MUM MikroTik User Meeting



Tips para segurizar correctamente un router.

Ing. Mario Clep

MKE Solutions



8 de Febrero de 2019

Lima, Perú.

CC BY NC SA

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
- Principales actividades
  - Soporte IT
  - Entrenamientos Oficiales

MKE solutions

COMUTEL WIRELESS SPECIALISTS

info@mkesolutions.net

@mkesolutions

/mkesolutions

/mkesolutions

www.MKESolutions.net

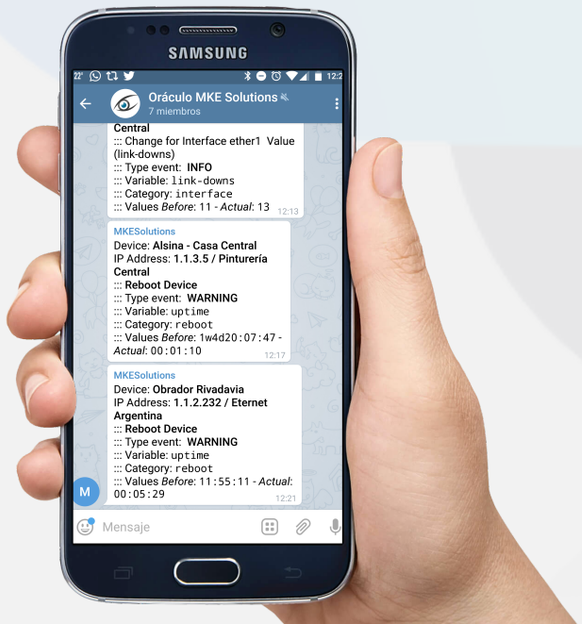
+54 9 358 4210029

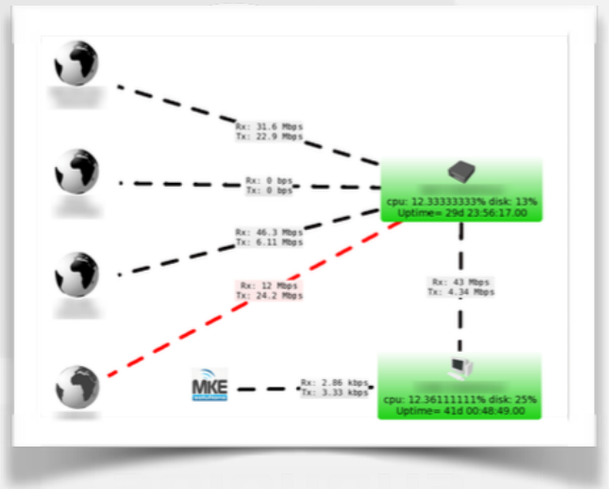
MikroTik

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

Academia de Entrenamientos

MikroTik MTCNA

MikroTik MTCWE

MikroTik MTCTCE

MikroTik MTCUME

MikroTik MTCIPv6E

MikroTik MTCRE

MikroTik MTCINE

- Entrenamientos Públicos y Privados.
- Coordinador del programa MikroTik Academy

Academia® DE ENTRENAMIENTOS

MikroTik

powered by MKE Solutions

MKE solutions

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

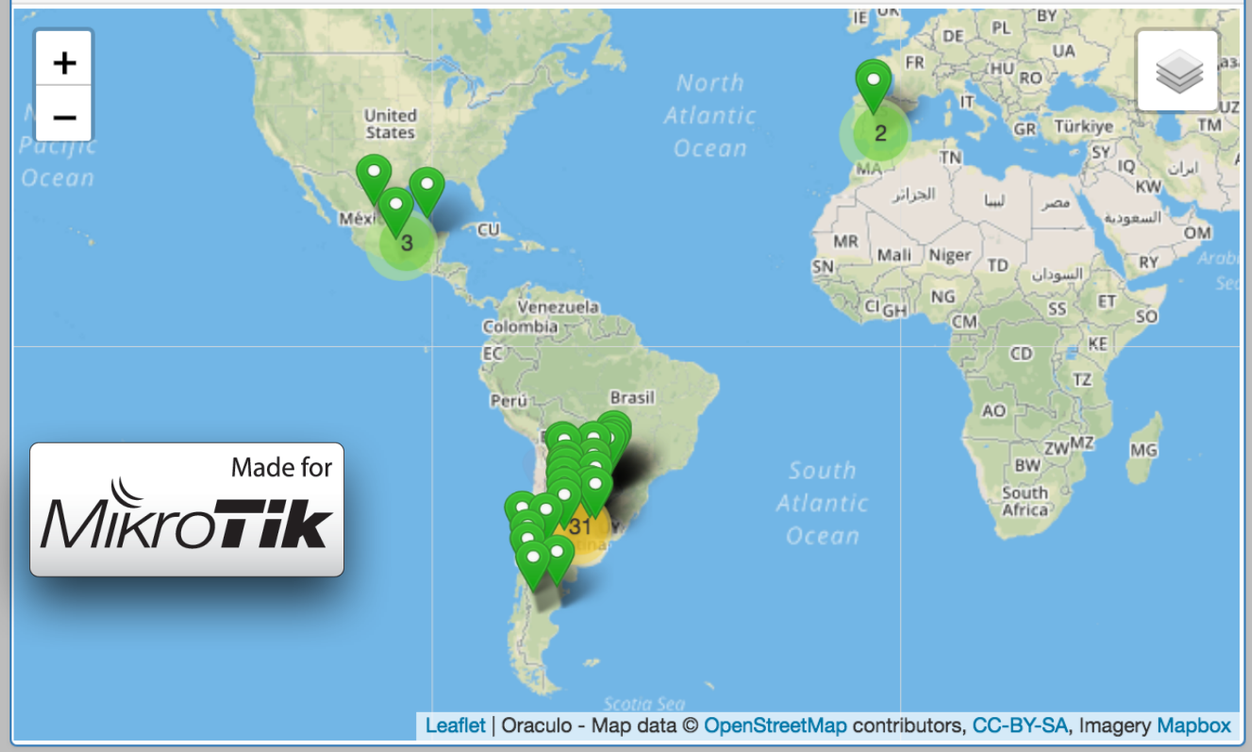
DISK USAGE
54%
Files Backups 21537 | Disk Backups 27G

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]		40 minutes ago	44 minutes ago	Timeout
[redacted]	ion S.A.	20 hours ago	20 hours ago	Timeout
[redacted]		March 28	March 28	Timeout
[redacted]	gentina	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

MUM

¡Felicitaciones!





MikroTik

solutions

Objetivos

- Compartir experiencias
- Introducir el concepto de los ataques.
- Hablar sobre *vulnerabilidades en sistemas operativos*.
- Introducir el concepto de Firewall.
- Segurizar un router en 3 etapas simples.
- DEMO en vivo!



