MUM MikroTik User Meeting

Tips para Principiantes

Ing. Mario Clep
MKE Solutions

20 de Enero de 2017

Ciudad de Guatemala

Guatemala

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**
  - Entrenamientos Oficiales
  - Soporte IT

info@mkesolutions.net

@mkesolutions

/mkesolutions

/mkesolutions

Entrenamientos Oficiales

- Certificaciones Disponibles

MTCNA

MTCUME

MTCTCE

MTCWE

MTCRE

MTCINE

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

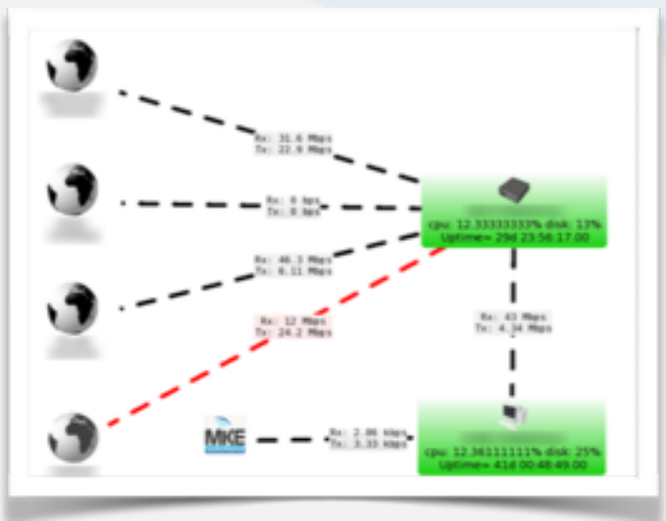
powered by Mke Solutions

Academia DE ENTRENAMIENTOS

Felicitaciones!!!

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



Introducción y Objetivos

¿Quienes son principiantes?

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

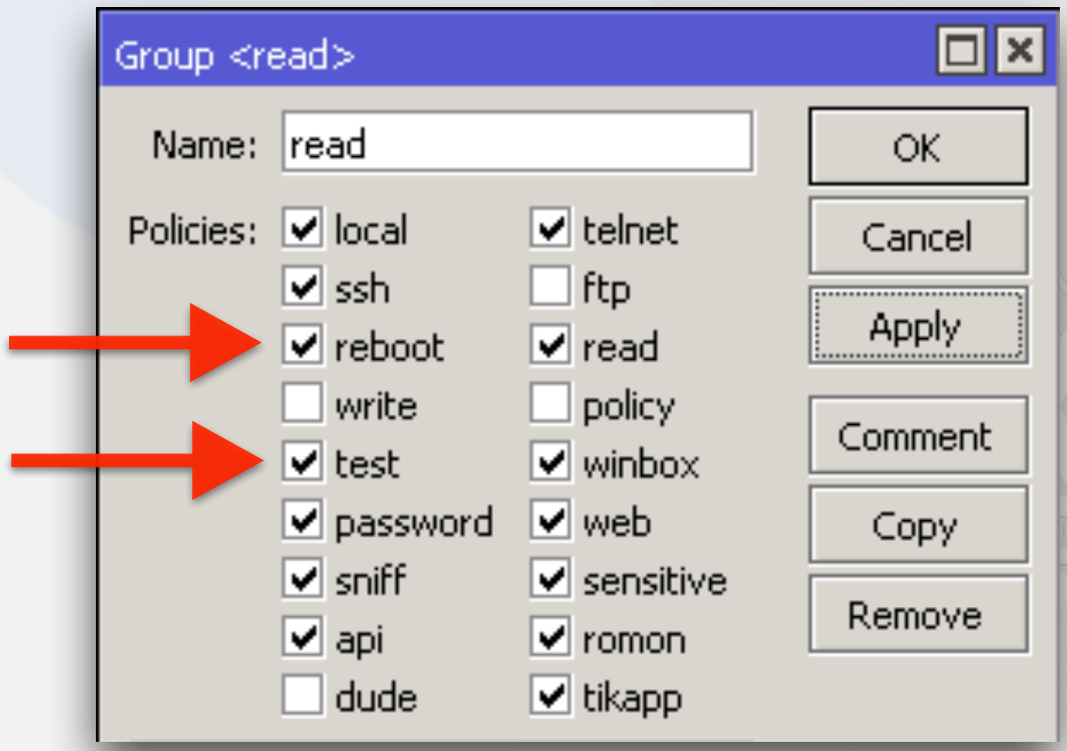
- Mostrar los descuidos mas comunes que encuentro cuando los clientes solicitan un relevamiento.
- Demostrar que con "unos pocos clics" se pueden mejorar las configuraciones, incrementando la seguridad y reduciendo las posibles fallas.

Usuario por Default

- 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.

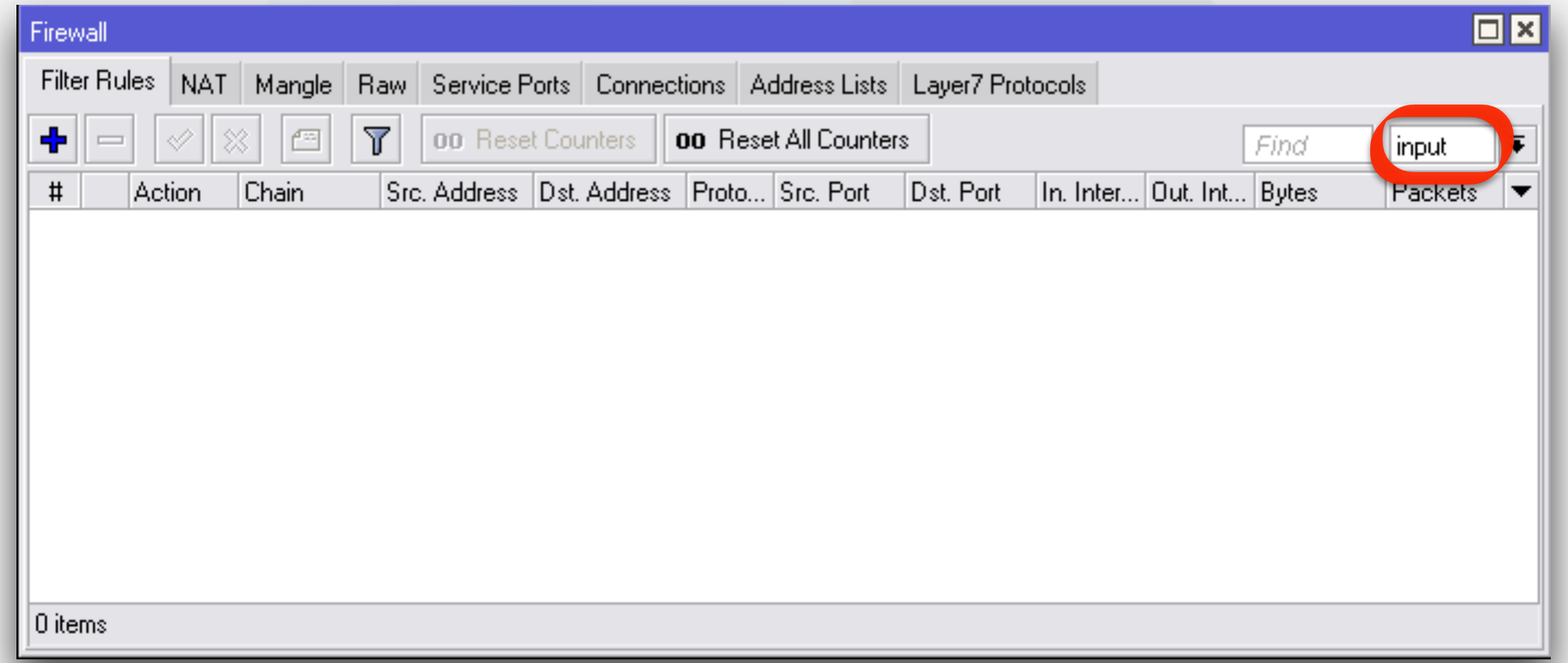
- A veces, la única medida es poner el usuario admin en el perfil ***read*** y crear un nuevo usuario y contraseña con permisos FULL.

- *El grupo por defecto del usuario de sólo lectura tiene los permisos de REBOOT y TEST.*



Firewall

- 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).



Ataques por fuerza bruta

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

Ataques al DNS

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

Ataque al WebProxy

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:

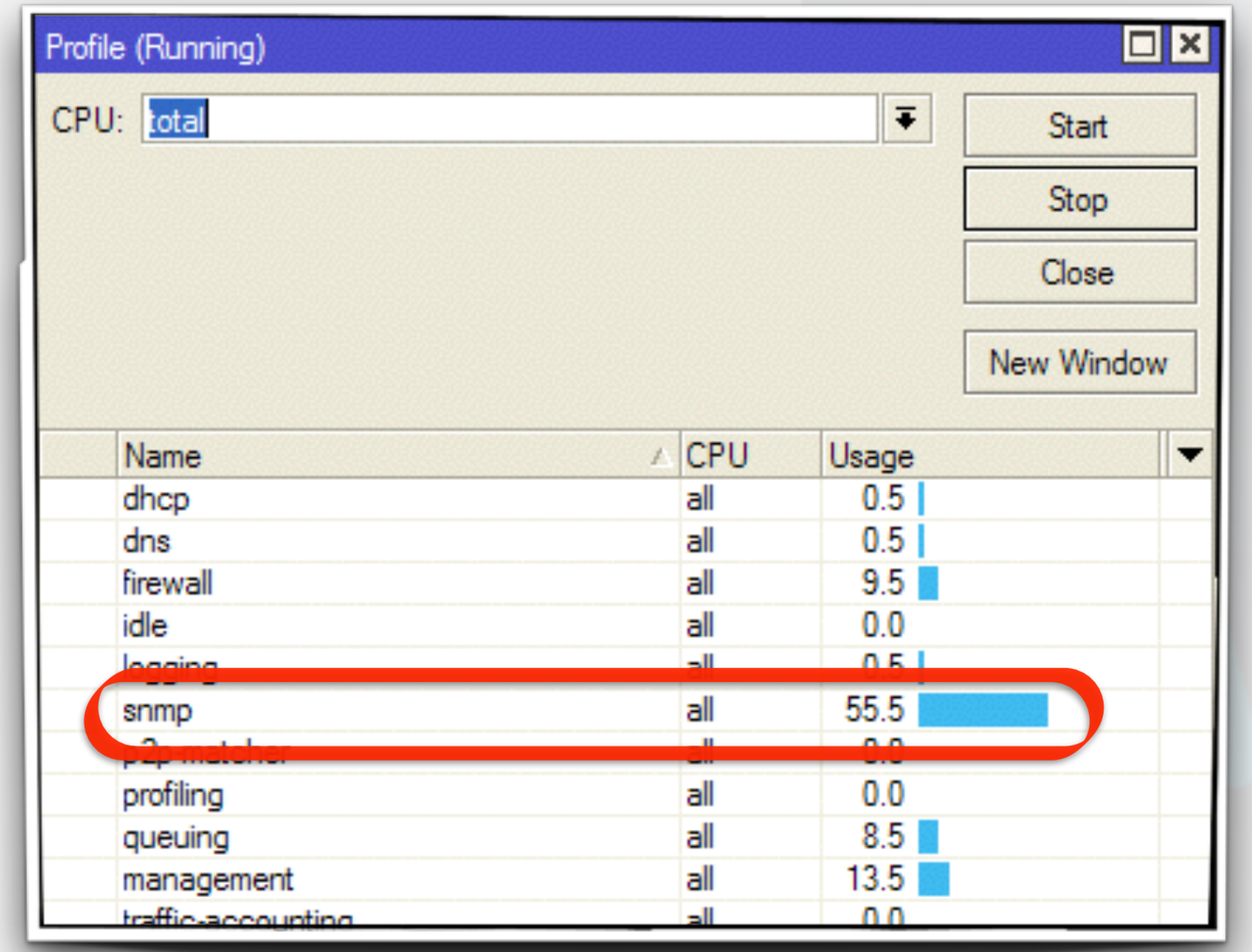
Enviar

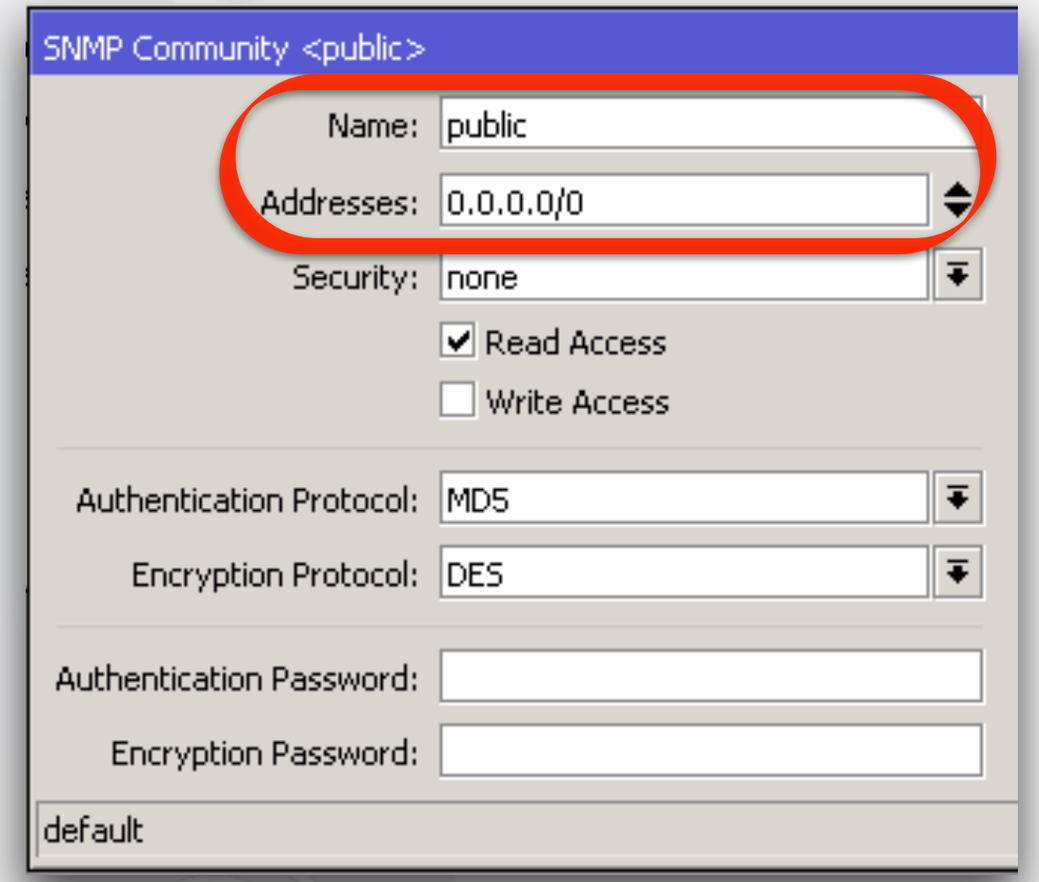
Acerca de esta página

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

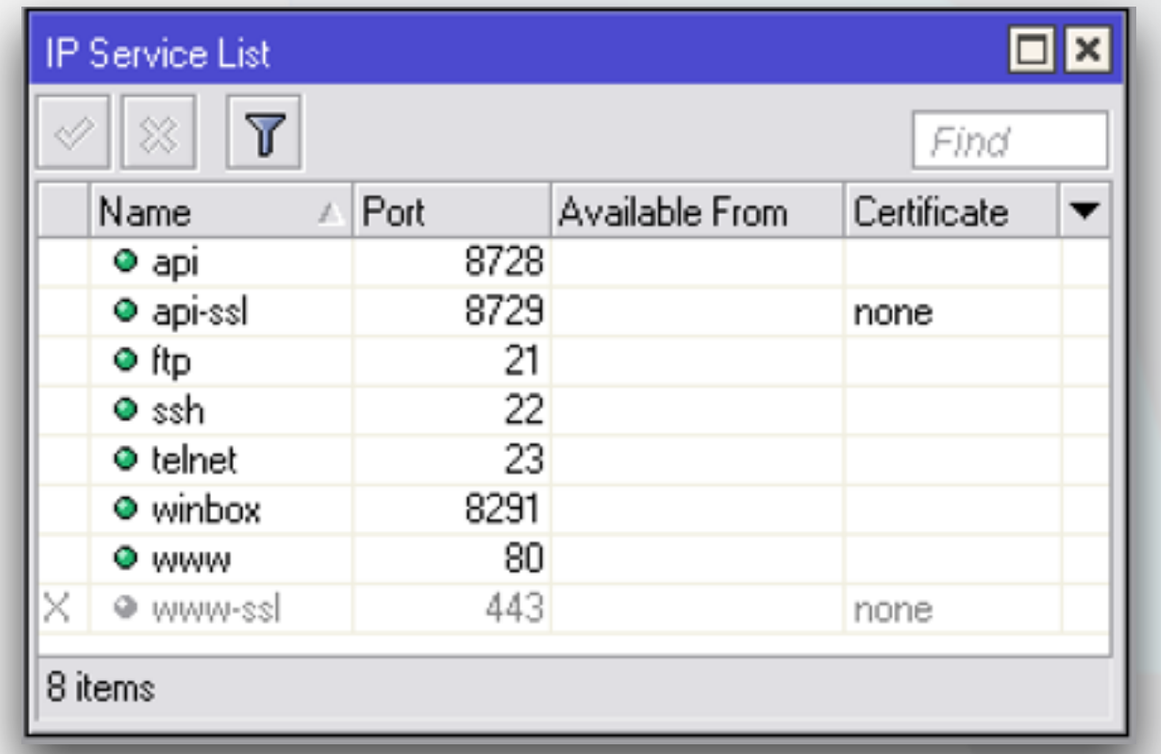
Al habilitar el servicio de ***SNMP***, por defecto el router queda expuesto a cualquier consulta por cualquiera de sus interfaces.

