



# IP Spoofing & BCP38

---

Ing. Mario Clep  
MKE Solutions



16 - 17 de Abril de 2018

Ciudad de México





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



@ - [marioclep@mkesolutions.net](mailto:marioclep@mkesolutions.net)

S - marioclep

t - @marioclep



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




 [info@mkesolutions.net](mailto:info@mkesolutions.net)

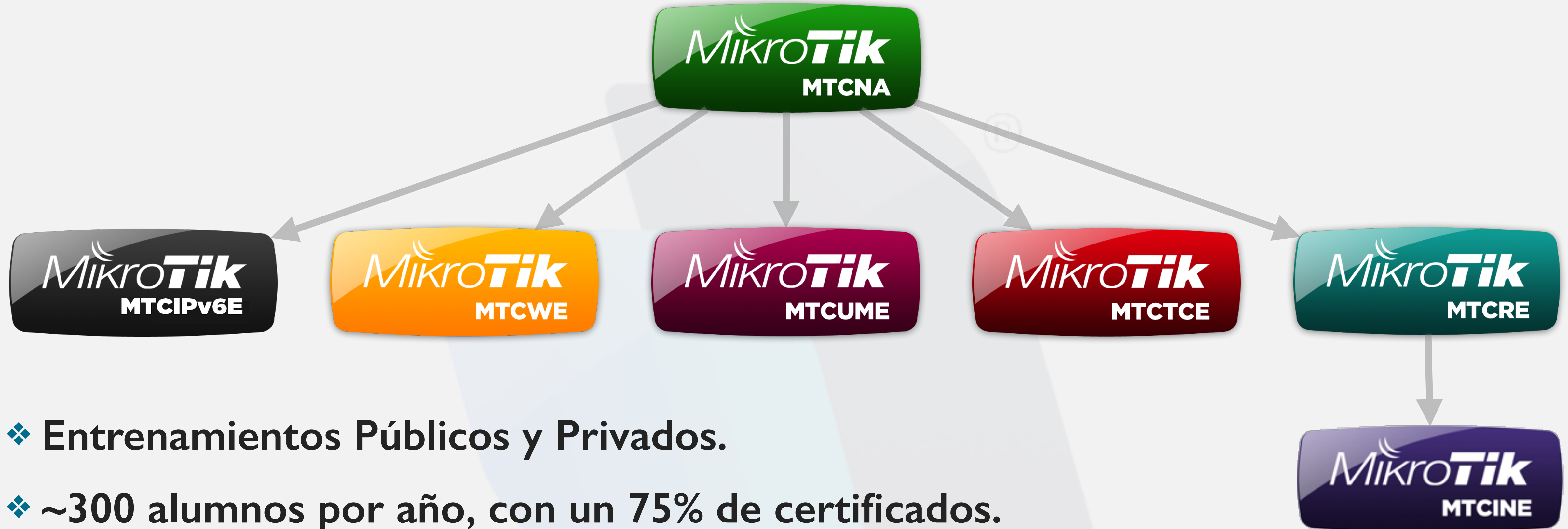
 [/mkesolutions](https://www.facebook.com/mkesolutions)

 [www.MKESolutions.net](http://www.MKESolutions.net)

 [@mkesolutions](https://twitter.com/mkesolutions)

 [/mkesolutions](https://www.youtube.com/mkesolutions)

