

Buenas Prácticas[®] para Segurizar un Router de Fábrica

Guillermo Nonino
MKE Solutions



9 y 10 de Noviembre
Buenos Aires
Argentina



- ✓ Nombre: Guillermo Nonino
- ✓ Profesión: Estudiante Ingeniería en Telecomunicaciones
- ✓ Soporte y Networking - **MKE Solutions**
- ✓ Consultor **MikroTik**
- ✓ Experiencia desde 2013
- ✓  - gnonino@mkesolutions.net
- ✓  - guillermo.mke



- ✓ Tareas dentro del *OutSourcing*:

Relevamiento - Optimización - Mantenimiento

- ✓ La idea de esta charla es mostrar en base a mi experiencia, los *descuidos más comunes que uno encuentra al relevar la configuración de los equipos*, que dejan expuesto al router a posibles ataques.
- ✓ Los ataques tienen principalmente 2 objetivos: *tomar el control del router* o simplemente *provocarle una denegación de servicios* (CPU al 100%).



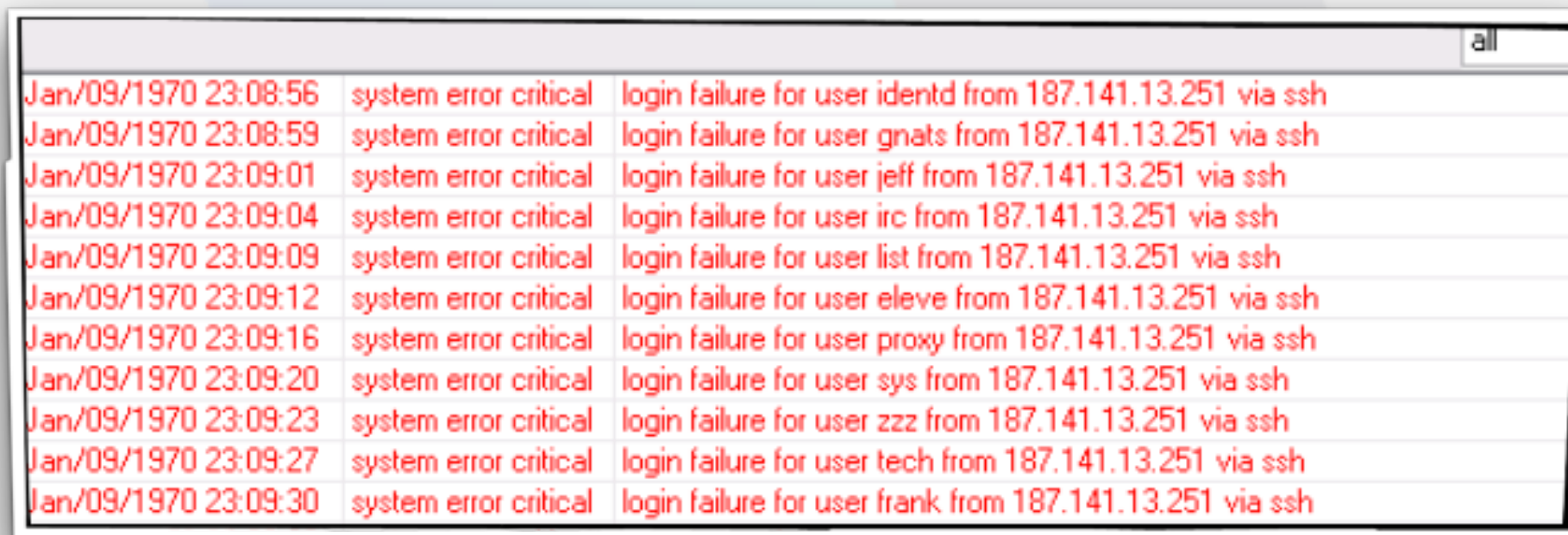
- ✓ No hay una única manera de prevenir los ataques.
- ✓ No todos los routers sufren los mismos ataques ni de la misma manera.
- ✓ Se asume que el usuario tiene un mínimo conocimiento del uso del firewall de **RouterOS** (uso de clasificadores, cadenas y acciones).



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 contraseñas por fuerza bruta.

✓ **WEB** y **Winbox** son menos frecuentes, pero también puede ocurrir el mismo ataque.



The screenshot shows a terminal window with a title bar containing the text 'all'. The log entries are as follows:

Timestamp	Severity	Message
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

Torch (Running)

Interface: wan

Entry Timeout: 00:00:03 s

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

Start

Stop

Close

New Window

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	0
800 (ip)		115.238.184.125:26701	:53 (dns)		6.0 kbps	344 bps	0	0
800 (ip)		115.238.184.126:43549	:53 (dns)		6.0 kbps	344 bps	0	0
800 (ip)		115.238.184.125:16379	:53 (dns)		6.0 kbps	344 bps	0	0
800 (ip)		101.71.74.109:17231	:53 (dns)		6.0 kbps	344 bps	0	0
800 (ip)		101.71.74.110:20153	:53 (dns)		6.0 kbps	344 bps	0	0
800 (ip)		115.238.184.125:50075	:53 (dns)		6.0 kbps	344 bps	0	0
800 (ip)		115.238.184.126:55531	:53 (dns)		6.0 kbps	344 bps	0	0
800 (ip)		115.238.184.126:62555	:53 (dns)		6.0 kbps	344 bps	0	0
800 (ip)		115.238.184.126:34379	:53 (dns)		6.0 kbps	344 bps	0	0
800 (ip)		115.238.184.126:48267	:53 (dns)		6.0 kbps	344 bps	0	0
800 (ip)		101.71.74.109:58126	:53 (dns)		6.0 kbps	344 bps	0	0
800 (ip)		101.71.74.110:24377	:53 (dns)		6.0 kbps	344 bps	0	0
800 (ip)		115.238.184.126:26973	:53 (dns)		6.0 kbps	344 bps	0	0
800 (ip)		115.238.184.126:43181	:53 (dns)		6.0 kbps	344 bps	0	0
800 (ip)		115.238.184.126:48380	:53 (dns)		6.0 kbps	344 bps	0	0
800 (ip)		101.71.74.109:14222	:53 (dns)		6.0 kbps	344 bps	0	0
800 (ip)		115.238.184.126:17981	:53 (dns)		6.0 kbps	344 bps	0	0
800 (ip)		115.238.184.125:49099	:53 (dns)		6.0 kbps	344 bps	0	0
800 (ip)		101.71.74.109:9467	:53 (dns)		6.0 kbps	344 bps	0	0
800 (ip)		101.71.74.109:42021	:53 (dns)		6.0 kbps	344 bps	0	0
800 (ip)		101.71.74.109:62197	:53 (dns)		6.0 kbps	344 bps	0	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:

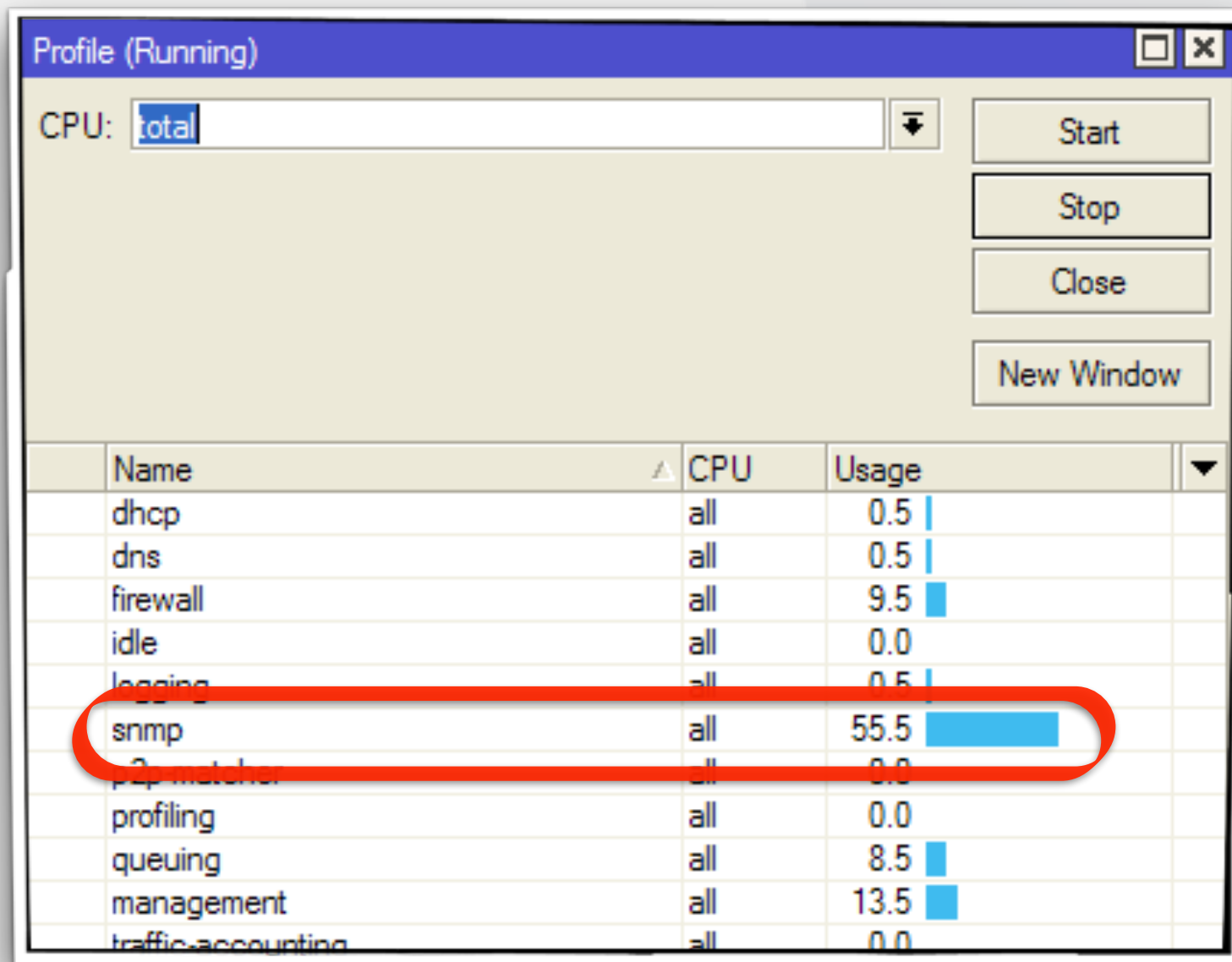
 Enviar

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.



SNMP Community <public>

Name:

Addresses:

Security:

☒ Read Access

☐ Write Access

Authentication Protocol:

Encryption Protocol:

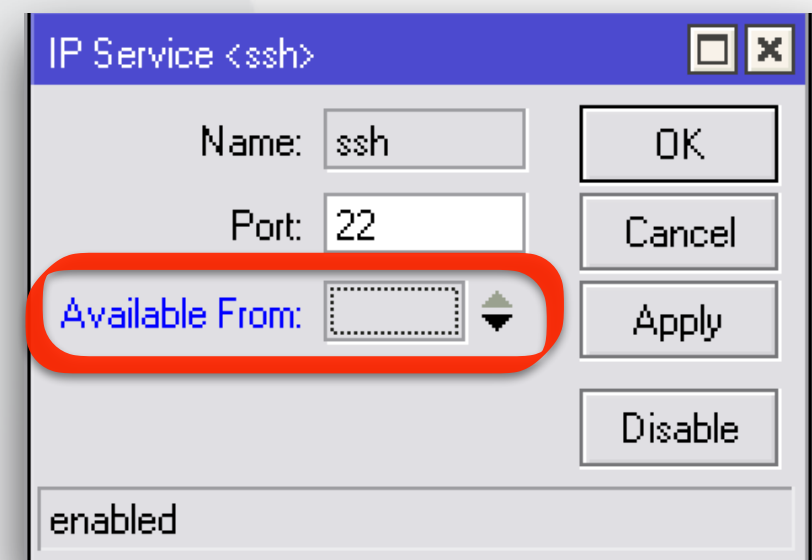
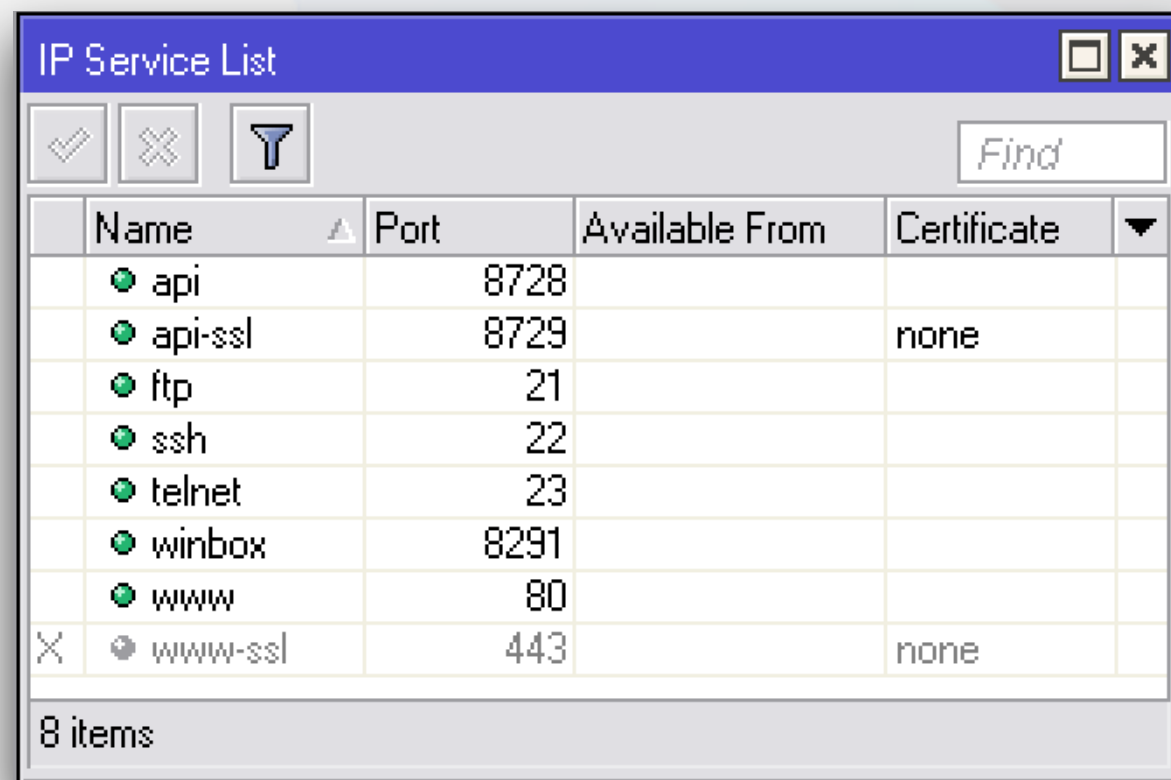
Authentication Password:

Encryption Password:

default

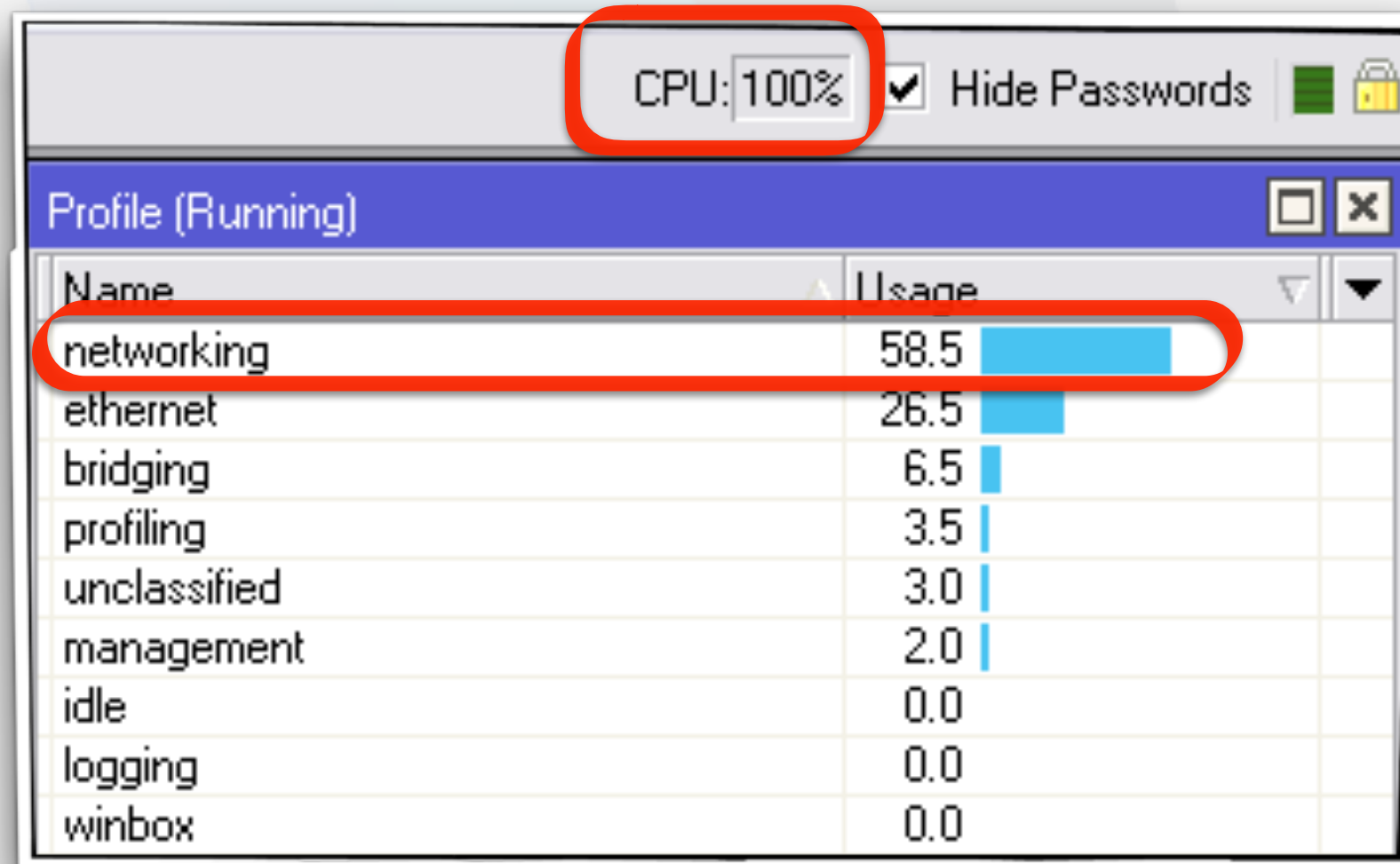
MIKE
solutions

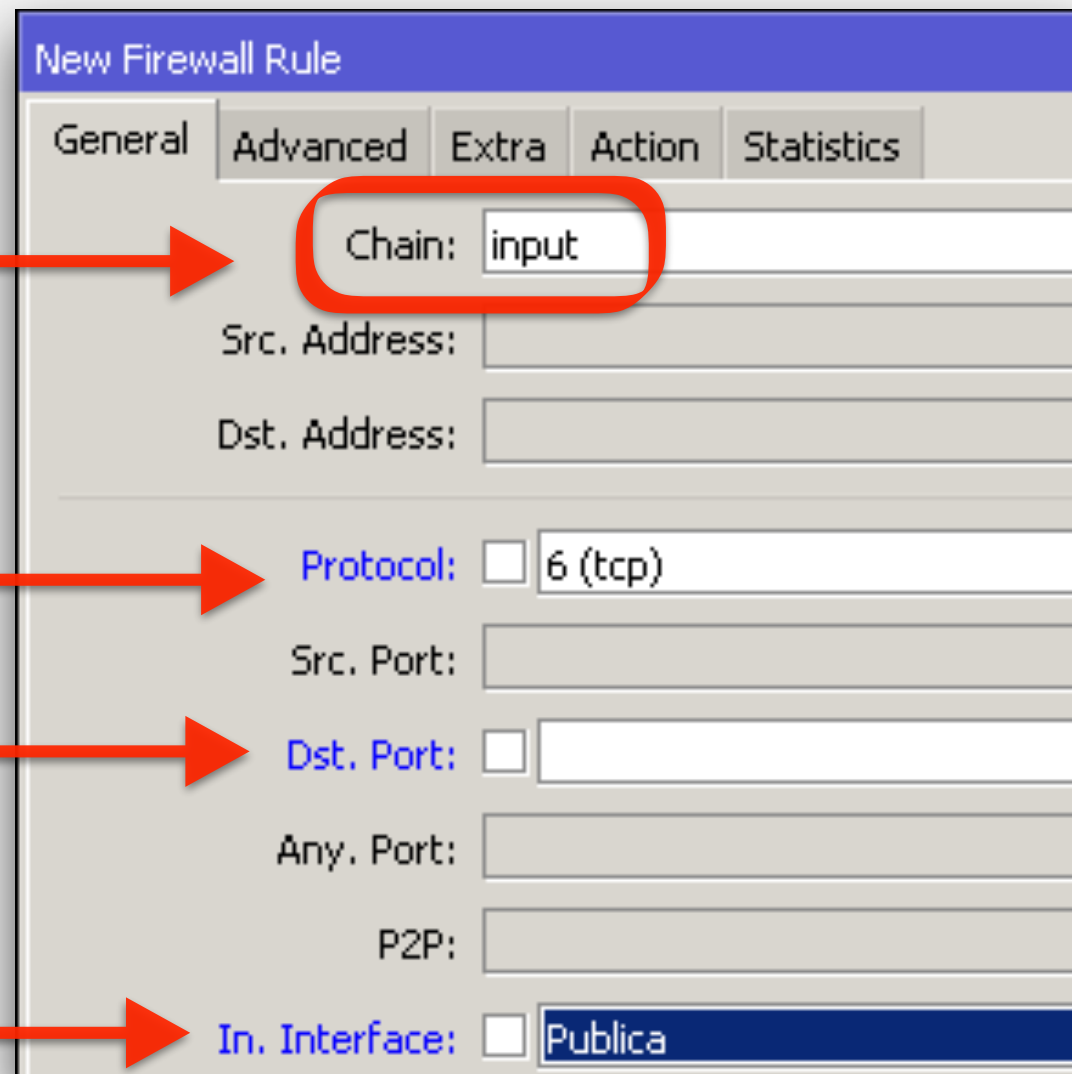
Una manera simple de protegerse, es deshabilitando los servicios que no se usen y proteger los demás con reglas de *firewall* o desde la opción de *IP > Service*



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**.

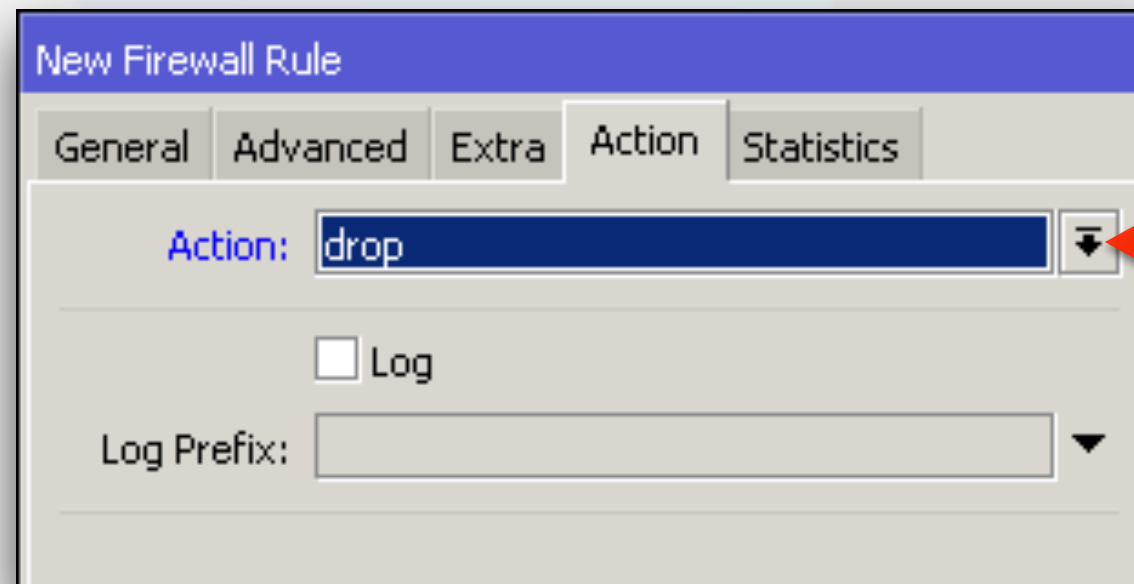




The image shows the 'New Firewall Rule' configuration window with the 'General' tab selected. Several fields are highlighted with red arrows and a red circle:

- Chain:** input (circled in red)
- Protocol:** 6 (tcp)
- Dst. Port:** (empty)
- In. Interface:** Publica

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



The image shows the 'New Firewall Rule' configuration window with the 'Action' tab selected. A red arrow points to the 'Action' dropdown menu, which is set to 'drop'.