Ataques más comunes

Los ataques tienen principalmente 2 objetivos:

- Tomar el control del router.
- Provocarle una denegación de servicios (CPU al 100%, consumo de todo el ancho de banda, reinicios, etc).
- Más comunes:
  - *Escaneo de Puertos / PSD.*
  - *BruteForce SSH / Telnet / WEB*
  - *Vulnerabilidades & Exploits*
  - *ICMP Flooding*
  - *Ataques de Syn Flooding*
  - *UDP Amplification*
  - *DDoS / IP Spoofing*

Información Pública

- Existen bases de datos públicas que recolectan información de todos los hosts del mundo!

SHODAN | country:"PE" mikrotik | Explore | Downloads | Reports | Developer Pricing

Exploits | Maps | Share Search | Download Results | Create Report

TOTAL RESULTS

5,400

TOP COUNTRIES



Peru	5,400

TOP CITIES

Lima	2,553
Arequipa	402
Ica	103
Trujillo	64
Chimbote	40

TOP SERVICES

190.236.166.154
Telefonica del Peru
Added on 2019-02-04 11:44:09 GMT
Peru, Lima

```
220 firewall FTP server (MikroTik 6.38.5) ready
530 Login incorrect
500 'HELP': command not understood
500 'FEAT': command not understood
```

181.176.221.127
Viettel Perú S.a.c.
Added on 2019-02-04 11:42:01 GMT
Peru

```
HTTP/1.0 403 Forbidden
Content-Length: 1135
Content-Type: text/html
Date: Mon, 04 Feb 2019 11:42:01 GMT
Expires: Mon, 04 Feb 2019 11:42:01 GMT
Server: Mikrotik HttpProxy
Proxy-Connection: close
```

181.176.215.42
Viettel Perú S.a.c.
Added on 2019-02-04 11:20:37 GMT
Peru

```
Firmware: 1
Hostname: Core Minera Paraiso SAC
Vendor: MikroTik
```

Exploits

SHODAN | Exploits

mikrotik

TOTAL RESULTS

17

PLATFORM

hardware	12
windows	2
php	2
linu	

TYPE

remote	7
dos	6
webapps	4

AUTHOR

FarazPajohan	4
ShadOS	2
Lorenzo Santina	2
xis_one	1

MikroTik RouterOS - sshd (ROSSSH) Remote Heap Corruption

kingcope

remote

... During an audit the Mikrotik RouterOS sshd (ROSSSH) has been identified to have a remote previous to

Exploitation of this vulnerability will allow full access to the router device.

This analysis describes the bug and includes a way to get ...

Exploitation of this vulnerability will allow full access to the router device.

... During an audit the Mikrotik RouterOS sshd (ROSSSH) has been identified to have a remote previous to

Exploitation of this vulnerability will allow full access to the router device.

This analysis describes the bug and includes a way to get ...

Mikrotik Syslog Server for Windows 1.15 - Denial of Service (Metasploit)

xis_one

dos 514

... # Exploit Title: Mikrotik Syslog Server for Windows - remote BOF DOS
Date: 19.04.2013
Exploit Author: xis_one@STM Solutions

Exploits

SHODAN | Exploits

cisco

TOTAL RESULTS

250

SOURCE

exploitdb	245
metasploit	5

PLATFORM

hardware	139
windows	50
multiple	15
jsp	5
asp	5

TYPE

remote	100
dos	71
webapps	53
local	21

Cisco ASA 8.x - 'EXTRABACON' Authentication Bypass

Shadow Brokers

remote 161

```
...  # Exploit Title: Cisco ASA 8.X Authentication Bypass
# Date: 17-08-2016
# Exploit Author: Equation Group
# Vendor Homepage: Cisco
# Software Link: Cisco
# Version: Cisco ASA 8.X
# Tested on: Cisco ASA 8.4.2
# CVE : Not sure

Requirements:
* SNMP read (public) string
* Access to SNMP service
* SSH port accessible


Full Exploit:
https://github.com/offensive-security/exploitdb-bin-sploits/raw/master/bin-sploits/40258.zip ...
```

Cisco ASA 8.x - 'EXTRABACON' Authentication Bypass

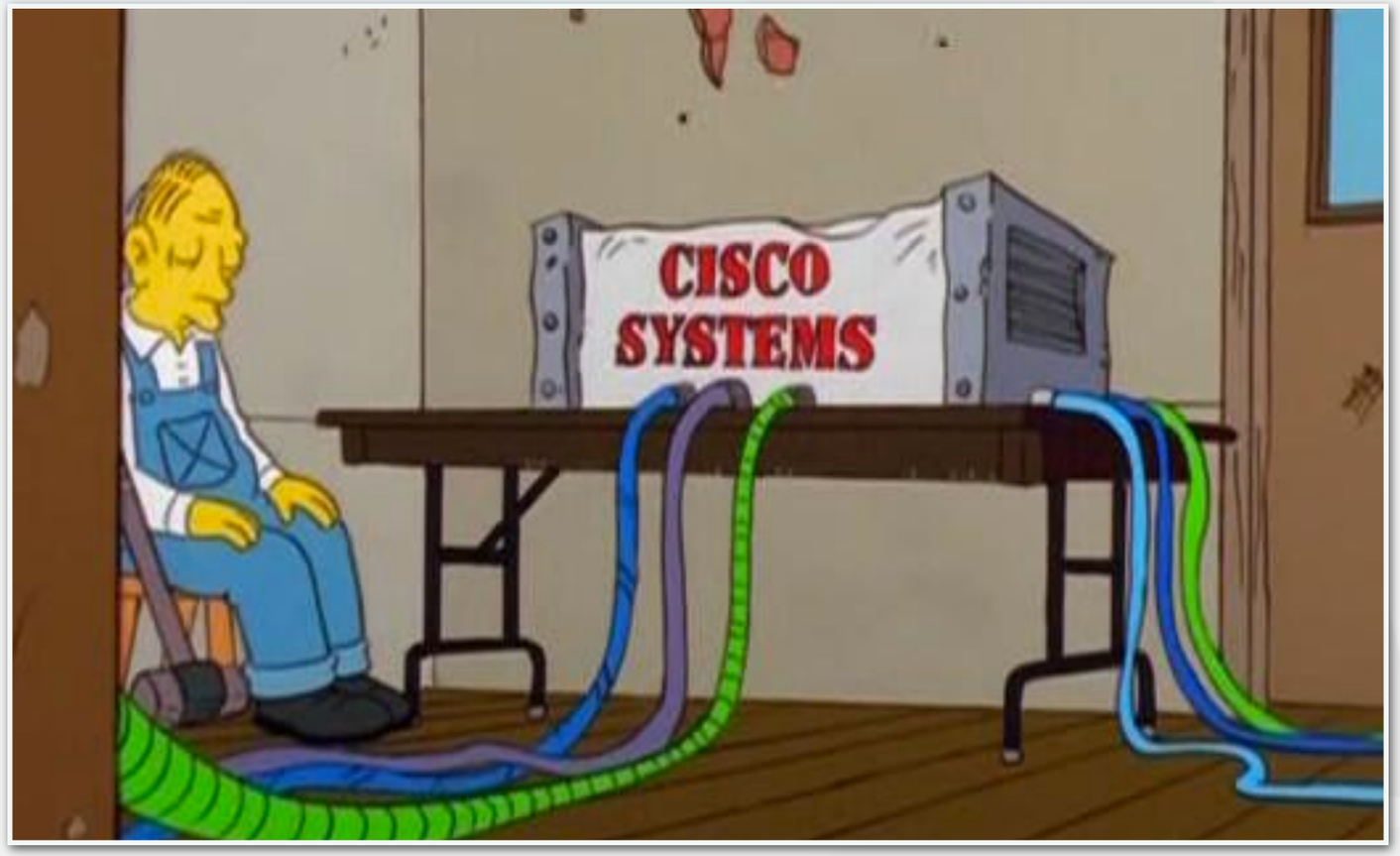
Shadow Brokers

remote 161

```
...  # Exploit Title: Cisco ASA 8.X Authentication Bypass
# Date: 17-08-2016
```

¿Puedo hacer algo?