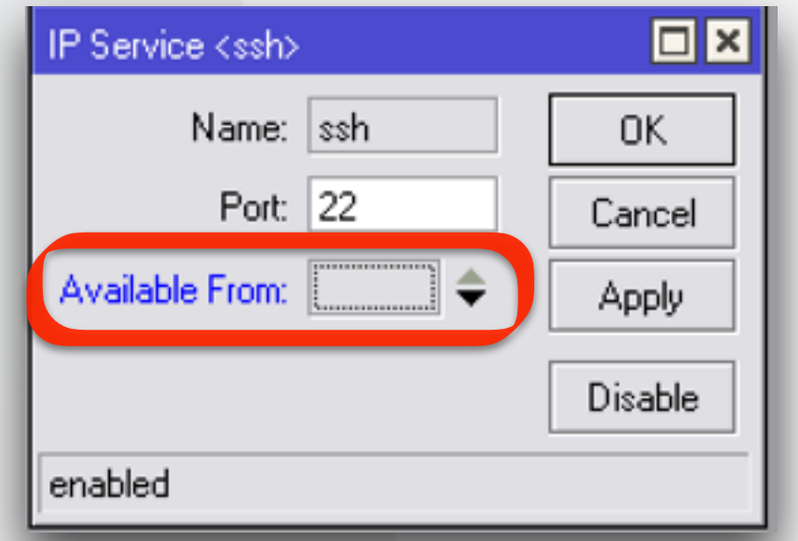




IP > Services

- 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***

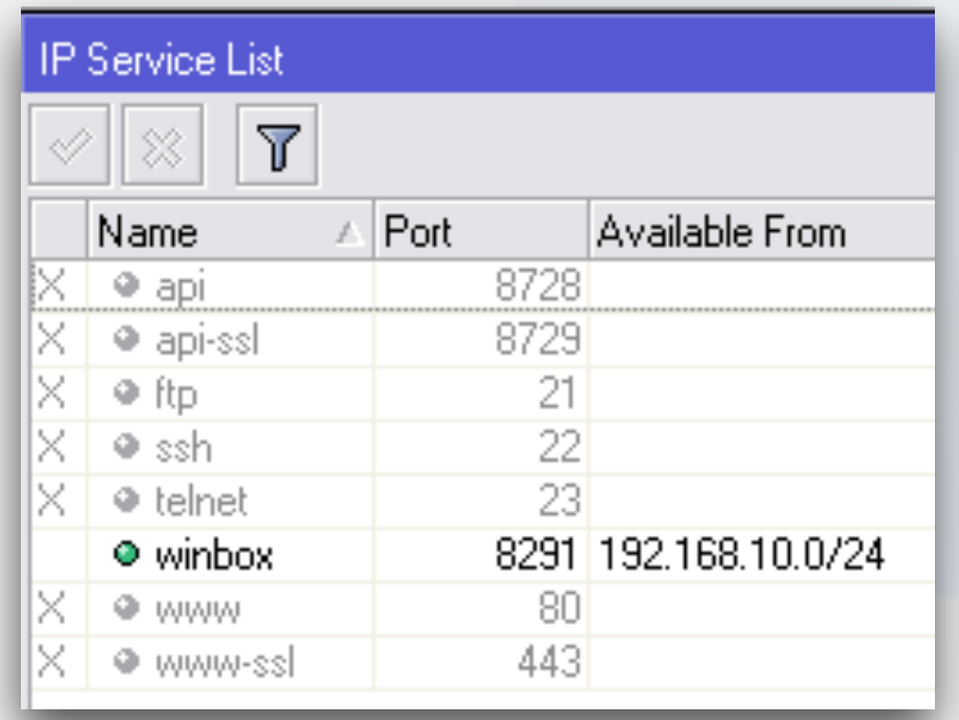


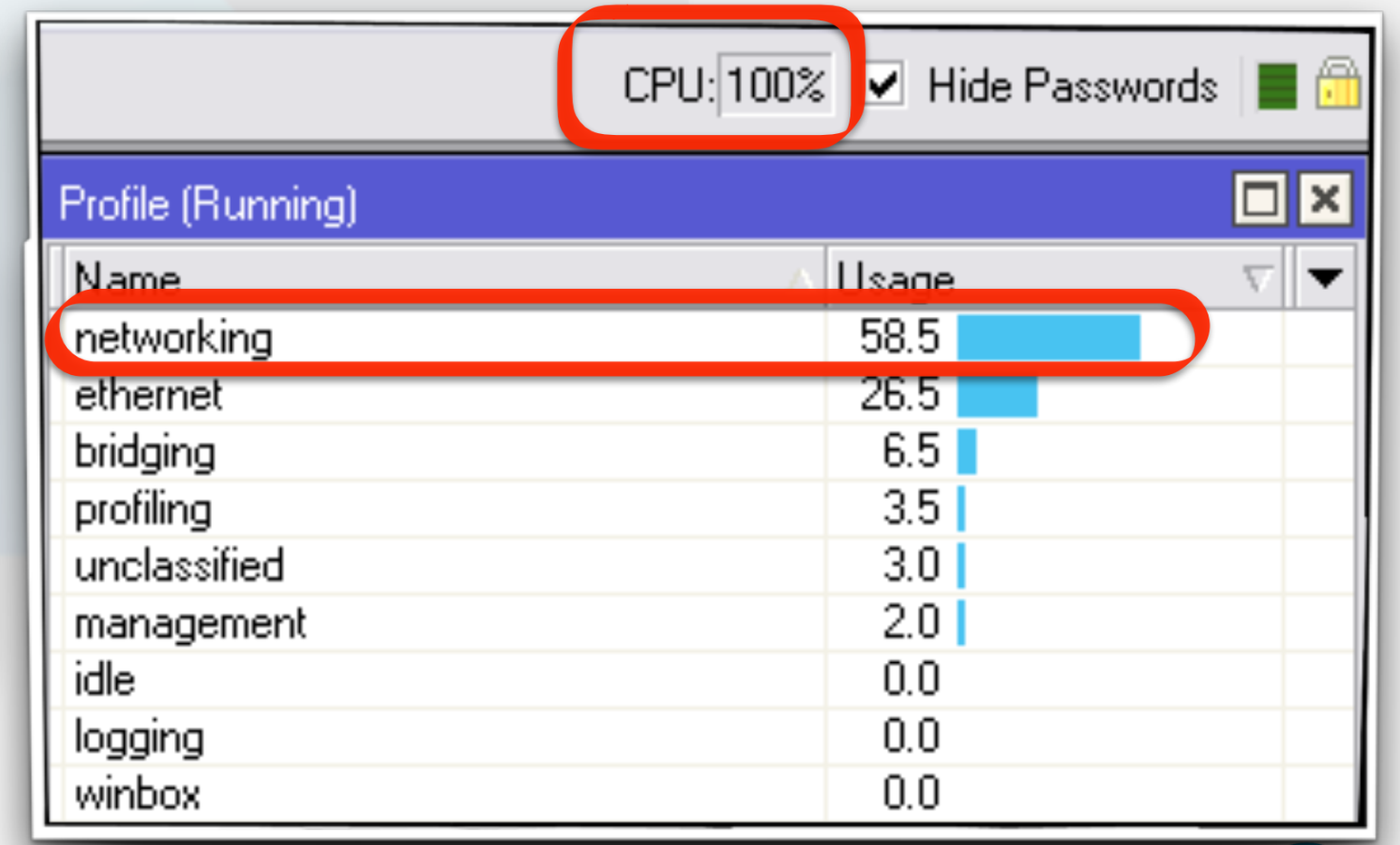


Otros Servicios

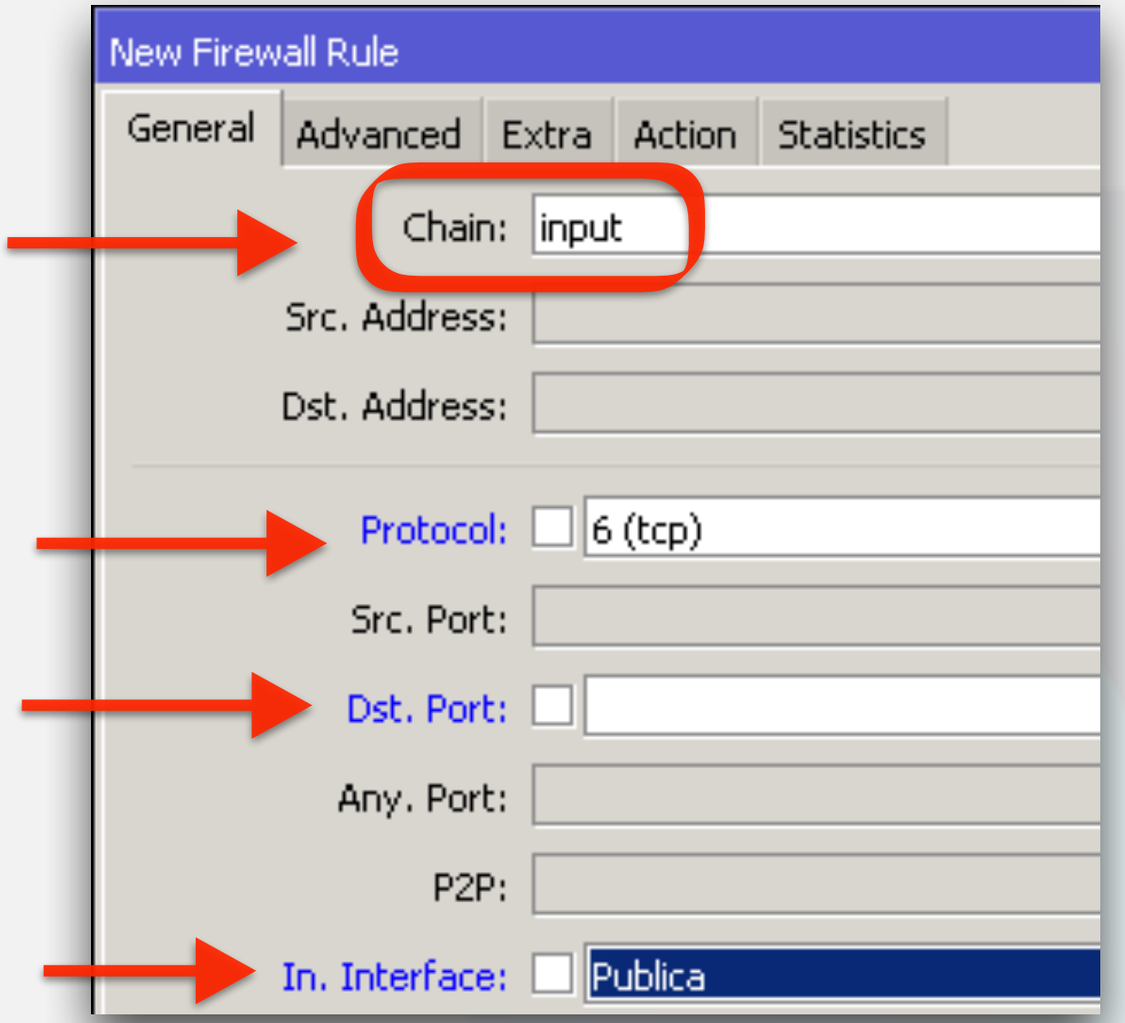
Tener deshabilitados todos los servicios no garantiza que el router esté 100% protegido.

