Mejores Prácticas

Nada protege a tu equipo en un 100%, ninguna herramienta o procedimiento actual es capaz de lograrlo

INDEX SOLUCIONES IP

MikroTik MEXICO

Ponente

Ing. Adrián Arturo Díaz Cota

- Administrador de redes desde el año 2000
- Administrador Windows y Linux
- CTO Index Datacom
- Certificaciones:

- Empresa dedicada al desarrollo y comercialización de soluciones en tecnologías de la información y comunicación.
- Más de 15 años en el mercado.
- Servicios de Internet Simétrico, Asimétrico y E-PyME; Ethernet Local y Multilocal.
- Soluciones en Redes de Banda Ancha, Internet móvil, Telefonía IP, WISP.

Los Mochis, Culiacán y Mazatlán, Sinaloa.
Obregón y Guaymas, Sonora.
Cabo San Lucas, Baja California Sur.

- Distribuidor oficial de Mikrotik Routerboard
- Centro de entrenamiento oficial en Mikrotik RouterOS

Los Mochis, Sinaloa.
Guadalajara
Ciudad de México

- Empresa dedicada a servicios de Internet residencial
- + de 4600 abonados

Presencia Sinaloa y Sonora

- Sistema de gestión en la nube para ISPs

Objetivos

- Crear conciencia de la importancia de asegurar las políticas de acceso a los equipos.
- Compartir experiencias de algunos accesos no autorizados.
- Principales cambios que llevan a cabo al ingresar a los routers.

Contenido

- Ataques masivos
- Problemas de seguridad
- ¿Qué hacer para reducir el riesgo?
  - Generar políticas elementales
  - Ajustes Básicos
  - Ajustar Firewall

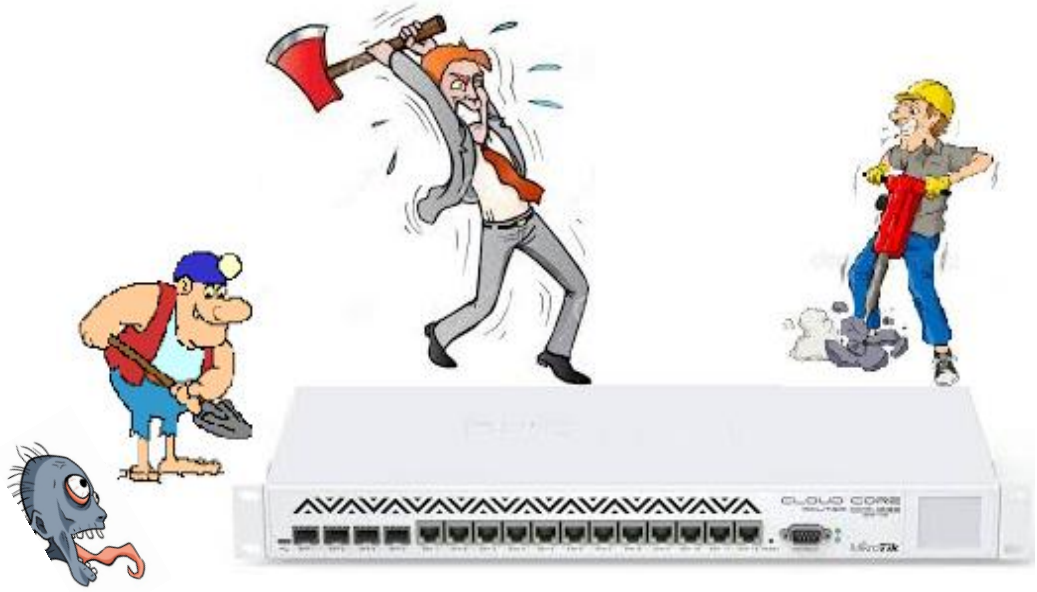
Mejorando las políticas de seguridad

- Ataques masivos

Estamos en la era de la información, todo equipo interconectado recibe en algún momento ataques.

En su mayoría, se lanzan automáticamente desde otros equipos infectados (a través de virus, troyanos, gusanos, etc.).

En otros casos, son ejecutados por piratas informáticos.



Problemática de Seguridad

- Todos los equipos son vulnerables

- Intercepción de comunicaciones
  - Secuestro de sesión.
  - Falsificación de identidad.
  - Redireccionamiento o alteración de mensajes.
  - Control del equipo
- Denegación de servicios
  - Explotación de las debilidades de configuración.
    - Ataques FuerzaBruta SSH / Telnet / WEB
    - DNS
  - Explotación de las vulnerabilidades del software.
    - Vulnerabilidades & Exploits
    - DoS y DDoS

Problemática de Seguridad

https://securelist.lat/new-trends-in-the-world-of-iot-threats/87948/

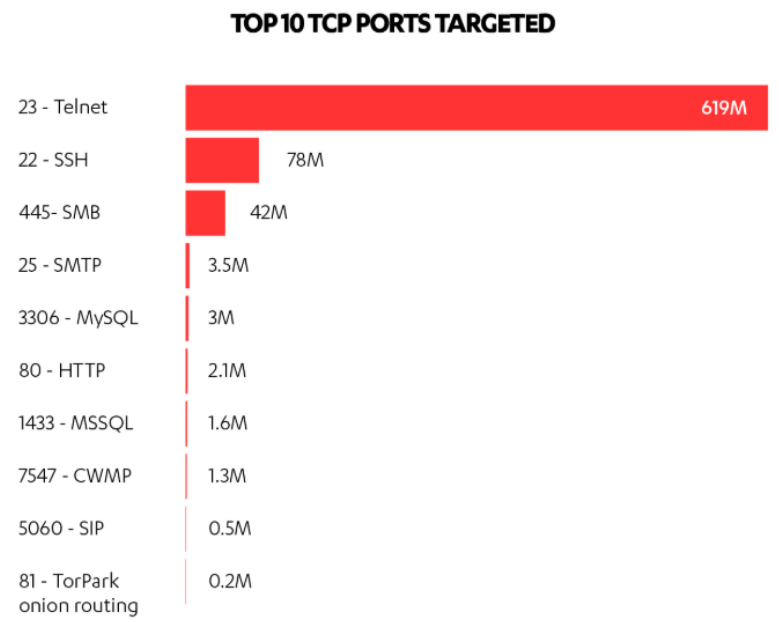
SECURELIST AMENAZAS CATEGORÍAS ETIQUETAS ESTADÍSTICAS ENCICLOPE

Servicio	Puerto	% de ataques	Vector de ataque	Familias de malware
Telnet	23, 2323	82,26%	Fuerza bruta	Mirai, Gafgyt
SSH	22	11,51%	Fuerza bruta	Mirai, Gafgyt
Samba	445	2,78%	EternalBlue, EternalRed, CVE-2018-7445	–
tr-069	7547	0,77%	RCE en la implementación del protocolo TR-069	Mirai, Hajime
HTTP	80	0.76%	Intentos de explotar vulnerabilidades en el servidor web o averiguar la contraseña del panel de administración	–
winbox (RouterOS)	8291	0.71%	Utilizado para identificar RouterOS (MikroTik) y para ataques a través del servicio winbox	Hajime
Mikrotik http	8080	0.23%	RCE en MikroTik RouterOS <6.38.5 Chimay-Red	Hajime
MSSQL	1433	0.21%	Ejecución de código arbitrario para ciertas versiones (2000, 2005 y 2008) o cambio de la contraseña del administrador, robo de datos	–
GoAhead httpd	81	0.16%	RCE en cámaras IP GoAhead	Persirai, Gafgyt
Mikrotik http	8081	0.15%	Chimay-Red	Hajime
Etherium JSON-RPC	8545	0.15%	Evasión de la autorización (CVE-2017-12113)	–
RDP	3389	0.12%	Fuerza bruta	–
XionMai uc-httpd	8000	0.09%	Desbordamiento de búfer (CVE-2018-10088) en XionMai uc-httpd 1.0.0 (algunos dispositivos de fabricantes chinos)	Satori

https://blog.f-secure.com/es/mapa-de-los-ataques-ciberneticos-del-segundo-semestre-2018

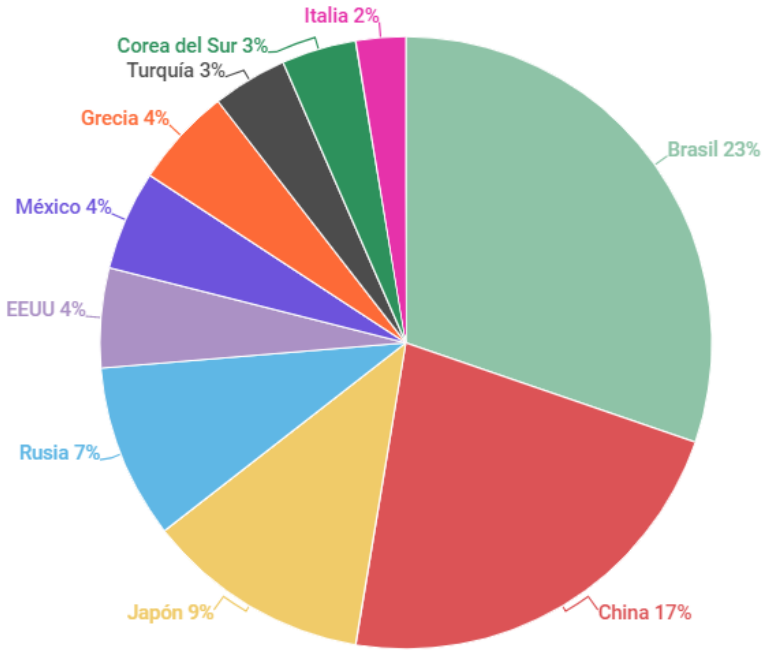
Seguridad del hogar Seguridad empresarial Amenazas e investigación

Puertos y protocolos



Problemática de Seguridad

- Países desde donde se lanzan mas ataques vía TELNET SSH

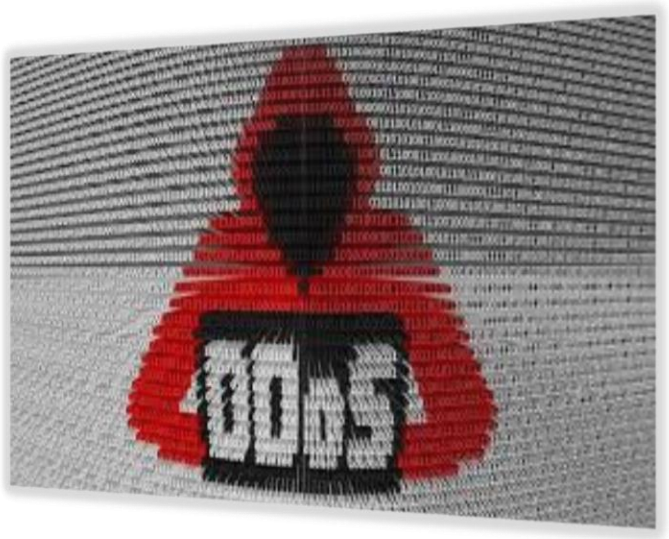


Problemática de Seguridad

- Ataque DoS & DDoS

Name	CPU	Usage
cpu4		100.0
cpu11		100.0
cpu18		100.0
cpu20		100.0
cpu25		100.0
cpu29		100.0
cpu3		99.5
cpu10		99.5
cpu15		99.5
cpu23		99.5
cpu24		99.5
cpu12		99.0
cpu26		99.0
cpu14		98.5
cpu21		98.5
cpu32		98.5
cpu2		98.0
cpu8		98.0
cpu17		98.0
cpu19		98.0
cpu1		97.5
cpu9		97.5
cpu13		96.5
cpu27		96.5
cpu16		94.5
cpu0		93.5
cpu7		93.5
cpu30		93.5
cpu6		93.0
cpu28		93.0
cpu22		92.0
cpu34		91.5
cpu35		91.5
cpu5		91.0
cpu33		85.5

Name	CPU	Usage
cpu33		85.5
cpu31		84.0
firewall	1	70.0
firewall	10	66.0
firewall	0	65.5
firewall	3	65.0
firewall	13	62.0
firewall	2	61.5
firewall	6	60.5
firewall	12	60.5
firewall	14	60.5
firewall	9	60.0
firewall	4	59.0
firewall	19	59.0
firewall	17	56.5
firewall	7	56.0
firewall	18	56.0
firewall	21	54.5
firewall	5	53.0
firewall	8	52.5
firewall	29	52.5
queuing	32	52.5
firewall	16	52.0
firewall	25	51.0
firewall	20	50.5
firewall	24	49.5
firewall	30	49.5
firewall	15	48.0
firewall	35	48.0
firewall	11	47.5
queuing	23	47.5
queuing	27	46.0
queuing	26	44.5
firewall	22	44.0
queuing	20	43.0