 +54 9 358 4210029

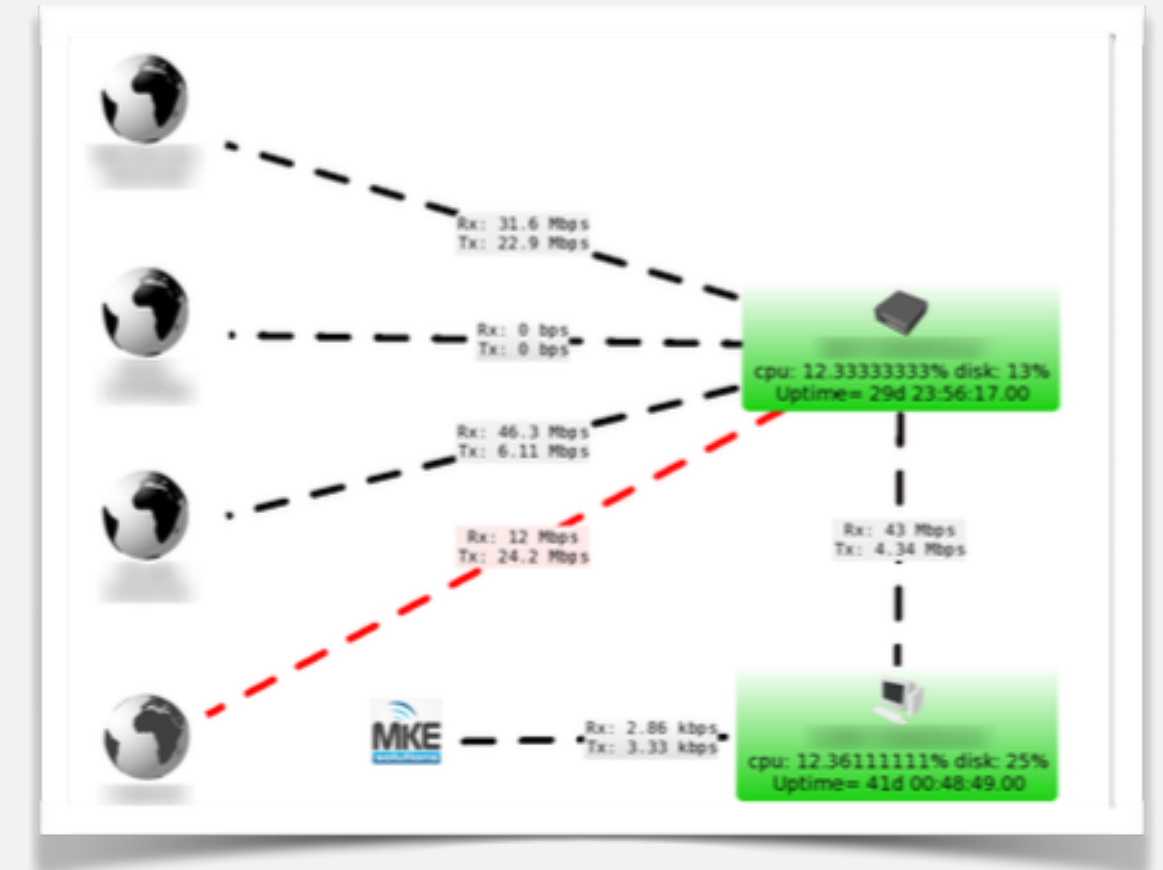


**Academia**  
DE ENTRENAMIENTOS

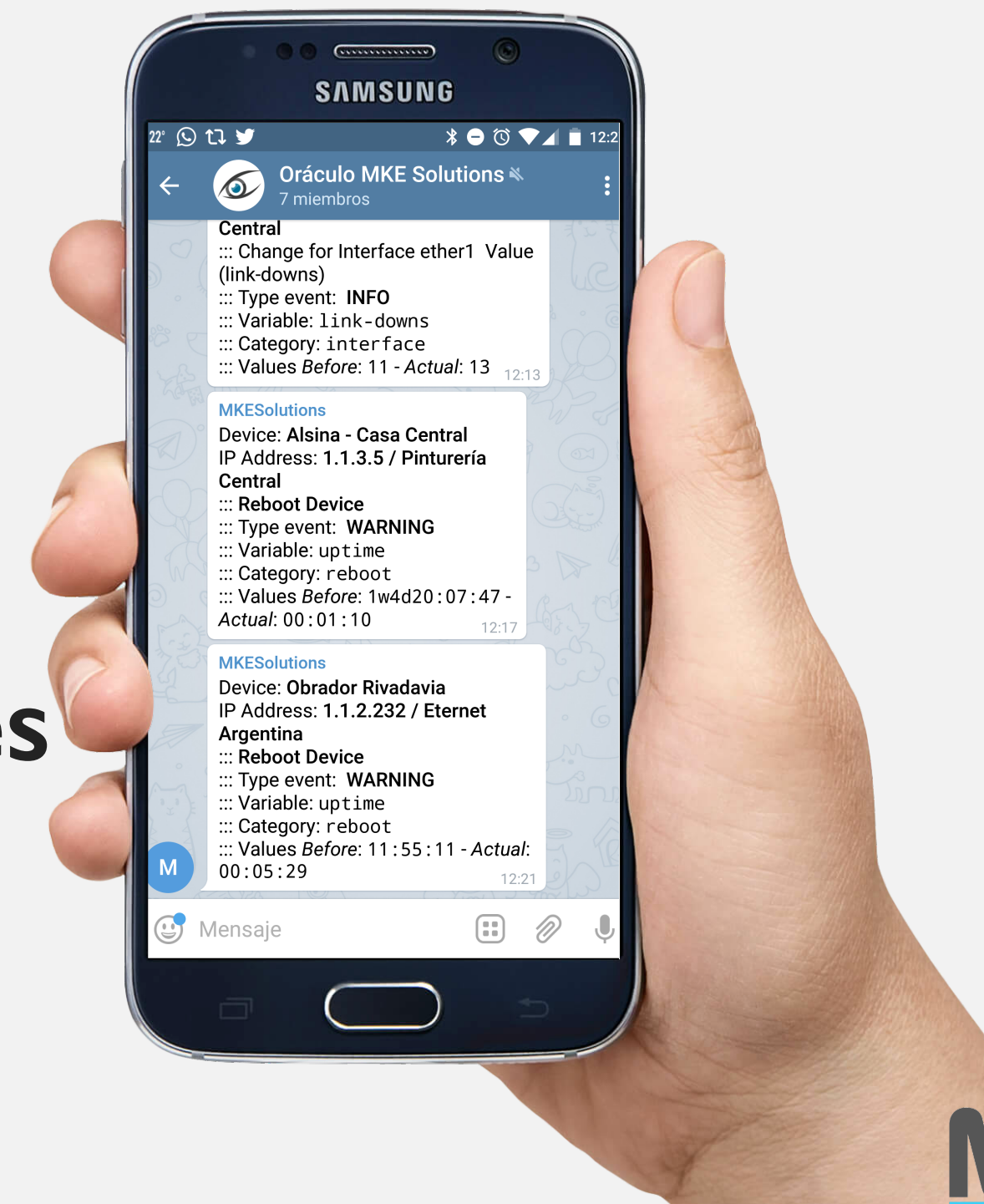
powered by MKE Solutions



- ❖ Diseño, desarrollo e implementación de soluciones.
- ❖ Incidencias puntuales.
- ❖ Soporte mensual (OutSourcing).



- ❖ Revisión y Optimización
- ❖ Asesoramiento
- ❖ Actualización
- ❖ Soporte Prioritario
- ❖ Mantenimiento preventivo
- ❖ Guardia 24x7
- ❖ Monitoreo
- ❖ Implementaciones Adicionales