- Tener el router ***LO MAS SEGURO POSIBLE!***
  - Mantener actualizado el sistema operativo.
  - Implementar reglas de firewall (INPUT) para controlar el acceso al router.



¿Por donde empiezo?



Actualización de RouterOS

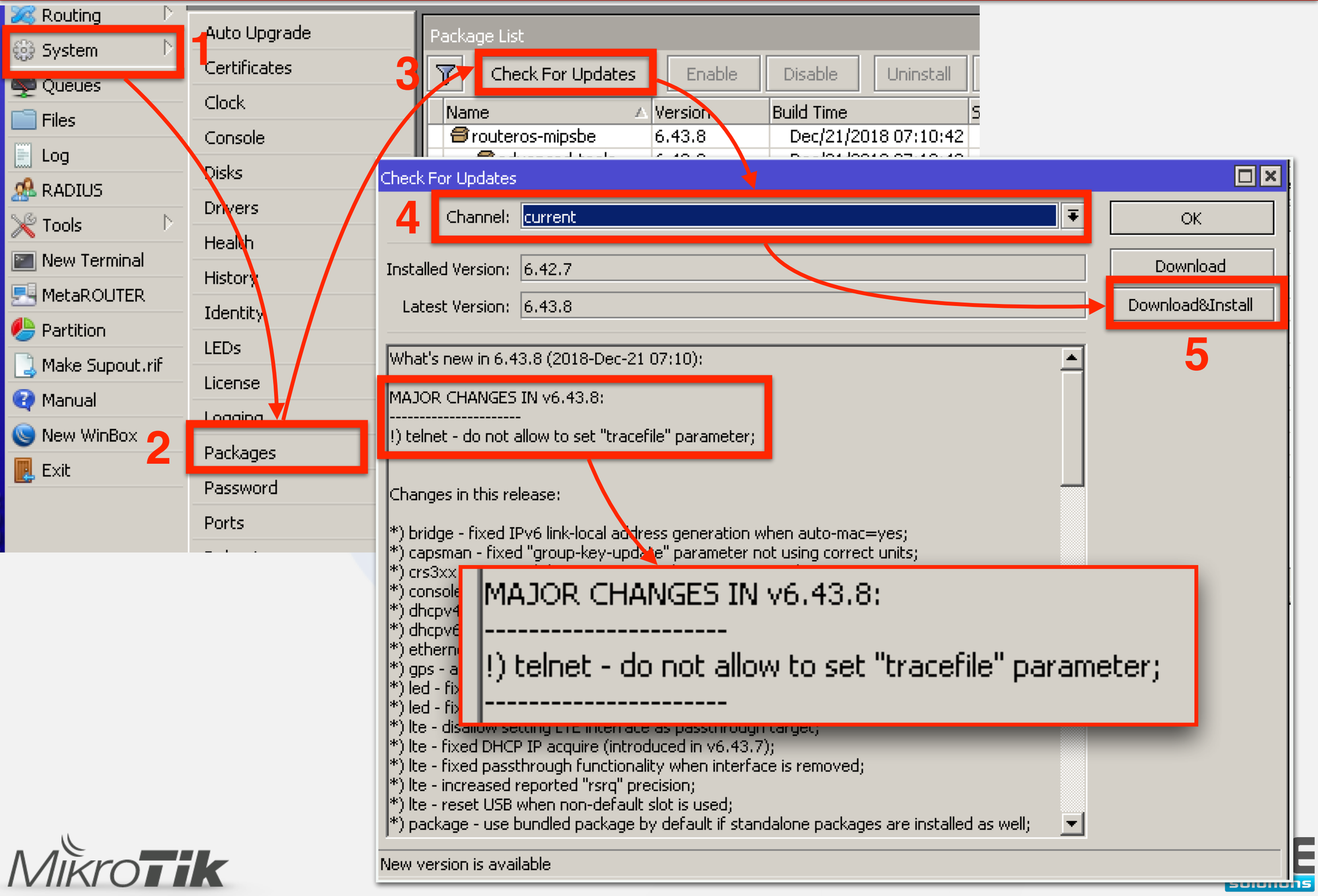
Hay muchas maneras de hacerlo, según conveniencia:

- Actualización manual (descargar, subir, reiniciar).
- Actualización centralizada (System ➟ Autoupgrade).
- The DUDE / NetInstall
- Actualización por consola:

/tool fetch url=https://www.mikrotik.com…

- *System ➟ Packages ➟ Check For Updates*

MUM Actualización de RouterOS



Seguridad en 3 etapas

- ETAPA 1: Deshabilitar los servicios que no se van a usar.

- ETAPA 2: Implementación de un firewall simple que sólo permita el acceso a los servicios a las IP que estén dentro de una ***lista blanca***.