Problemática de Seguridad

- Ataque Fuerza Bruta

Log

Freeze

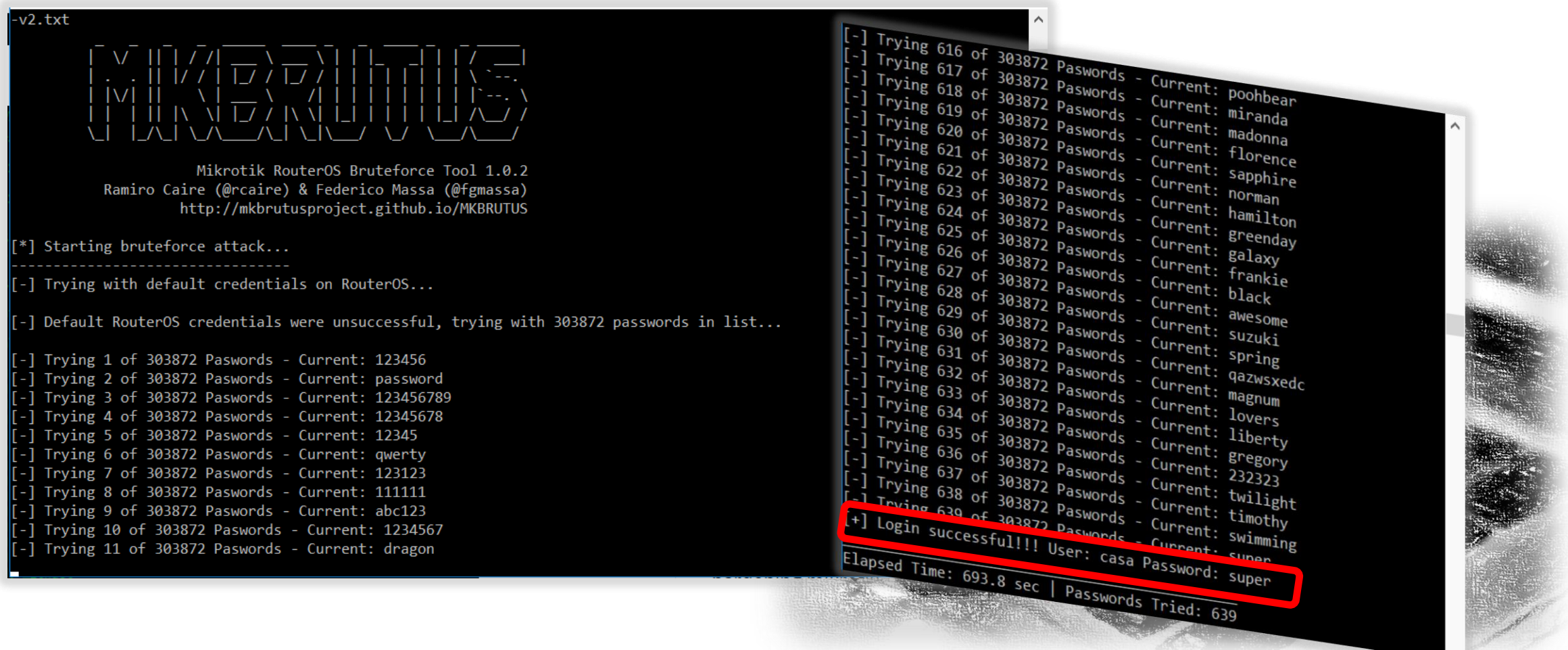
all

Apr/01/2019 05:59:28	memory	system, error, critical	login failure for user admin from 115.21.123.116 via ssh
Apr/01/2019 06:22:04	memory	system, error, critical	login failure for user usuario from 139.59.74.143 via ssh
Apr/01/2019 06:30:34	mem	stem, error, critical	login failure for user root from 203.248.18.135 via ssh
Apr/01/2019 06:38:37	mem	stem, error, critical	login failure for user root from 35.194.81.42 via ssh
Apr/01/2019 06:48:09	memory	system, error, critical	login failure for user root from 68.183.27.152 via ssh
Apr/01/2019 07:06:50	memory	system, error, critical	login failure for user ftp from 61.72.254.71 via ssh
Apr/01/2019 07:07:07	memory	system, error, critical	login failure for user admin from 111.40.66.28 via ssh
Apr/01/2019 07:08:44	memory	system, error, critical	login failure for user root from 165.227.49.242 via ssh
Apr/01/2019 07:24:06	memory	system, error, critical	login failure for user setup from 206.189.86.17 via ssh
Apr/01/2019 07:29:02	memory	system, error, critical	login failure for user ftpuser from 47.90.200.173 via ssh
Apr/01/2019 07:42:18	memory	system, error, critical	login failure for user applmgr from 178.128.81.125 via ssh
Apr/01/2019 08:01:26	memory	system, error, critical	login failure for user user from 211.33.129.248 via ssh
Apr/01/2019 08:11:12	memory	system, error, critical	login failure for user wp-user from 206.189.141.63 via ssh
Apr/01/2019 08:24:42	memory	system, error, critical	login failure for user hadoop from 139.59.173.161 via ssh
Apr/01/2019 08:29:42	memory	system, error, critical	login failure for user applmgr from 211.104.13.125 via ssh
Apr/01/2019 08:36:35	memory	system, error, critical	login failure for user admin from 201.139.89.55 via ssh
Apr/01/2019 08:36:36	memory	system, error, critical	login failure for user admin from 201.139.89.55 via ssh
Apr/01/2019 08:36:36	memory	system, error, critical	login failure for user admin from 201.139.89.55 via ssh
Apr/01/2019 08:36:36	memory	system, error, critical	login failure for user admin from 201.139.89.55 via ssh
Apr/01/2019 08:36:36	memory	system, error, critical	login failure for user admin from 201.139.89.55 via ssh
Apr/01/2019 08:36:37	memory	system, error, critical	login failure for user admin from 201.139.89.55 via ssh
Apr/01/2019 08:36:48	memory	system, error, critical	login failure for user usuario from 45.119.81.253 via ssh

memory

Problemática de Seguridad

- Ataque Fuerza Bruta



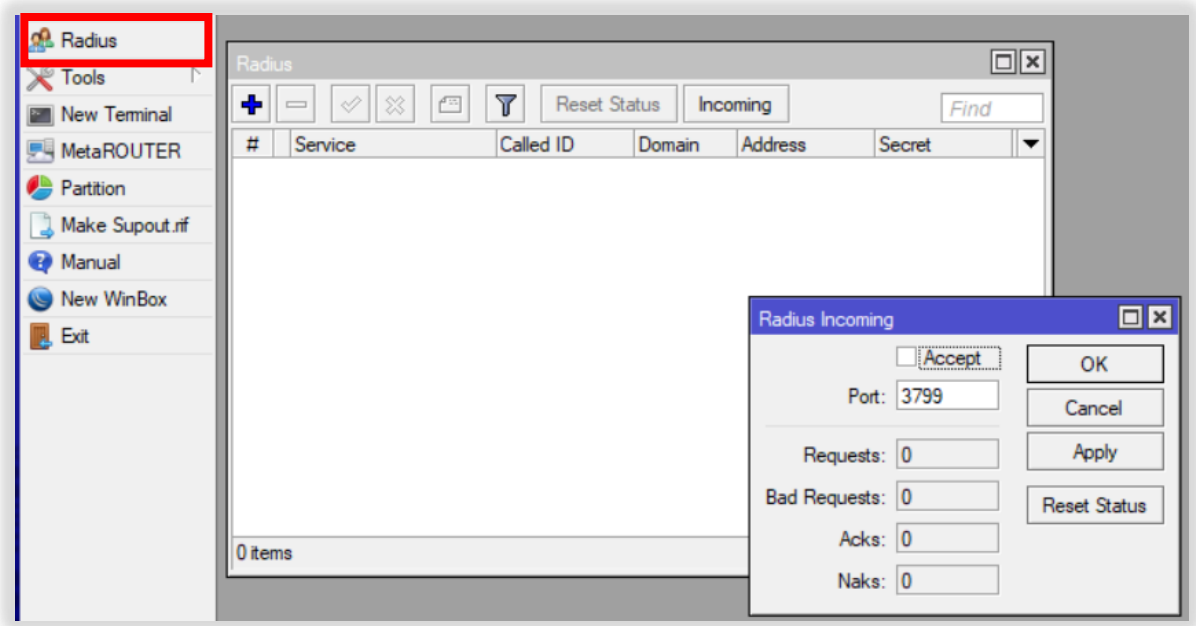
Problemática de Seguridad

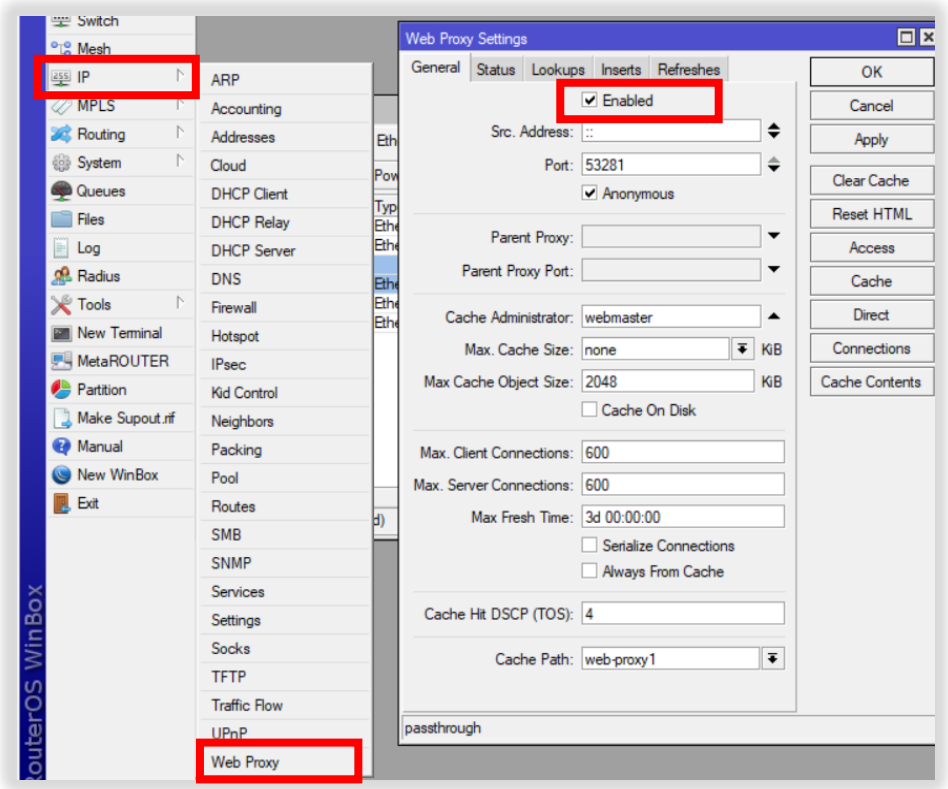
- Accesos no autorizados

Jul/24/2018 07:49:13	disk	system, info, account	user support logged out from 47.75.108.28 via winbox
Jul/24/2018 07:49:14	disk	system, info	new script added by support
Jul/24/2018 07:49:15	disk	system, info	script removed by support
Jul/24/2018 07:49:15	disk	system, info	ip service changed by support
Jul/24/2018 07:49:16	disk	system, info	ip service changed by support
Jul/24/2018 07:49:20	disk	system, info	new script added by support
Jul/24/2018 07:49:20	disk	system, info	new script scheduled by support
Jul/24/2018 07:49:21	disk	system, info	pool pool1 added by support
Jul/24/2018 07:49:22	disk	system, info	ppp profile <test> added by support
Jul/24/2018 07:49:23	disk	system, info	PPP AAA settings changed by support
Jul/24/2018 07:49:23	disk	system, info	PPTP Server settings changed by support
Jul/24/2018 07:49:24	disk	system, info	nat rule added by support
Jul/24/2018 07:49:24	disk	system, info	system identity changed by support
Jul/24/2018 07:49:25	disk	system, info	RADIUS client added by support
Jul/24/2018 07:49:25	disk	system, info	radius incoming changed by support
Jul/24/2018 07:49:26	disk	system, info	PPP AAA settings changed by support

