



Tips para Principiantes

Ing. Mario Clep
MKE Solutions



13 de Noviembre de 2017

Montevideo - Uruguay



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

@ - 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



@mkesolutions



/mkesolutions



/mkesolutions



www.MKESolutions.net

- ❖ 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



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

Academia
DE ENTRENAMIENTOS



Overview

Graphs

Interfaces

Firewall

Logs

Files

History

Binary

Export

Probe

Clean

Delete

MikroTik - CCR1036-12G-4S

v6.36.3 (stable)

Device Name:

Category / Group:

IP Address:

Host Alive:

Last Seen Alive:

Uptime:

Uptime (Reboot) Counter:

Cron Details

Last Probe:

Last Job Status:

Log Probe:

Last Checked:

Last Time Modify Event:

Last Backup Export:

Last Backup Binary:

Hardware Details

System License

Connection Tracking

RouterBOARD

Architecture-name:

Current-firmware:

Factory-firmware:

Firmware-type:

System Resources

Memory Used (2.29%):

Disk Used (13.87%):

CPU Load (0%):

cpu0: %	cpu1: %	cpu2: %	cpu3: 3%	cpu4: %
cpu5: %	cpu6: %	cpu7: %	cpu8: %	cpu9: %
cpu10: %	cpu11: %	cpu12: %	cpu13: %	cpu14: %
cpu15: %	cpu16: %	cpu17: %	cpu18: %	cpu19: %
cpu20: %	cpu21: %	cpu22: %	cpu23: %	cpu24: %
cpu25: %	cpu26: %	cpu27: %	cpu28: %	cpu29: %
cpu30: %	cpu31: %	cpu32: %	cpu33: %	cpu34: %
cpu35: %	CPU_total: 0.08%			

Interfaces Static

ether: ptp-out: vlan:

16 1 2

ether1 ether2 ether3 ether4 ether5 ether6 ether7 ether8 ether9 ether10 ether11 ether12 sfp1 sfp2 sfp3 sfp4 MKE-Support vlan.61 - Internet vlan.62 - Telefonía

2 Ethernet Link

14 Ethernet No Link

16 Ethernet Total

BGP

BGP Peers (6)

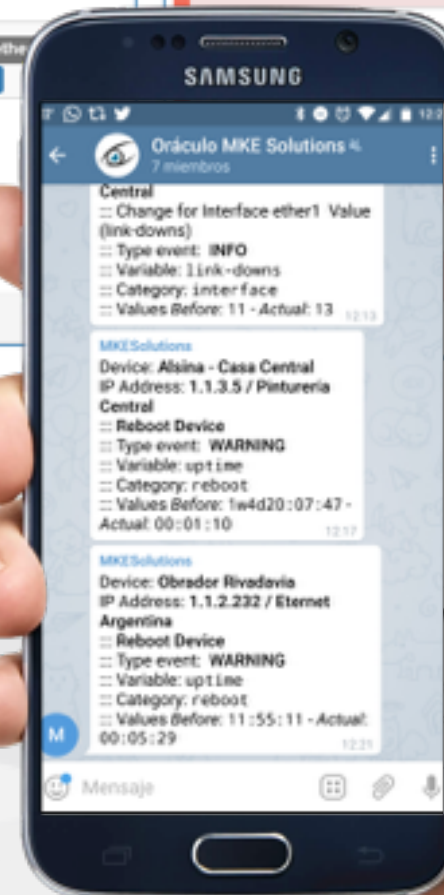
Peer	Remote Address	Remote AS	Updates Received	Updates Sent	Uptime
to-metrotel		4	7	21	
to-iplan		4	1	21	
ibgp-metrotel		39	88525	19	3

Device's Events - Showing last 5 events

Type	Date	Category	Description
INFO	8 hours ago	Interface	Change for Interface ether2 Value (link-downs)
WARNING	Monday at 11:20am	Ping	Device is DOWN since 6 minutes ago
WARNING	November 4	Ping	Device is DOWN since 5 minutes ago
INFO	November 4	Interface	Change for Interface ether8 Value (link-downs)
WARNING	November 4	Ping	Device is DOWN since 5 minutes ago

Monitor: Uptime Activity

Start	Duration	Status
2017-11-08 11:53:25	28 minutes	UP
2017-11-08 11:52:26	3 minutes	DOWN
	1 hours 9 minutes	UP
	4 minutes	DOWN
	1 days 1 hours 54 minutes	UP
	near a minute	DOWN
	8 minutes	UP
	1 minutes	DOWN
	2 days 9 hours 19 minutes	UP



Made for
MikroTik



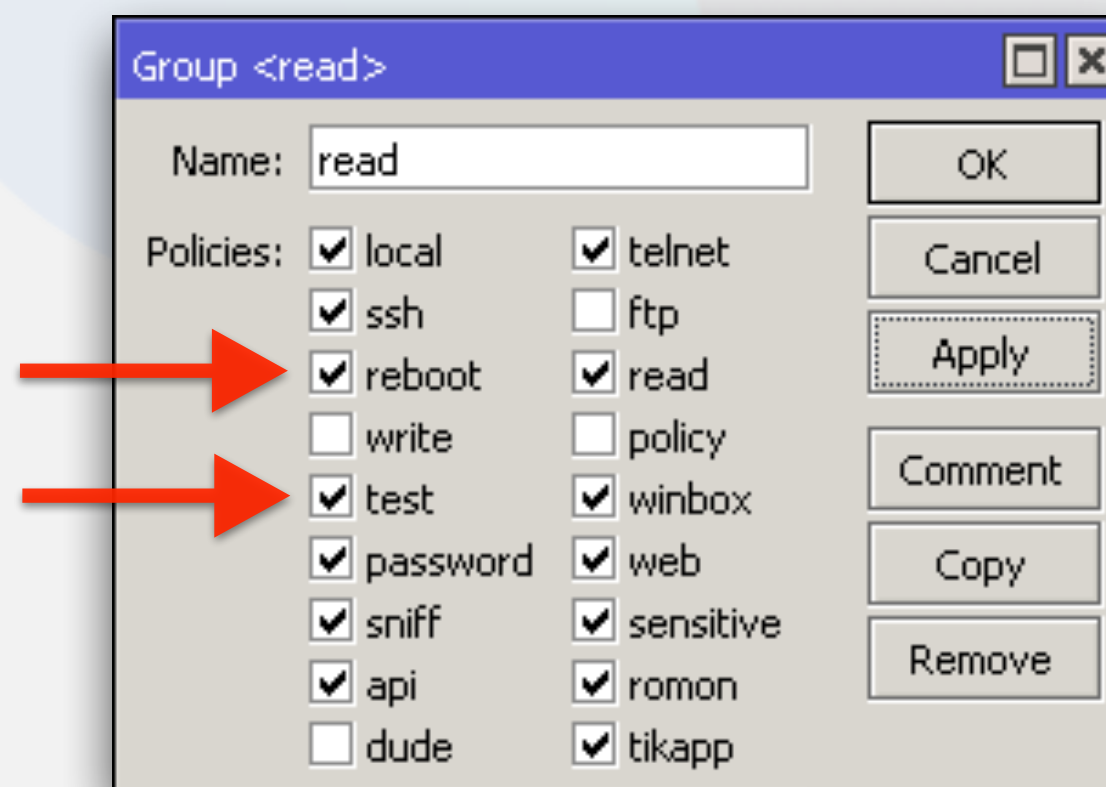
oraculo.mkesolutions.net

¿Quiénes somos principiantes?

