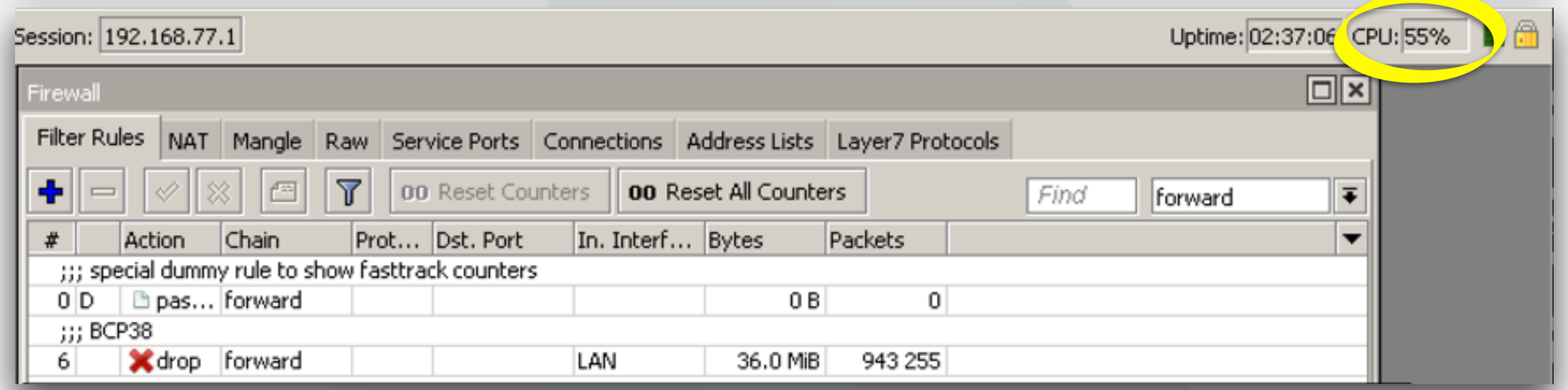
Start | Stop | Close | New Window

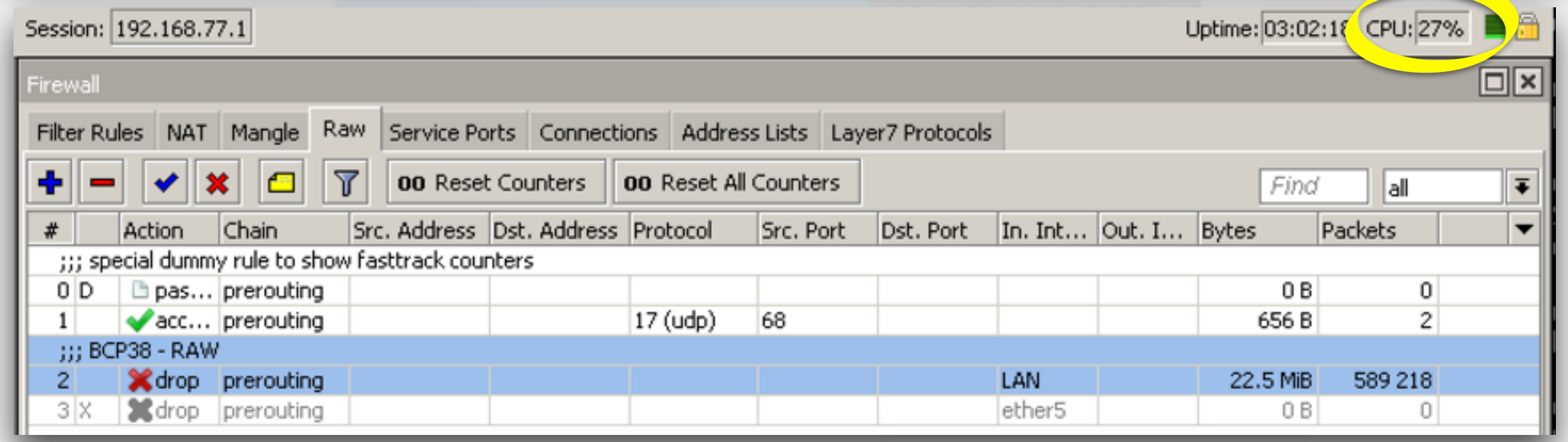
Name	CPU	Usage
cpu0		26.0
wireless	0	15.0
unclassified	0	5.0
firewall	0	3.0
management	0	1.5
bridging	0	1.0
networking	0	0.5
profiling	0	0.0
queuing	0	0.0
winbox	0	0.0

10 items

Comparación Final







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 este ataque.***

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