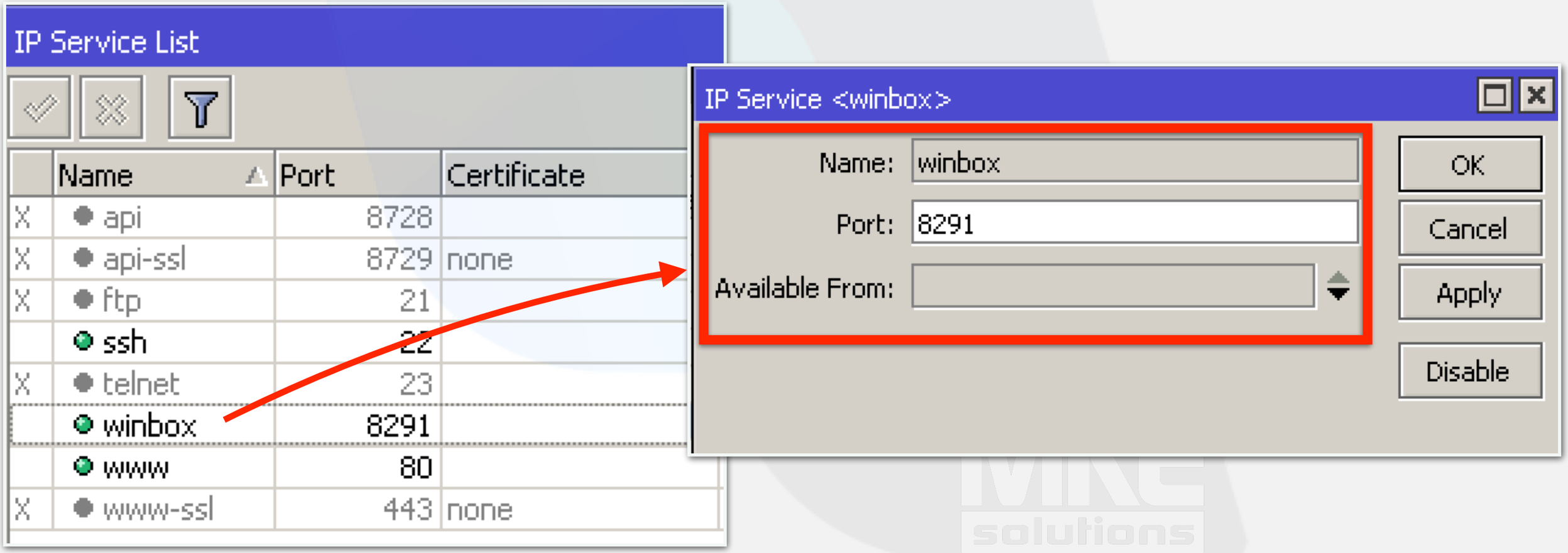
- ETAPA 3: ¿Cómo hacer que mi IP caiga en esa lista blanca?



MUM Etapa I: Servicios en RouterOS

- Los servicios son las diferentes puertas de ingreso a RouterOS. Es altamente recomendable deshabilitar todos aquellos servicios que no se usen en nuestro router.