**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**

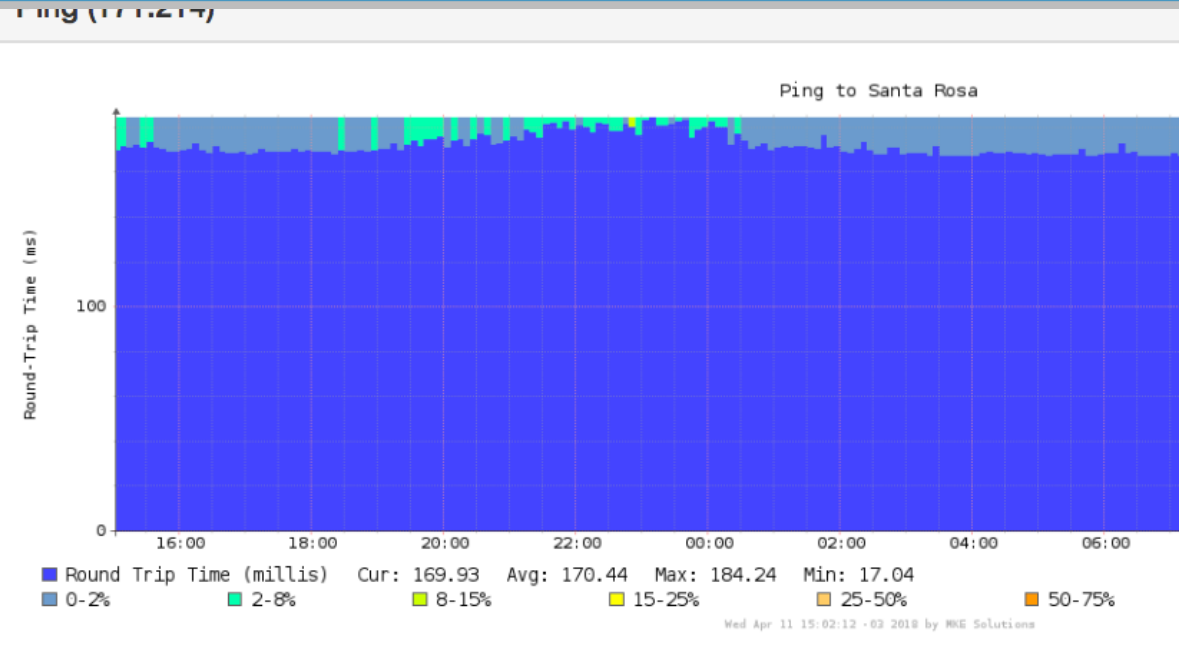
## 1450

👁 Monitoring Devices 1

**DISK USAGE**

## 54%

📁 Files Backups 21537 | 
 💾 Disk Backups 27G



**Oraculo Server Status**

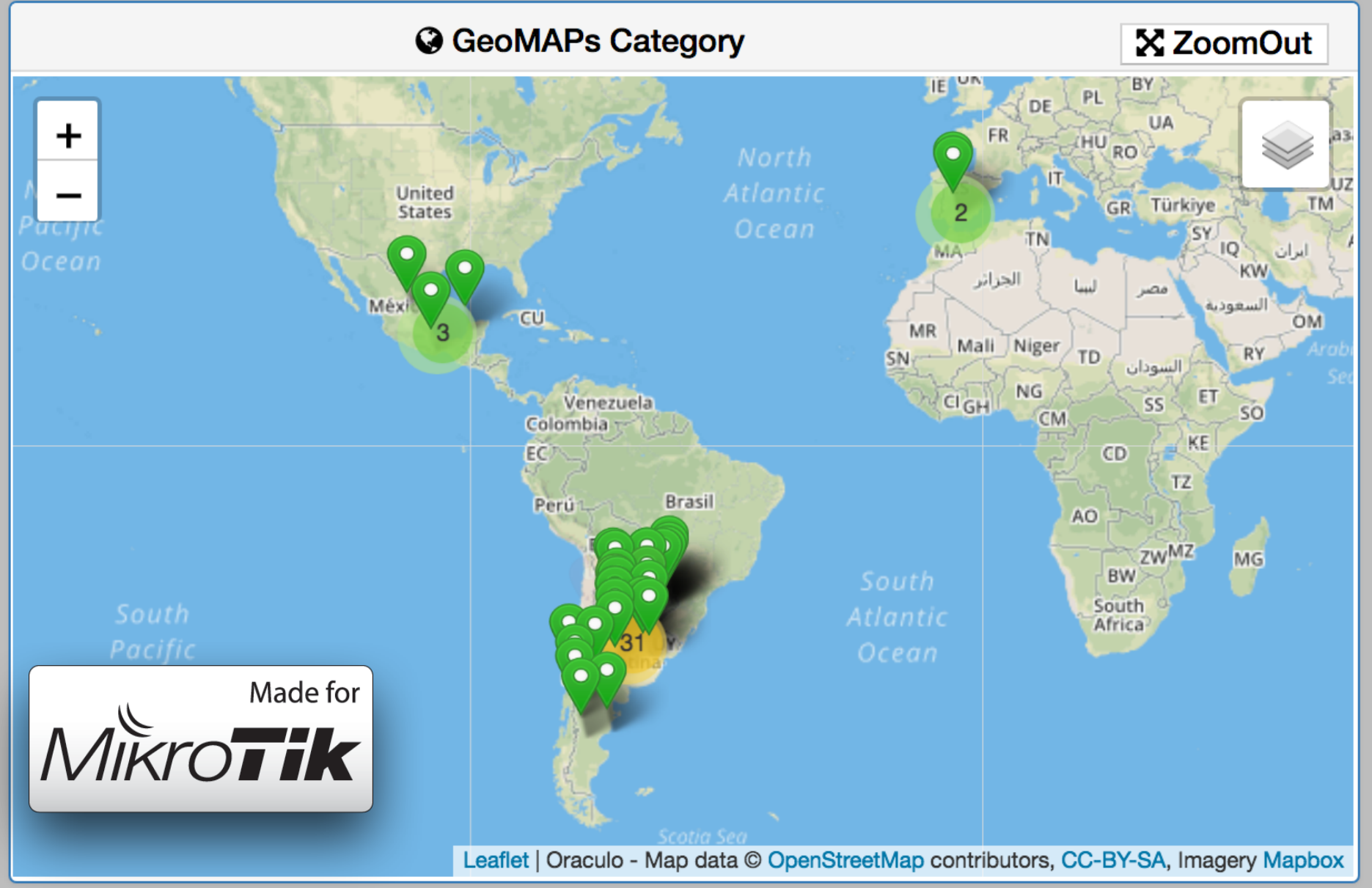
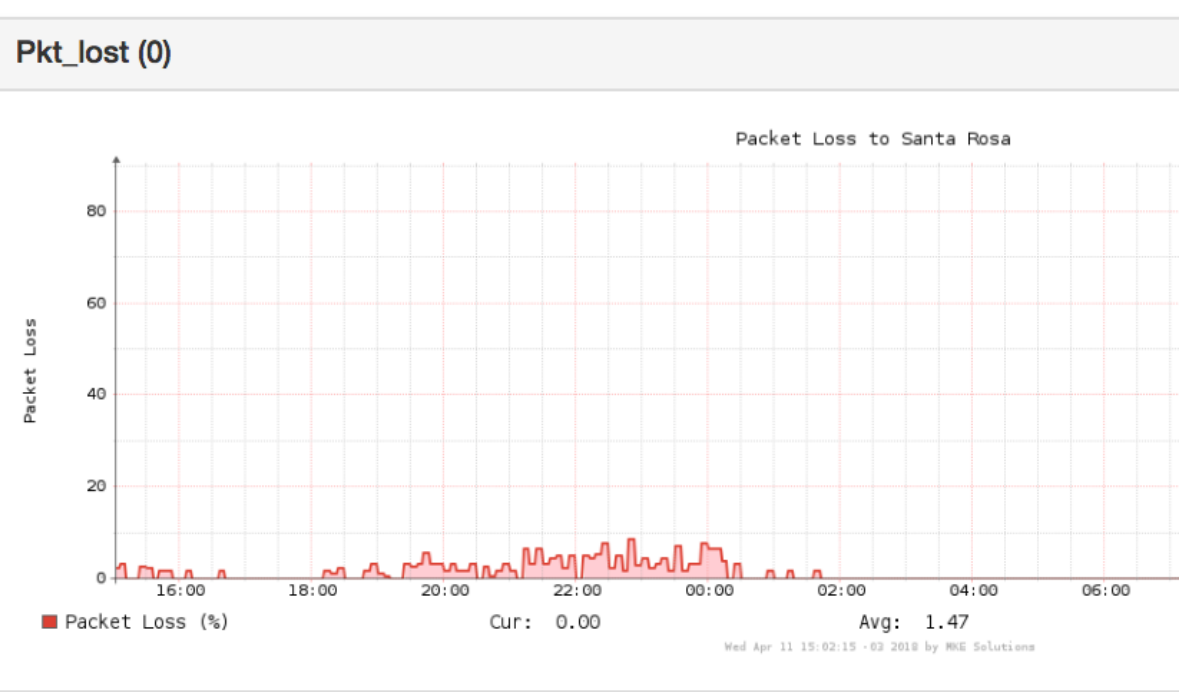
Date	Uptime	License	Status	Bot Telegram	WebService
2018-04-11 14:30:28	14:30:28	OUTSOURCING	VALID_LICENSE	OK	OK