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

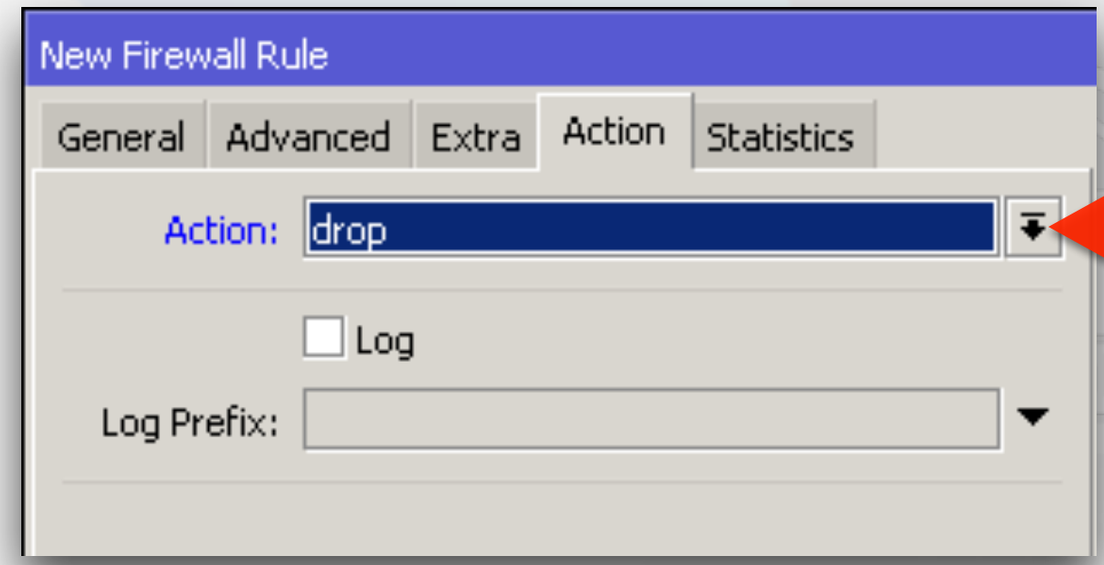




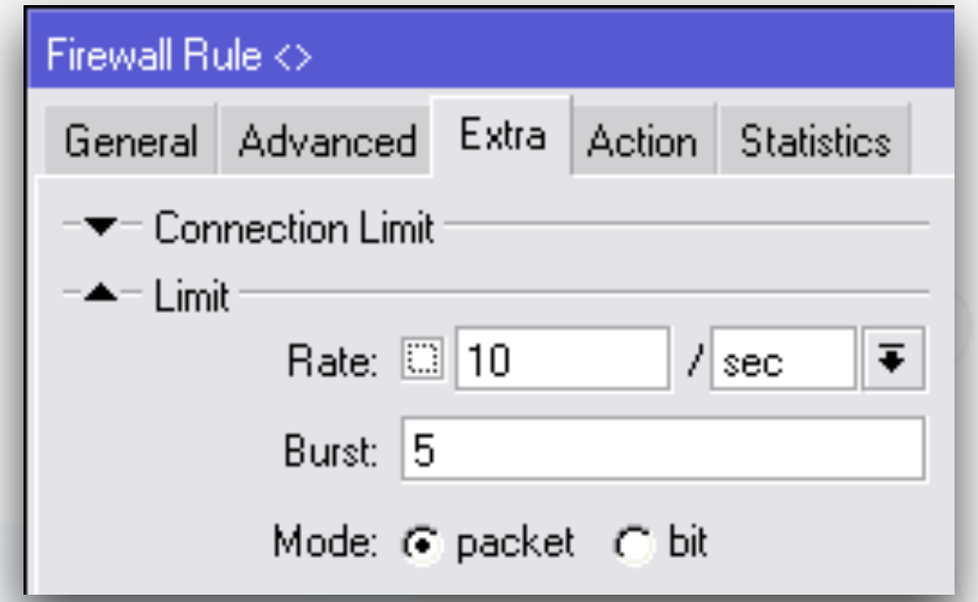
Protección con Firewall

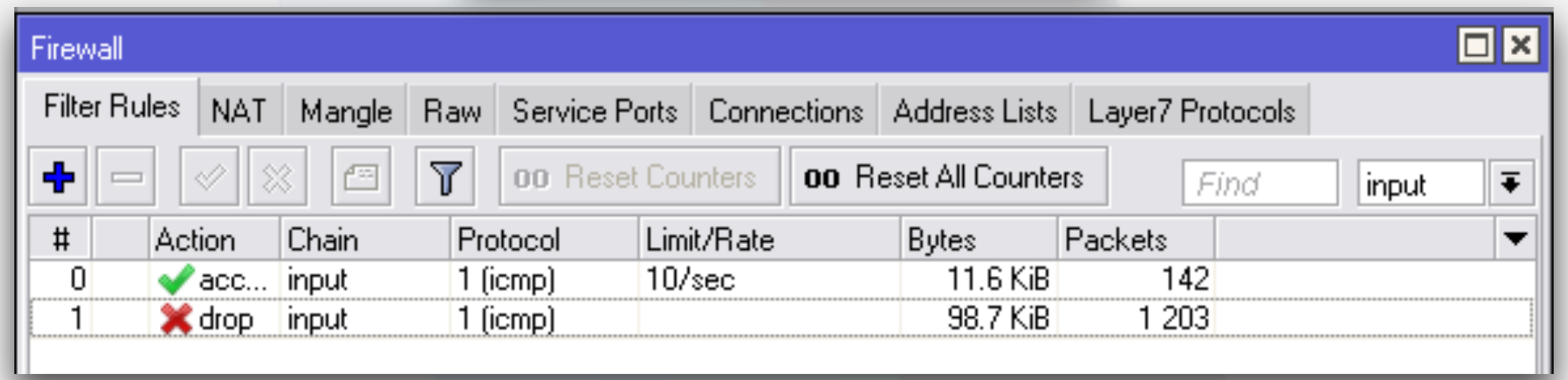


- ***SSH:*** TCP 22
- ***Telnet:*** TCP 23
- ***WEB:*** TCP 80
- ***Winbox:*** TCP 8291
- ***WebProxy:*** TCP 8080
- ***DNS:*** UDP 53
- ***SNMP:*** UDP 161



Ping Flooding






```
/ip firewall filter
add action=accept chain=input limit=10,5:packet protocol=icmp
add action=drop chain=input protocol=icmp
```

Recomendaciones Generales

- 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 destino 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).

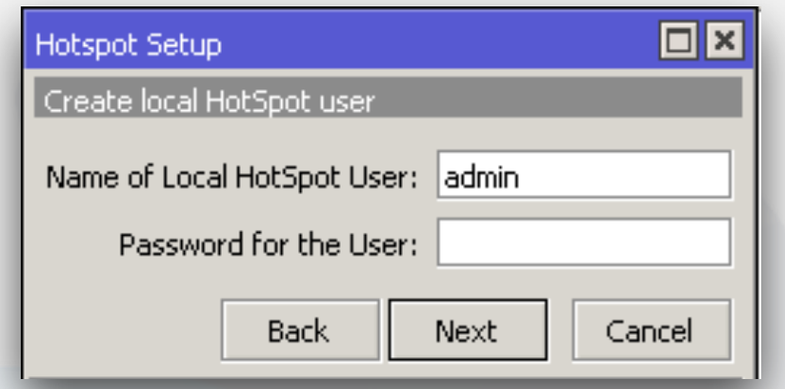
Servicios Principales a proteger

Puerto	Protocolo	Comentario
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)

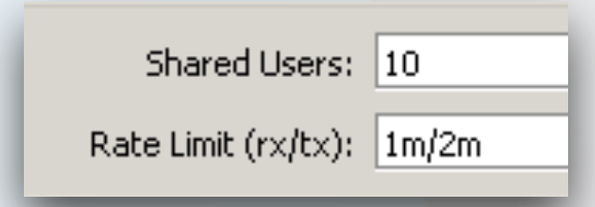
Puerto	Protocolo	Comentario
2000	TCP	Bandwidth Server
3128,8080	TCP	WebProxy
5678	UDP	Neighbour Discovery
8291	TCP	WinBox
8728	TCP	API
	1	ICMP
1701	UDP	L2tP
1723	TCP	PPtP
1812,1813	UDP	User Manager

HotSpot

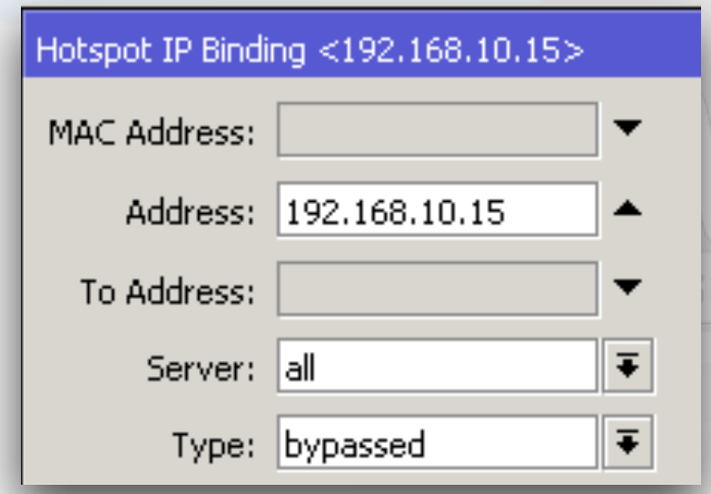
- No dejar el usuario "admin" del hotspot sin contraseña!



- El campo "shared-users" del perfil de hotspot permite que el mismo usuario pueda usarse en simultáneo N veces, pero cada uno tiene su propia queue!



- El ***bypass*** oculta el hotspot, pero no controla el ancho de banda!



Descubrimiento de Vecinos

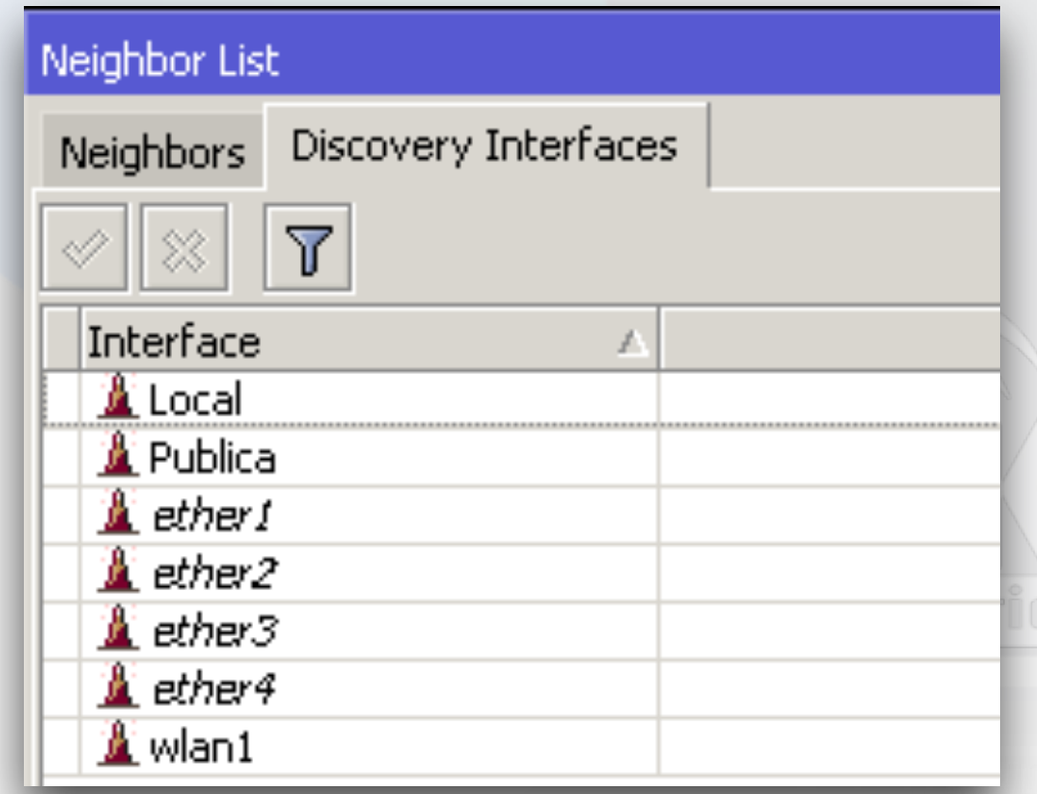
- *MNDP* está habilitado en todas sus interfaces.