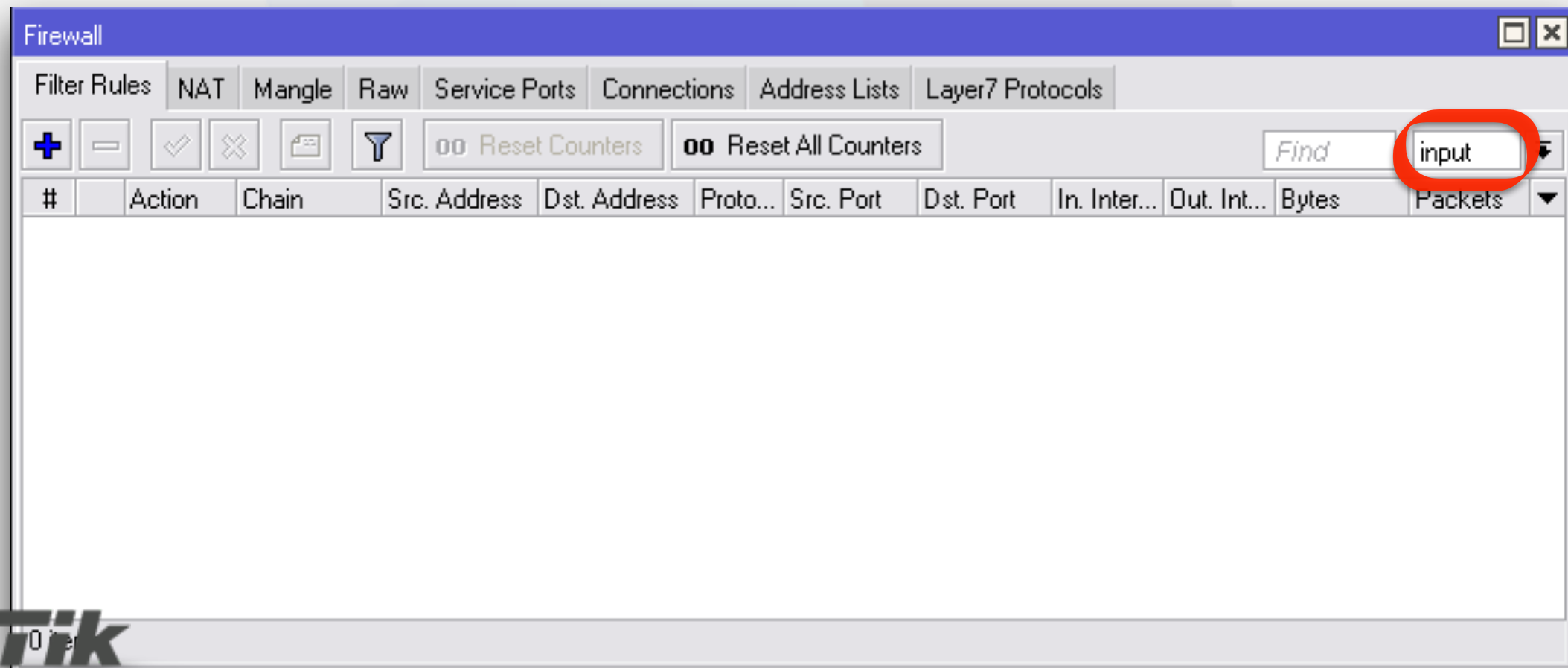
RouterOS es una herramienta MUY poderosa y sobre todo demasiado amplia, pero como en todos los casos, hay que saber configurarlo correctamente.

- ❖ Mostrar los descuidos mas comunes que encuentro cuando los clientes solicitan un relevamiento.
- ❖ Demostrar que con “unos pocos clics” se pueden mejorar las configuraciones, incrementando la seguridad y reduciendo las posibles fallas.

- ❖ Hay situaciones en las que se descuidan los accesos por default, dejando la puerta completamente abierta para ingresar al router con las credenciales por defecto.
- ❖ A veces, la única medida es poner el usuario admin en el perfil **read** y crear un nuevo usuario y contraseña con permisos FULL.
- ❖ *El grupo por defecto del usuario de sólo lectura tiene los permisos de REBOOT y TEST.*



- ❖ Una de las primeras acciones a realizar en todo equipo es poner al menos un pequeño firewall para prevenir los ataques más comunes.
- ❖ Los ataques tienen principalmente 2 objetivos: ***tomar el control del router*** o simplemente ***provocarle una denegación de servicios*** (CPU al 100%, consumo de todo el ancho de banda, etc).



Al no tener un firewall por defecto, todos los servicios están disponibles por todas sus interfaces, incluso la pública.

❖ **SSH** y **Telnet** son los más usados para conseguir acceso por fuerza bruta.

❖ **WEB** y **Winbox** son menos frecuentes, pero también ocurren.

all		
Jan/09/1970 23:08:56	system error critical	login failure for user identd from 187.141.13.251 via ssh
Jan/09/1970 23:08:59	system error critical	login failure for user gnats from 187.141.13.251 via ssh
Jan/09/1970 23:09:01	system error critical	login failure for user jeff from 187.141.13.251 via ssh
Jan/09/1970 23:09:04	system error critical	login failure for user irc from 187.141.13.251 via ssh
Jan/09/1970 23:09:09	system error critical	login failure for user list from 187.141.13.251 via ssh
Jan/09/1970 23:09:12	system error critical	login failure for user eleve from 187.141.13.251 via ssh
Jan/09/1970 23:09:16	system error critical	login failure for user proxy from 187.141.13.251 via ssh
Jan/09/1970 23:09:20	system error critical	login failure for user sys from 187.141.13.251 via ssh
Jan/09/1970 23:09:23	system error critical	login failure for user zzz from 187.141.13.251 via ssh
Jan/09/1970 23:09:27	system error critical	login failure for user tech from 187.141.13.251 via ssh
Jan/09/1970 23:09:30	system error critical	login failure for user frank from 187.141.13.251 via ssh

DNS Settings

Servers: 8.8.8.8

Dynamic Servers: 192.168.10.1
10.200.200.21

☒ Allow Remote Requests

Max UDP Packet Size: 4096

Query Server Timeout: 2.000

Query Total Timeout: 10.000

Max. Concurrent Queries: 100

Max. Concurrent TCP Sessions: 20

Cache Size: 2048 K

Cache Max TTL: 7d 00:00:00

Cache Used: 10

Torch (Running)

Basic
Interface: wan
Entry Timeout: 00:00:03 s

Collect
☒ Src. Address
☒ Dst. Address
☐ MAC Protocol
☐ Protocol
☒ Src. Address6
☒ 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: dns
VLAN Id: any

Et...	Prot...	Src.	Dst.	VLAN Id	Tx Rate	Rx Rate	Tx Pack...	Rx Pack
800 (ip)		115.238.184.126:12633	:53 (dns)		6.0 kbps	344 bps	0	
800 (ip)		115.238.184.125:26701	:53 (dns)		6.0 kbps	344 bps	0	
800 (ip)		115.238.184.126:43549	:53 (dns)		6.0 kbps	344 bps	0	
800 (ip)		115.238.184.125:16379	:53 (dns)		6.0 kbps	344 bps	0	
800 (ip)		101.71.74.109:17231	:53 (dns)		6.0 kbps	344 bps	0	
800 (ip)		101.71.74.110:20153	:53 (dns)		6.0 kbps	344 bps	0	
800 (ip)		115.238.184.125:50075	:53 (dns)		6.0 kbps	344 bps	0	
800 (ip)		115.238.184.126:55531	:53 (dns)		6.0 kbps	344 bps	0	
800 (ip)		115.238.184.126:62555	:53 (dns)		6.0 kbps	344 bps	0	
800 (ip)		115.238.184.126:34379	:53 (dns)		6.0 kbps	344 bps	0	
800 (ip)		115.238.184.126:48267	:53 (dns)		6.0 kbps	344 bps	0	
800 (ip)		101.71.74.109:58126	:53 (dns)		6.0 kbps	344 bps	0	
800 (ip)		101.71.74.110:24377	:53 (dns)		6.0 kbps	344 bps	0	
800 (ip)		115.238.184.126:26973	:53 (dns)		6.0 kbps	344 bps	0	
800 (ip)		115.238.184.126:43181	:53 (dns)		6.0 kbps	344 bps	0	
800 (ip)		115.238.184.126:48380	:53 (dns)		6.0 kbps	344 bps	0	
800 (ip)		101.71.74.109:14222	:53 (dns)		6.0 kbps	344 bps	0	
800 (ip)		115.238.184.126:17981	:53 (dns)		6.0 kbps	344 bps	0	
800 (ip)		115.238.184.125:49099	:53 (dns)		6.0 kbps	344 bps	0	
800 (ip)		101.71.74.109:9467	:53 (dns)		6.0 kbps	344 bps	0	
800 (ip)		101.71.74.109:42021	:53 (dns)		6.0 kbps	344 bps	0	
800 (ip)		101.71.74.109:62197	:53 (dns)		6.0 kbps	344 bps	0	

Total Tx: 724.7 kbps Total Rx: 176.6 kbps Total Tx Packet: 2 Total Rx Packet: 2

Google Sorry...

We're sorry...

... but your computer or network may be sending automated queries. To protect our users, we can't process your request right now.

See [Google Help](#) for more information.