Problemática de Seguridad

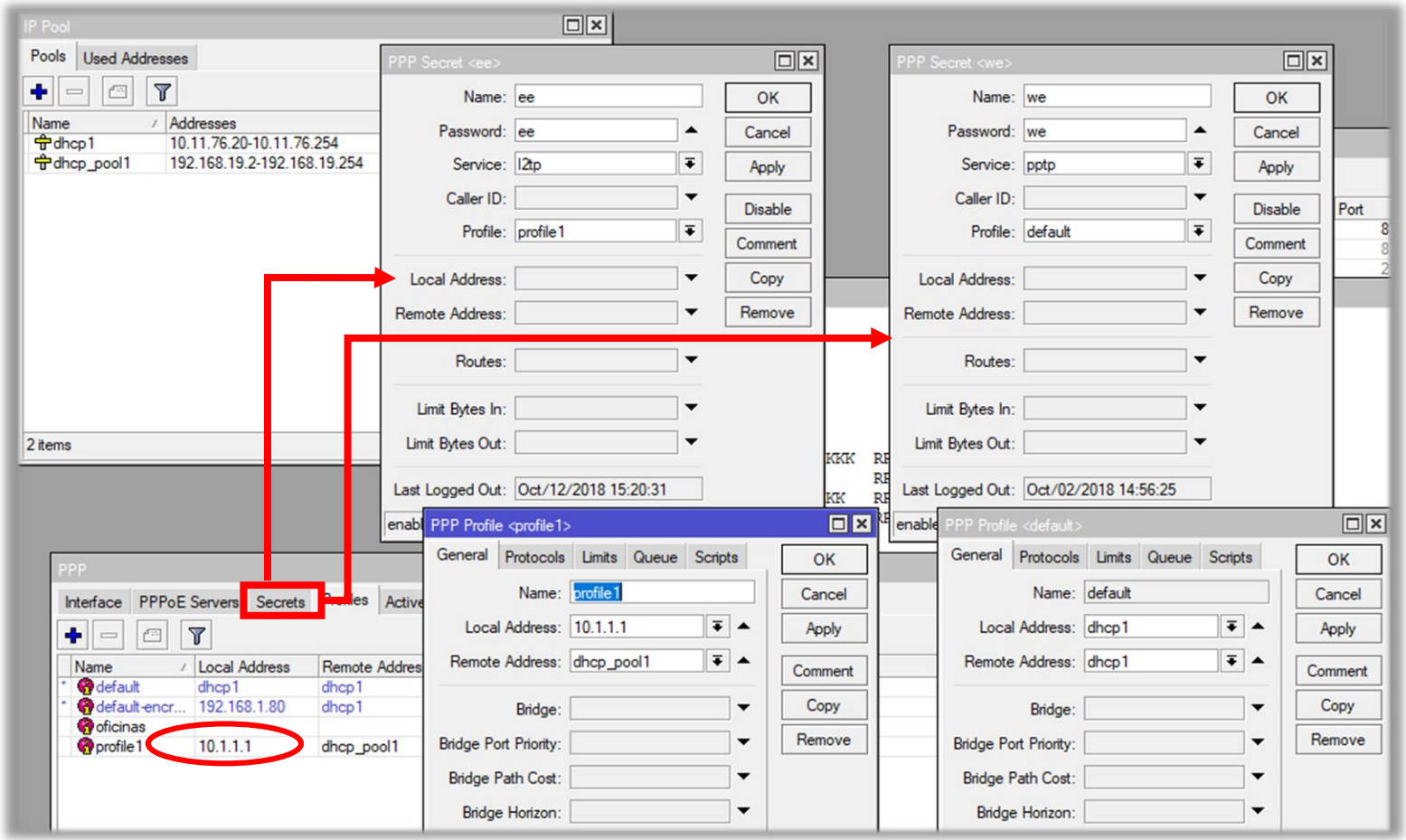
- Modificación No Autorizada
  - WebProxy, Radius