# 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%

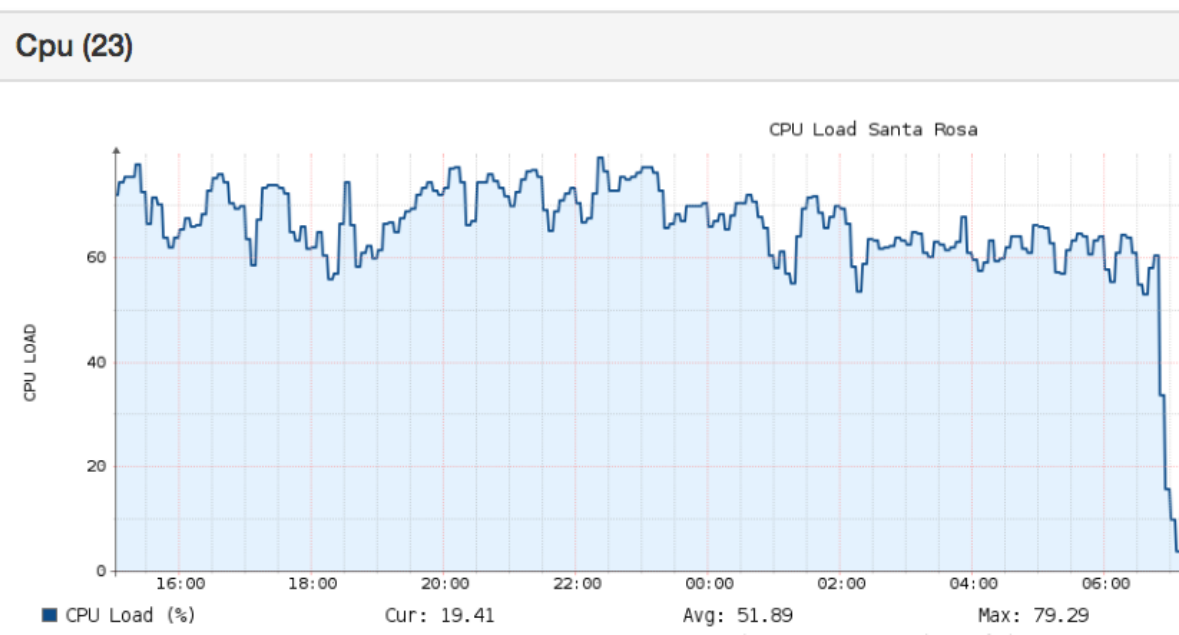
**Overview (1 Hour)**

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



**Last Devices Timeout**

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



**Last Events**

When	Device	Event	Variable	Before	Actual
⚠ 8 min	██████████	bgp	Change value for peer Cache de Facebook BGP	connect	active
⚠ 13 min	██████████	bgp	Change value for peer Cache de Facebook BGP	active	connect
⚠ 18 min	██████████	bgp	Change value for peer Cache de Facebook BGP	connect	active
⚠ 23 min	██████████	bgp	Change value for peer	active	connect







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.**





Torch (Running)

Basic

Interface: ether3

Entry Timeout: 00:00:03 s

Filters

Src. Address: 0.0.0.0/0

Dst. Address:

Collect

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	192.168.178.178:27610			0 bps	744 bps	0	1
800 (ip)	17 (udp)	32.19.202.196:39908	192.168.178.178:27147			0 bps	744 bps	0	1
800 (ip)	17 (udp)	32.37.142.48:61061	192.168.178.178:27201			0 bps	744 bps	0	1
800 (ip)	17 (udp)	31.83.117.100:17881	192.168.178.178:27041			0 bps	664 bps	0	1
800 (ip)	17 (udp)	31.56.178.81:27634	192.168.178.178:27767			0 bps	656 bps	0	1
800 (ip)	17 (udp)	31.102.163.139:44750	192.168.178.178:27558			0 bps	656 bps	0	1
800 (ip)	17 (udp)	31.193.74.77:10115	192.168.178.178:27868			0 bps	624 bps	0	1
800 (ip)	17 (udp)	31.196.149.127:19084	192.168.178.178:27912			0 bps	624 bps	0	1
800 (ip)	17 (udp)	31.200.180.117:52663	192.168.178.178:27638			0 bps	624 bps	0	1
800 (ip)	17 (udp)	30.211.242.93:50994	192.168.178.178:27398			0 bps	616 bps	0	1
800 (ip)	17 (udp)	31.6.180.183:50773	192.168.178.178:27126			0 bps	616 bps	0	1
800 (ip)	17 (udp)	31.73.198.161:17520	192.168.178.178:27649			0 bps	616 bps	0	1
800 (ip)	17 (udp)	31.92.41.152:18751	192.168.178.178:27107			0 bps	600 bps	0	1
800 (ip)	17 (udp)	31.103.203.105:38230	192.168.178.178:27232			0 bps	600 bps	0	1
800 (ip)	17 (udp)	31.164.165.10:28313	192.168.178.178:27204			0 bps	600 bps	0	1
800 (ip)	17 (udp)	31.175.155.111:11108	192.168.178.178:27476			0 bps	600 bps	0	1
800 (ip)	17 (udp)	32.18.148.207:55999	192.168.178.178:27964			0 bps	600 bps	0	1
800 (ip)	17 (udp)	30.204.198.217:27609	192.168.178.178:27628			0 bps	592 bps	0	1
800 (ip)	17 (udp)	31.11.133.75:39861	192.168.178.178:27848			0 bps	592 bps	0	1
800 (ip)	17 (udp)	31.33.125.24:46028	192.168.178.178:27493			0 bps	592 bps	0	1
800 (ip)	17 (udp)	31.77.218.138:16417	192.168.178.178:27743			0 bps	592 bps	0	1
800 (ip)	17 (udp)	31.88.132.122:50210	192.168.178.178:27391			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



Torch (Running)

Basic

Interface: ether3

Entry Timeout: 00:00:03 s

Filters

Src. Address: 0.0.0.0/0

Dst. Address: [redacted]

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

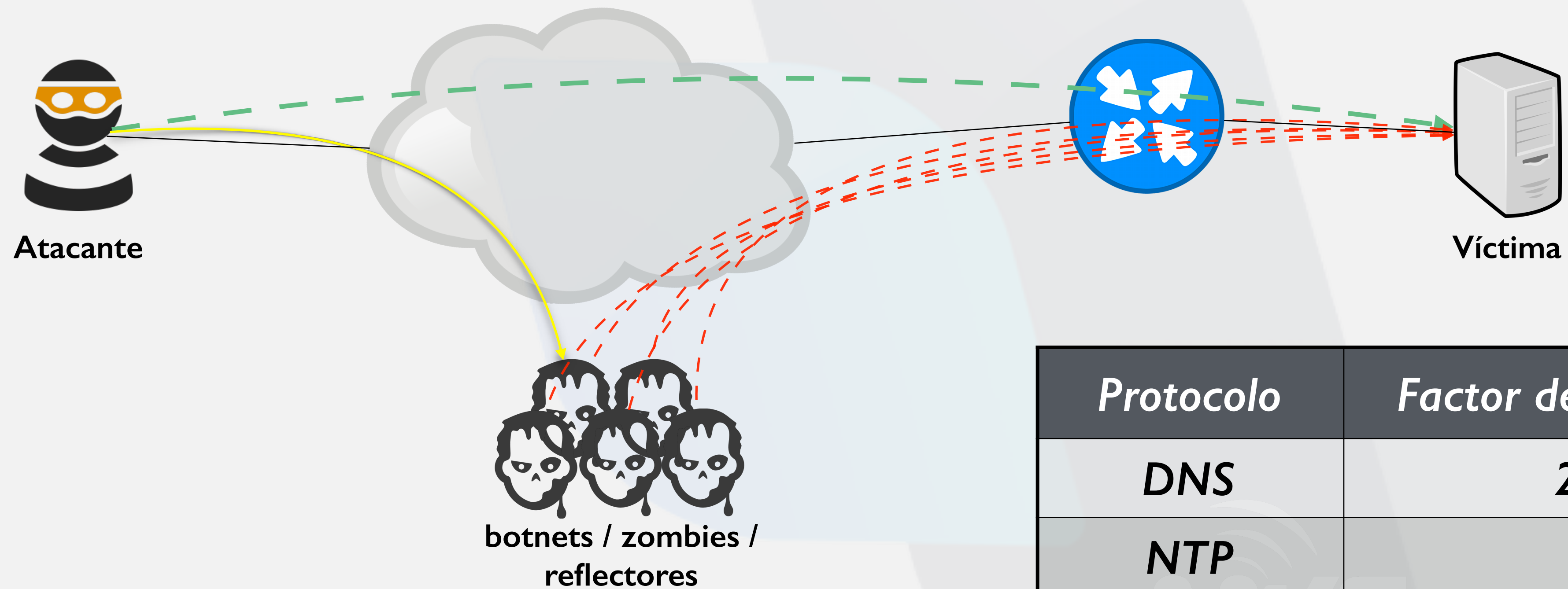
900 items    Total Tx: 0 bps    Total Rx: 13.9 Mbps    Total Tx Packet: 0    Total Rx Packet: 26 843