Para continuar, ingresa los siguientes caracteres:



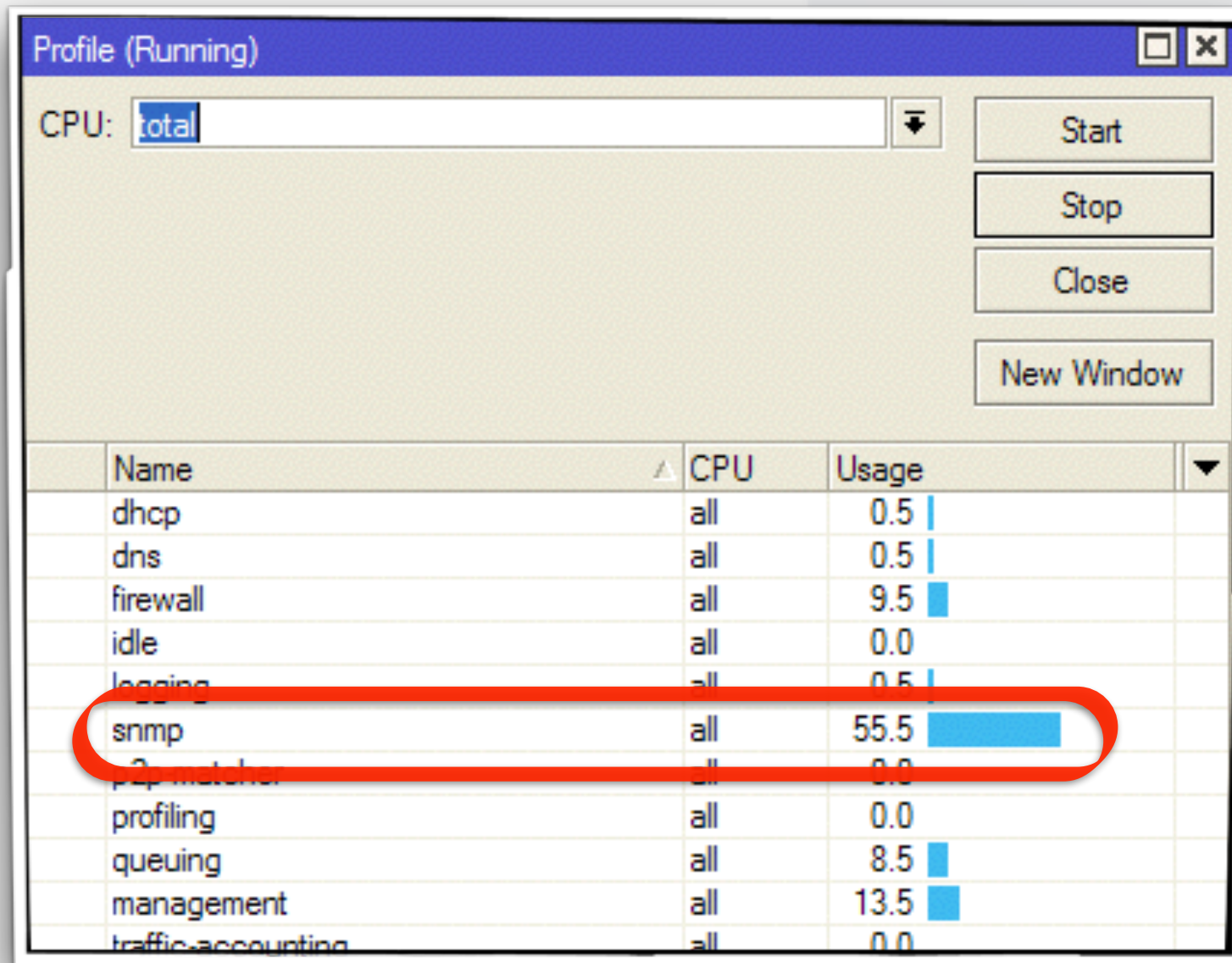
Acerca de esta página

Nuestros sistemas han detectado un tráfico inusual en tu red de equipo. Esta página verifica si realmente eres tú el que envía las solicitudes y no un robot. [¿Por qué sucedió esto?](#)

Ataques por SNMP



Al habilitar el servicio de **SNMP**, por defecto el router queda expuesto a cualquier consulta por cualquiera de sus interfaces.



SNMP Community <public>

Name:

Addresses:

Security:

☒ Read Access

☐ Write Access

Authentication Protocol:

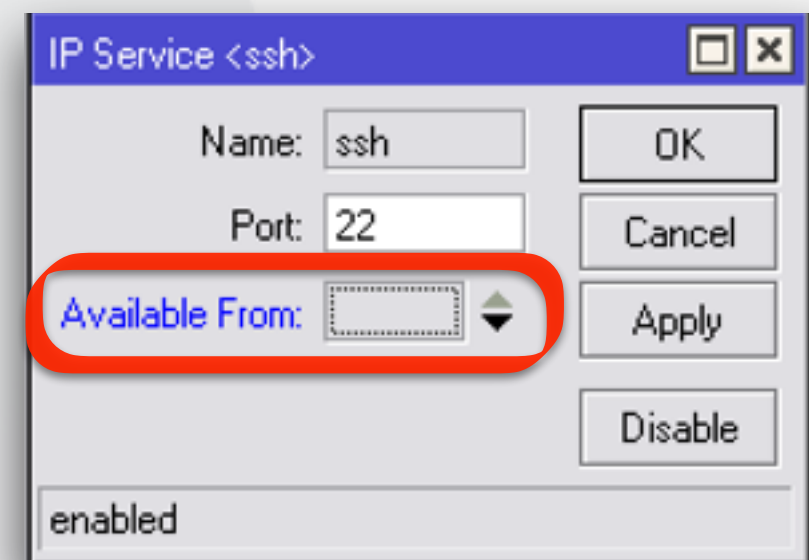
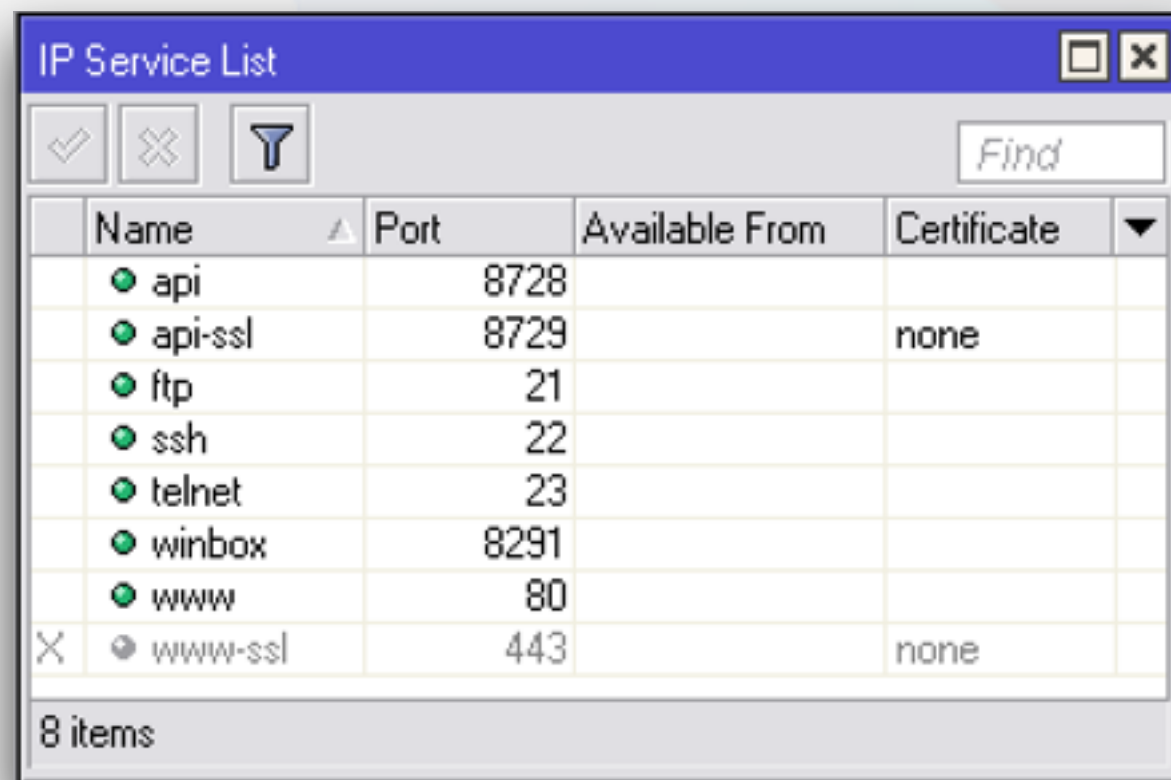
Encryption Protocol:

Authentication Password:

Encryption Password:

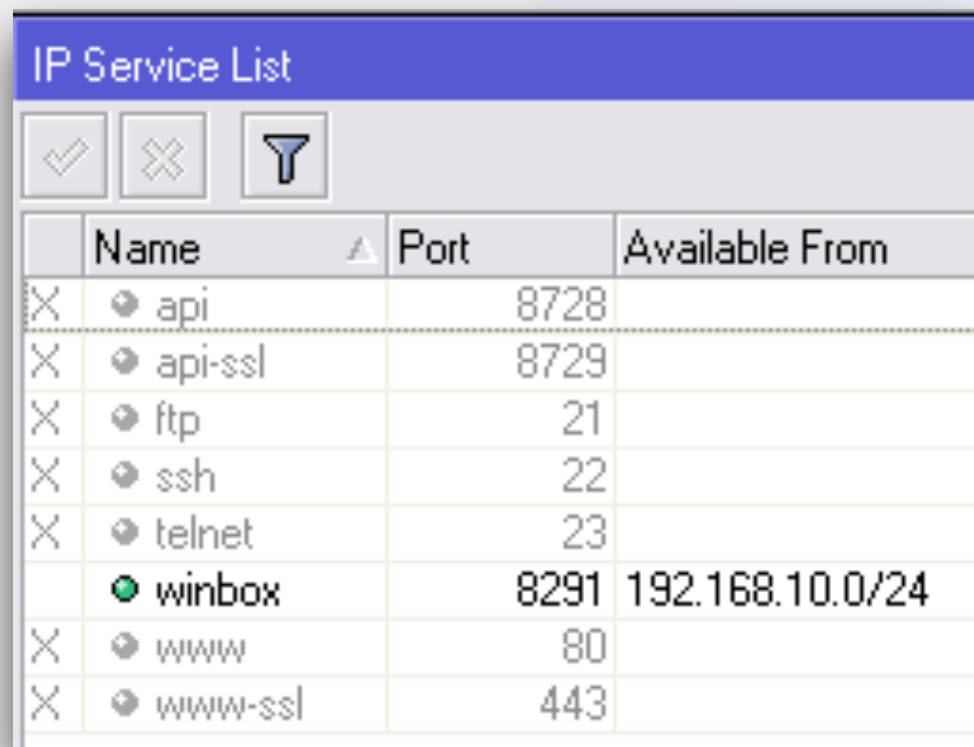
default

- ❖ Una manera simple de protegerse, es deshabilitando los servicios que no se usen y proteger los demás con reglas de *firewall* o especificar el rango de direcciones IP desde la opción de *IP > Service*



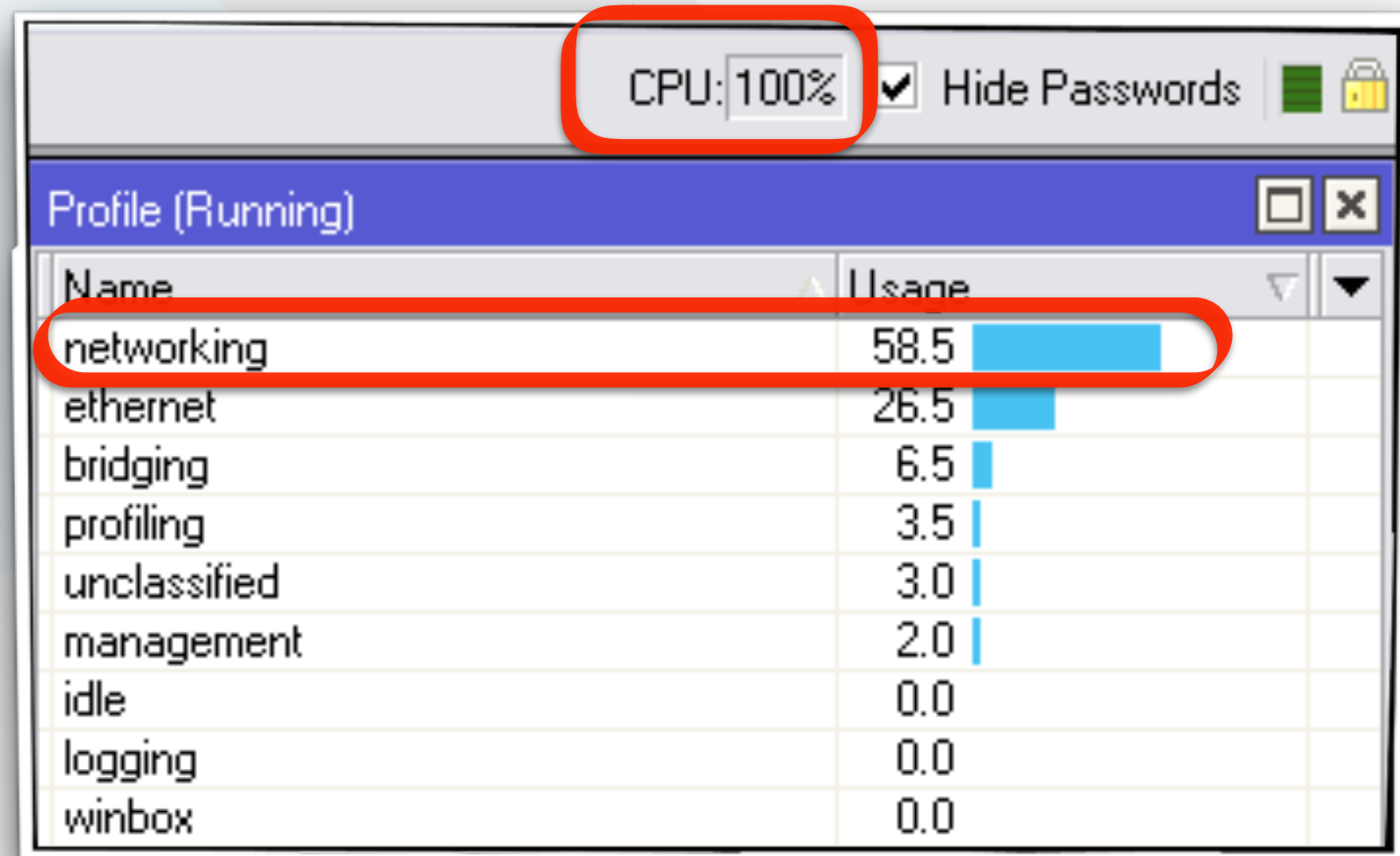
Tener deshabilitados todos los servicios no garantiza que el router esté 100% protegido.

❖ El protocolo **ICMP** mal usado, puede elevar el consumo del CPU y provocar denegación de servicio > **Ping Flooding**.