Managed | Neighbors

Refresh | Find

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

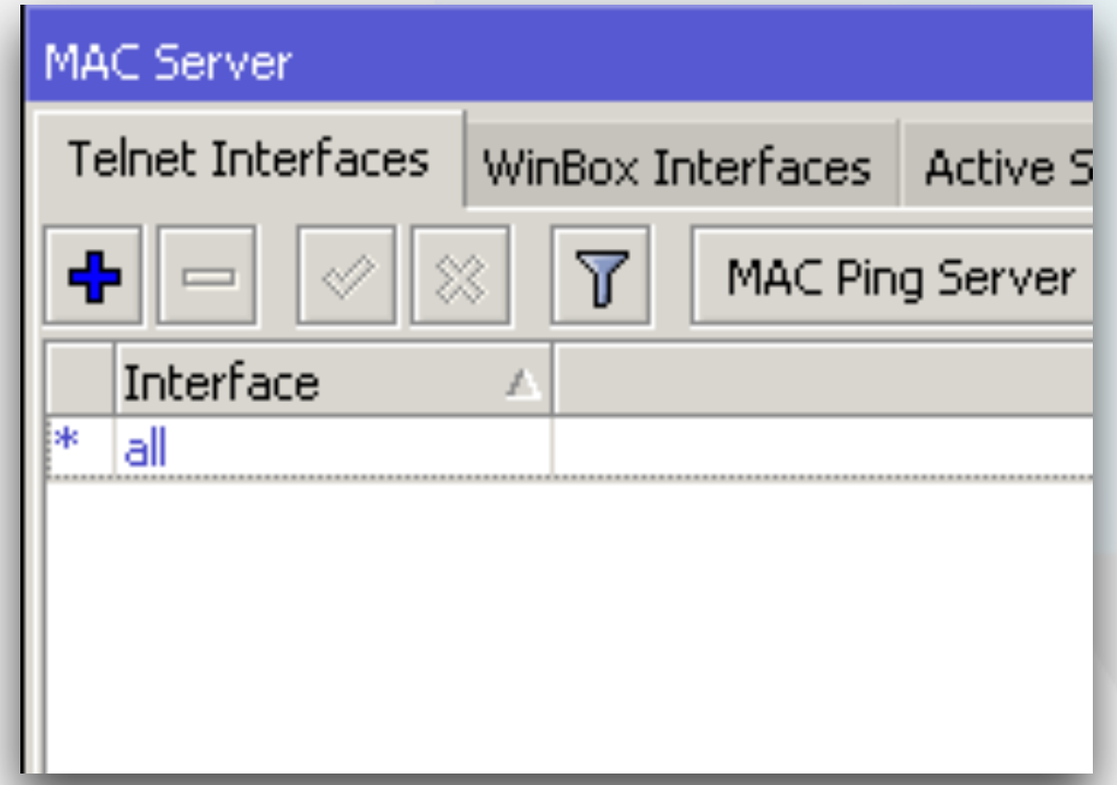
- *Ip > Neighbors*

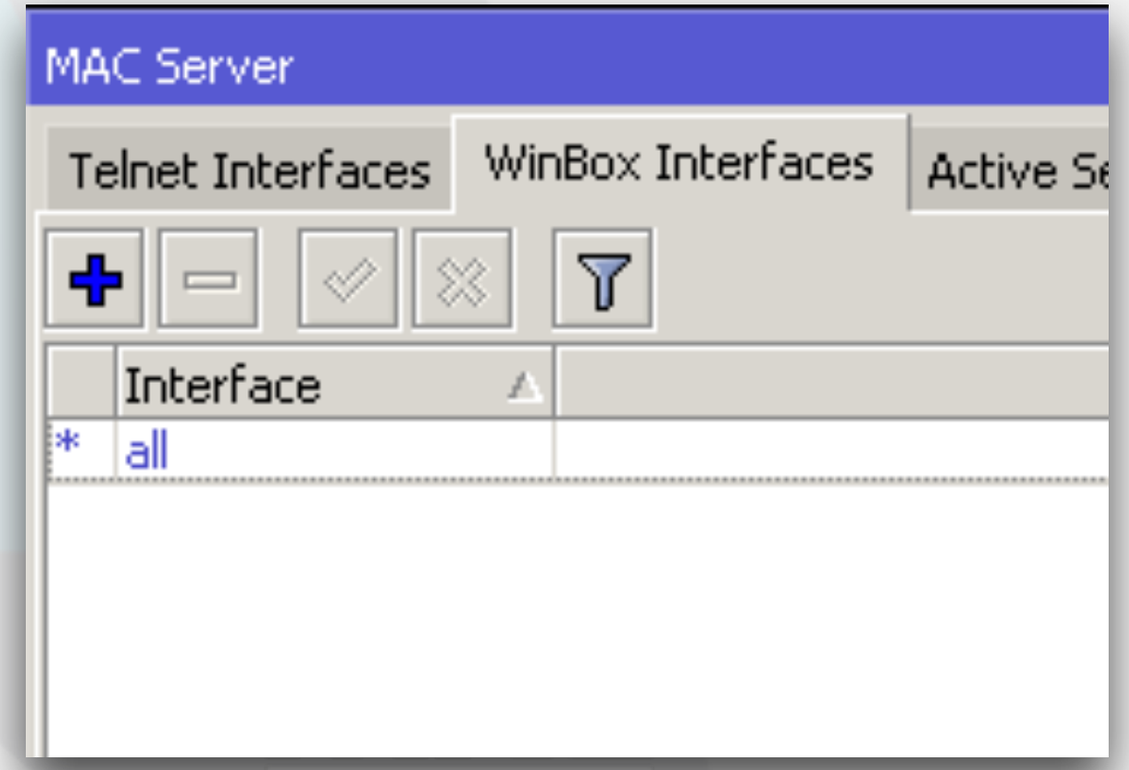


Acceso en Capa 2

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

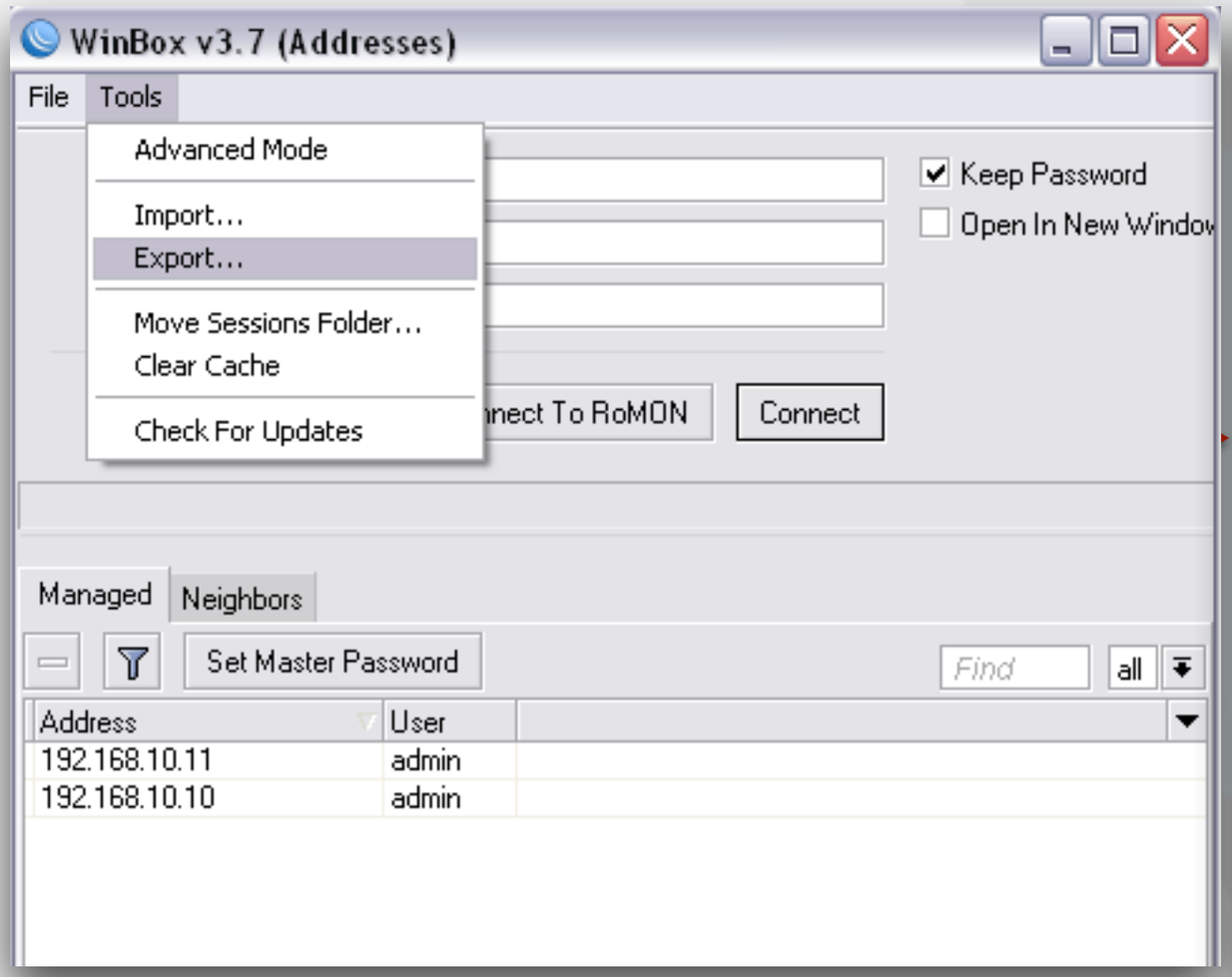
- Para cerrar el acceso en capa 2: ***Tools > Mac Server***