- ❖ 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.

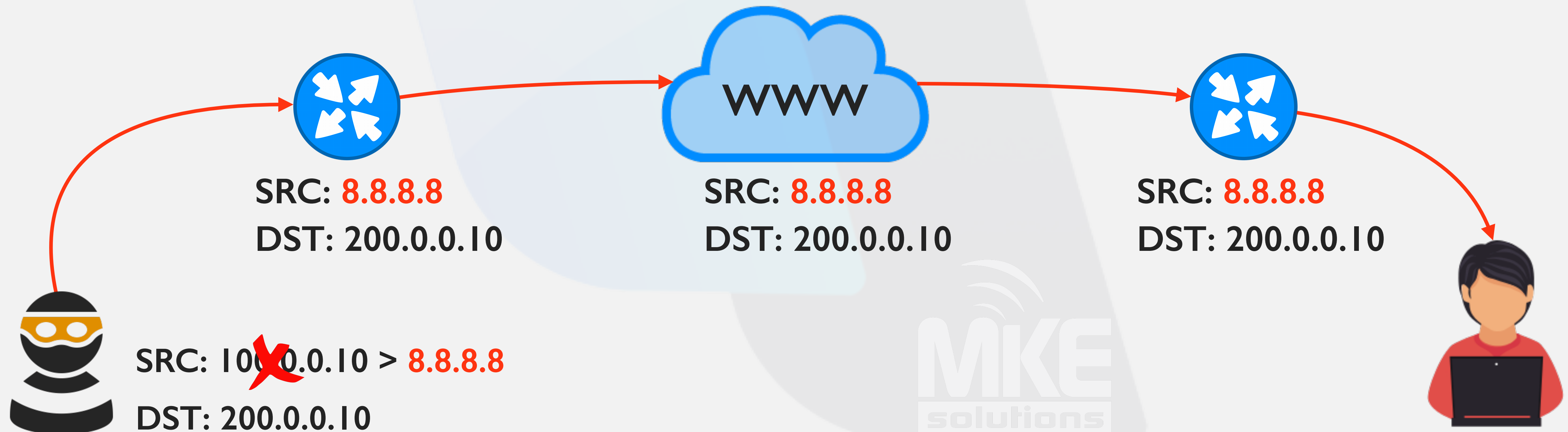


❖ Los ataques de denegación de servicio tienen como principal objetivo atacar el vínculo más débil para provocar una caída del servicio: capacidad contratada, capacidad de procesamiento, enlaces troncales, distribuciones, AB del cliente, etc.

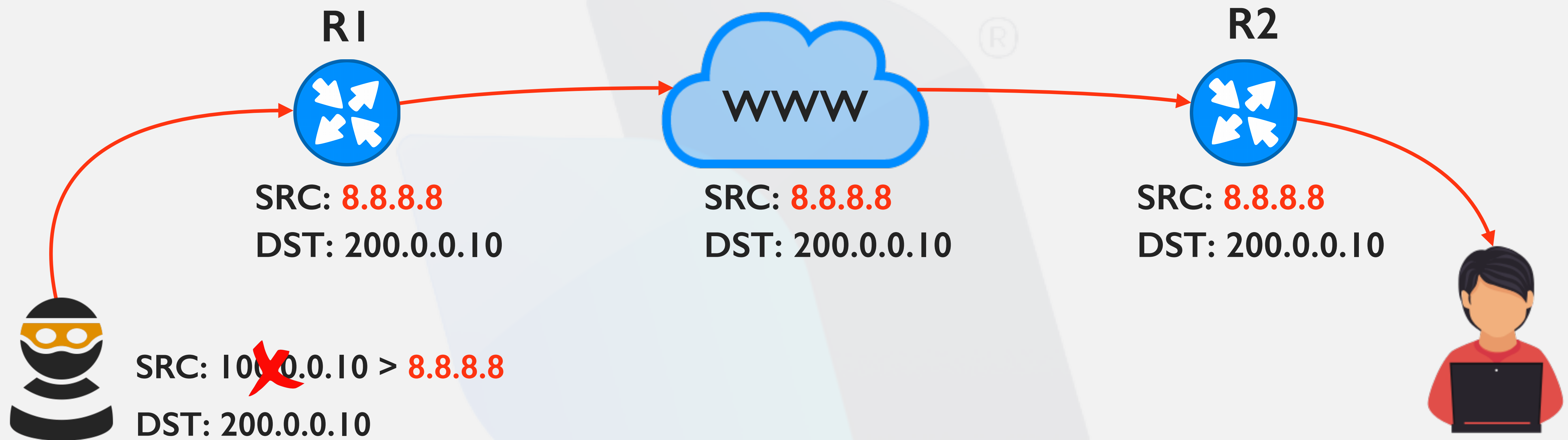


<i>Protocolo</i>	<i>Factor de Amplificación</i>
<b>DNS</b>	<b>28 - 54</b>
<b>NTP</b>	<b>557</b>
<b>SNMPv2</b>	<b>6.3</b>
<b>NetBIOS</b>	<b>3.8</b>
<b>CharGEN</b>	<b>358</b>

- ❖ 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.