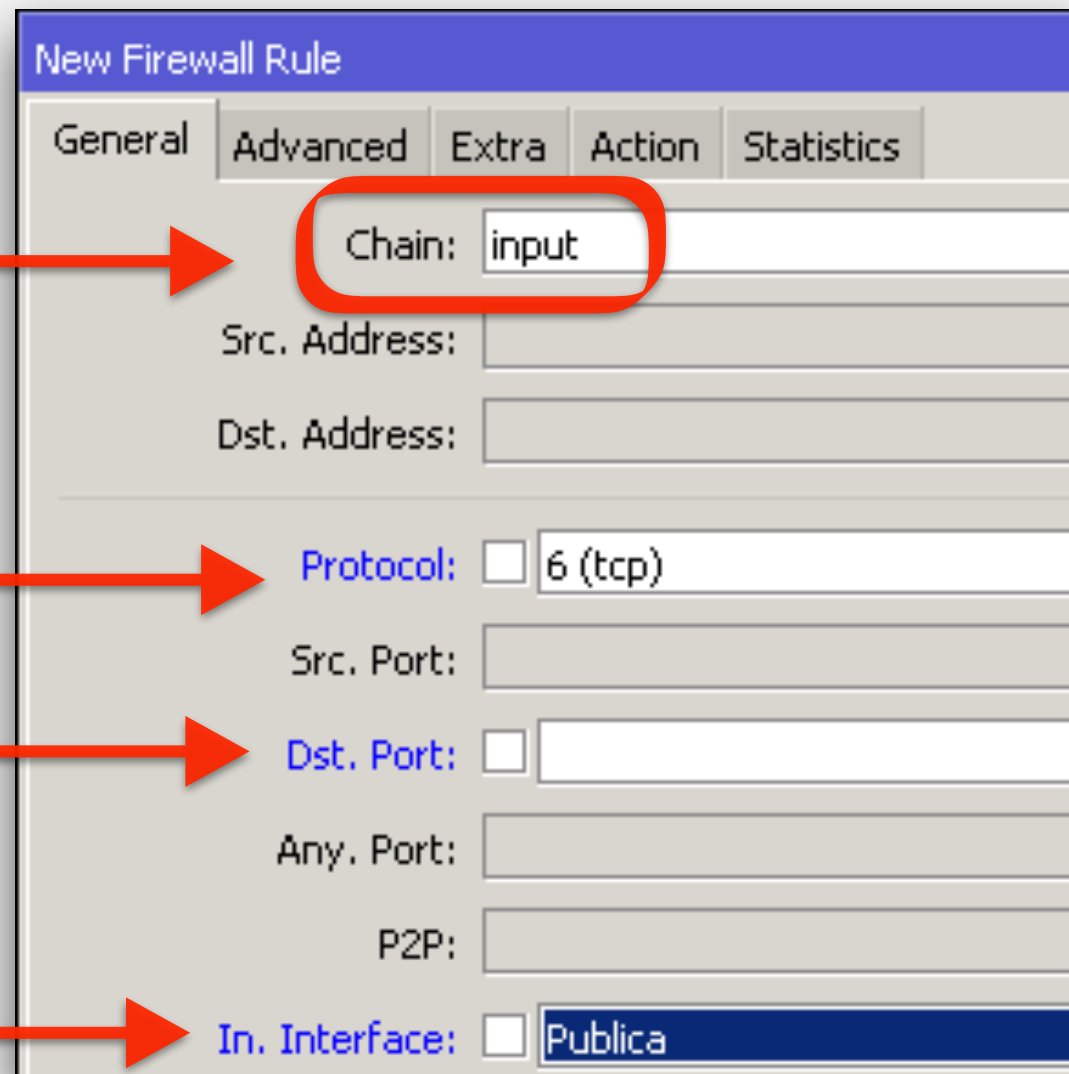
IP Service List

	Name	Port	Available From
X	api	8728	
X	api-ssl	8729	
X	ftp	21	
X	ssh	22	
X	telnet	23	
	winbox	8291	192.168.10.0/24
X	www	80	
X	www-ssl	443	



Profile (Running)

Name	Usage
networking	58.5
ethernet	26.5
bridging	6.5
profiling	3.5
unclassified	3.0
management	2.0
idle	0.0
logging	0.0
winbox	0.0



New Firewall Rule

General Advanced Extra Action Statistics

Chain: **input**

Src. Address:

Dst. Address:

Protocol: ☐ 6 (tcp)

Src. Port:

Dst. Port: ☐

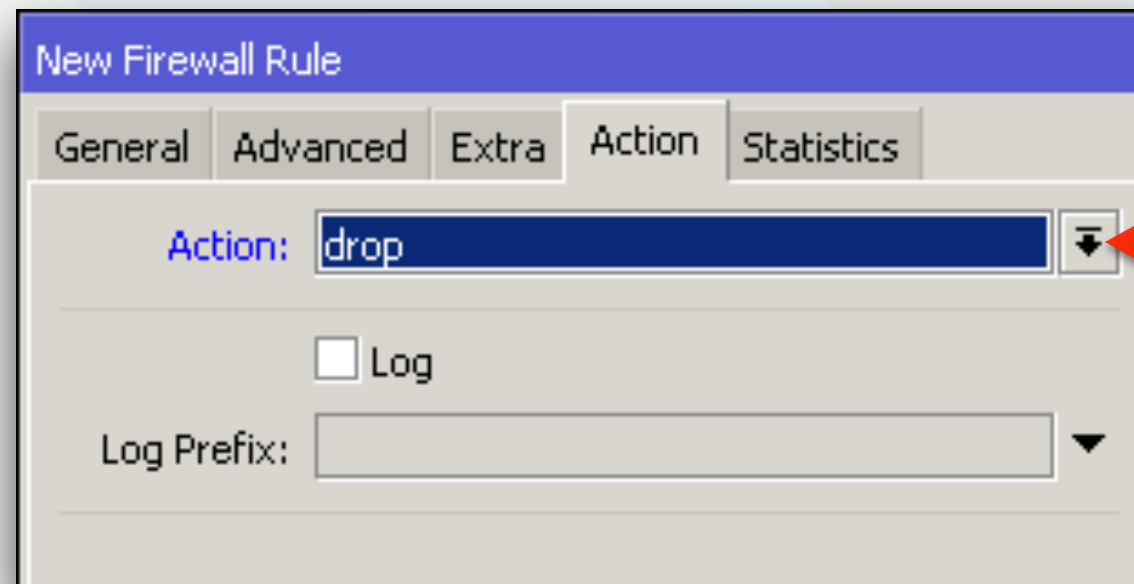
Any. Port:

P2P:

In. Interface: ☐ Publica

Four red arrows point to the Chain, Protocol, Dst. Port, and In. Interface fields.

- ❖ *SSH*: TCP 22
- ❖ *Telnet*: TCP 23
- ❖ *WEB*: TCP 80
- ❖ *Winbox*: TCP 8291
- ❖ *WebProxy*: TCP 8080
- ❖ *DNS*: UDP 53
- ❖ *SNMP*: UDP 161/162



New Firewall Rule

General Advanced Extra Action Statistics

Action: **drop**

☐ Log

Log Prefix:

A red arrow points to the dropdown arrow next to the Action field.

Firewall Rule <>

General Advanced **Extra** Action Statistics

▼ Connection Limit

▲ Limit

Rate: ☐ 10 / sec

Burst:

Mode: ☒ packet ☐ bit

Firewall

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

+ - ✓ ✗

#	Action	Chain	Protocol	Limit/Rate	Bytes	Packets
0	✓ acc...	input	1 (icmp)	10/sec	11.6 KiB	142
1	✗ drop	input	1 (icmp)		98.7 KiB	1 203

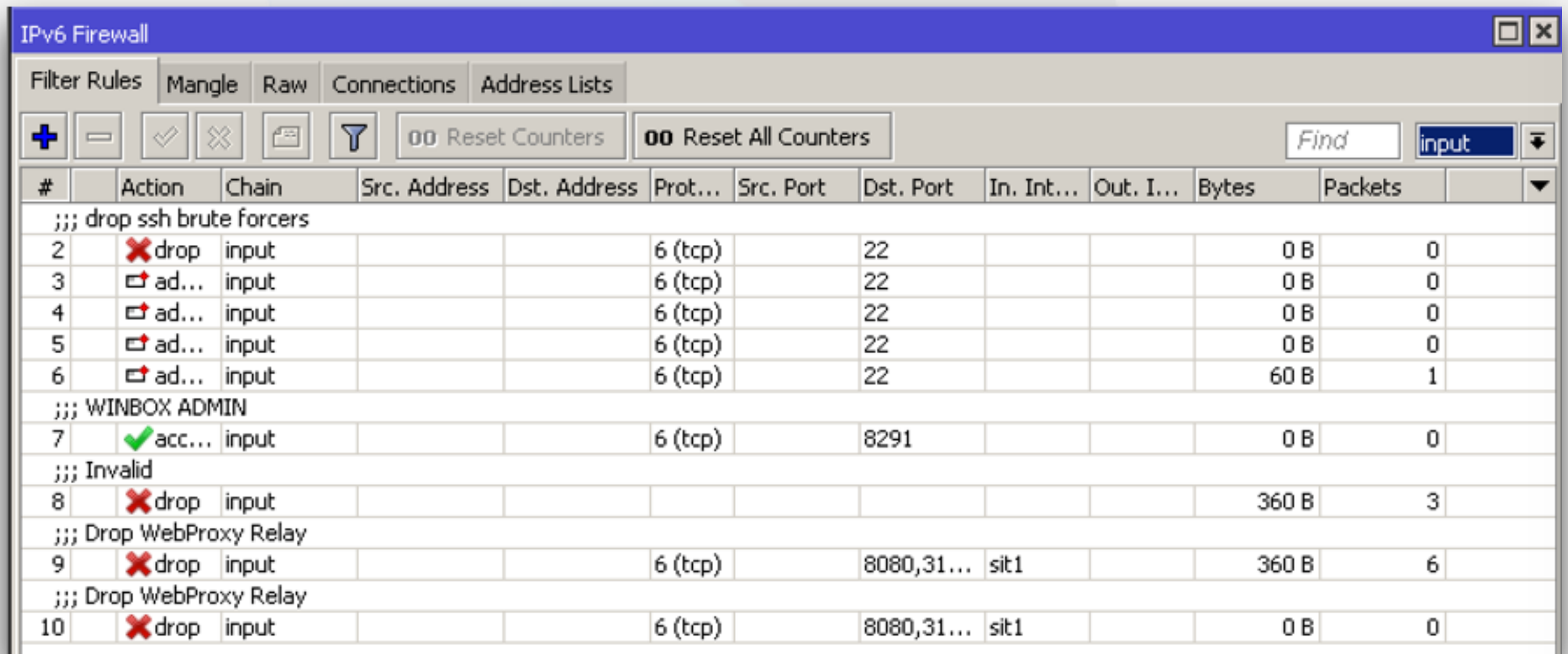
```
/ip firewall filter
```

```
add action=accept chain=input limit=10,5:packet protocol=icmp
```

```
add action=drop chain=input protocol=icmp
```

Al habilitar la compatibilidad con IPv6, aparecen nuevas funcionalidades, entre ellas, su propio firewall.