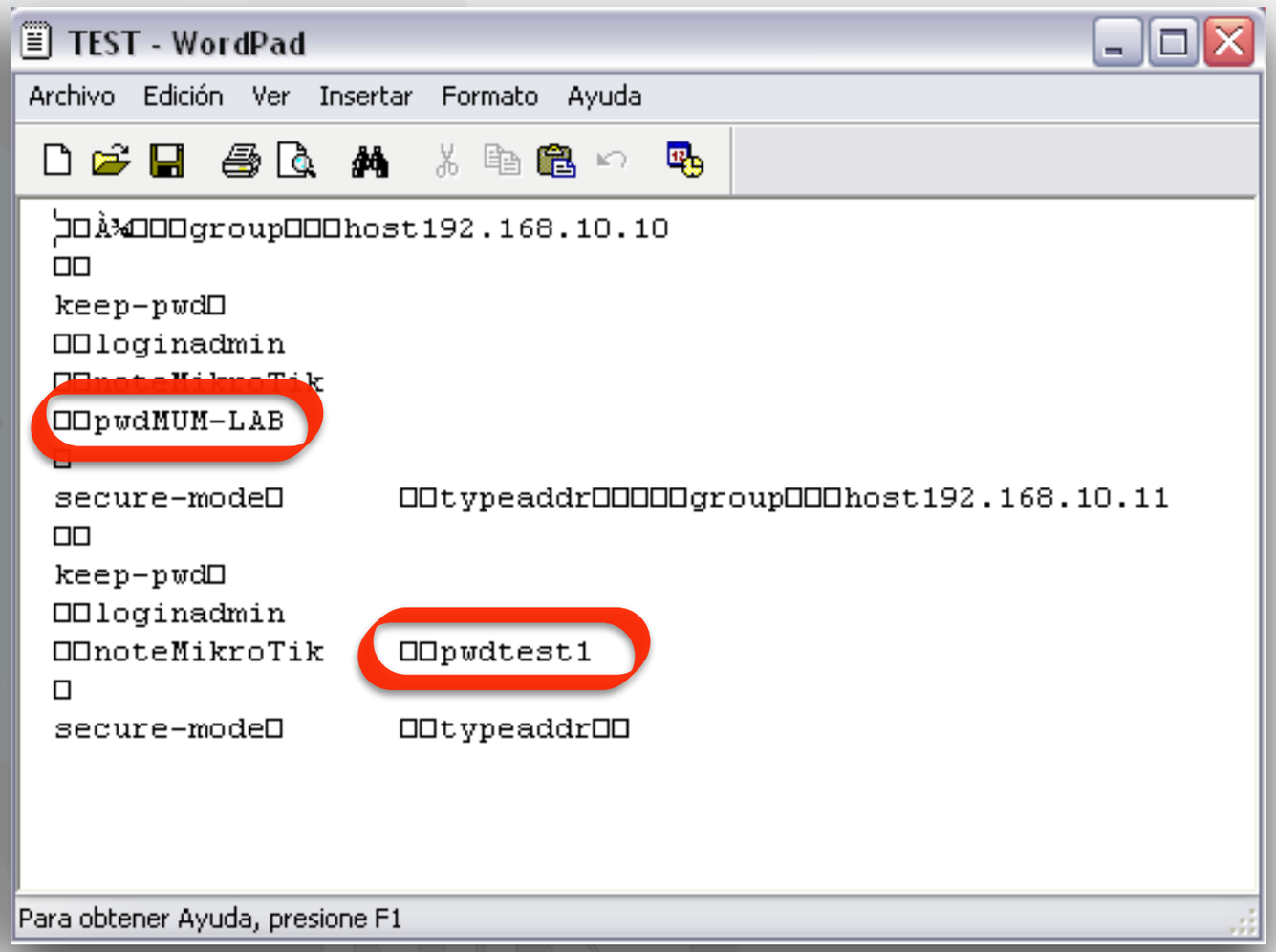




Accesos guardados en Winbox

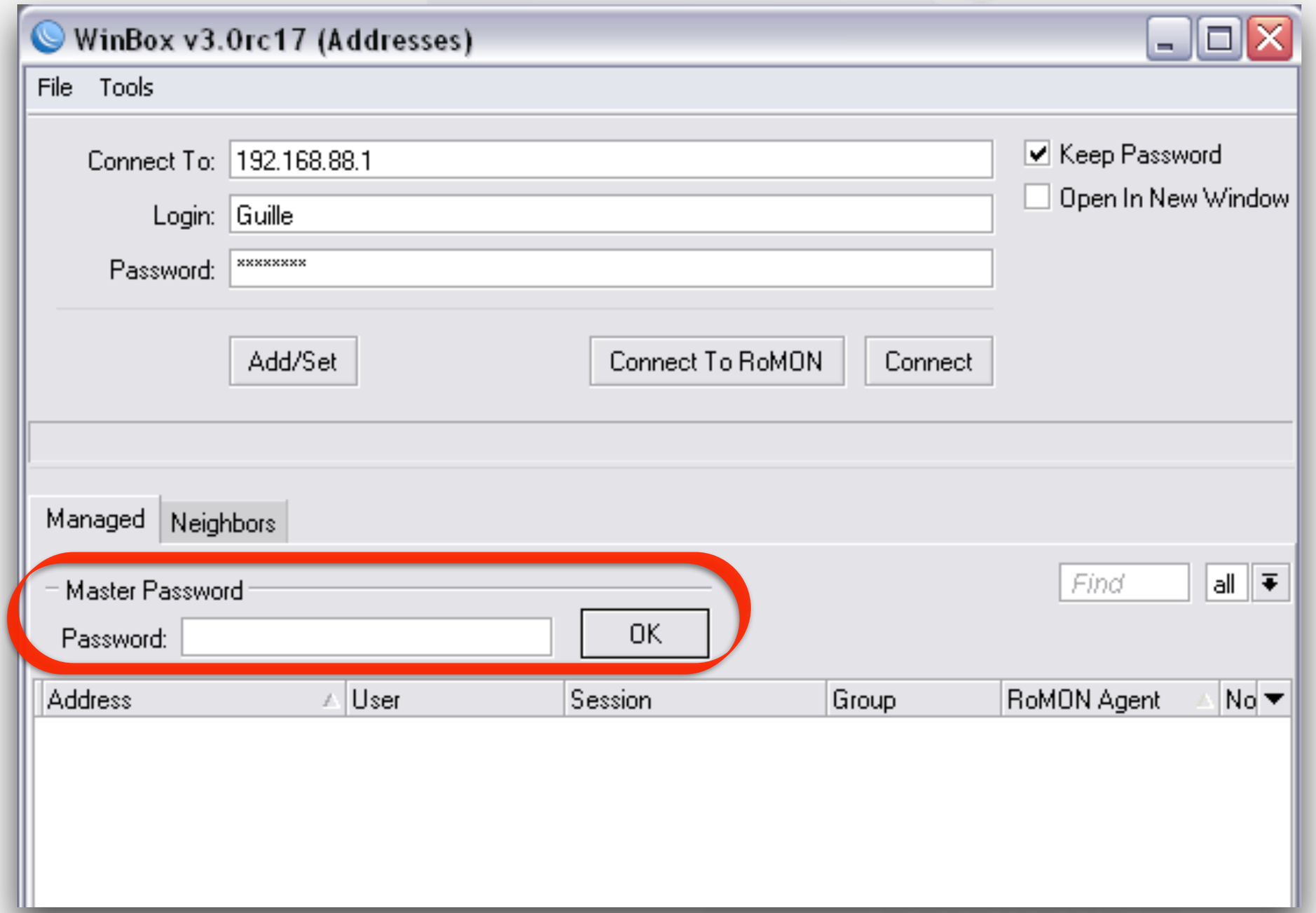
Si están guardados los accesos dentro del Winbox, fácilmente se puede exportar una lista y ver la contraseña con cualquier editor de texto!!!





Winbox v.3

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



Actualización de RouterOS

- 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.

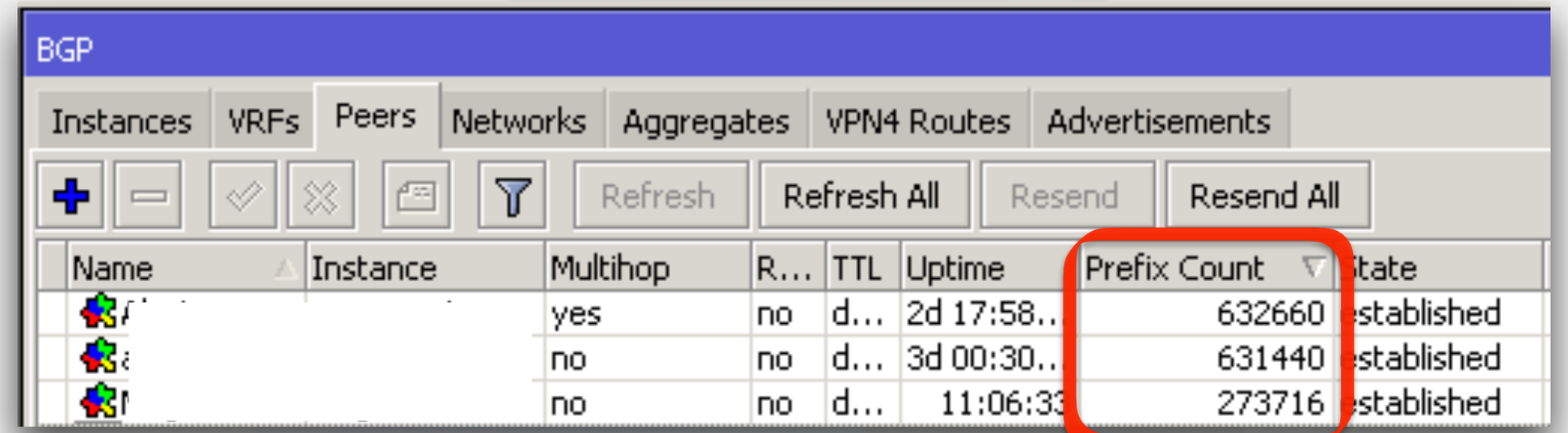
v6.38 [current] is released!
Posted by **strods**, Mon Jan 02, 2017 3:41 pm » in Announcements