Action: drop

☐ Log

Log Prefix: (empty)

Ping Flooding

1)

Firewall Rule <>

General Advanced Extra Action Statistics

Chain: input

Src. Address:

Dst. Address:

Protocol: ☐ 1 (icmp)

Src. Port:

Firewall Rule <>

General Advanced Extra Action Statistics

Connection Limit

Limit

Rate: 10 / sec

Burst: 5

Dst. Limit

Nth

Time

Src. Address Type

Firewall Rule <>

General Advanced Extra Action Statistics

Action: accept

☐ Log

Log Prefix:

2)

Firewall Rule <>

General Advanced Extra Action Statistics

Chain: input

Src. Address:

Dst. Address:

Protocol: ☐ 1 (icmp)

Src. Port:

Firewall Rule <>

General Advanced Extra Action Statistics

Action: drop

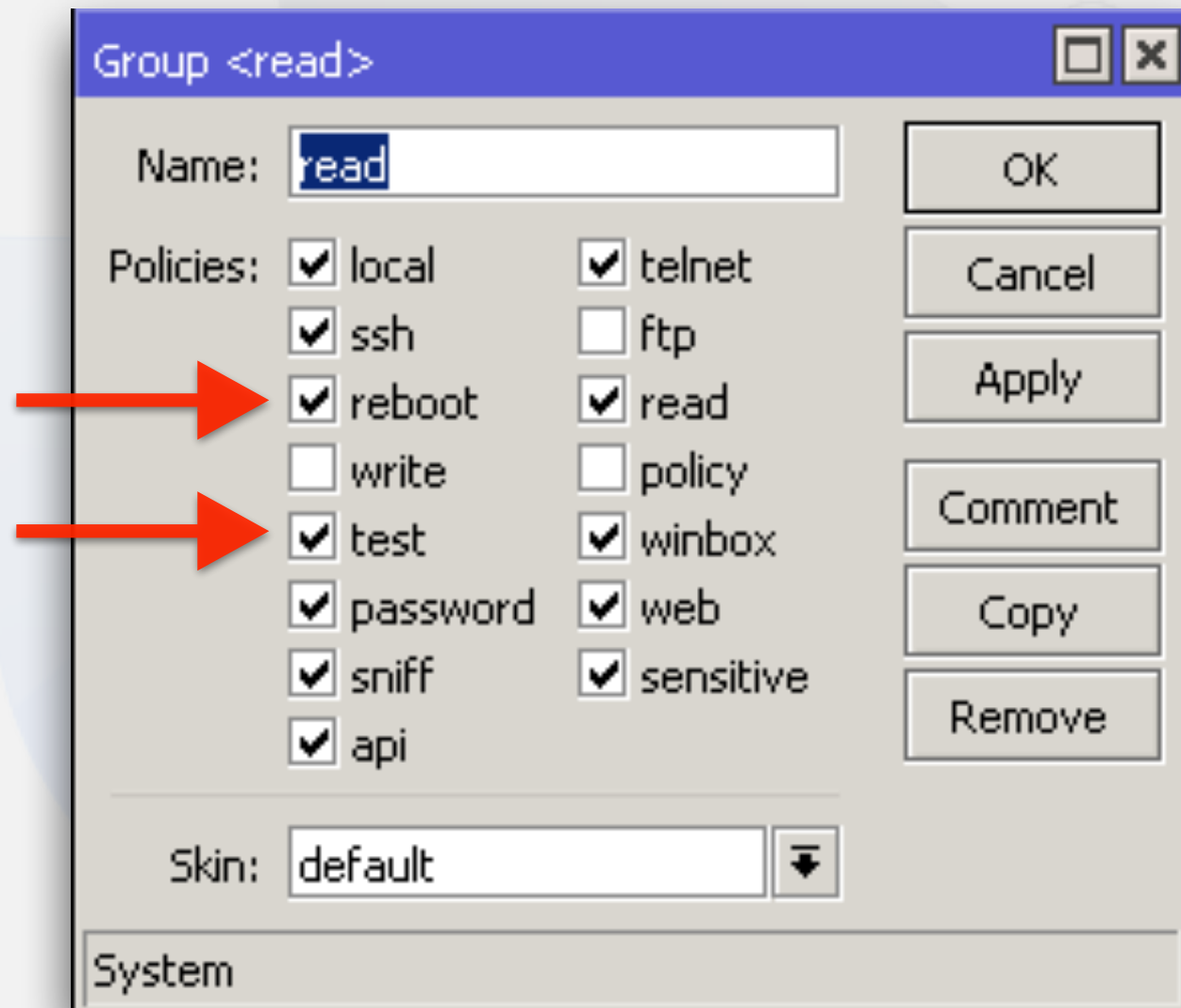
Firewall

Filter Rules NAT Mangle Service Ports Connections

+ - ✓ ✗ [icon] [icon] Reset Count

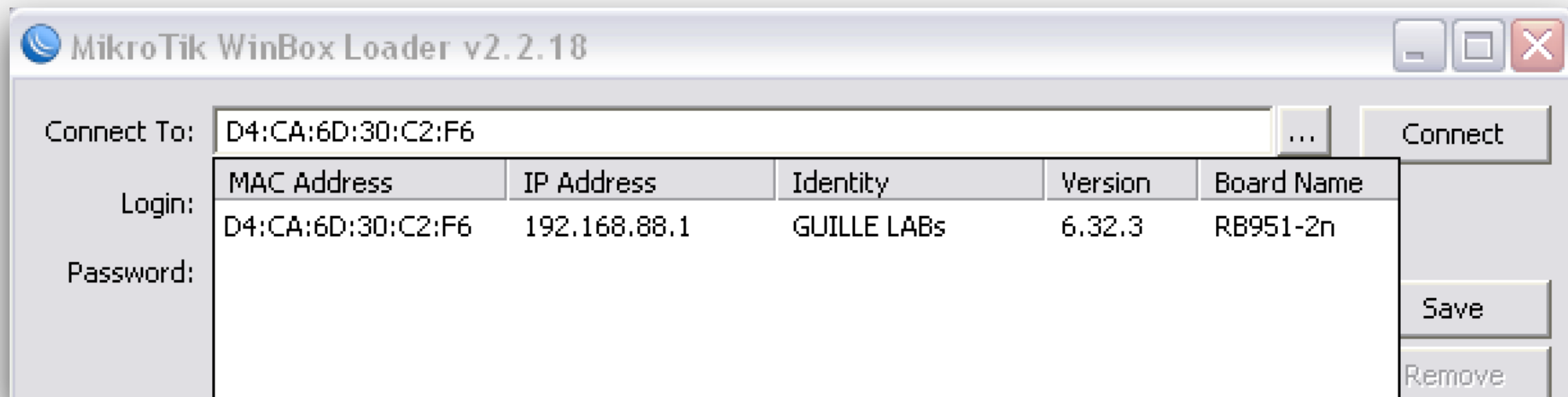
#	Action	Chain	Protocol
0	✓ accept	input	1 (icmp)
1	✗ drop	input	1 (icmp)