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

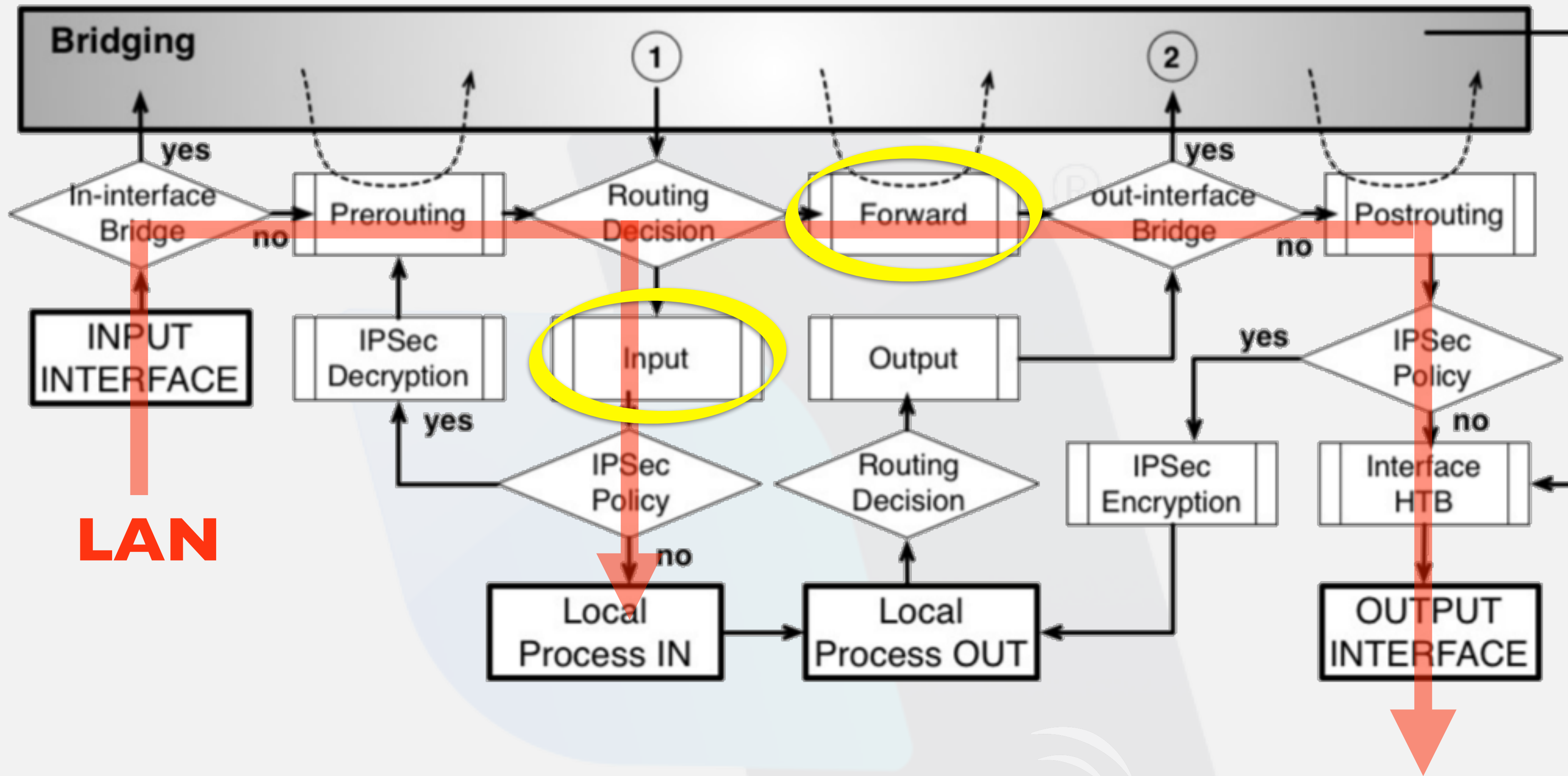


- ❖ R2 no tiene manera de reconocer si el nuevo origen 8.8.8.8 es verdadero o falso.
- ❖ Implementar BCP38 ó uRPF.



- ❖ 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.





❖ *ip firewall filter add chain=forward / chain=input...*







Firewall			
Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols			
+ - ✓ ✗ 📄 🔍		Find	REDES LOCALES
Name	Address	Creation Time	
● REDES LOCALES	192.168.77.0/24	Jul/12/2017 02:5...	
● REDES LOCALES	10.30.50.0/29	Jul/12/2017 02:5...	

Firewall Rule <>

General Advanced Extra Action Statistics

Chain: forward

Src. Address:

Dst. Address:

---

Protocol:

Src. Port:

Dst. Port:

Any. Port:

In. Interface:  LAN

Out. Interface:

Firewall Rule <>

General Advanced Extra Action Statistics

Src. Address List: REDES LOCALES

Dst. Address List:

Layer7 Protocol:

Content:

Connection Bytes:

Connection Rate:

Per Connection Classifier:

Src. MAC Address:

Firewall Rule <>

General Advanced Extra Action Statistics

Action: drop

Log

Log Prefix:



```
/ 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
```





Torch (Running)

Basic: Interface: ether3, Entry Timeout: 00:00:03 s

Filters: Src. Address: 0.0.0.0/0, Dst. Address: 0.0.0.0/0

Start, Stop, Close

Eth. ...	Protocol	Src.	Dst.	Tx Rate	Rx Rate	Tx Packet Rate	Rx Packet Rate
800 (ip)	17 (udp)	4.18.244.69:43735	200.200.200.1:41589	0 bps	0 bps	0	0
800 (ip)	17 (udp)	2.27.45.121:43736	200.200.200.1:41590	0 bps	0 bps	0	0
800 (ip)	17 (udp)	6.238.169.63:43741	200.200.200.1:41595	0 bps	480 bps	0	1
800 (ip)	17 (udp)	0.250.191.202:43744	200.200.200.1:41598	0 bps	0 bps	0	0
800 (ip)	17 (udp)	6.152.157.161:44325	200.200.200.1:42179	0 bps	480 bps	0	1
800 (ip)	17 (udp)	0.137.228.188:44345	200.200.200.1:42199	0 bps	0 bps	0	0
800 (ip)	17 (udp)	0.147.29.231:44398	200.200.200.1:42252	0 bps	0 bps	0	0
800 (ip)	17 (udp)	8.129.151.151:44402	200.200.200.1:42256	0 bps	480 bps	0	1
800 (ip)	17 (udp)	6.0.6.137:44409	200.200.200.1:42263	0 bps	0 bps	0	0
800 (ip)	17 (udp)	3.60.171.66:44423	200.200.200.1:42277	0 bps	0 bps	0	0
800 (ip)	17 (udp)	6.103.110.152:45409	200.200.200.1:43263	0 bps	0 bps	0	0
800 (ip)	17 (udp)	2.169.120.162:45422	200.200.200.1:43276	0 bps	0 bps	0	0
800 (ip)	17 (udp)	11.129.24.120:45431	200.200.200.1:43285	0 bps	480 bps	0	1
800 (ip)	17 (udp)	4.102.212.8:45444	200.200.200.1:43298	0 bps	0 bps	0	0
800 (ip)	17 (udp)	4.200.190.89:45448	200.200.200.1:43302	0 bps	0 bps	0	0

500 items | Total Tx: 0 bps | Total Rx: 4.3 Mbps | Total Tx Packet: 0 | Total Rx Packet: 9 032