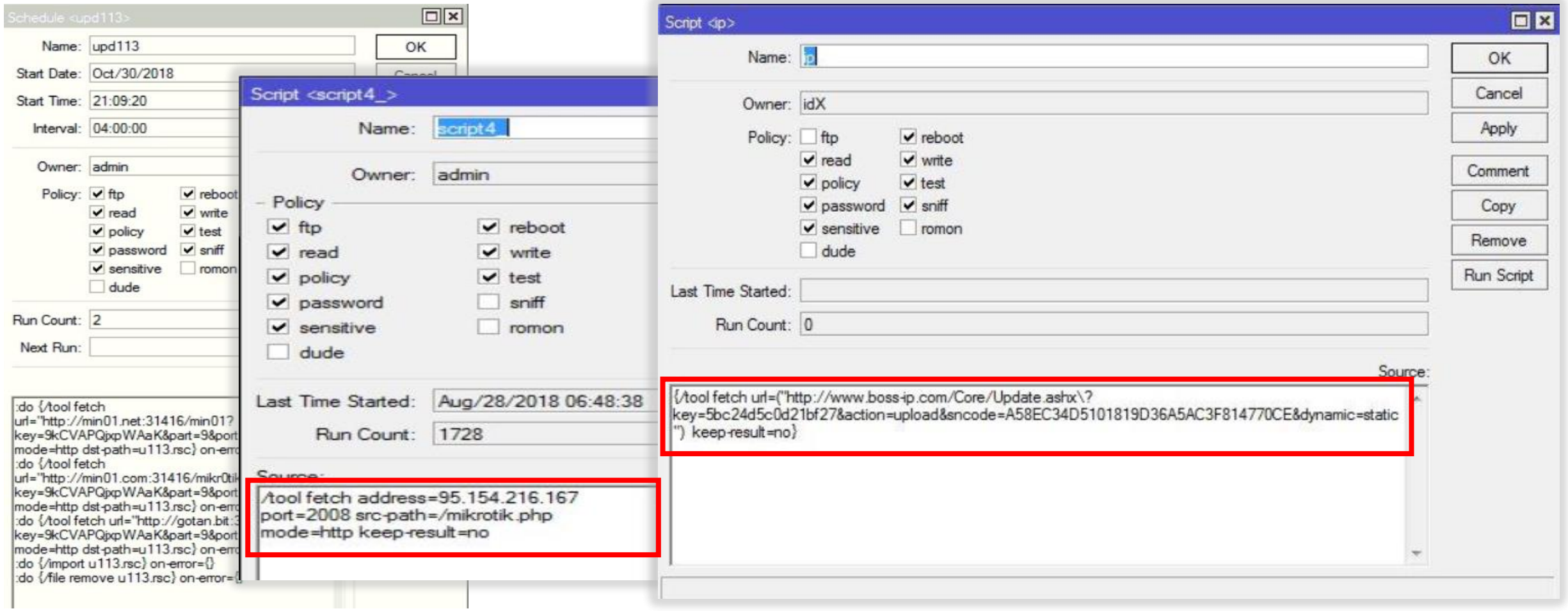
Problemática de Seguridad

- Modificación No Autorizada



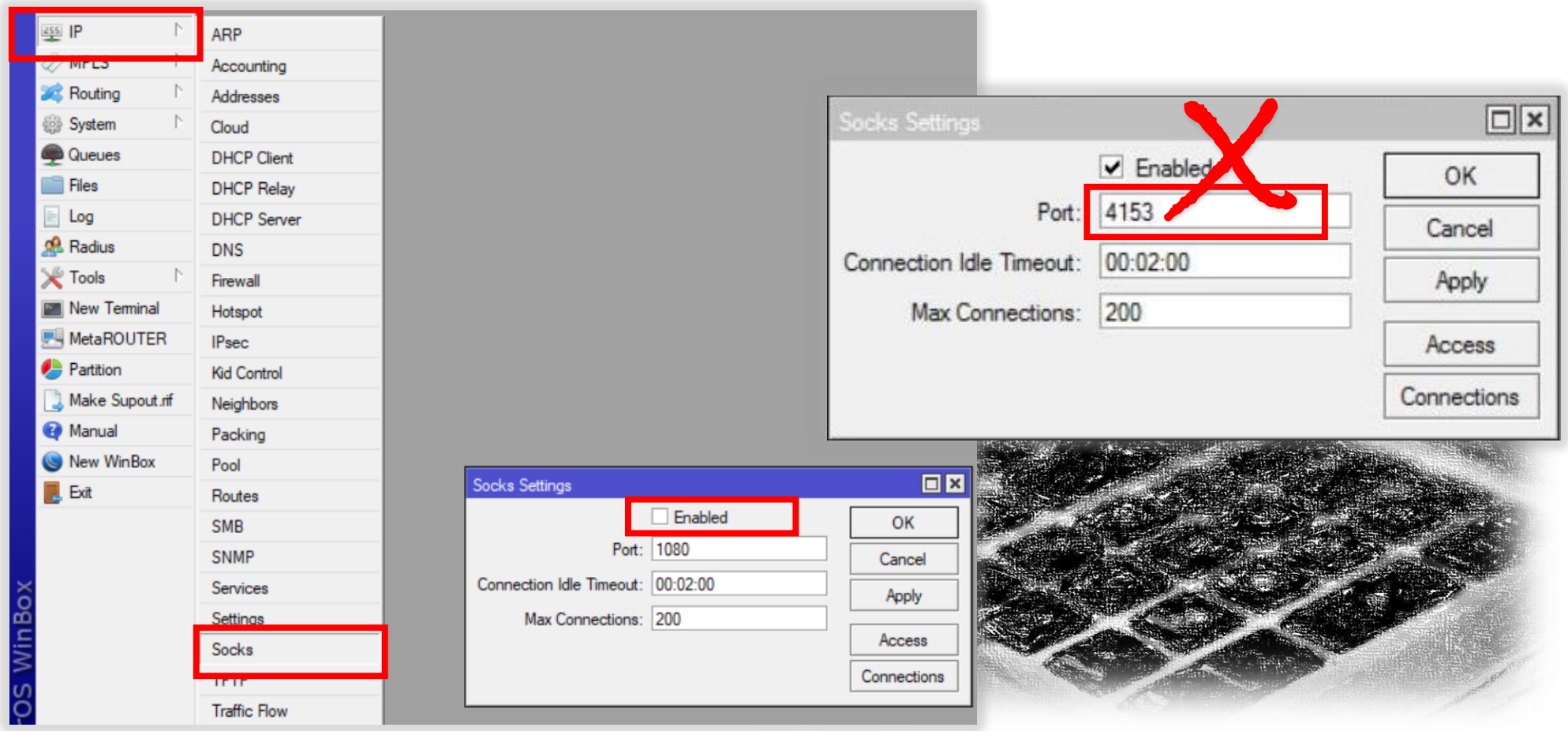
Problemática de Seguridad

- Modificación No Autorizada



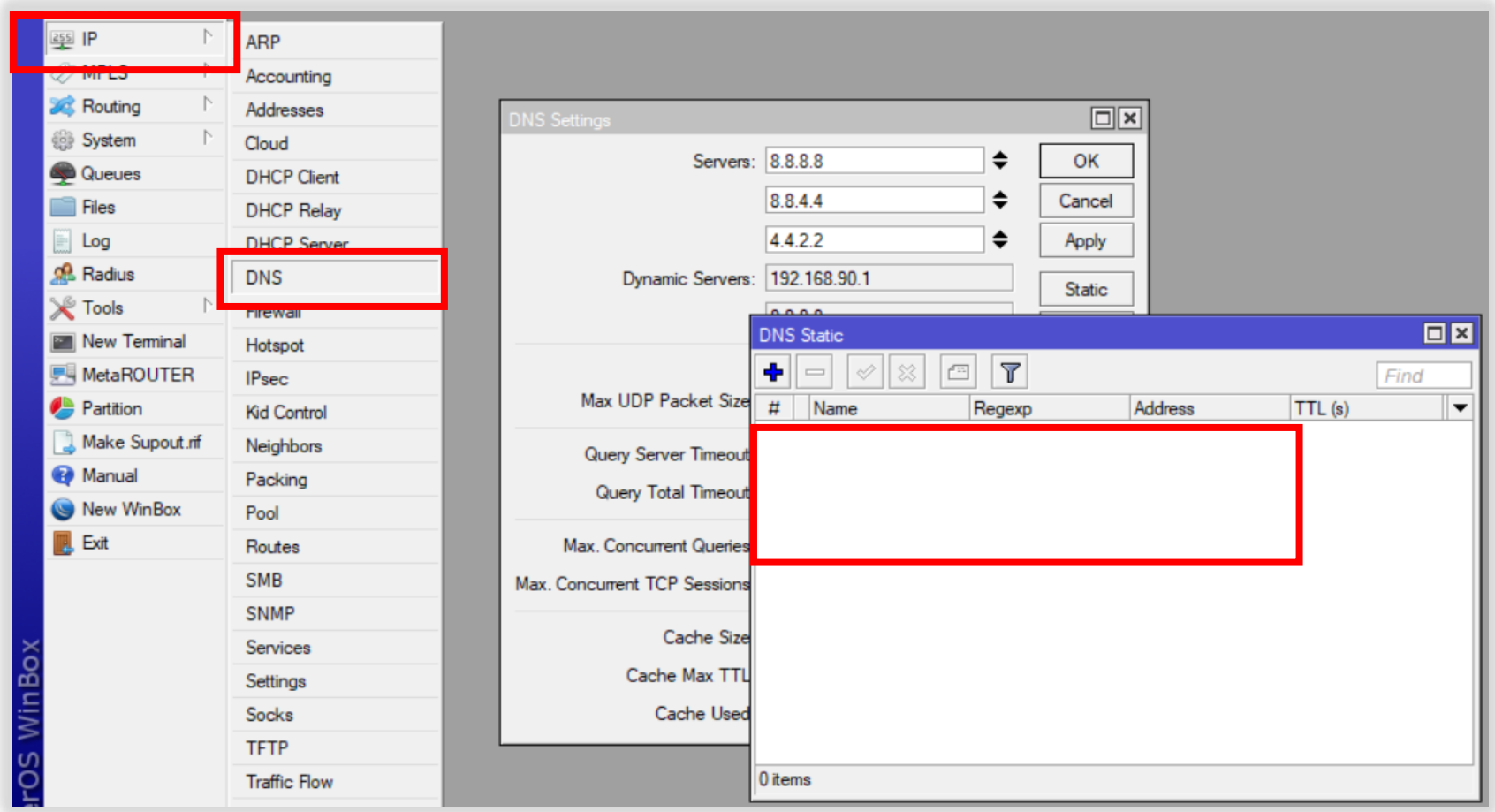
Problemática de Seguridad

- Modificación No Autorizada



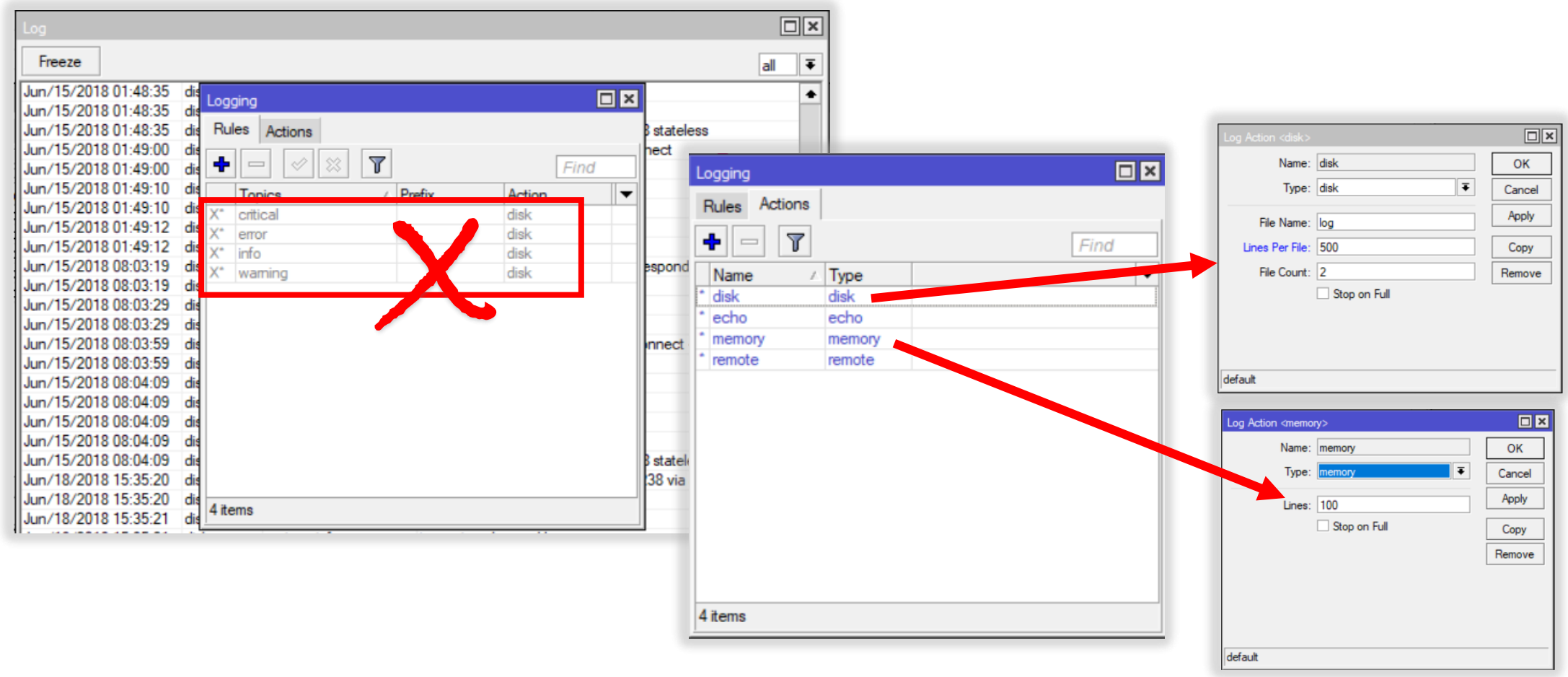
Problemática de Seguridad

- Modificación No Autorizada



Problemática de Seguridad

- Modificación No Autorizada



¿Qué hacer para reducir el riesgo?

Mejorando las políticas de seguridad

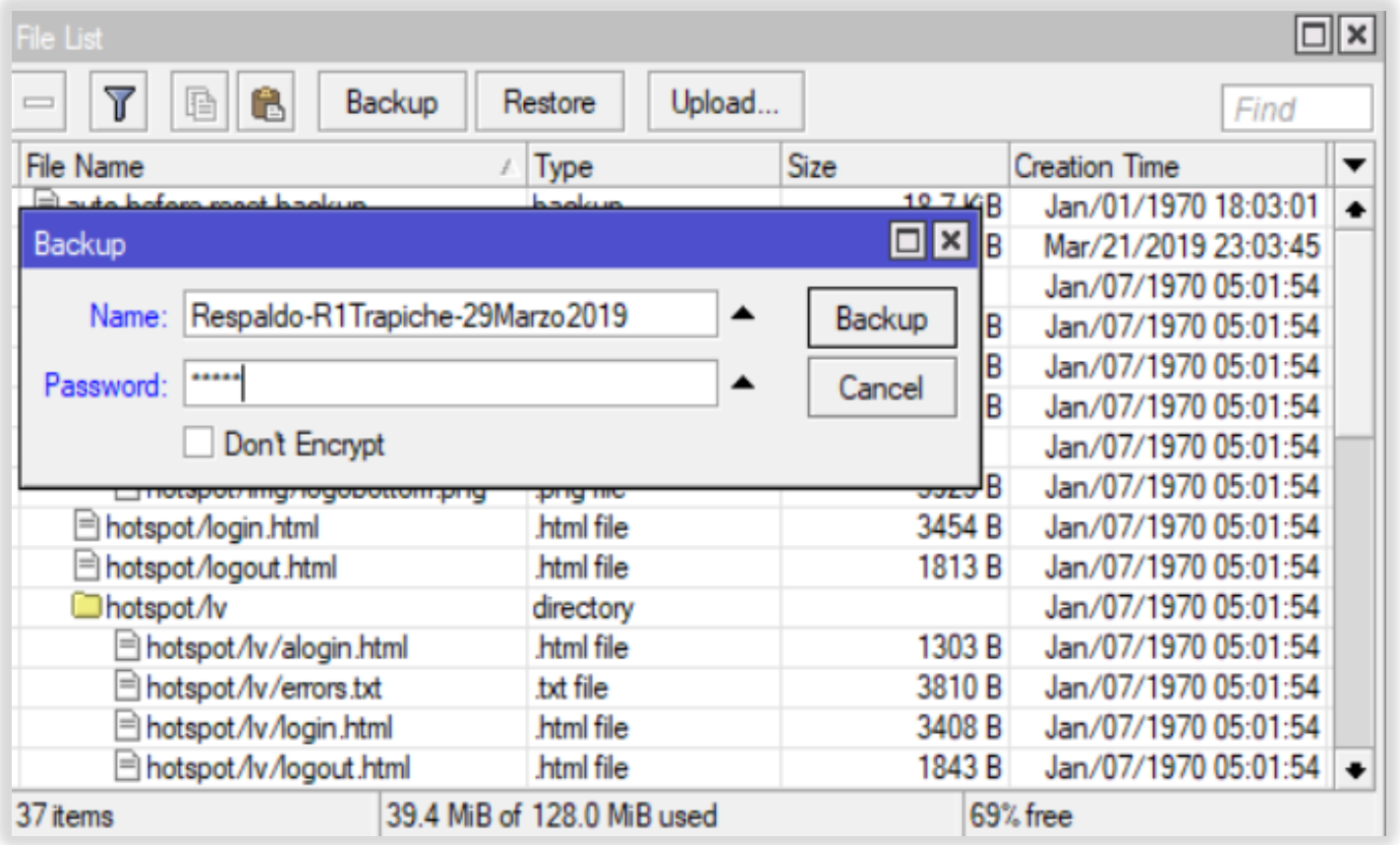
- Todos los equipos son vulnerables

- Algunos riesgos de los cuales tenemos que ser conscientes:
  - Intervención física
  - Vandalismo
  - Daño físico equipo

- Tener sistemas de respaldo de la configuración de cada equipo deseable vía script

Mejorando las políticas de seguridad

- Reducir el riesgo
  - ✓Generar Respaldo



Mejorando las políticas de seguridad

- Reducir el riesgo
  - ✓Script generar respaldo y agendar en tarea para enviarlo por email

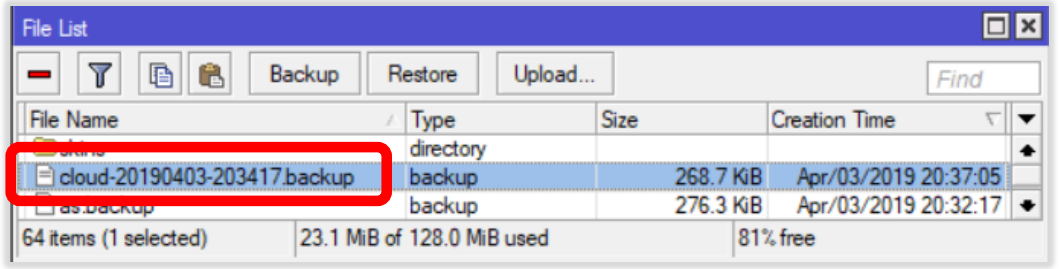
```
/system backup save name=([/system identity get name] . "-" . \
[:pick [/system clock get date] 7 11] . [:pick [/system clock get date] 0 3] . [:pick [/system clock get date]
4 6]); :delay 10; \
/tool e-mail send from=adiaz@index.com.mx start-tls=yes user=respaldomail password=****x server=202.48.16.53
port=587  to=soporte@midominio.com.mx subject=([/system identity get name] . " Respaldo Binario " . \
[/system clock get date]) file=([/system identity get name] . "-" . [:pick [/system clock get date] 7 11] . \
[:pick [/system clock get date] 0 3] . [:pick [/system clock get date] 4 6] . ".backup"); :delay 10; \
/file rem [/file find name=([/system identity get name] . "-" . [:pick [/system clock get date] 7 11] . \
[:pick [/system clock get date] 0 3] . [:pick [/system clock get date] 4 6] . ".backup")]; \
:log info ("System Backup email " . [/sys cl get time] . " " . [/sys cl get date])

/system scheduler
add interval=1d name=Backup-mail on-event=email-backup-bin
policy=ftp,reboot,read,write,policy,test,password,sniff,sensitive start-time=startup
```

Mejorando las políticas de seguridad

- Generar respaldo

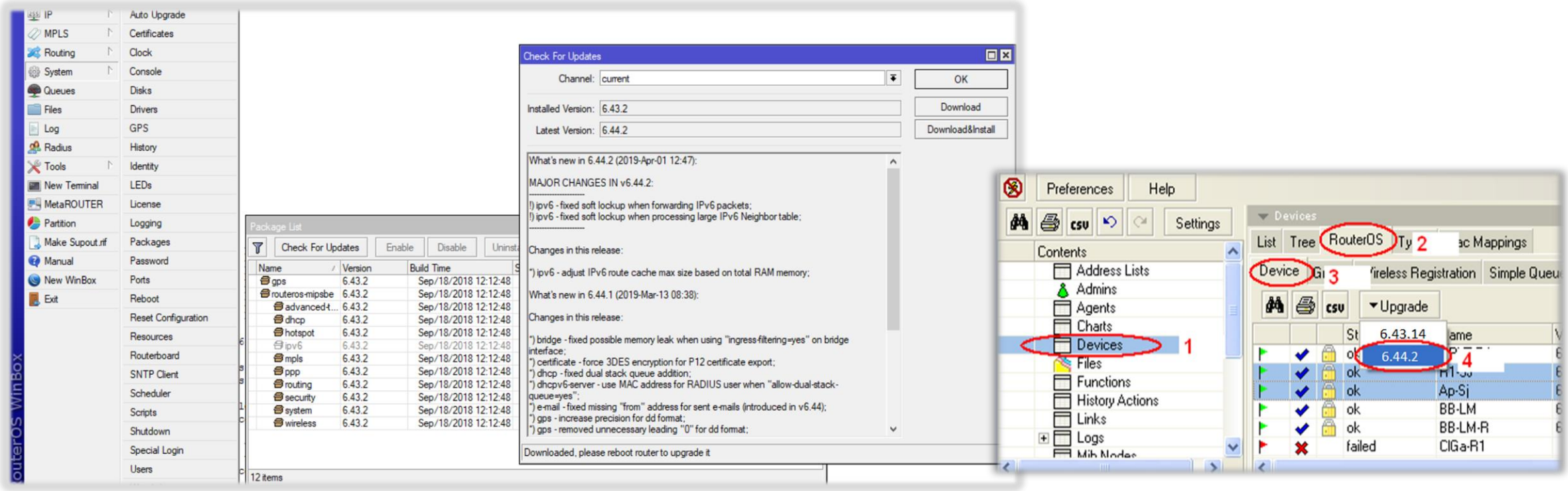
RouterOS v6.44beta9 en adelante tenemos backup en MikroTik's Cloud server

```
/system backup cloud upload-file action=create-and-upload password=MUMMexic0
/system backup cloud print
 0 name="cloud-20190403-203417" size=268.7KiB ros-version="6.44.1"
   date=apr/03/2019 20:34:22 status="ok"
   secret-download-key="jIB*iY*****2ysW*****r9Fw"
/system backup cloud download-file action=download secret-download-key="jIB*iY*****2ysW*****r9Fw"
```