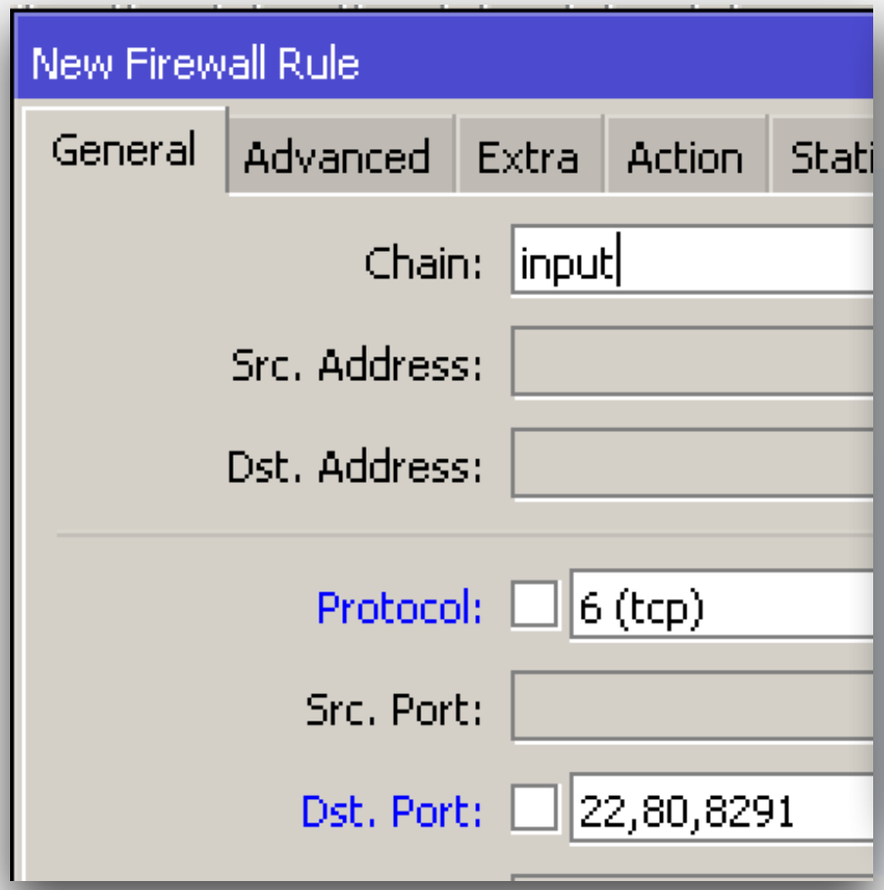
- IP ➟ Services

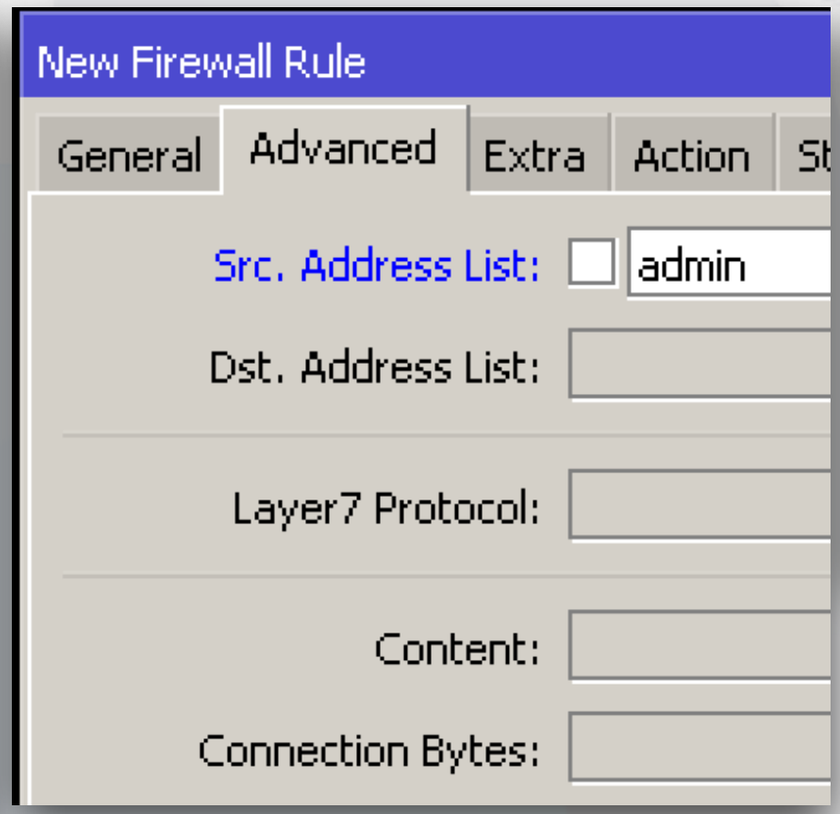


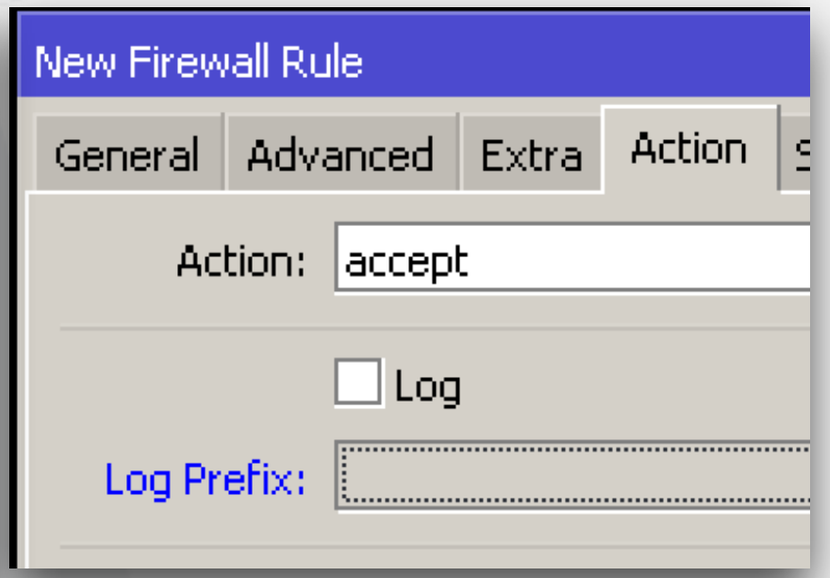
MikroTik
MKE solutions

MUM Etapa 2: Firewall Simple (parte I)

- Las direcciones IP que estén en la lista "admin" tendrán acceso a los servicios habilitados (SSH, WEB y WinBox).

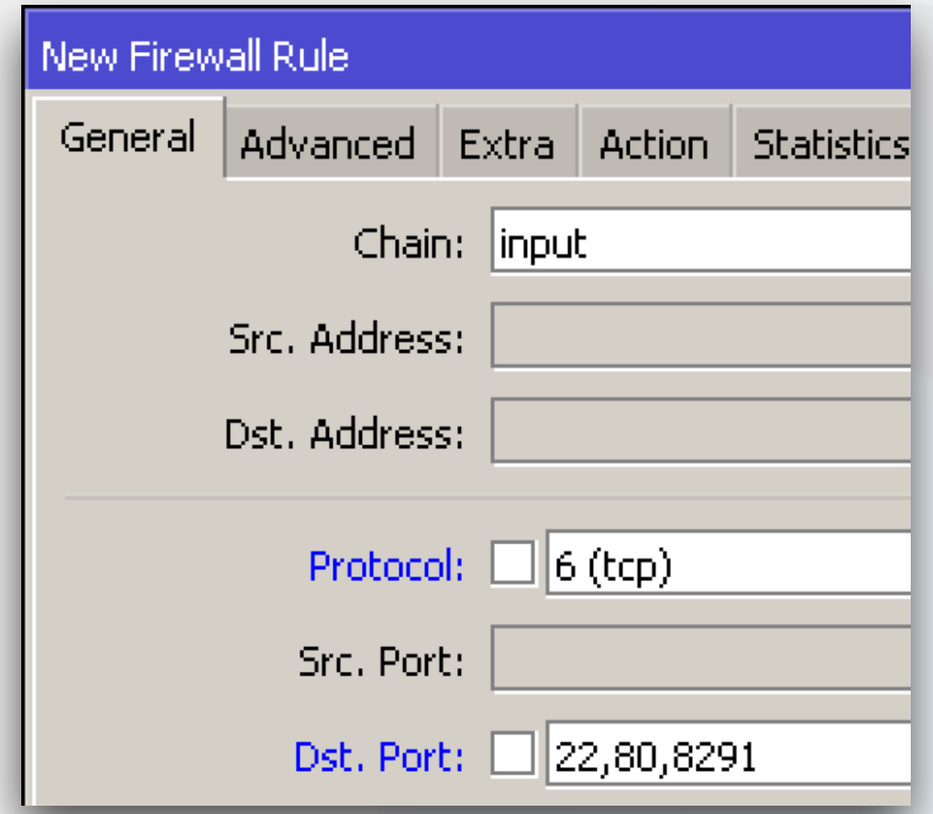






MUM Etapa 2: Firewall Simple (parte II)

- Todas las direcciones IP restantes tendrán los servicios cerrados.






```
/ip firewall filter
add action=accept chain=input dst-port=22,80,8291 protocol=tcp
src-address-list=admin
add action=drop chain=input dst-port=22,80,8291 protocol=tcp
```

MKE solutions

Resultados parciales…

Firewall

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

00 Reset Counters | 00 Reset All Counters | Find | input

#		Action	Chain	Src....	Ds...	Prot...	Src. Port	Dst. Port	Src. Add...	Bytes	Packets
0		acc...	input			6 (tcp)		22,80,8291	admin	0 B	0
1		drop	input			6 (tcp)		22,80,8291		2000 B	32

Firewall

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

Find | admin

Name	Address	Timeout	Creation Time

- ¿Porque sigo dentro del router si el firewall está funcionando y (aún) no estoy dentro de la lista blanca?

MUM Etapa III: ¿Cómo caer en la lista?

- **Port Knocking!**

- Técnica usada para "golpear" el router con una secuencia de puertos sólo conocida por el administrador.

- Al finalizar la secuencia en el orden correcto, la IP del administrador deberá caer en la lista blanca indicada anteriormente.

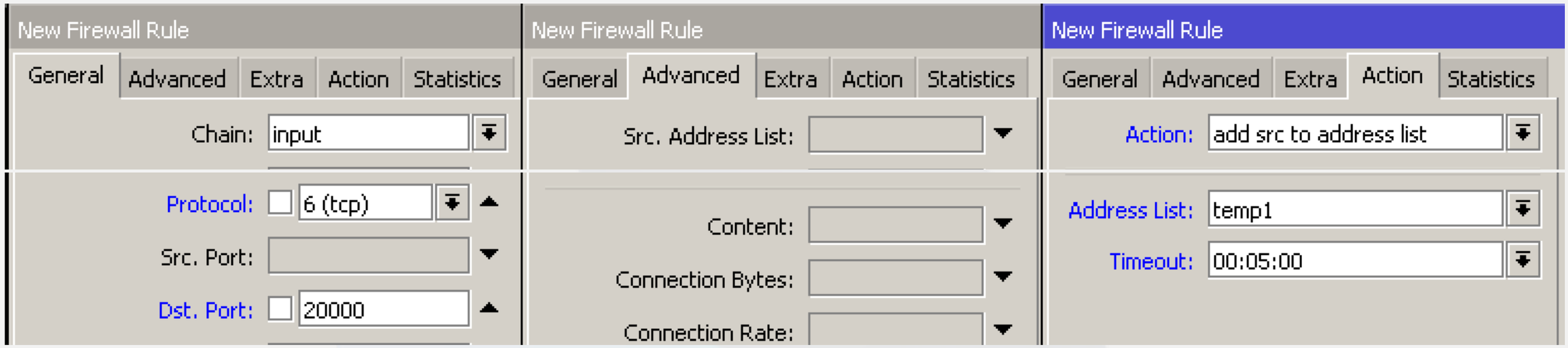
- Hasta que esto no suceda, los servicios estarán cerrados.