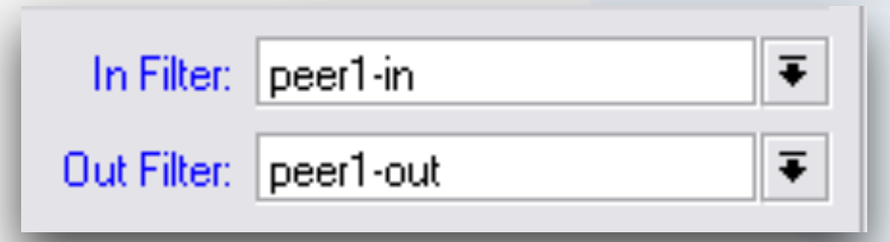
14,526 views 159

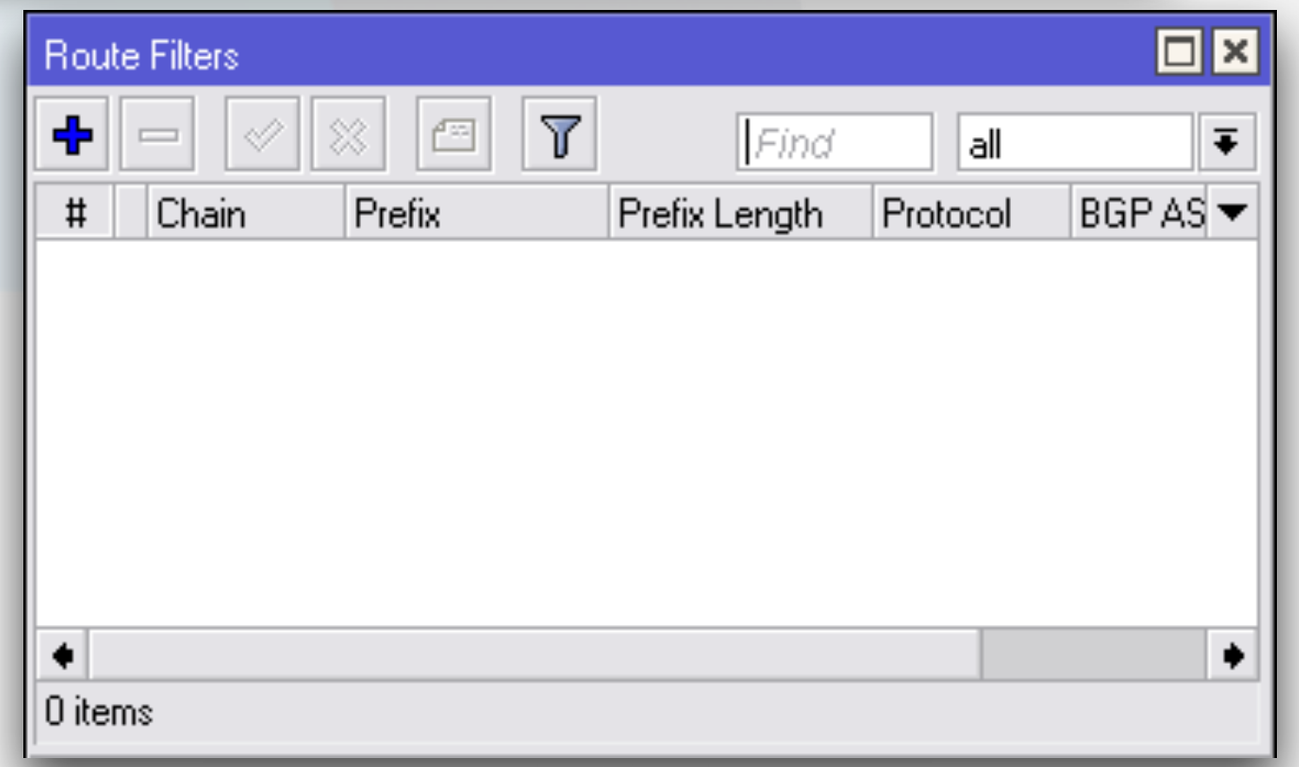
macgaiver
Wed Jan 11, 2017 7:32 pm

BGP

- Usar filtros para evitar recibir publicaciones indeseadas (in).
- Usar filtros para evitar convertirse en tránsito (out).

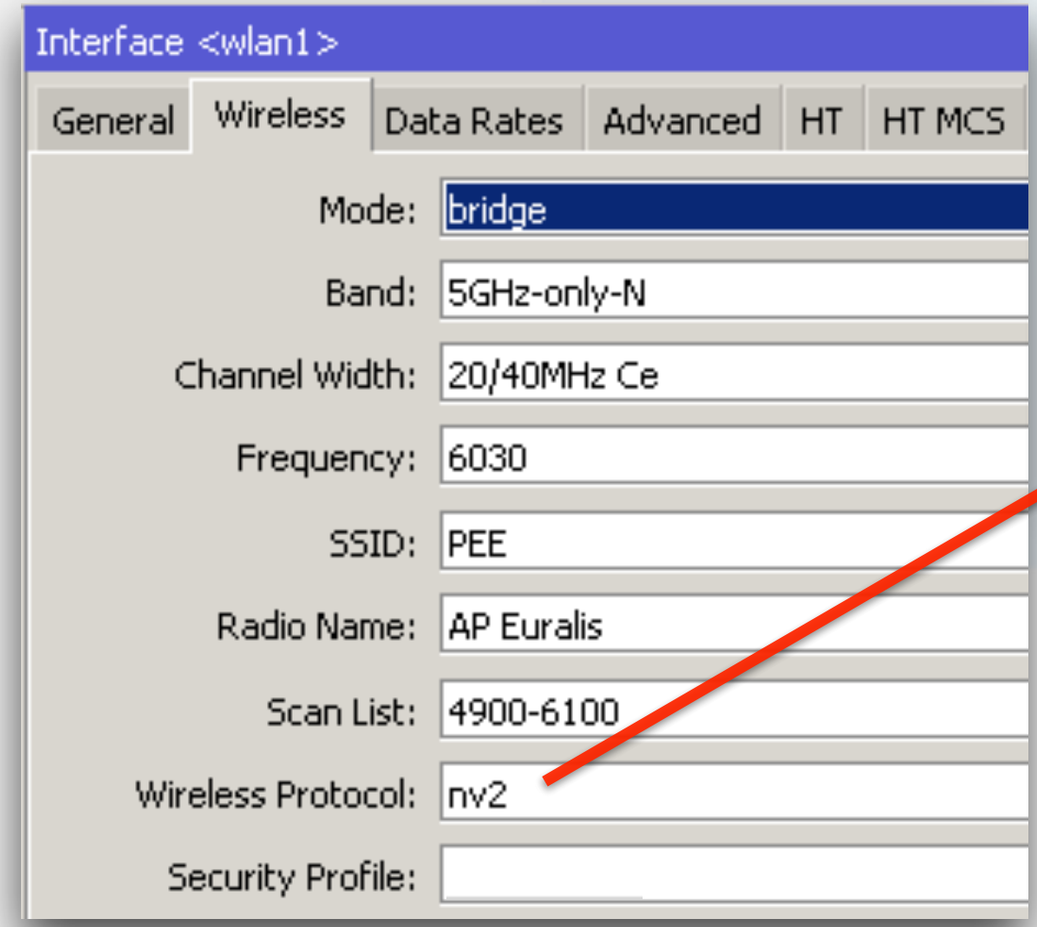


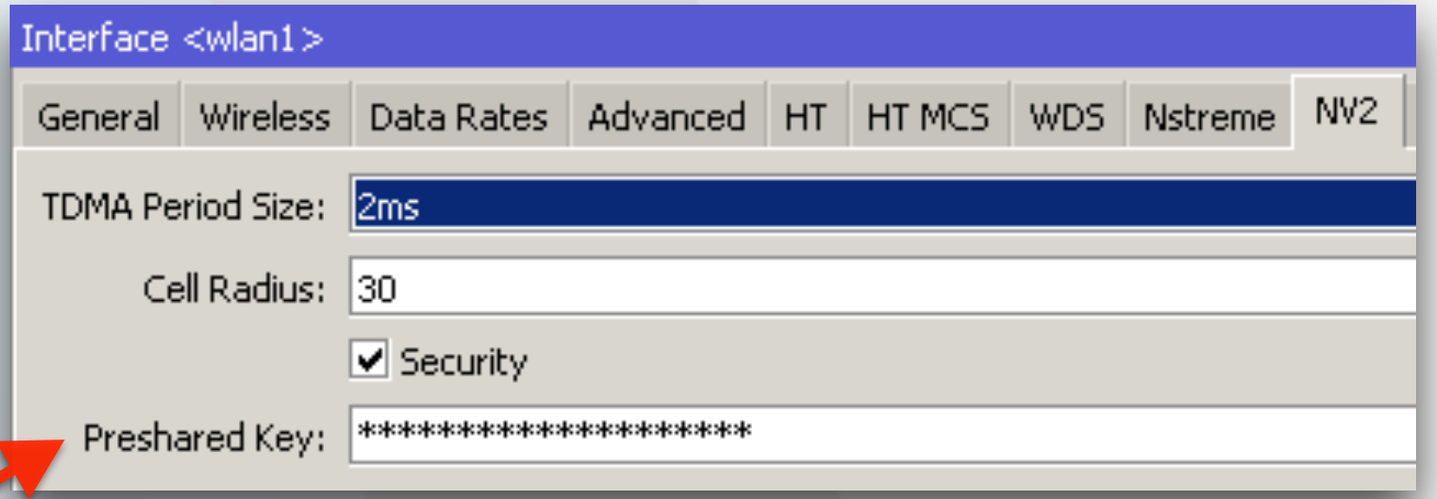




Contraseña en Nv2

- El uso de Nv2 ignora la configuración del ***security-profile***.
- La configuración de la llave compartida se hace desde la solapa de Nv2.
- En caso de no usarse, cualquier ***RouterOS*** puede enlazarse.





Herramientas Usadas

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)

Basic

Interface: wan

Entry Timeout: 00:00:03 s

Collect

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

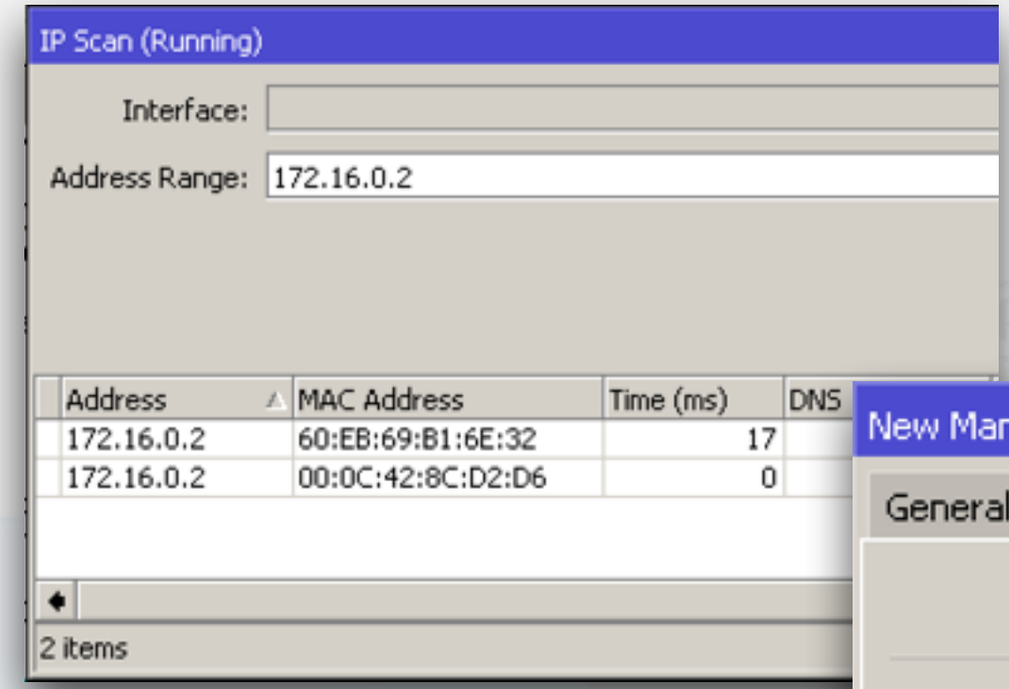
Eth. ...	Pro...	Src.	Dst.	VLAN Id	DSCP	Tx Rate	Rx Rate	Tx Pack...	Rx Pack...
800 ...	6 (t...	184.107.141.20:9087	:51555			2.6 kbps	148.5 k...	5	14
806 ...						0 bps	39.8 kbps	0	83
800 ...	47	187.189.147.70				1760 bps	5.7 kbps	2	5
800 ...	6 (t...	64.233.186.125:5222	:64445			5.8 kbps	5.4 kbps	11	10
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	(https)			592 bps	624 bps	1	1
800 ...	6 (t...	190.0.22.98:51893	(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