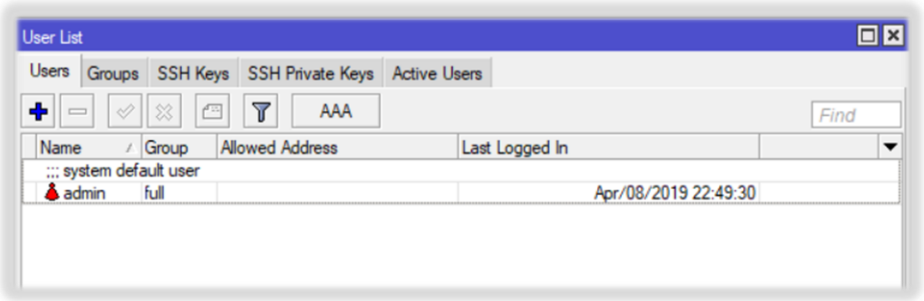
Mejorando las políticas de seguridad

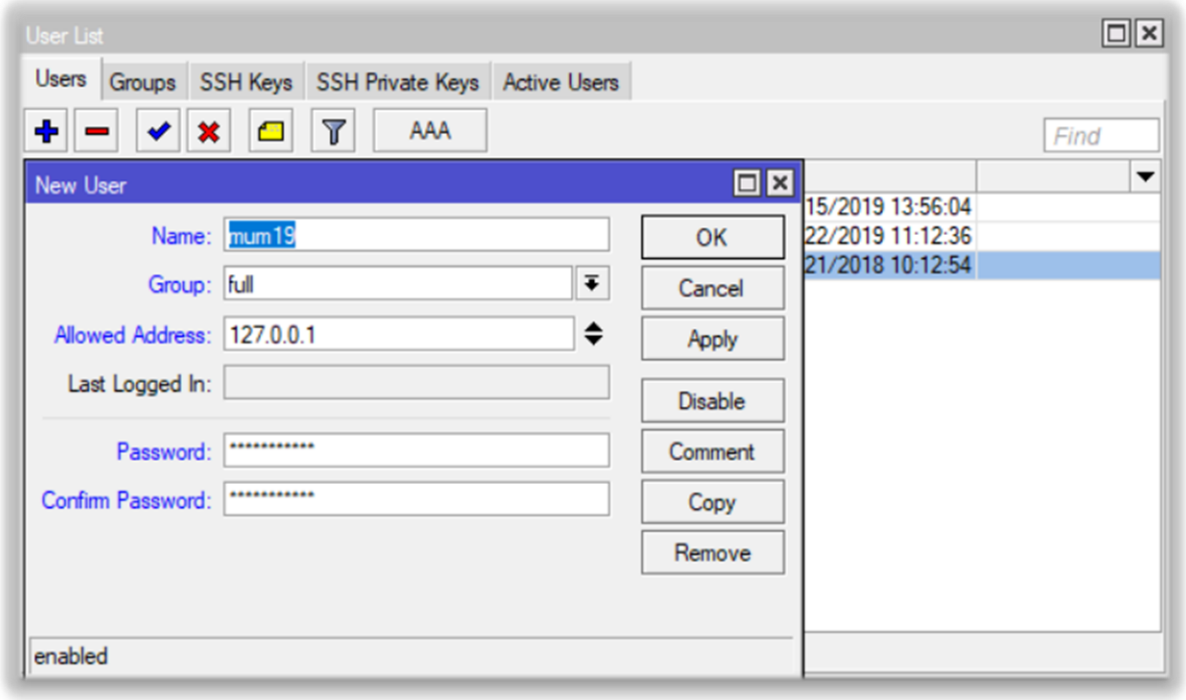
- Ajustes Básicos
  - Actualizar SO al último firmware disponible



Mejorando las políticas de seguridad

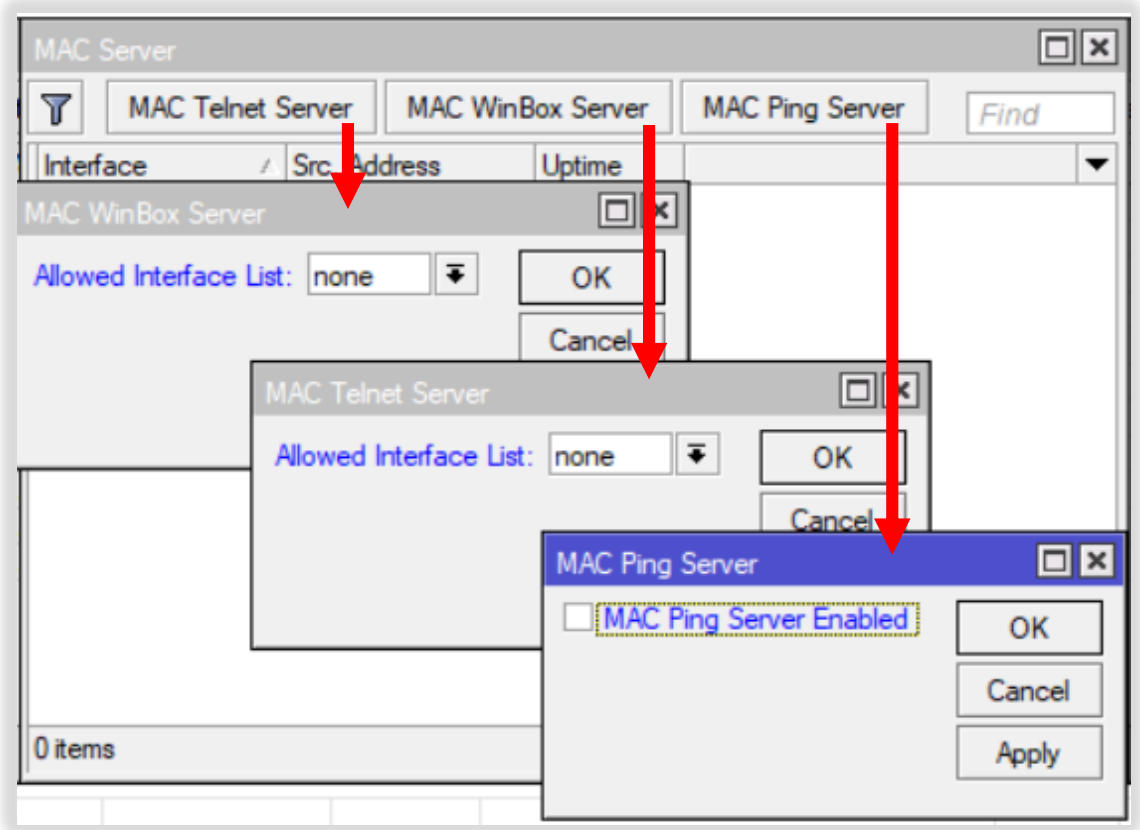
- Ajustes Básicos
  - Elimina el usuario por default
  - Cambia credenciales regularmente
  - Si te es posible usa radius





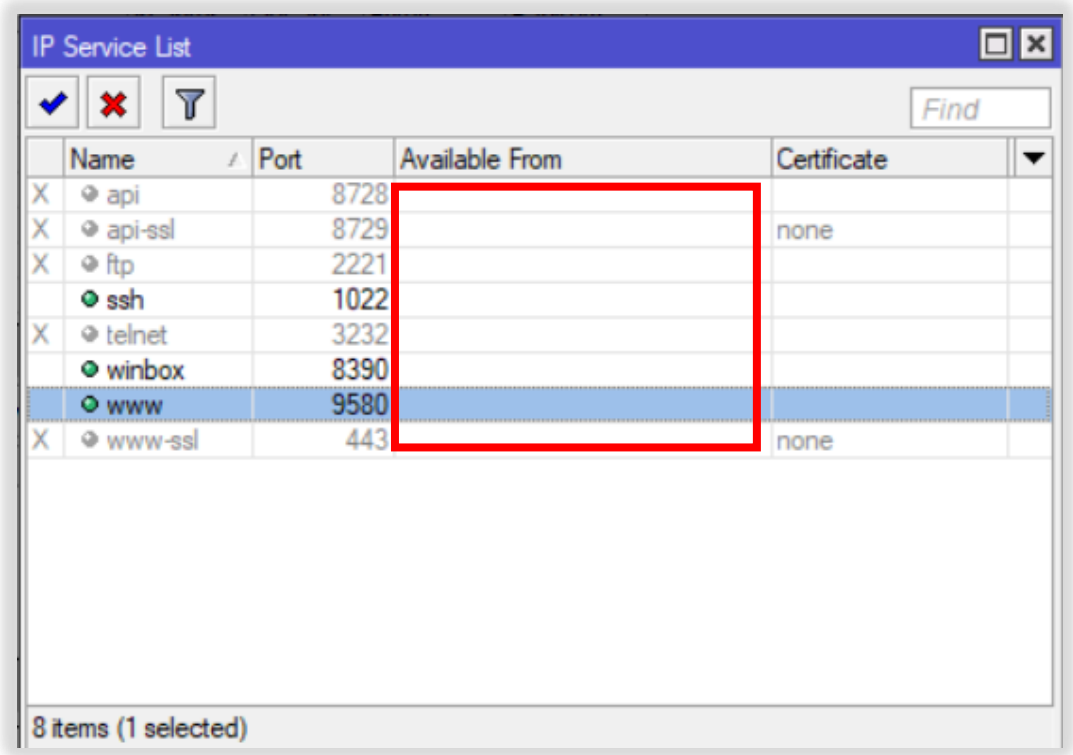
Mejorando las políticas de seguridad

- Ajustes Básicos
  - Cambiar las políticas de los servicios de acceso al equipo de capa 2



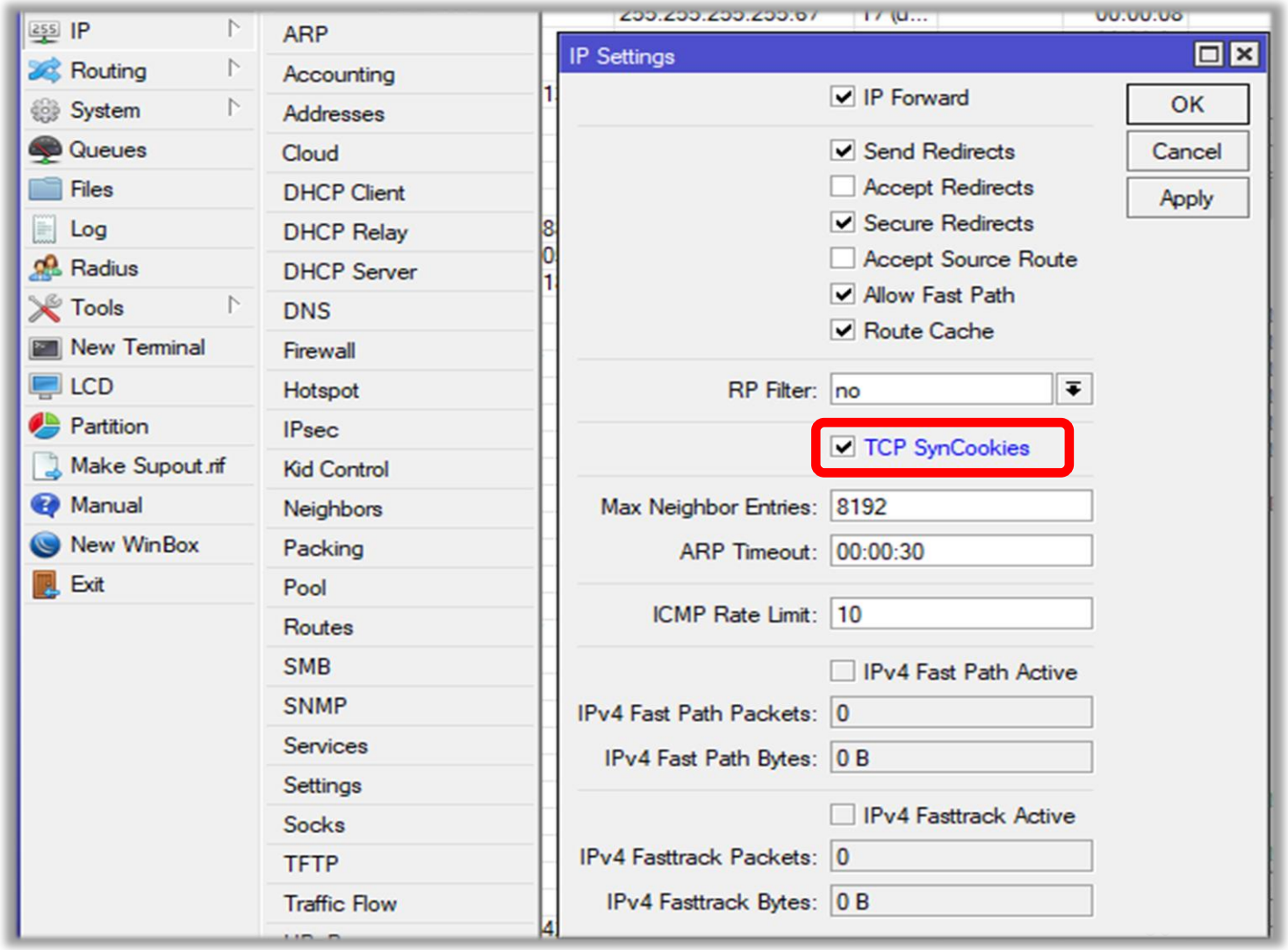
Mejorando las políticas de seguridad

- Ajustes Básicos
  - Cambiar las políticas de los servicios de acceso al equipo
  - Definir redes permitidas en cada servicio