Session: E4:8D:8C:52:FF:06 CPU: 100%

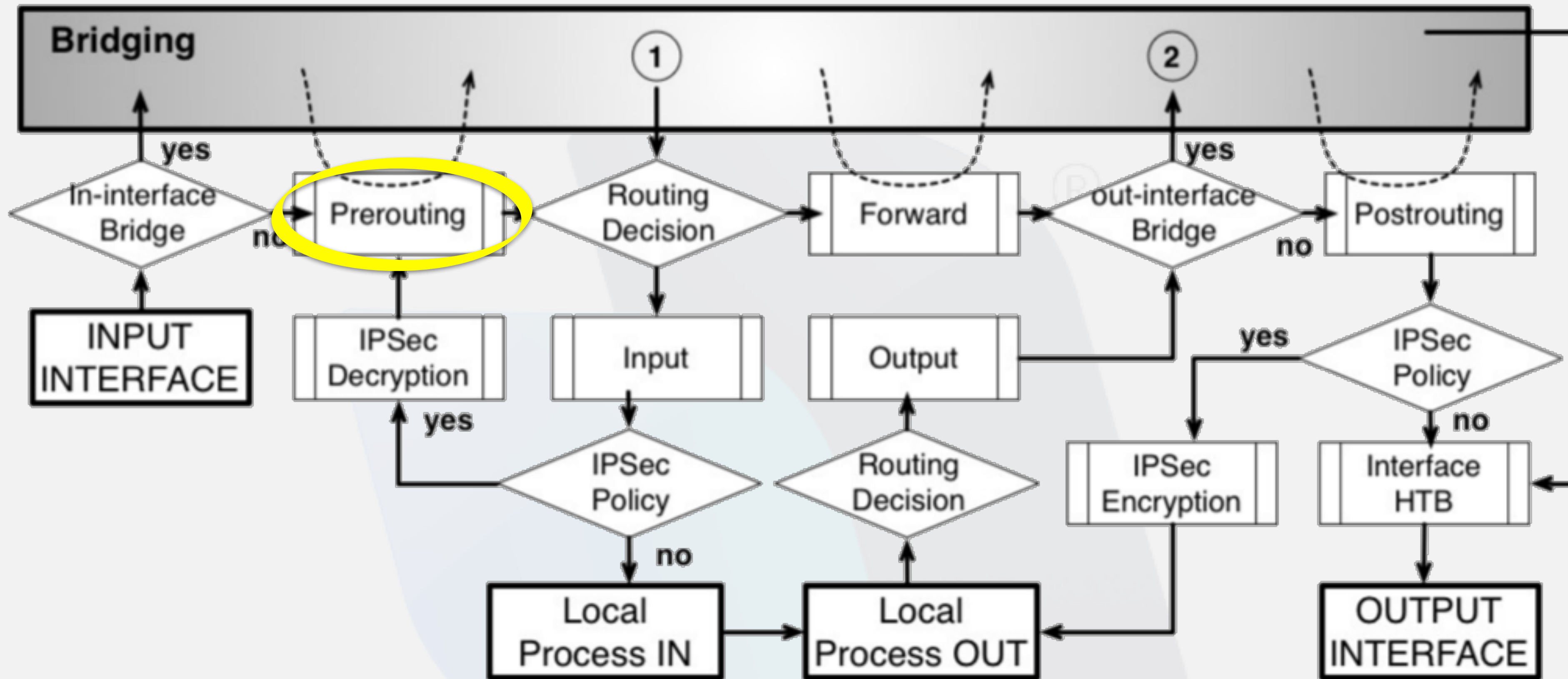
Firewall

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

Tracking Find

	Src. Address	△ Dst. Address	Protocol	Timeout	TCP State	Orig./Repl. Rate	Orig./Repl. Bytes	
C	0.0.0.0:68	255.255.255.255:67	17 (udp)	00:00:00		0 bps/0 bps	328 B/0 B	▼
Cs	2.16.251.194:12794	200.200.200.1:10207	17 (udp)	00:00:07		0 bps/0 bps	28 B/0 B	▲
Cs	2.34.214.65:7090	200.200.200.1:4503	17 (udp)	00:00:07		0 bps/0 bps	28 B/0 B	
Cs	2.117.177.134:22316	200.200.200.1:19729	17 (udp)	00:00:07		0 bps/0 bps	28 B/0 B	
Cs	2.132.57.100:11105	200.200.200.1:8518	17 (udp)	00:00:07		0 bps/0 bps	28 B/0 B	
Cs	2.151.178.168:12796	200.200.200.1:10209	17 (udp)	00:00:07		0 bps/0 bps	28 B/0 B	
Cs	3.21.141.233:5641	200.200.200.1:3054	17 (udp)	00:00:08		0 bps/0 bps	28 B/0 B	
Cs	3.62.35.221:2731	200.200.200.1:144	17 (udp)	00:00:08		0 bps/0 bps	28 B/0 B	
Cs	3.91.141.107:4537	200.200.200.1:1950	17 (udp)	00:00:06		0 bps/0 bps	28 B/0 B	
Cs	3.99.25.178:9392	200.200.200.1:6805	17 (udp)	00:00:08		0 bps/0 bps	28 B/0 B	
Cs	3.110.51.185:4548	200.200.200.1:1961	17 (udp)	00:00:08		0 bps/0 bps	28 B/0 B	
Cs	3.121.129.178:2766	200.200.200.1:179	17 (udp)	00:00:08		0 bps/0 bps	28 B/0 B	
Cs	3.136.45.37:3338	200.200.200.1:751	17 (udp)	00:00:07		0 bps/0 bps	28 B/0 B	
Cs	3.178.47.45:18812	200.200.200.1:16225	17 (udp)	00:00:07		0 bps/0 bps	28 B/0 B	
Cs	3.228.77.57:15289	200.200.200.1:12702	17 (udp)	00:00:06		0 bps/0 bps	28 B/0 B	
Cs	6.10.134.144:2718	200.200.200.1:131	17 (udp)	00:00:06		0 bps/0 bps	28 B/0 B	
Cs	6.32.163.236:11107	200.200.200.1:8520	17 (udp)	00:00:07		0 bps/0 bps	28 B/0 B	
Cs	6.188.242.147:5666	200.200.200.1:3079	17 (udp)	00:00:08		0 bps/0 bps	28 B/0 B	
Cs	6.233.200.104:2977	200.200.200.1:390	17 (udp)	00:00:08		0 bps/0 bps	28 B/0 B	
Cs	7.2.147.141:5050	200.200.200.1:2463	17 (udp)	00:00:08		0 bps/0 bps	28 B/0 B	
Cs	7.14.212.101:3340	200.200.200.1:753	17 (udp)	00:00:07		0 bps/0 bps	28 B/0 B	
Cs	7.55.204.166:3659	200.200.200.1:1072	17 (udp)	00:00:06		0 bps/0 bps	28 B/0 B	
Cs	7.98.51.67:3373	200.200.200.1:786	17 (udp)	00:00:07		0 bps/0 bps	28 B/0 B	
Cs	7.123.134.98:12859	200.200.200.1:10272	17 (udp)	00:00:07		0 bps/0 bps	28 B/0 B	
Cs	7.144.161.45:3983	200.200.200.1:1396	17 (udp)	00:00:07		0 bps/0 bps	28 B/0 B	
Cs	7.163.143.222:2803	200.200.200.1:216	17 (udp)	00:00:06		0 bps/0 bps	28 B/0 B	
Cs	7.190.91.177:15854	200.200.200.1:13267	17 (udp)	00:00:06		0 bps/0 bps	28 B/0 B	▼

817 items out of 47553 Max Entries: 218040





Session: 192.168.10.27 CPU: 2%

firewall

Filter Rules NAT **Raw** Service Ports Connections Address Lists Layer7 Protocols

+ - ✓ ✗ 📁 🏠 00 Reset Counters 00 Reset All Counters

#	Action	Chain	Src. Address	Dst. Address	Prot...	Src. Port	Dst. Port	In. Int...	Out. I...	Bytes	Packets
0	✓ acc...	prerouting			17 (...)	68		ether3		7.5 KIB	230
1	✗ drop	prerouting						ether3		394.0 MIB	14 755 732

Raw Rule <>

General Advanced Extra Action Statistics

Chain: prerouting

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

In. Interface:  ether3

Out. Interface:

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:

Ingress Priority:

Priority:

New Raw Rule

General Advanced Extra Action Statistics

Action: drop

Log

Log Prefix:

Regla simplificada!!!