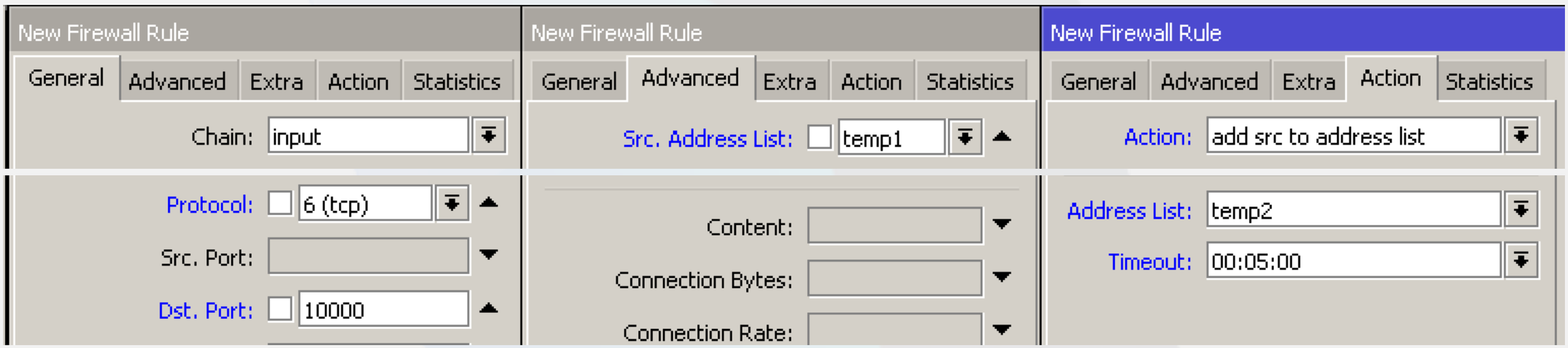


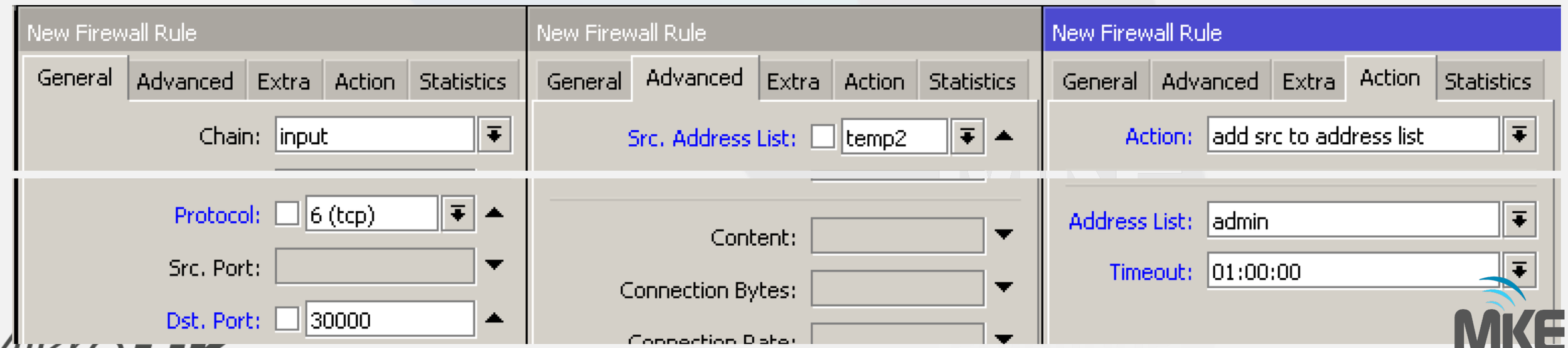
MikroTik

MKE solutions

MUM Etapa III: Port Knocking







MikroTik

MKE solutions

Resultados Finales…

Firewall

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

00 Reset Counters | 00 Reset All Counters | Find | input

#		Action	Chain	Src....	Ds...	Prot...	Src. Port	Dst. Port	Src. Add...	Bytes	Packets
0		acc...	input			6 (tcp)		22,80,8291	admin	0 B	0
1		drop	input			6 (tcp)		22,80,8291		2000 B	32
2		ad...	input			6 (tcp)		20000		0 B	0
3		ad...	input			6 (tcp)		10000	temp1	0 B	0
4		ad...	input			6 (tcp)		30000	temp2	0 B	0

- Ahora sólo resta enviarle paquetes al router en la secuencia definida anteriormente para que nuestra IP caiga en la lista blanca definida.

Resultados Finales…

```
MacBook-Pro-de-Mario:~ marioclep$ telnet 192.168.88.241 20000
Trying 192.168.88.241...
telnet: connect to address 192.168.88.241: Connection refused
telnet: Unable to connect to remote host
MacBook-Pro-de-Mario:~ marioclep$ telnet 192.168.88.241 10000
Trying 192.168.88.241...
telnet: connect to address 192.168.88.241: Connection refused
telnet: Unable to connect to remote host
MacBook-Pro-de-Mario:~ marioclep$ telnet 192.168.88.241 30000
Trying 192.168.88.241...
telnet: connect to address 192.168.88.241: Connection refused
telnet: Unable to connect to remote host
```

Firewall

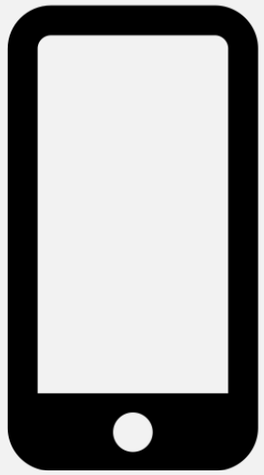
Filter Rules | NAT | Mangle | Raw | Service Ports | Connections | Address Lists | Layer7 Protocols

Find | all

	Name	Address	Timeout	Creation Time
D	admin	192.168.88.246	00:59:30	Feb/04/2019 17:...
D	temp1	192.168.88.246	00:04:21	Feb/04/2019 17:...
D	temp2	192.168.88.246	00:04:27	Feb/04/2019 17:...

DEMO!