Mejorando las políticas de seguridad

- Ajustes Básicos
  - >ip settings set tcp-syncookies=Yes



Mejorando las políticas de seguridad

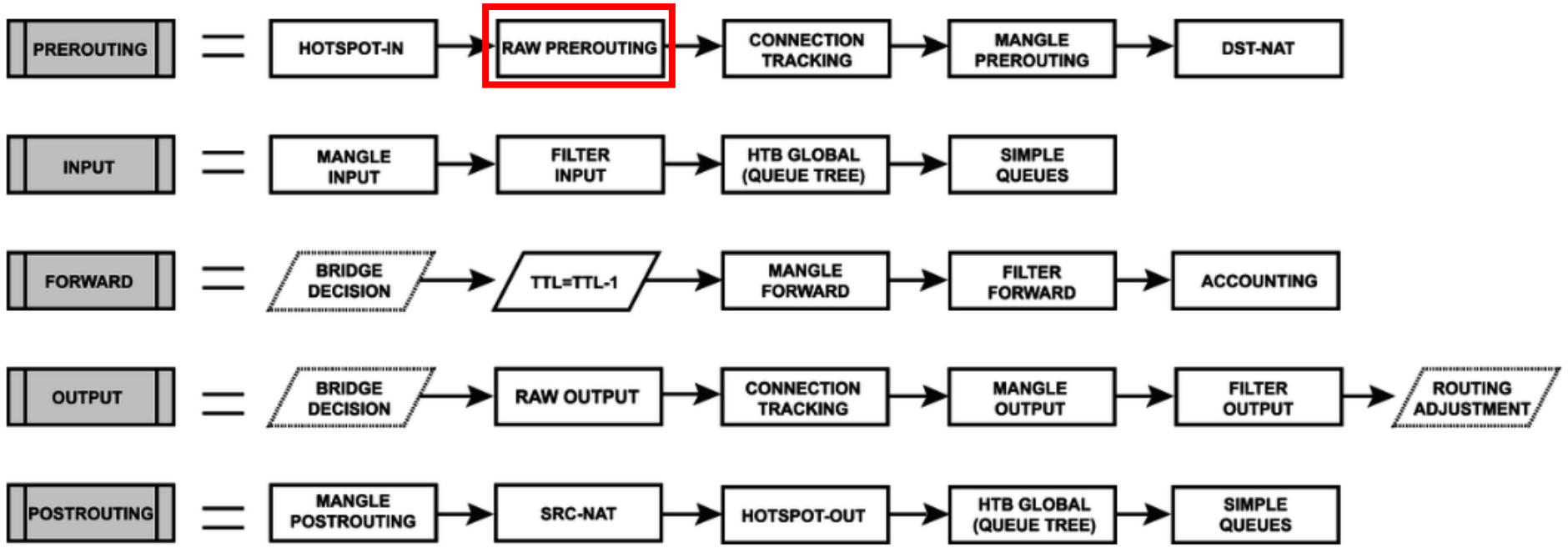
- Ajustes Básicos
  - Mejorando Criptografía para SSH

```
Terminal
[go@MUM MEXICO] > ip ssh set strong-crypto=yes
[go@MUM MEXICO] > ip ssh pr
            forwarding-enabled: no
  always-allow-password-login: no
                strong-crypto: yes
             allow-none-crypto: no
                host-key-size: 2048
[go@MUM MEXICO] >
```

Ajustando Firewall

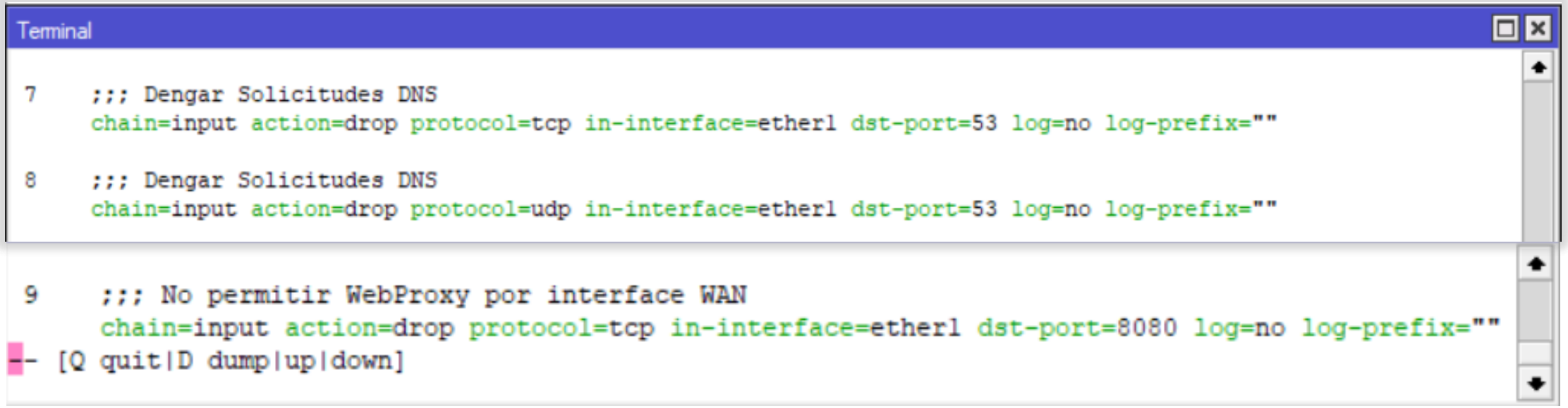
Mejorando las políticas de seguridad

- RAW
  - Permite o dropea paquetes antes de connection tracking
  - Reduce carga del CPU.
  - Muy útil para mitigar ataques DoS.



Mejorando las políticas de seguridad

- Configurando políticas en firewall
  - Denegar solicitudes DNS y WebProxy por interface WAN



Mejorando las políticas de seguridad

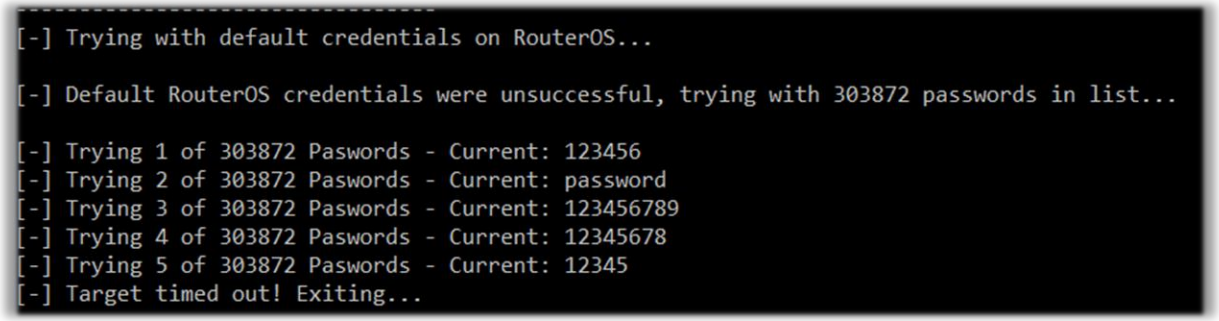
- Configurando políticas en firewall
  - Limitando el servicio API a 5 intentos de conexión por IP

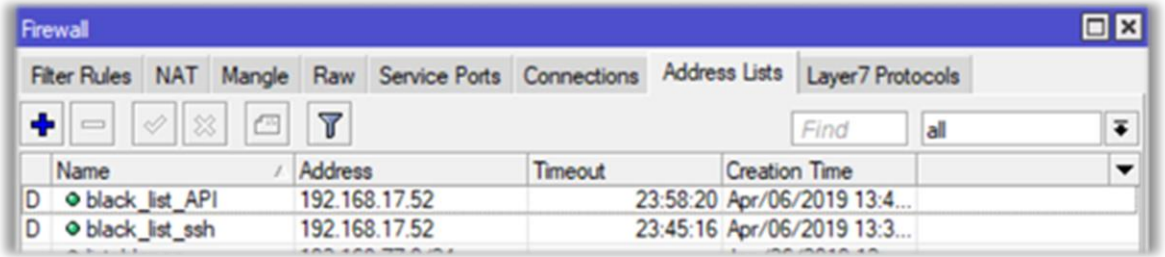
Terminal

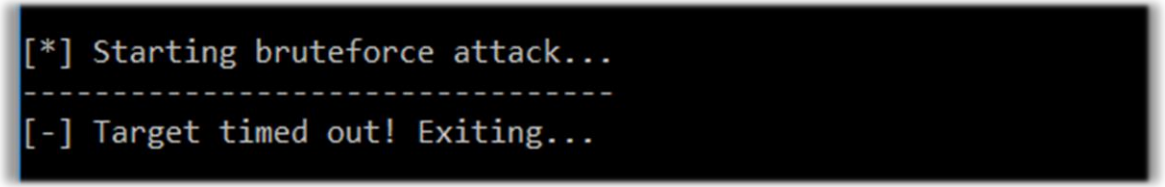
```
[go@MUM MEXICO] > ip fi fi pr
Flags: X - disabled, I - invalid, D - dynamic
 0    ;;; BLOQUEA LA IP DURANTE 24 HORAS SI PASA POR LAS 5 LISTAS  API!
      chain=input action=drop protocol=tcp src-address-list=black_list_API dst-port=8728 log=no log-prefix=""

 1    chain=input action=add-src-to-address-list connection-state=new protocol=tcp src-address-list=API_list5
      address-list=black_list_API address-list-timeout=1d dst-port=8728

 2    chain=input action=add-src-to-address-list connection-state=new protocol=tcp src-address-list=API_list4
      address-list=API_list5 address-list-timeout=1m dst-port=8728

 3    chain=input action=add-src-to-address-list connection-state=new protocol=tcp src-address-list=API_list3
      address-list=API_list4 address-list-timeout=1m dst-port=8728

 4    chain=input action=add-src-to-address-list connection-state=new protocol=tcp src-address-list=API_list2
      address-list=API_list3 address-list-timeout=1m dst-port=8728

 5    chain=input action=add-src-to-address-list connection-state=new protocol=tcp src-address-list=API_list1
      address-list=API_list2 address-list-timeout=1m dst-port=8728

 6    chain=input action=add-src-to-address-list connection-state=new protocol=tcp address-list=API_list1
      address-list-timeout=20s dst-port=8728
```

Mejorando las políticas de seguridad

- Limitando el servicio API a 5 intentos de conexión por IP

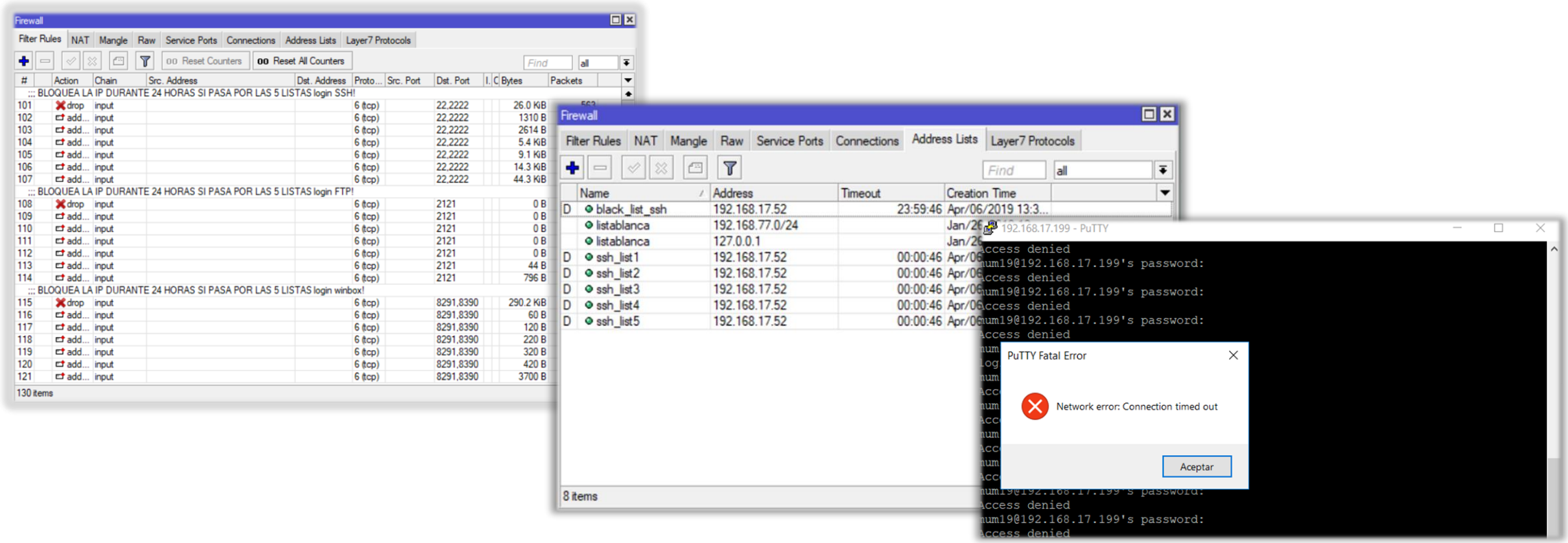






Mejorando las políticas de seguridad

- Limitando el número de intentos servicio SSH



Mejorando las políticas de seguridad

- Configurando políticas en firewall
  - Generamos una lista de acceso temporal en base a una secuencia de puertos