Seguizar un router por IPv6 es tan importante como hacerlo por IPv4.



#	Action	Chain	Src. Address	Dst. Address	Prot...	Src. Port	Dst. Port	In. Int...	Out. I...	Bytes	Packets
;;; drop ssh brute forcers											
2	 drop	input			6 (tcp)		22			0 B	0
3	 ad...	input			6 (tcp)		22			0 B	0
4	 ad...	input			6 (tcp)		22			0 B	0
5	 ad...	input			6 (tcp)		22			0 B	0
6	 ad...	input			6 (tcp)		22			60 B	1
;;; WINBOX ADMIN											
7	 acc...	input			6 (tcp)		8291			0 B	0
;;; Invalid											
8	 drop	input								360 B	3
;;; Drop WebProxy Relay											
9	 drop	input			6 (tcp)		8080,31...	sit1		360 B	6
;;; Drop WebProxy Relay											
10	 drop	input			6 (tcp)		8080,31...	sit1		0 B	0

- ❖ Bloquear en el router principal el tráfico de download que no vaya con destino a nuestras propias direcciones IP (forward).
- ❖ Bloquear en el router principal el tráfico de upload que no venga con origen desde nuestras propias IP (forward).
- ❖ En caso de dar IP publicas, bloquear (o limitar) los servicios mas vulnerables para evitar ataques de amplificación (DNS, NTP, SNMP).



mum Servicios Principales a proteger



<i>Puerto</i>	<i>Protocolo</i>	<i>Comentario</i>
20,21	TCP	FTP
22	TCP	SSH, SFTP
23	TCP	TELNET
53	TCP/UDP	DNS
80	TCP	HTTP
123	UDP	NTP
161,162	UDP	SNMP
179	TCP	BGP
443	TCP	HTTPS /(HotSpot)

<i>Puerto</i>	<i>Protocolo</i>	<i>Comentario</i>
2000	TCP	Bandwidth Server
3128,8080	TCP	WebProxy
5678	UDP	Neighbour Discovery
8291	TCP	WinBox
8728	TCP	API
	I	ICMP
1701	UDP	L2tP
1723	TCP	PPtP
1812,1813	UDP	User Manager

- ❖ **MNDP** está habilitado en todas sus interfaces.

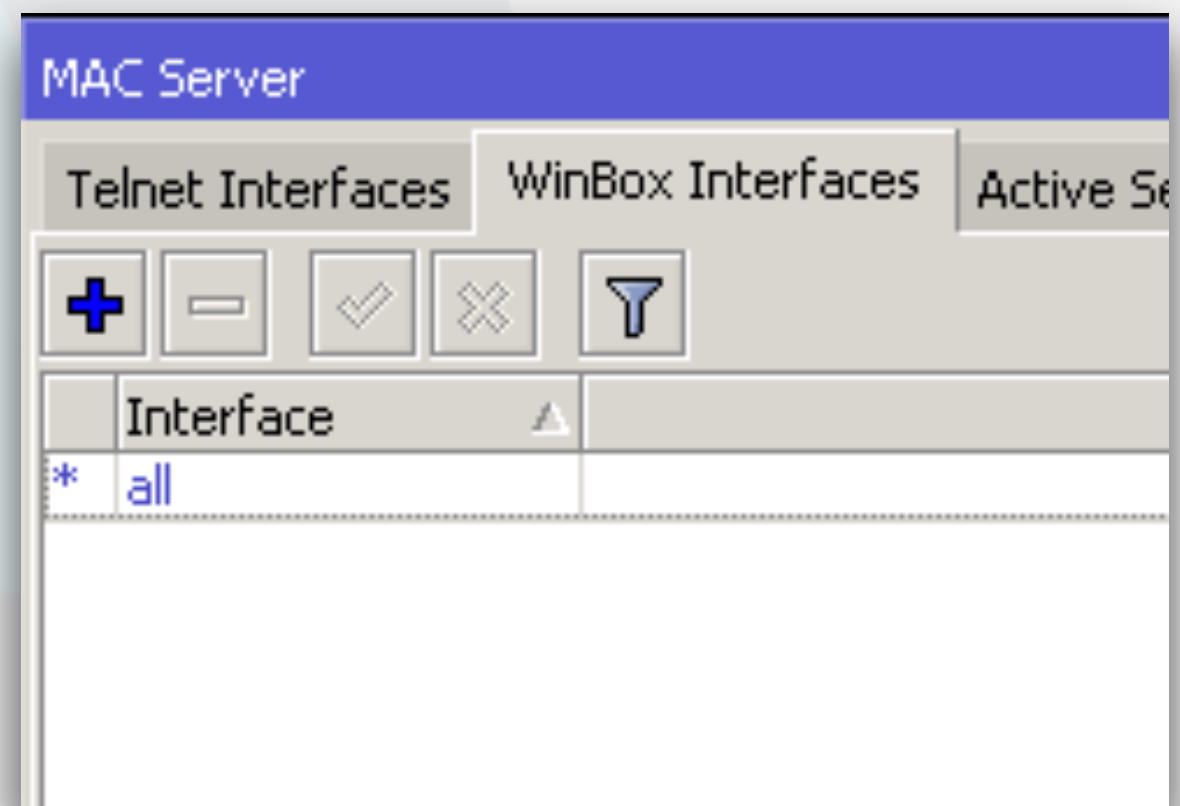
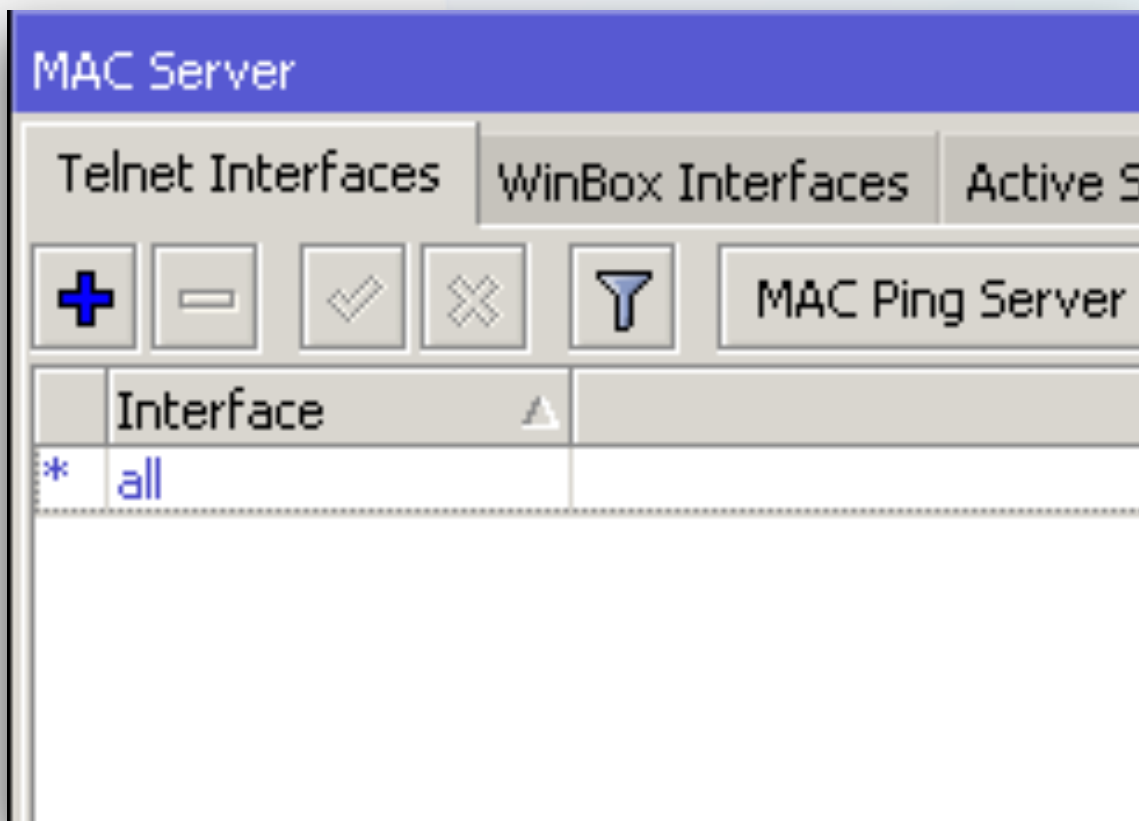
Managed Neighbors				
Find Refresh				
MAC Address	IP Address	Identity	Version	Board
00:1C:42:53:CD:36	192.168.10.10	MikroTik	6.38 (stable)	x86
D4:CA:6D:88:E1:B7	192.168.10.211	Portero IP	6.36.3 (stable)	RBmAP2n
E4:8D:8C:0A:4E:37	192.168.10.1	Router Core by MKE Solutions	6.37.1 (stable)	RB3011UiAS