Session: 192.168.10.27 CPU: 85%

Firewall

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

+ - [check] [x] [lock] [filter] 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		ether3		6.6 KiB	221
1	✗ drop	prerouting						ether3		383.2 MiB	14 351 777

Interface <ether3>

Overall Stats Rx Stats Tx Stats Status Traffic ...

Tx/Rx Rate: 624 bps / 61.9 Mbps

Tx/Rx Packet Rate: 1 p/s / 120 941 p/s

FP Tx/Rx Rate: 592 bps / 59.3 Mbps

FP Tx/Rx Packet Rate: 1 p/s / 123 589 p/s

Tx/Rx Bytes: 36.6 MiB / 1293.4 MiB

Tx/Rx Packets: 36 529 / 21 179 088

Tx/Rx Drops: 0 / 0

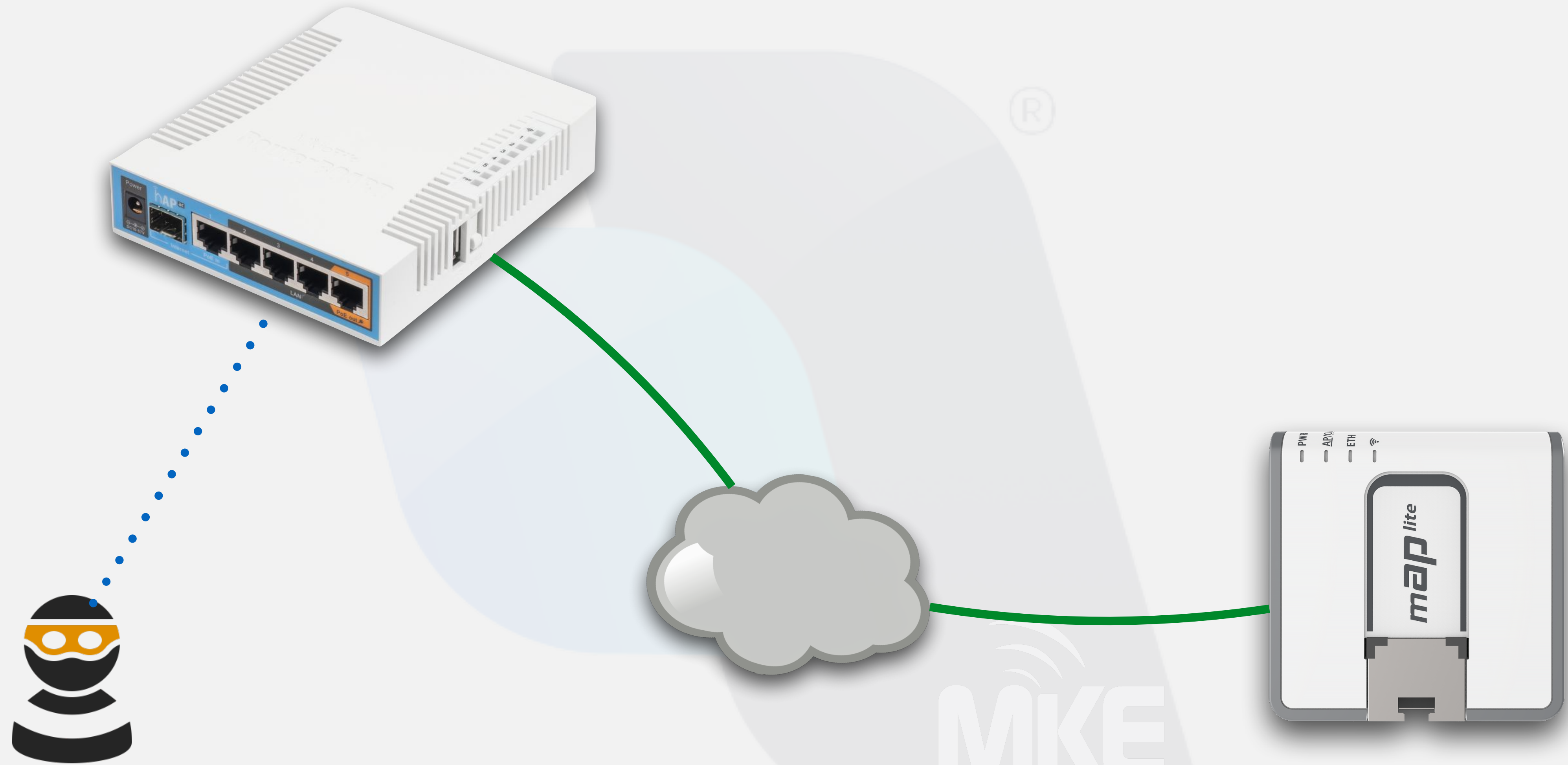
Tx/Rx Errors: 0 / 0

OK  
Cancel  
Apply  
Disable  
Comment  
Torch  
Cable Test  
Blink  
Reset MAC Address  
Reset Counters

Profile (Running)

CPU: all Start Stop Close New Window

Name	CPU	Usage
bridging	0	0.0
cpu0		89.0
dhcp	0	0.0
ethernet	0	22.0
firewall	0	16.5
logging	0	0.0
management	0	1.5
networking	0	42.5
profiling	0	3.0
unclassified	0	3.0
winbox	0	0.5
wireless	0	0.0







- ❖ 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.*



- ❖ <https://www.ietf.org/rfc/rfc2827.txt>
- ❖ [https://en.wikipedia.org/wiki/IP\\_address\\_spoofing](https://en.wikipedia.org/wiki/IP_address_spoofing)
- ❖ [https://en.wikipedia.org/wiki/Ingress\\_filtering](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://wiki.mikrotik.com/wiki/Manual:Packet_Flow_v6)
- ❖ [https://en.wikipedia.org/wiki/Best\\_current\\_practice](https://en.wikipedia.org/wiki/Best_current_practice)





# ¿Preguntas?


## MUCHAS GRACIAS!

---

 - [marioclep@mkesolutions.net](mailto:marioclep@mkesolutions.net)

 - marioclep

 - @marioclep

 +54 9 358 4210029