MUM Perú



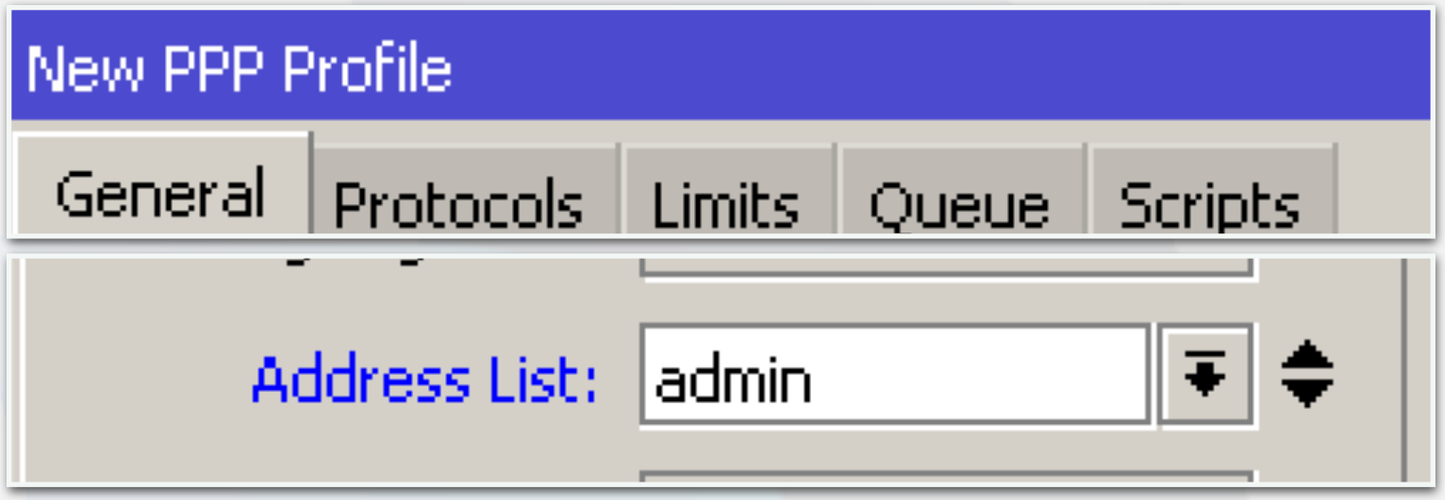




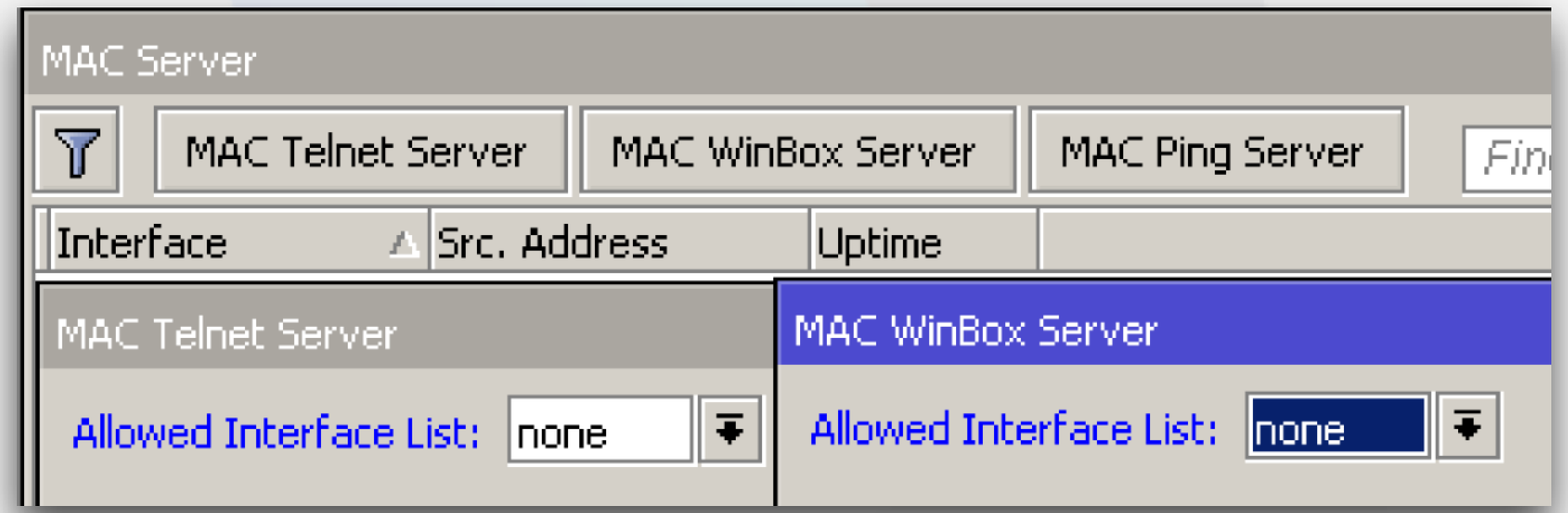


Tips!

- Una alternativa es trabajar con VPN, y al conectarse, agrega la IP a la lista admin.