- ❖ **Ip > Neighbors**

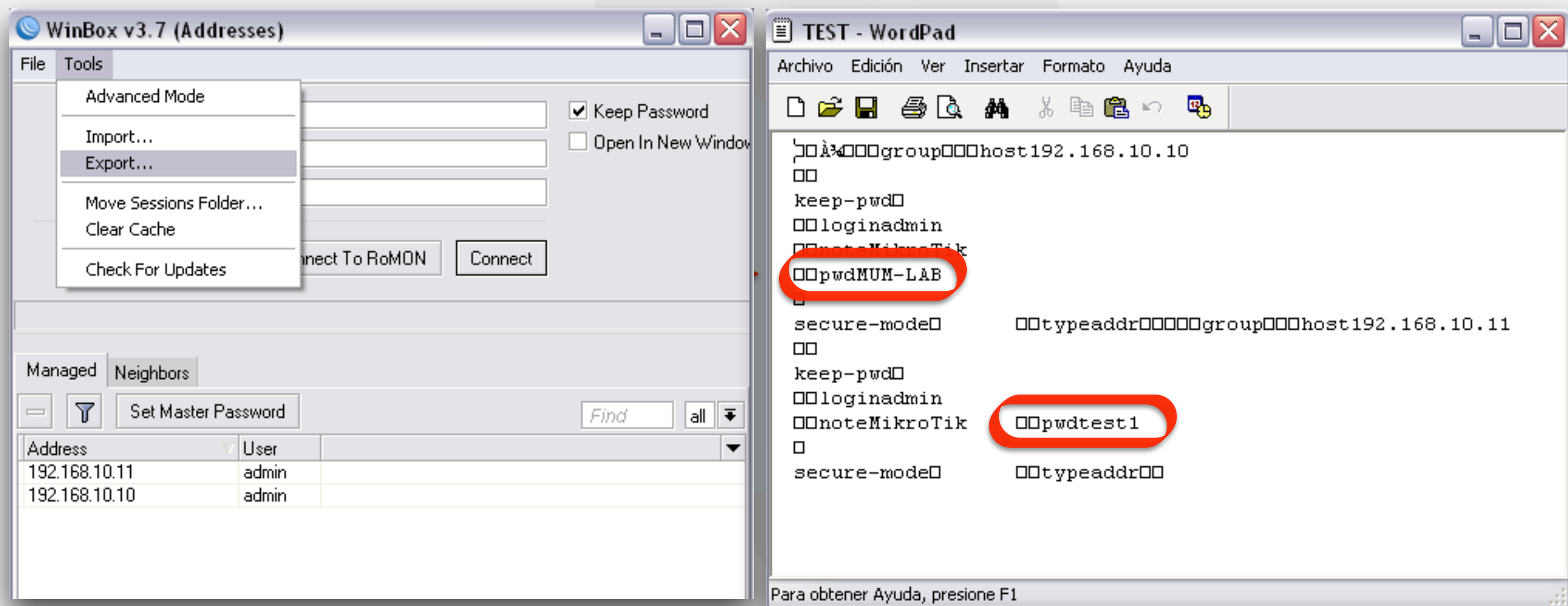
Neighbor List	
Neighbors Discovery Interfaces	
Interface	
Local	
Publica	
ether1	
ether2	
ether3	
ether4	
wlan1	

Aún deshabilitando el “Discovery Interface” se puede acceder por *Mac-Telnet* y *Mac-Winbox* sabiendo la **MAC** del equipo.

❖ Para cerrar el acceso en capa 2: *Tools > Mac Server*



Si están guardados los accesos dentro del Winbox, fácilmente se puede exportar una lista y ver la contraseña con cualquier editor de texto!!!



WinBox v3.7 (Addresses)

File Tools

- Advanced Mode
- Import...
- Export...
- Move Sessions Folder...
- Clear Cache
- Connect To RoMON
- Connect

Managed Neighbors

Set Master Password Find all

Address	User
192.168.10.11	admin
192.168.10.10	admin

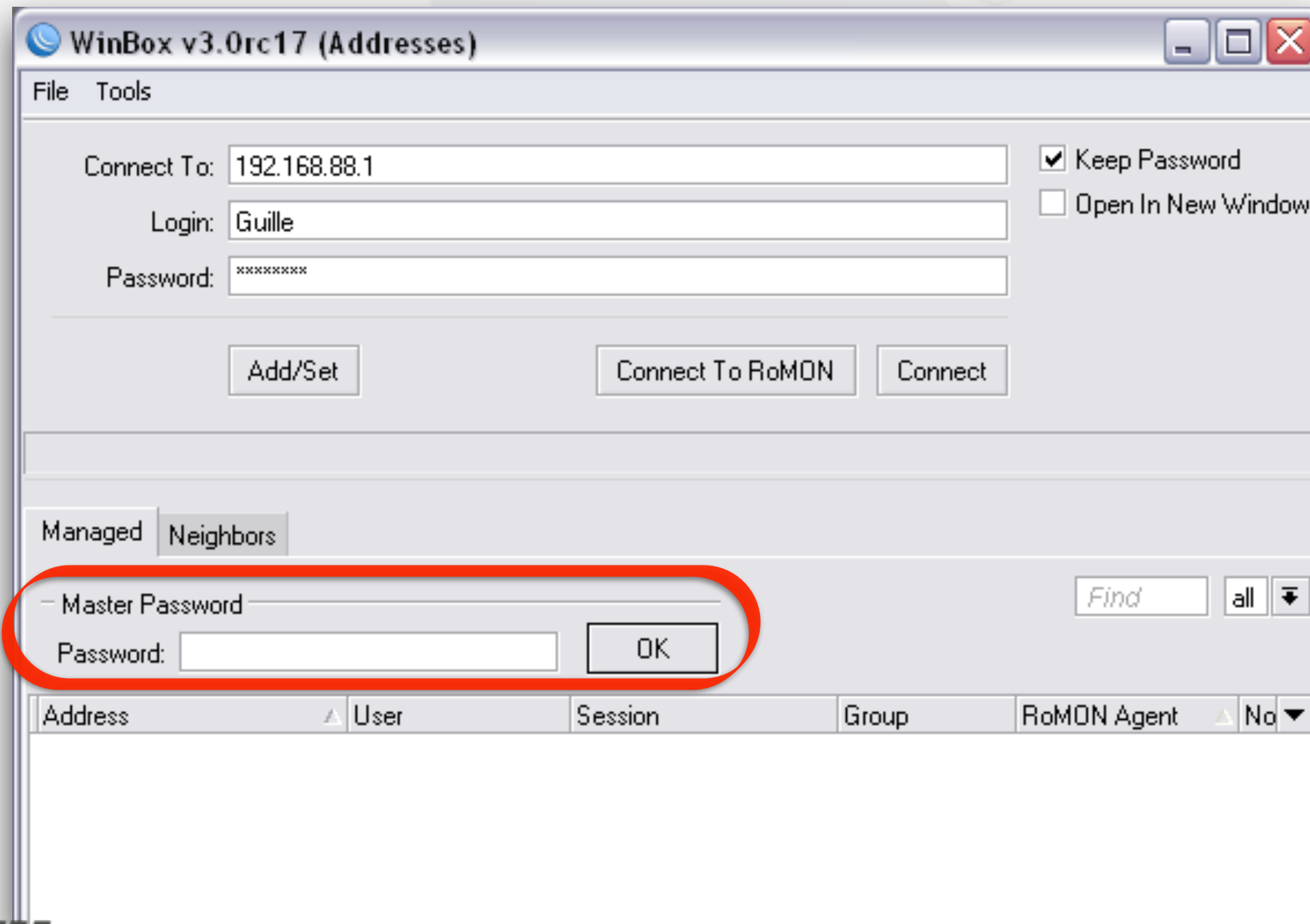
TEST - WordPad

Archivo Edición Ver Insertar Formato Ayuda

```
group host 192.168.10.10
keep-pwd
login admin
note MikroTik
pwd MUM-LAB
secure-mode type addr group host 192.168.10.11
keep-pwd
login admin
note MikroTik
pwd test1
secure-mode type addr
```

Para obtener Ayuda, presione F1

- ❖ En la versión 3, se puede setear un master password para que no muestre la lista y se pueda exportar.