Port Knocking

Secuencia puertos tcp 9326 9127 2739

Mejorando las políticas de seguridad

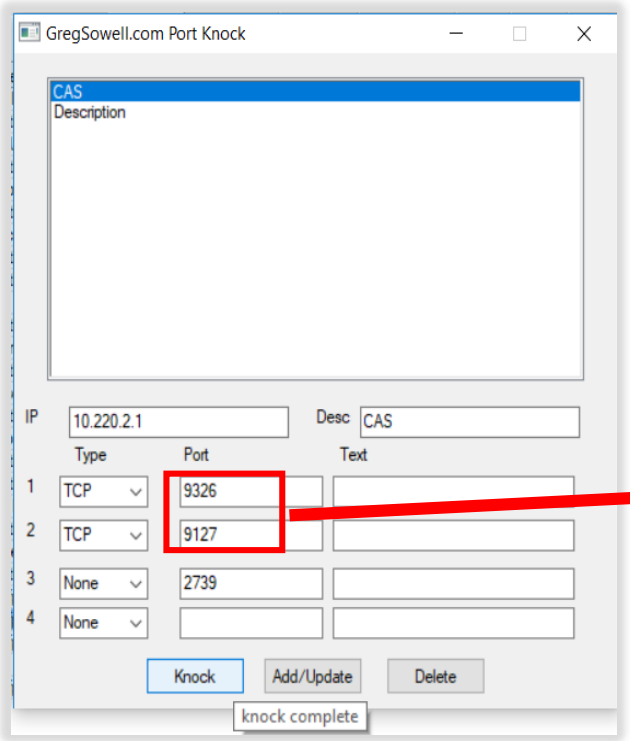
- **Port Knocking**

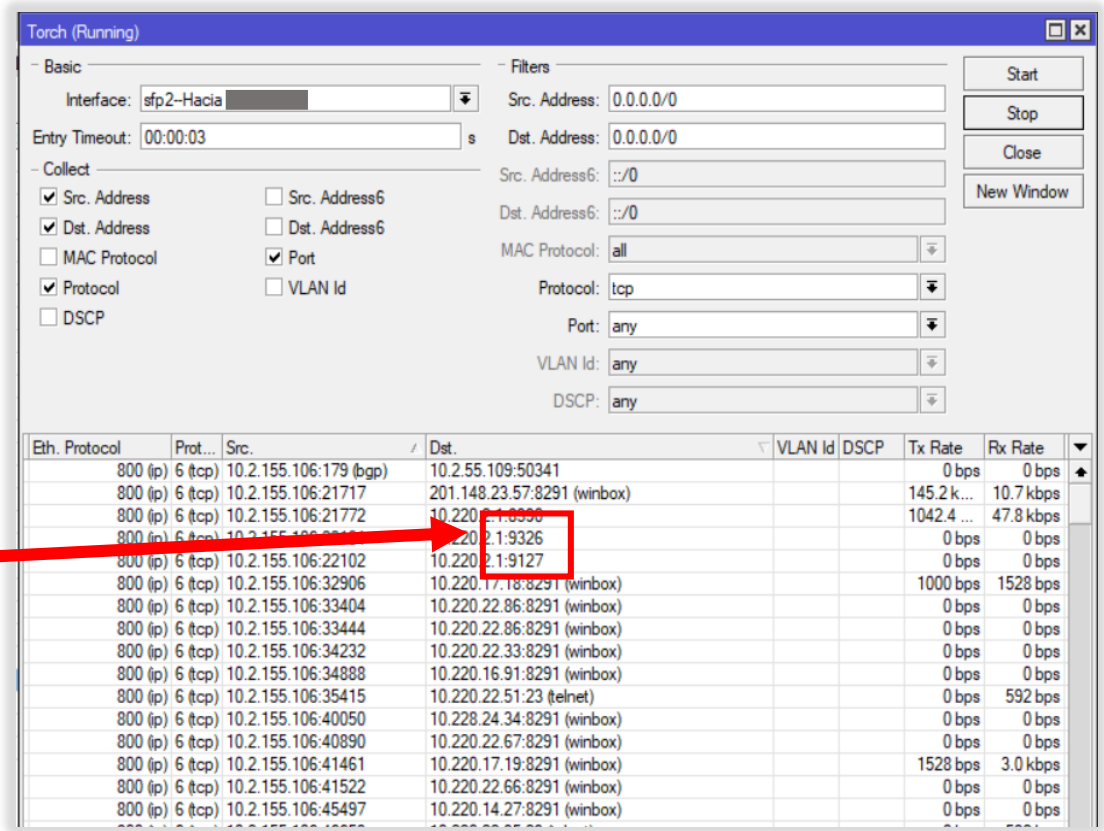
Router> /ip firewall filter

```
add action=add-src-to-address-list address-list=pase1
address-list-timeout=1m chain=input comment=Autorizacion
dst-port=9326 protocol=tcp

add action=add-src-to-address-list address-list=pase2
address-list-timeout=1m chain=input dst-port=9127
protocol=tcp src-address-list=pase1

add action=add-src-to-address-list address-list=listablanca
address-list-timeout=2m chain=input dst-port=2739
protocol=tcp src-address-list=pase2

add action=drop chain=input comment="permitir conexión
Winbox  si esta en lista blanca" dst-port=8395 protocol=tcp
src-address-list=! listablanca
```