- ✓ El grupo **READ** por defecto puede hacer fetch y reboot!

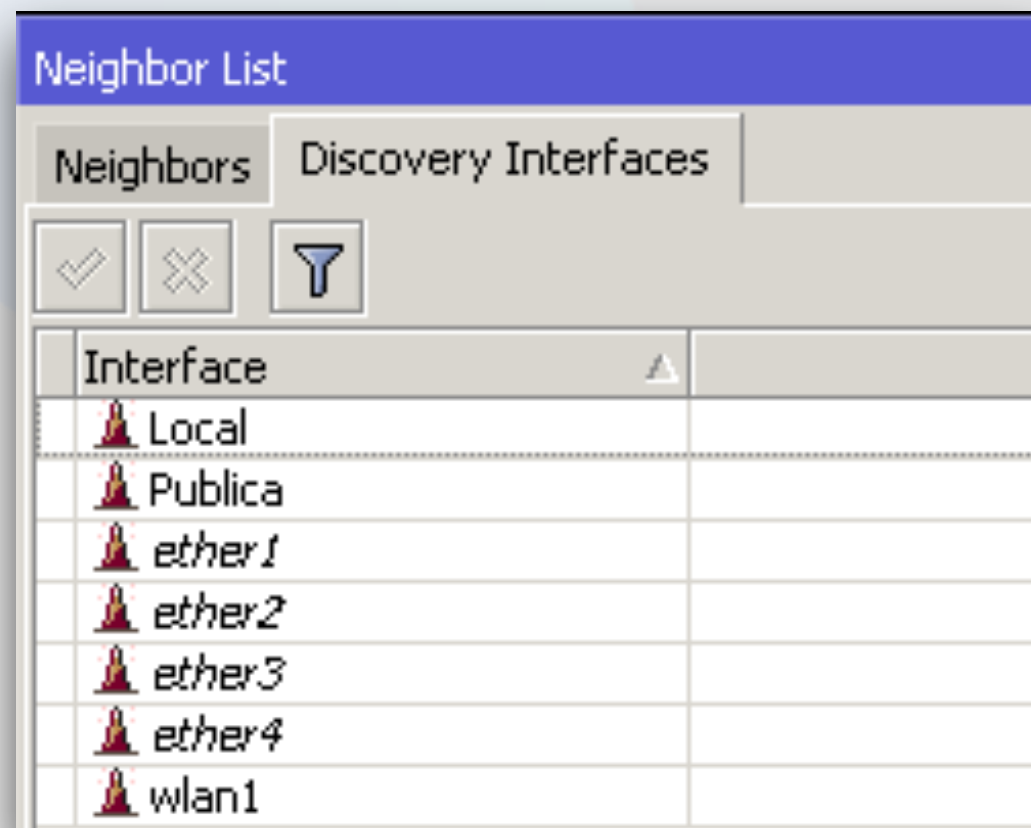


MIKE
solutions

✓ *MNDP* está habilitado en todas sus interfaces.