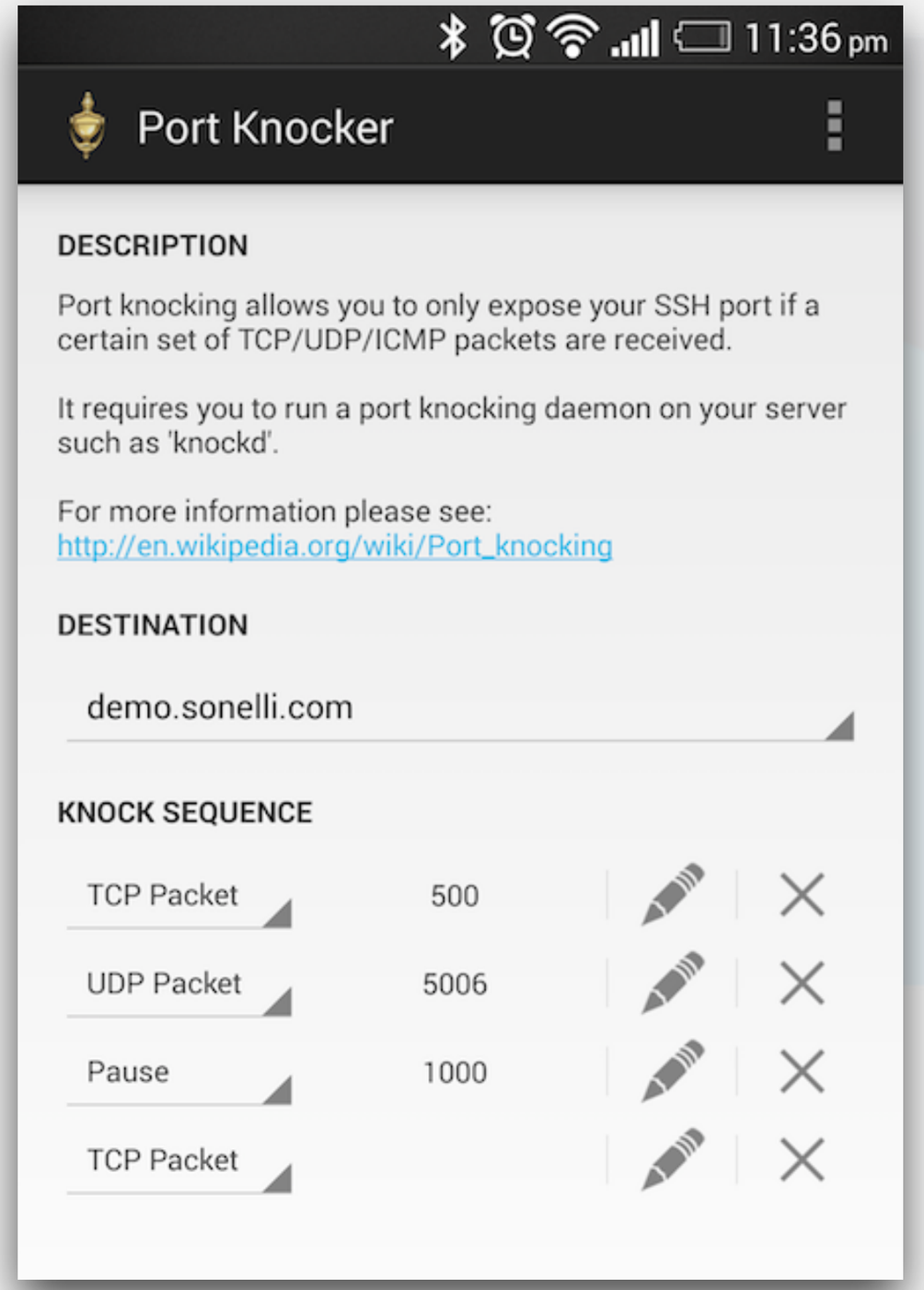


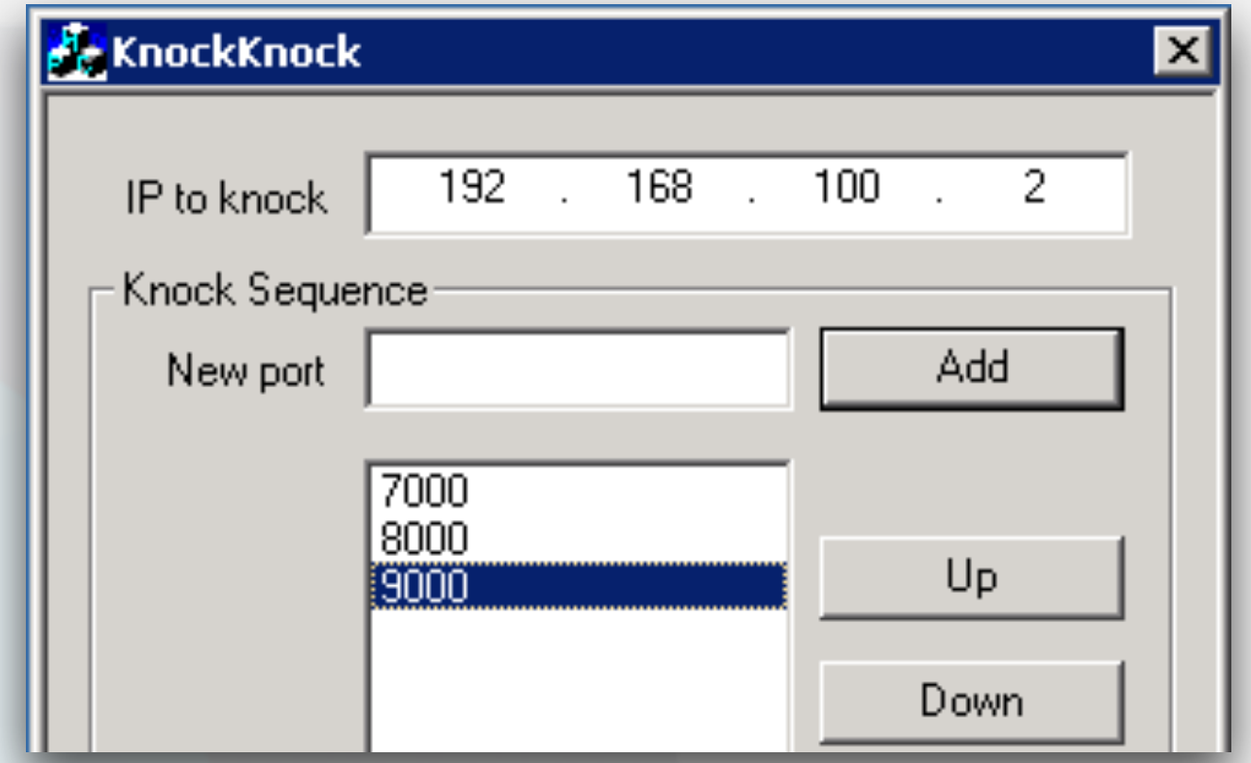
- Deshabilitar MAC-Telnet y MAC-Winbox (Tools > Mac Server).

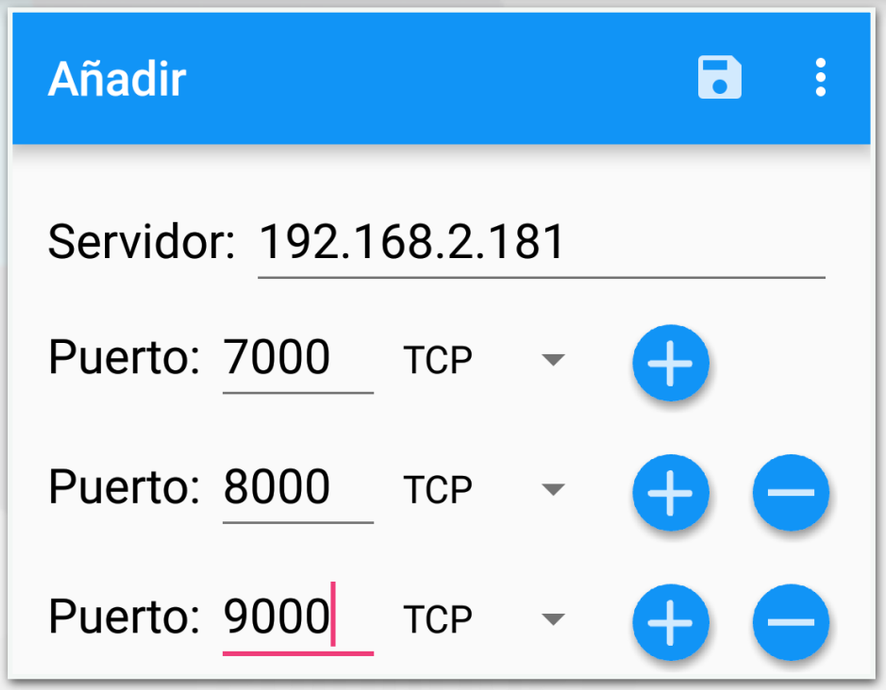


Tips!

- Vienen muchas aplicaciones de Port Knocking para cualquier S.O.!







Conclusiones!

- Hay muchas maneras de proteger un router, algunas más simples, otras más complejas, pero **en todas hay que usar el Firewall.**

- Mantener actualizado RouterOS cierra las vulnerabilidades que van apareciendo.

- La técnica mostrada anteriormente sólo cierra el acceso al router, protegiendo los ataques que tienen como objetivo tomar el control del equipo. Sin embargo, hay otros ataques que sólo tienen intención de provocar una denegación de servicio, que requieren otro tipo de tratamiento y configuraciones.

¿Preguntas?

MUCHAS GRACIAS!

Ing. Mario Clep
MKE Solutions

- marioclep@mkesolutions.net
- marioclep
- @marioclep

CC BY NC SA