Mejorando las políticas de seguridad

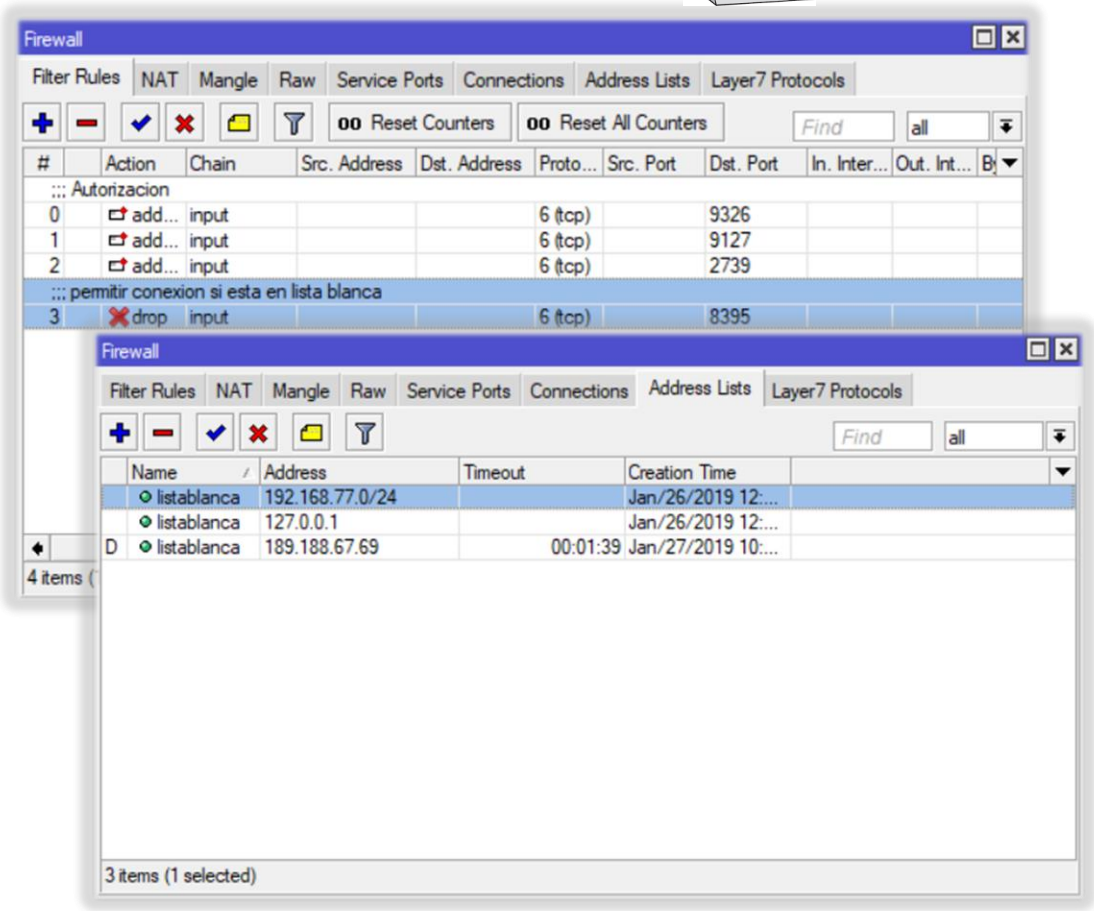
- **Port Knocking**

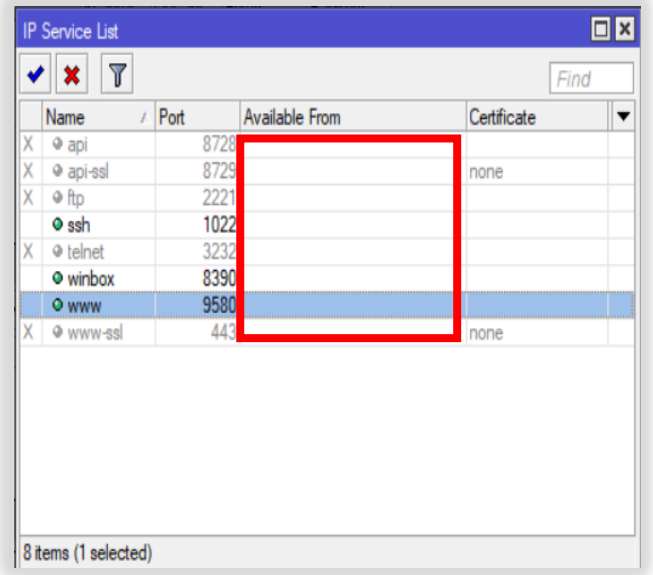




Mejorando las políticas de seguridad

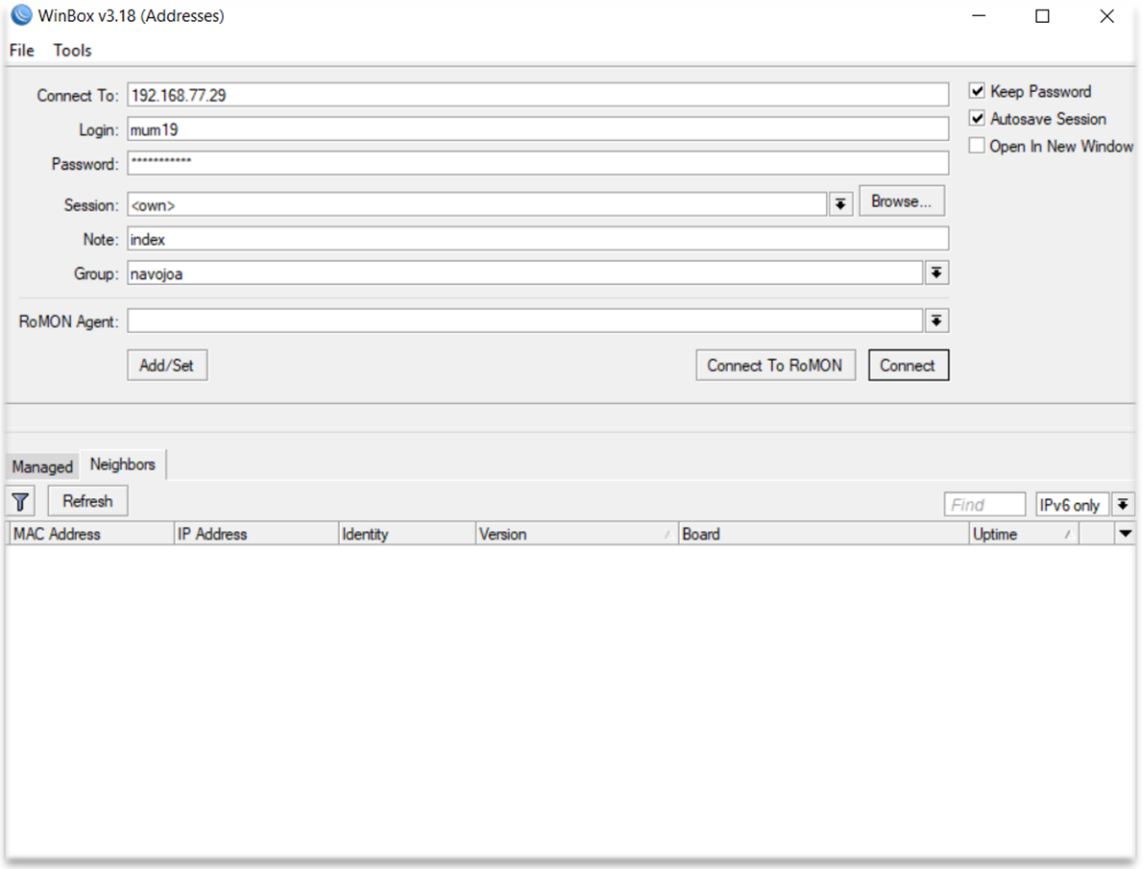
- **Port Knocking**

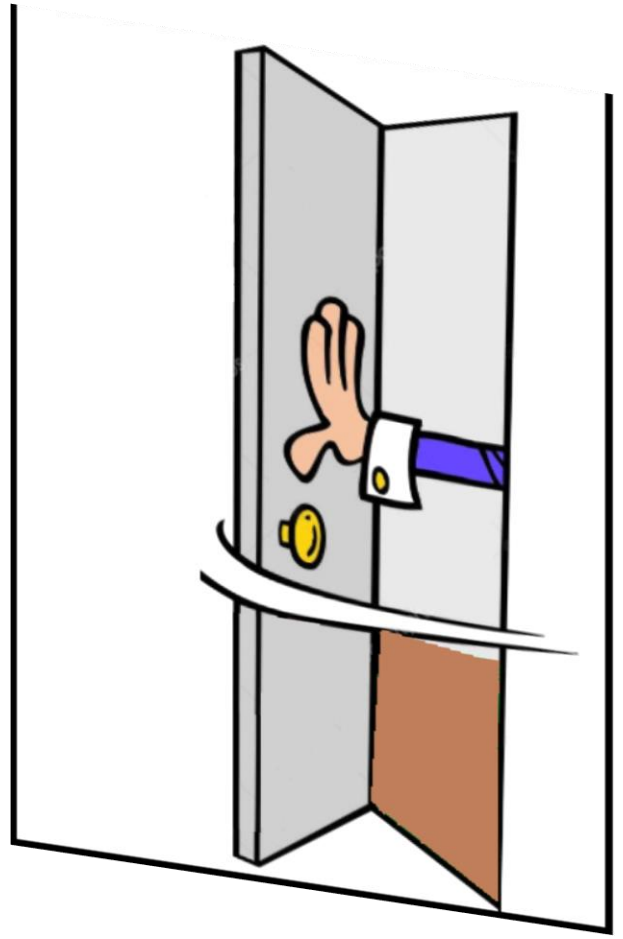




Mejorando las políticas de seguridad

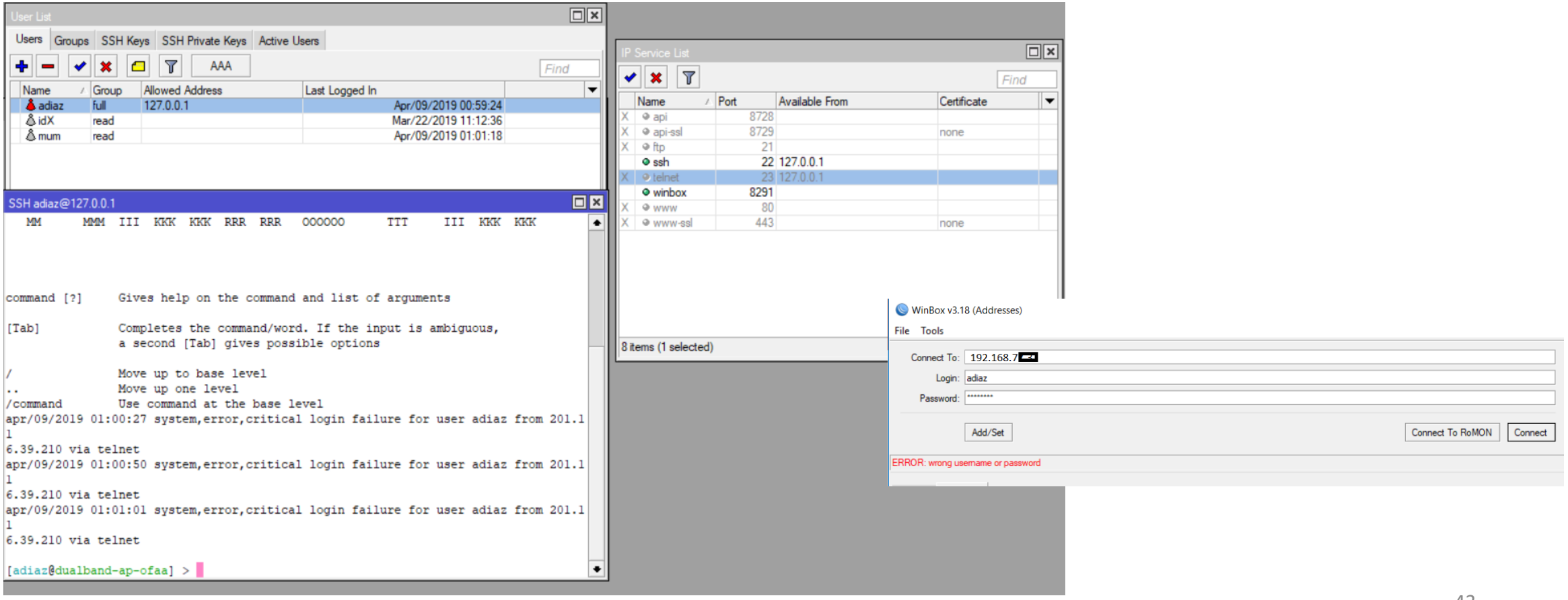
- **Port Knocking**





Mejorando las políticas de seguridad

- Limitando usuarios



Mejorando las políticas de seguridad

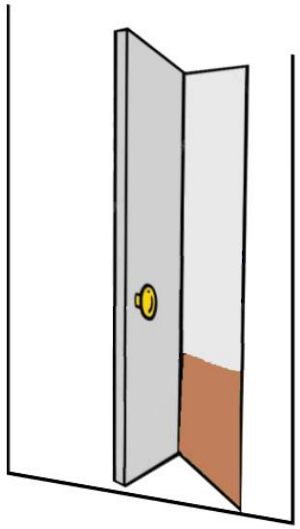
- **Resumiendo**

Ip firewall filter
telnet 23 drop
ftp 21 drop
www 8183 drop
ssh 2210 drop
api 8728 drop
winbox 8491 drop

Tocamos secuencias de puertos en un lapso corto
tcp 9326 9127 2739

Si los toques fueron en el orden definido permitimos la ip origen que tocó dichos puertos

Nos asomamos si permitimos la conexión de esa ip en las redes de ip services port



Si la ip esta en lista blanca y esta permitida en los services esta lista para autenticarse por winbox

Mejorando las políticas de seguridad

###SSH y WINBOX BLOCK

/ip firewall filter

add action=drop chain=input comment="BLOQUEA LA IP DURANTE 24 HORAS SI PASA POR LAS 5 LISTAS login SSH!" dst-port=22 protocol=tcp src-address-list=black_list_ssh

add action=add-src-to-address-list address-list=black_list_ssh address-list-timeout=1d chain=input connection-state=new dst-port=22 protocol=tcp src-address-list=ssh_list5

add action=add-src-to-address-list address-list=ssh_list5 address-list-timeout=1m chain=input connection-state=new dst-port=22 protocol=tcp src-address-list=ssh_list4

add action=add-src-to-address-list address-list=ssh_list4 address-list-timeout=1m chain=input connection-state=new dst-port=22 protocol=tcp src-address-list=ssh_list3

add action=add-src-to-address-list address-list=ssh_list3 address-list-timeout=1m chain=input connection-state=new dst-port=22 protocol=tcp src-address-list=ssh_list2

add action=add-src-to-address-list address-list=ssh_list2 address-list-timeout=1m chain=input connection-state=new dst-port=22 protocol=tcp src-address-list=ssh_list1

add action=add-src-to-address-list address-list=ssh_list1 address-list-timeout=1m chain=input connection-state=new dst-port=22 protocol=tcp

add action=drop chain=input comment="BLOQUEA LA IP DURANTE 24 HORAS SI PASA POR LAS 5 LISTAS login winbox!" dst-port=8291 protocol=tcp src-address-list=black_list_winbox

add action=add-src-to-address-list address-list=black_list_winbox address-list-timeout=1d chain=input connection-state=new dst-port=8291 protocol=tcp src-address-list=winbox_list5

add action=add-src-to-address-list address-list=winbox_list5 address-list-timeout=3m chain=input connection-state=new dst-port=8291 protocol=tcp src-address-list=winbox_list4

add action=add-src-to-address-list address-list=winbox_list4 address-list-timeout=3m chain=input connection-state=new dst-port=8291 protocol=tcp src-address-list=winbox_list3

add action=add-src-to-address-list address-list=winbox_list3 address-list-timeout=3m chain=input connection-state=new dst-port=8291 protocol=tcp src-address-list=winbox_list2

add action=add-src-to-address-list address-list=winbox_list2 address-list-timeout=3m chain=input connection-state=new dst-port=8291 protocol=tcp src-address-list=winbox_list1

add action=add-src-to-address-list address-list=winbox_list1 address-list-timeout=3m chain=input connection-state=new dst-port=8291 protocol=tcp

/ip firewall filter

add action=add-src-to-address-list address-list=pase1 address-list-timeout=1m chain=input comment=Autorizacion dst-port=9326 protocol=tcp

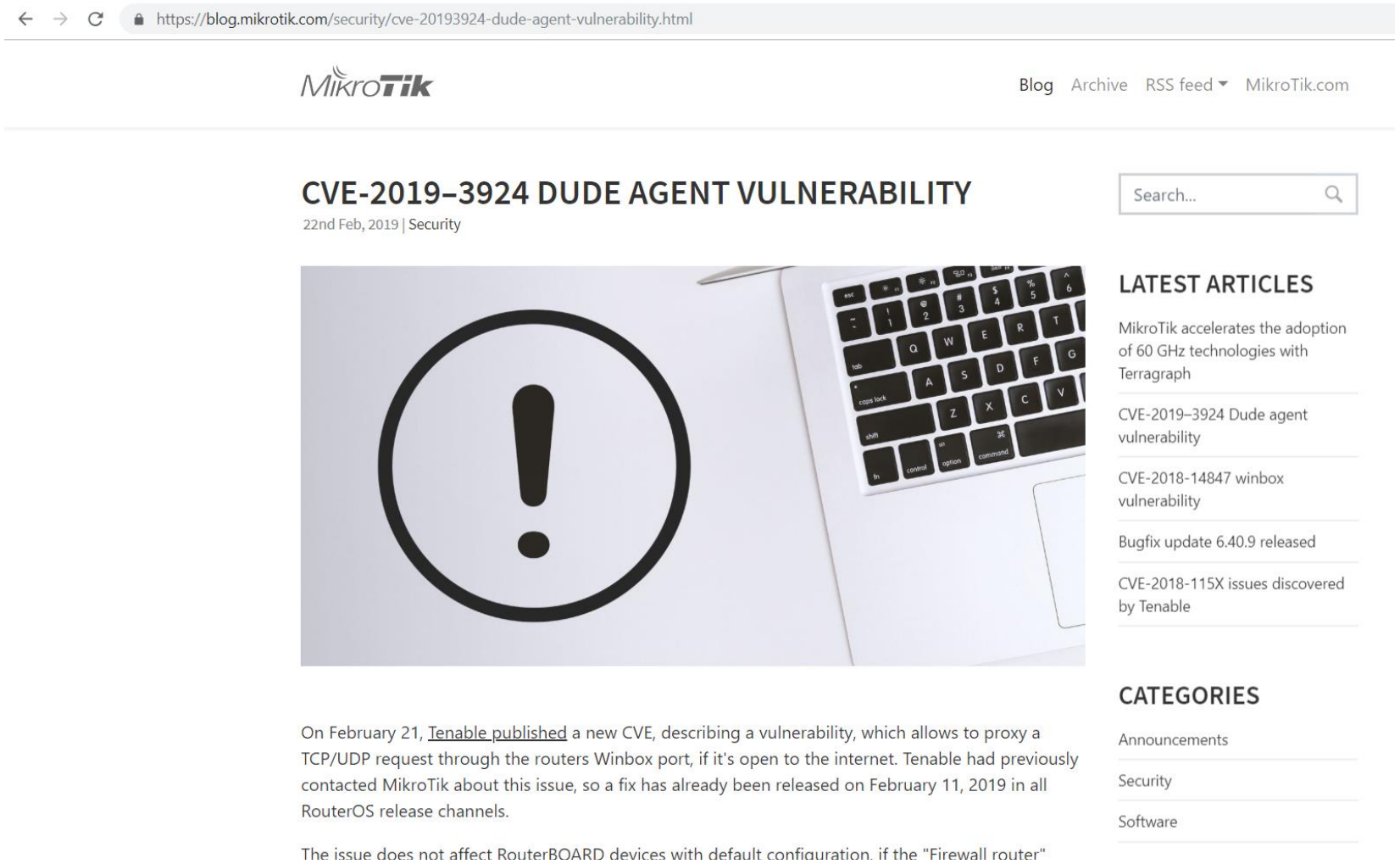
add action=add-src-to-address-list address-list=pase2 address-list-timeout=1m chain=input dst-port=9127 protocol=tcp src-address-list=pase1

add action=add-src-to-address-list address-list=listablanca address-list-timeout=2m chain=input dst-port=2739 protocol=tcp src-address-list=pase2

add action=drop chain=input comment="permitir conexión Winbox si esta en lista blanca" dst-port=8395 protocol=tcp src-address-list=! listablanca

Mejorando las políticas de seguridad

- https://blog.mikrotik.com/security/



Preguntas

¡Gracias!

http://www.index.com.mx

http://www.mikrotik-mexico.com.mx

01 800 22 INDEX • (668) 816 46 00 • (0155) 71 58 93 87

Email: adiaz@index.com.mx