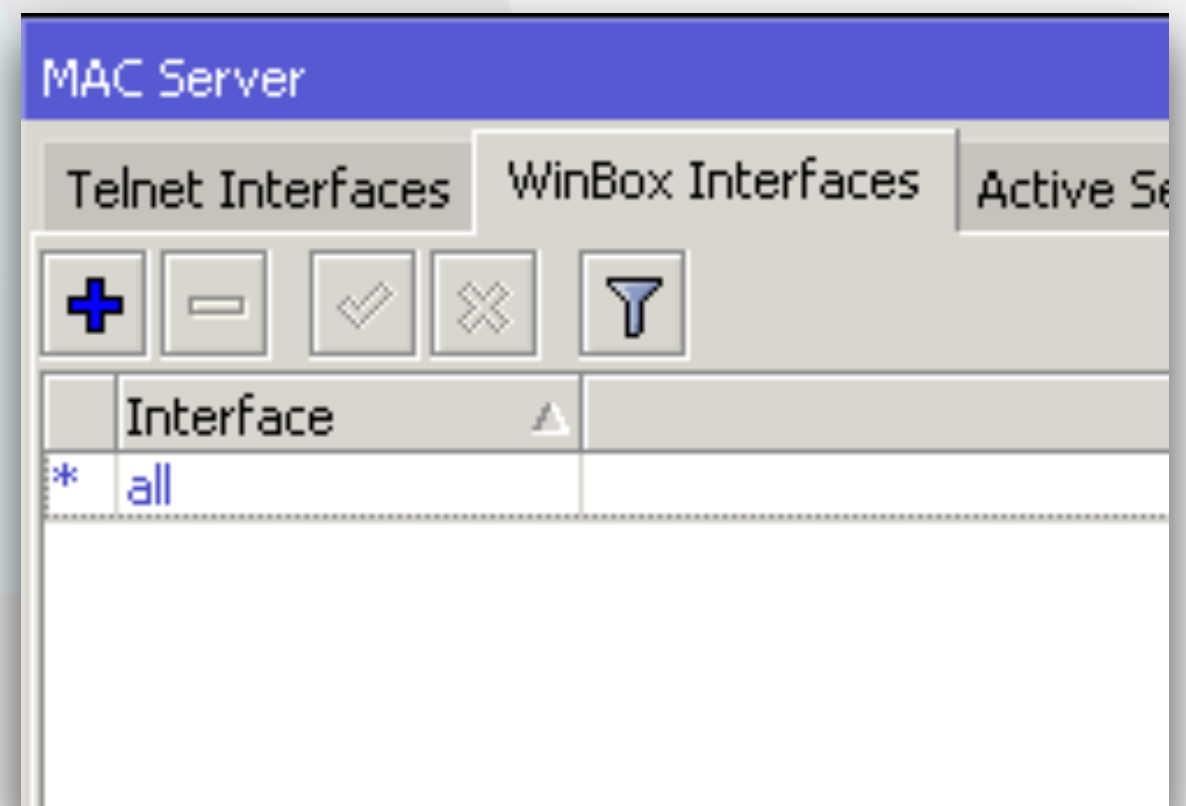
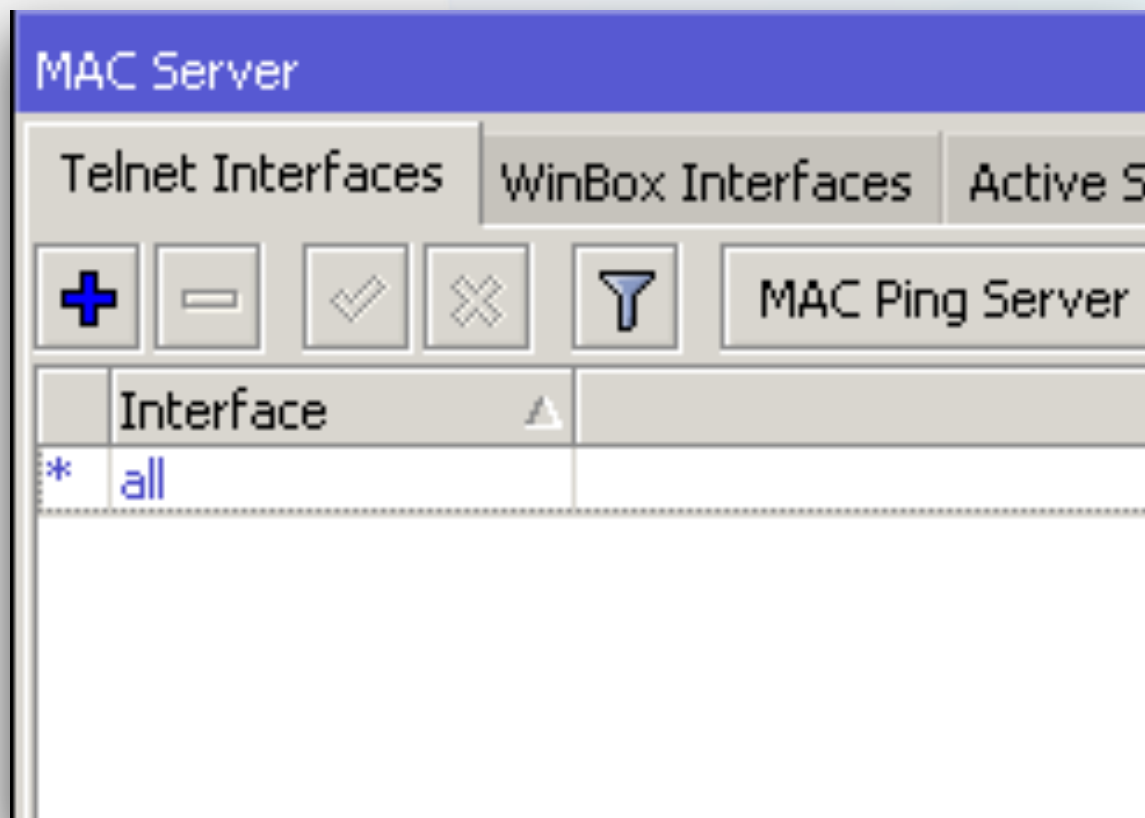