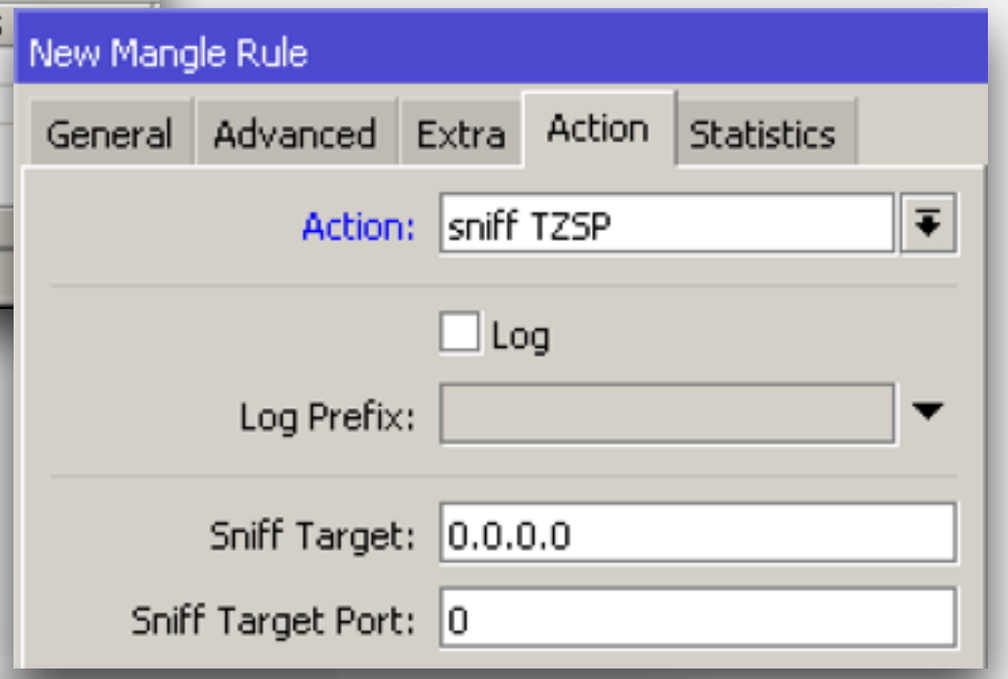
191 items | Total Tx: 28.0 kbps | Total Rx: 222.0 kbps | Total Tx Packet: 50 | Total Rx Packet: 152

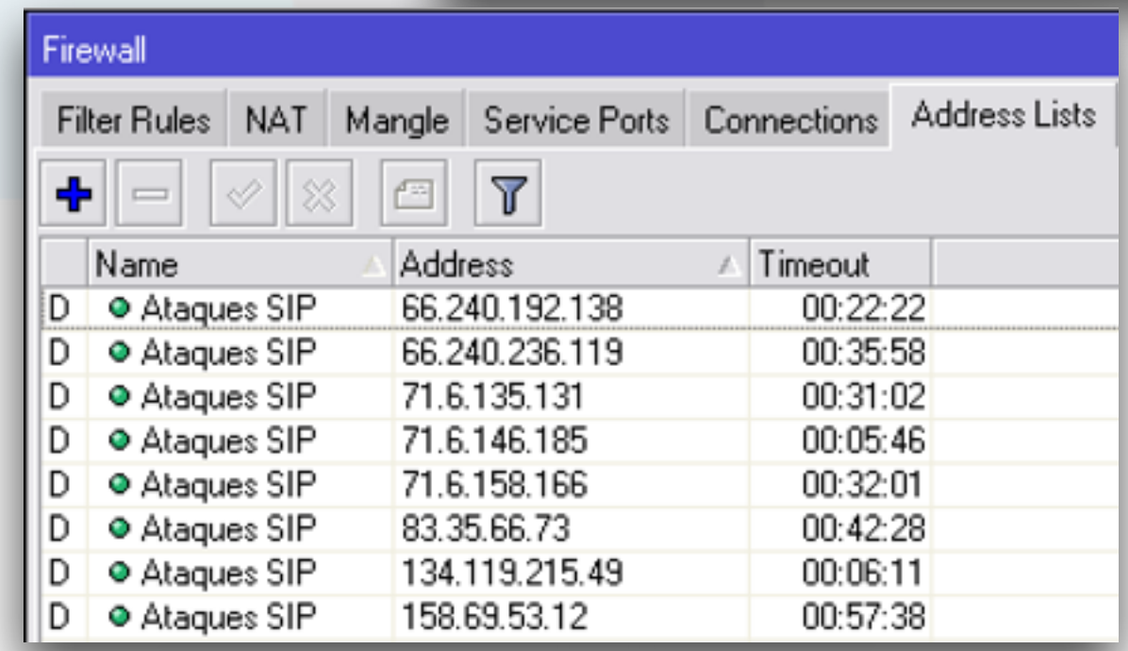
Oct/30/2015 15:27:05	memory	system, error, critical	login failure for user admin from 192.168.88.179 via winbox
Oct/30/2015 15:44:18	memory	system, info, account	user admin logged out from 192.168.10.4 via winbox
Oct/30/2015 15:47:11	memory	system, info, account	user admin logged in from 192.168.10.4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

Más Herramientas

- IP scan
- Packet Sniffer
- Mangle > TZCP
- Netflow / IPFIX / Port Mirror
- Add src / dst to address-list

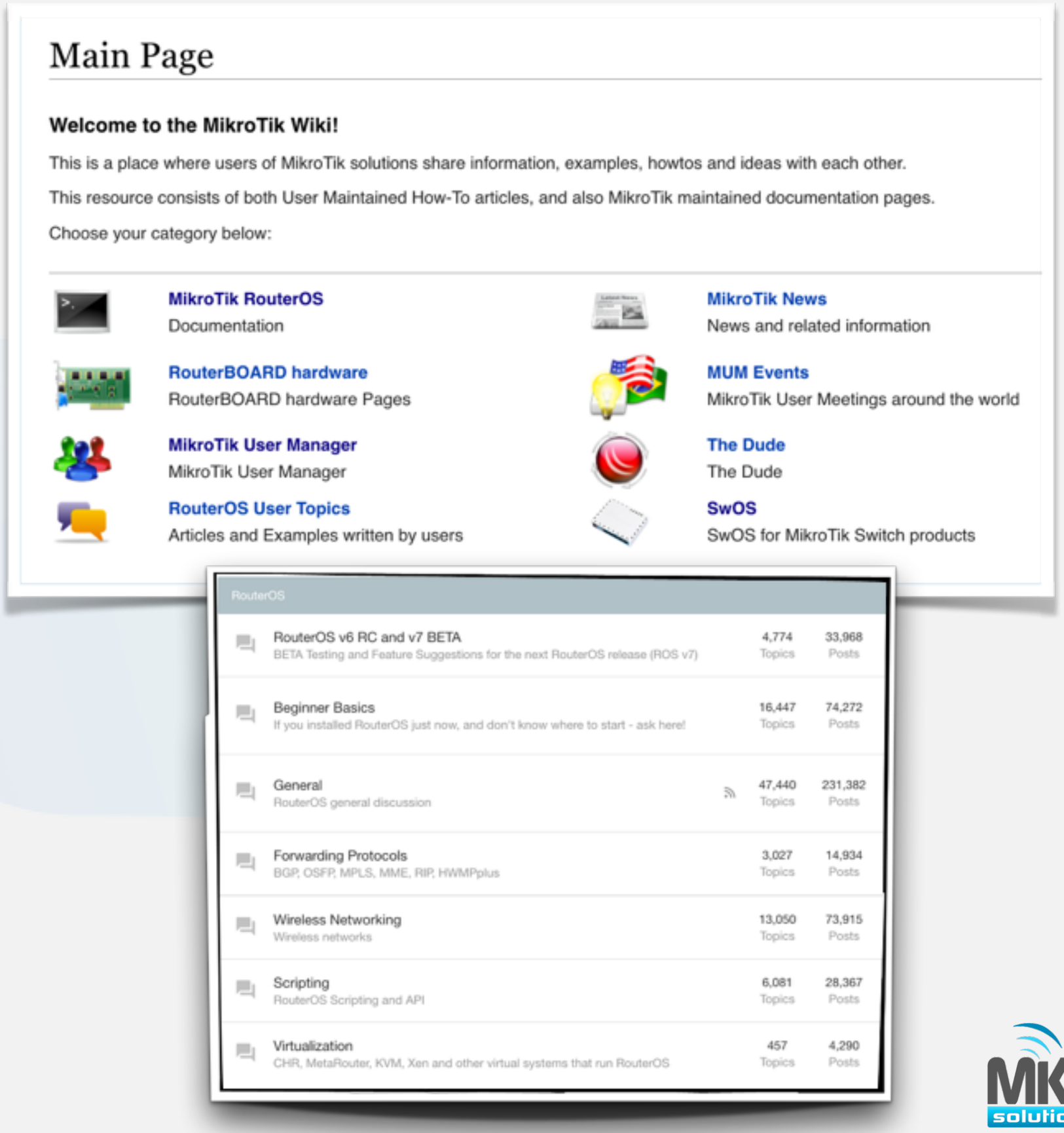






Recomendaciones

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



¿Preguntas?

MUCHAS GRACIAS!

Ing. Mario Clep
MKE Solutions

- marioclep@mkesolutions.net
- marioclep
- @marioclep