The image shows the WinBox v3.0rc17 (Addresses) window. The window has a menu bar with 'File' and 'Tools'. Below the menu bar, there are three input fields: 'Connect To:' with the value '192.168.88.1', 'Login:' with the value 'Guille', and 'Password:' with the value 'xxxxxxx'. To the right of these fields are two checkboxes: 'Keep Password' (checked) and 'Open In New Window' (unchecked). Below these fields are three buttons: 'Add/Set', 'Connect To RoMON', and 'Connect'. Below the buttons, there are two tabs: 'Managed' and 'Neighbors'. Below the tabs, there is a 'Master Password' section with a 'Password:' input field and an 'OK' button. To the right of this section is a 'Find' input field and a dropdown menu with 'all' and a downward arrow. At the bottom of the window, there is a table with the following columns: 'Address', 'User', 'Session', 'Group', 'RoMON Agent', and 'No'. The table is currently empty.

Address	User	Session	Group	RoMON Agent	No
---------	------	---------	-------	-------------	----

- ❖ NUNCA actualizar porque si.
- ❖ Leer changelog y las experiencias en el foro de MikroTik

Release 6.38

2017-01-02

What's new in 6.38 (2016-Dec-30 11:33):

Important note!!!

RouterOS v6.38 contains STP/RSTP changes which makes bridges compatible with IEEE 802.1Q-2014 by sending and processing BPDU packets without VLAN tag.

To avoid STP/RSTP compatibility issues with older RouterOS versions, upgrade RouterOS to v6.38 on all routers in Layer2 networks with VLAN and STP/RSTP configurations.

The recommended procedure is to start by upgrading the remotest routers and gradually do it to the Root Bridge device.

If after upgrade you experience loss of connectivity, then disabling STP/RSTP on RouterOS bridge interface will restore connectivity so you can complete upgrade process on your network.



v6.38 [current] is released!

Posted by **stroas**, Mon Jan 02, 2017 3:41 pm » in [Announcements](#)

14,526 views



159

macgaiver

Wed Jan 11, 2017 7:32 pm

Profile (Running)

Name	Usage
idle	76.5
winbox	6.5
management	4.5
networking	3.0
firewall	2.0
ppp	2.0
dns	1.5
queuing	1.5
ethernet	1.0
unclassified	1.0
logging	0.5
bridging	0.0
flash	0.0
graphing	0.0
l2tp	0.0
p2p-matcher	0.0
profiling	0.0
routing	0.0
ssl	0.0
traffic-accounting	0.0

Torch (Running)

Interface: wan

Entry Timeout: 00:00:03 s

Collect:

- ☒ Src. Address
- ☒ Dst. Address
- ☒ MAC Protocol
- ☒ Protocol
- ☒ DSCP
- ☒ Src. Address6
- ☒ 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. ...	Pro...	Src.	Dst.	VLAN Id	DSCP	Tx Rate	Rx Rate	Tx Pack...	Rx Pack...
800 ...	6 (t...	184.107.141.20:9087	:51555			2.6 kbps	148.5 k...	5	14
806 ...						0 bps	39.8 kbps	0	83
800 ...	47	187.189.147.70				1760 bps	5.7 kbps	2	5
800 ...	6 (t...	64.233.186.125:5222	:64445			5.8 kbps	5.4 kbps	11	10
4 (8...						0 bps	1856 bps	0	2
800 ...	2 (i...	192.168.0.1			48	0 bps	1440 bps	0	3
800 ...	2 (i...	192.168.0.1			48	0 bps	1440 bps	0	3
800 ...	17 ...	8.8.4.4:53 (dns)	:53373			648 bps	1176 bps	1	1
800 ...	17 ...	190.104.143.50:1701 (l2tp)	:1701 (l2tp)			928 bps	976 bps	2	2
800 ...	47	179.60.254.46				496 bps	976 bps	1	2
800 ...	1 (i...	8.8.8.8				944 bps	944 bps	1	1
800 ...	6 (t...	190.0.22.98:51241	:3 (https)			592 bps	624 bps	1	1
800 ...	6 (t...	190.0.22.98:51893	:3 (https)			592 bps	624 bps	1	1
800 ...	17 ...	64.233.186.189:443 (htt...	:53224			528 bps	600 bps	1	1
800 ...	6 (t...	179.41.15.50:44292	:3 (pptp)			1184 bps	592 bps	2	1

191 items Total Tx: 28.0 kbps Total Rx: 222.0 kbps Total Tx Packet: 50 Total Rx Packet: 152

Oct/30/2015 15:10:21	memory	system, info	changed snmp settings by admin
Oct/30/2015 15:27:05	memory	system, error, critical	login failure for user admin from 192.168.88.179 via winbox
Oct/30/2015 15:44:18	memory	system, info, account	user admin logged out from 192.168.10.4 via winbox
Oct/30/2015 15:47:11	memory	system, info, account	user admin logged in from 192.168.10.4 via winbox

❖ IP scan

❖ Packet Sniffer

❖ Mangle > TZSP

❖ Netflow / IPFIX / Port Mirror

❖ Add src / dst to address-list

IP Scan (Running)

Interface:

Address Range: 172.16.0.2

Address	MAC Address	Time (ms)	DNS
172.16.0.2	60:EB:69:B1:6E:32	17	
172.16.0.2	00:0C:42:8C:D2:D6	0	

2 items

New Mangle Rule

General Advanced Extra Action Statistics

Action: sniff TZSP

☐ Log

Log Prefix:

Sniff Target: 0.0.0.0

Sniff Target Port: 0

Firewall

Filter Rules NAT Mangle Service Ports Connections Address Lists

+ - ✓ ✗ 

	Name	Address	Timeout
D	Ataques SIP	66.240.192.138	00:22:22
D	Ataques SIP	66.240.236.119	00:35:58
D	Ataques SIP	71.6.135.131	00:31:02
D	Ataques SIP	71.6.146.185	00:05:46
D	Ataques SIP	71.6.158.166	00:32:01
D	Ataques SIP	83.35.66.73	00:42:28
D	Ataques SIP	134.119.215.49	00:06:11
D	Ataques SIP	158.69.53.12	00:57:38

- ❖ Leer!
- ❖ Implementar
- ❖ Fallar
- ❖ Volver a Leer
- ❖ Corregir
- ❖ Testear
- ❖ Documentar!

Main Page

Welcome to the MikroTik Wiki!

This is a place where users of MikroTik solutions share information, examples, howtos and ideas with each other.

This resource consists of both User Maintained How-To articles, and also MikroTik maintained documentation pages.

Choose your category below:



MikroTik RouterOS

Documentation



RouterBOARD hardware

RouterBOARD hardware Pages



MikroTik User Manager

MikroTik User Manager



RouterOS User Topics

Articles and Examples written by users



MikroTik News

News and related information



MUM Events

MikroTik User Meetings around the world



The Dude

The Dude



SwOS

SwOS for MikroTik Switch products

RouterOS

	RouterOS v6 RC and v7 BETA BETA Testing and Feature Suggestions for the next RouterOS release (ROS v7)	4,774 Topics	33,968 Posts
	Beginner Basics If you installed RouterOS just now, and don't know where to start - ask here!	16,447 Topics	74,272 Posts
	General RouterOS general discussion	47,440 Topics	231,382 Posts
	Forwarding Protocols BGP, OSPF, MPLS, MME, RIP, HWMPPplus	3,027 Topics	14,934 Posts
	Wireless Networking Wireless networks	13,050 Topics	73,915 Posts
	Scripting RouterOS Scripting and API	6,081 Topics	28,367 Posts
	Virtualization CHR, MetaRouter, KVM, Xen and other virtual systems that run RouterOS	457 Topics	4,290 Posts

¿Preguntas?

MUCHAS GRACIAS!

Ing. Mario Clep
MKE Solutions



- marioclep@mkesolutions.net



- marioclep



- @marioclep