✓ *Ip > Neighbors*



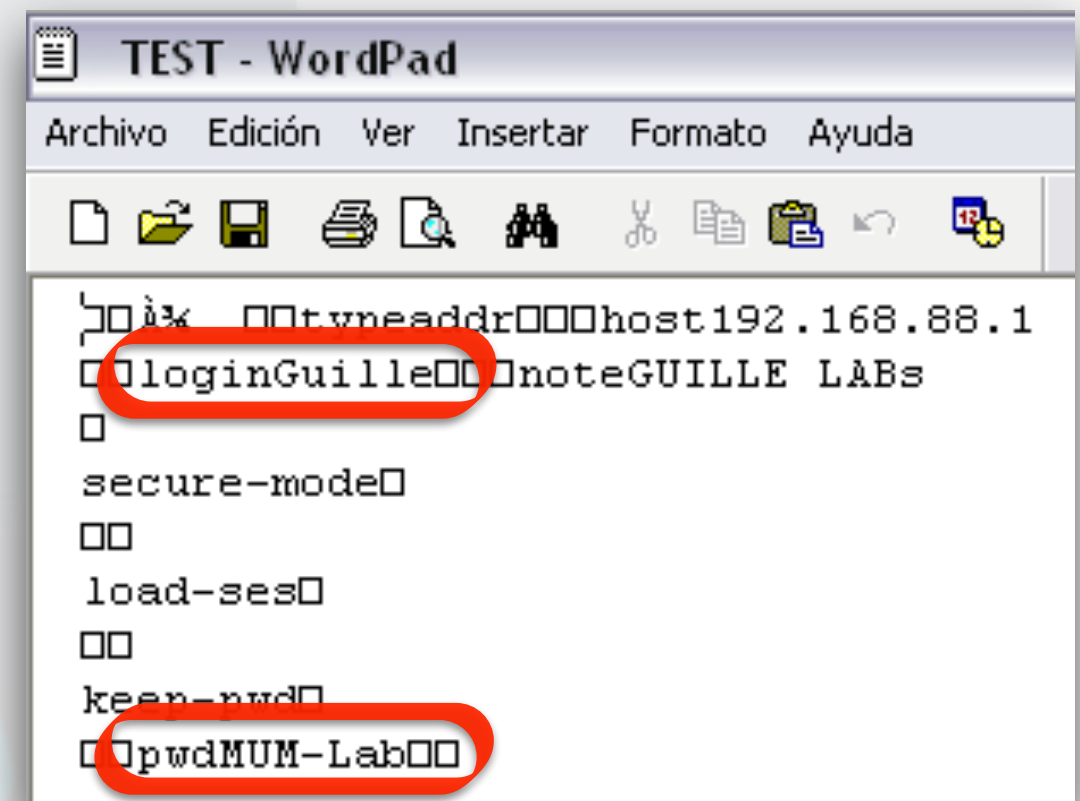
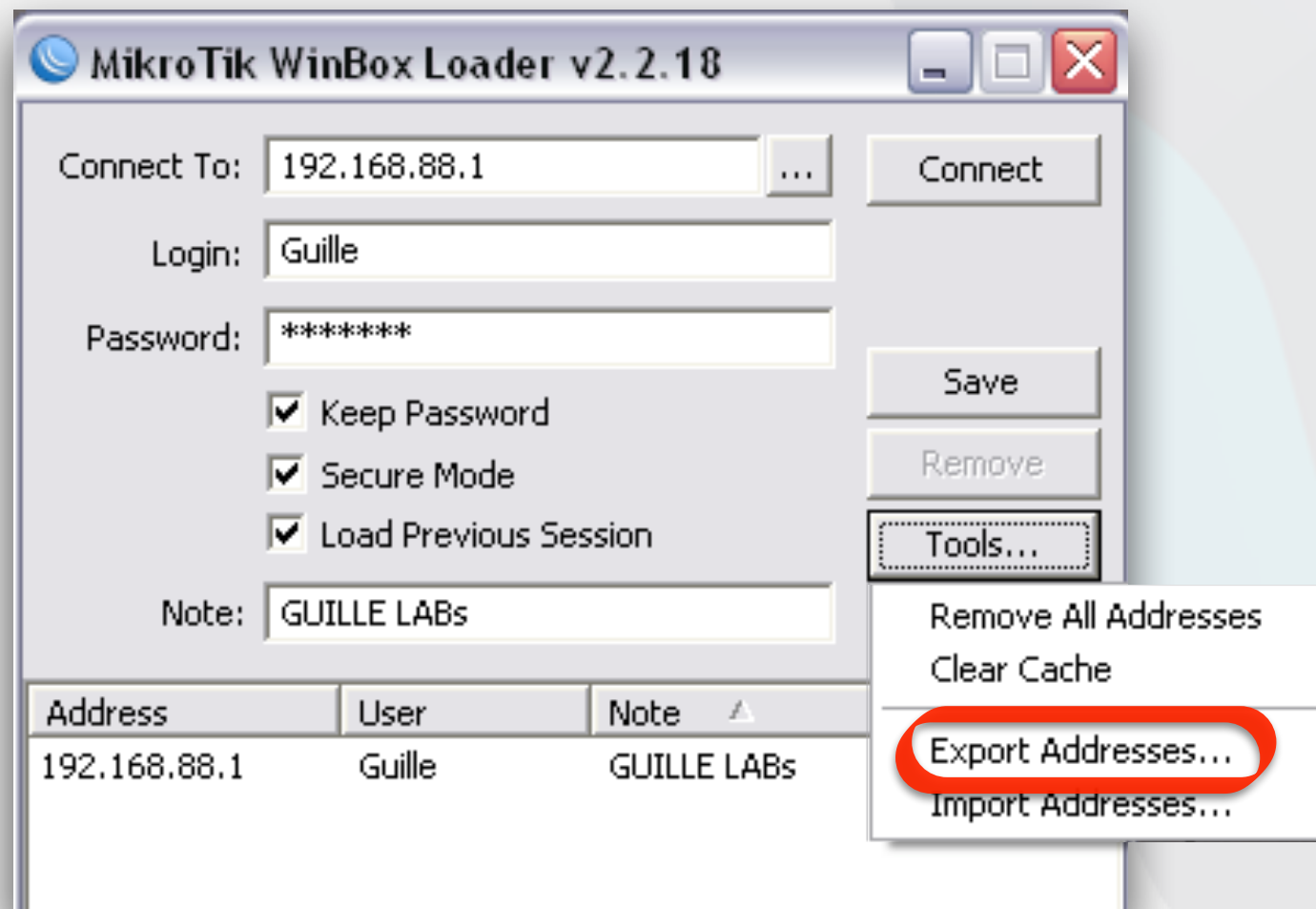
Aún deshabilitando el “Discovery Interface” se puede acceder por **Mac-Telnet** y **Mac-Winbox** sabiendo la **MAC** del equipo.

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



Contraseñas guardadas 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!!!



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

The screenshot shows the WinBox v3.0rc17 (Addresses) window. The 'Managed' tab is selected. A red circle highlights the 'Master Password' dialog box, which contains a 'Password:' field and an 'OK' button. The main window has a menu bar with 'File' and 'Tools'. Below the menu bar, there are input fields for 'Connect To:' (192.168.88.1), 'Login:' (Guille), and 'Password:' (masked with asterisks). To the right of these fields are two checkboxes: 'Keep Password' (checked) and 'Open In New Window' (unchecked). Below the input fields are three buttons: 'Add/Set', 'Connect To RoMON', and 'Connect'. At the bottom of the window, there is a table with columns: Address, User, Session, Group, RoMON Agent, and No. The table is currently empty.

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

- ✓ Muchos descuidan el acceso al software The DUDE. Si el mismo corre en una IP pública y está con las credenciales por defecto, fácilmente se puede acceder a él y tomar el control de los equipos que esté administrando.

The screenshot shows the 'LONG DISTANCE WIRELESS LINKS' web interface. The top navigation bar includes 'Preferencias', 'Servidor Local' (highlighted with a green dot), and 'Ayuda'. The main form contains the following fields and buttons:

- Servidor: 200.200.200.1
- Modo: ☐ plain ☒ seguro
- Puerto: 2211
- Nombre de usuario: admin
- Contraseña: (empty field)
- Buttons: Conectar, Guardar, Eliminar
- Checkboxes: ☒ Recordar contraseña
- Icons: A group of people icon and a calendar icon.
- Table headers: 'Direccion' and 'Nombre de usuario'.

A red oval highlights the 'Nombre de usuario' field containing 'admin' and the 'Contraseña' field, indicating the default credentials.

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 ☒ Src. Address6
☒ Dst. Address ☒ Dst. Address6
☒ MAC Protocol ☒ Port
☒ Protocol ☒ VLAN Id
☒ DSCP

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 15:10:21	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

¿Preguntas?

MUCHAS GRACIAS!

Guillermo Nonino
MKE Solutions



9 y 10 de Noviembre
Buenos Aires
Argentina

