Tips para Principiantes + HotSpot (Seguridad, User Manager)

Armando Cartagena
ITDES

23 de Julio de 2018

Tegucigalpa

Honduras

Presentación Personal

- ✓ Nombre: Jose Armando Cartagena Mendoza.
- ✓ Pasante Universitario.
- ✓ Estudiante del Instituto Técnico Departamental “Espíritu del Siglo”. (2011-2017)
- ✓ Experiencia desde 2015.


Cartagenam13


@Cartagenam13


+504 9511-5263


Cartagenam13@gmail.com

Acerca de la institución

- ✓ Fundado en 1930.
- ✓ Institución Publica.
- ✓ 65 Docentes.
- ✓ Colegio - Técnico Insignia Del Departamento De Colon.
- ✓ Oferta Educativa:
  - 5 BTP Y 1 BCH.
  - Ciclo Básico Técnico.

Introducción & Objetivos

Tips Básicos-Principiante

MikroTik® (RouterOS y Routerboard) nos ofrece herramientas muy poderosa y sobre todo demasiado amplias, pero como en todos los casos, hay que saber configurarlo correctamente.

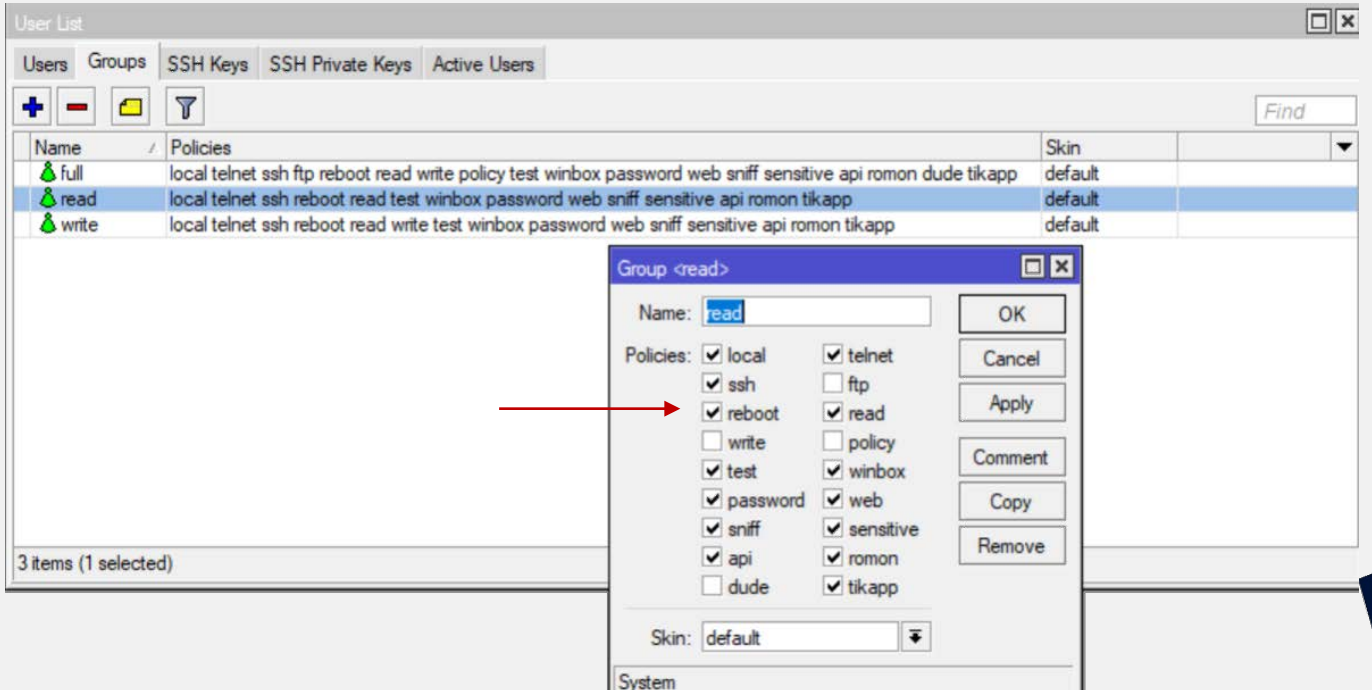
- ✓ Mostrar los descuidos mas comunes.
- ✓ Demostrar que con unos pocos pasos se pueden mejorar las configuraciones, incrementando la seguridad y reduciendo las posibles fallas.

Usuarios por Defecto

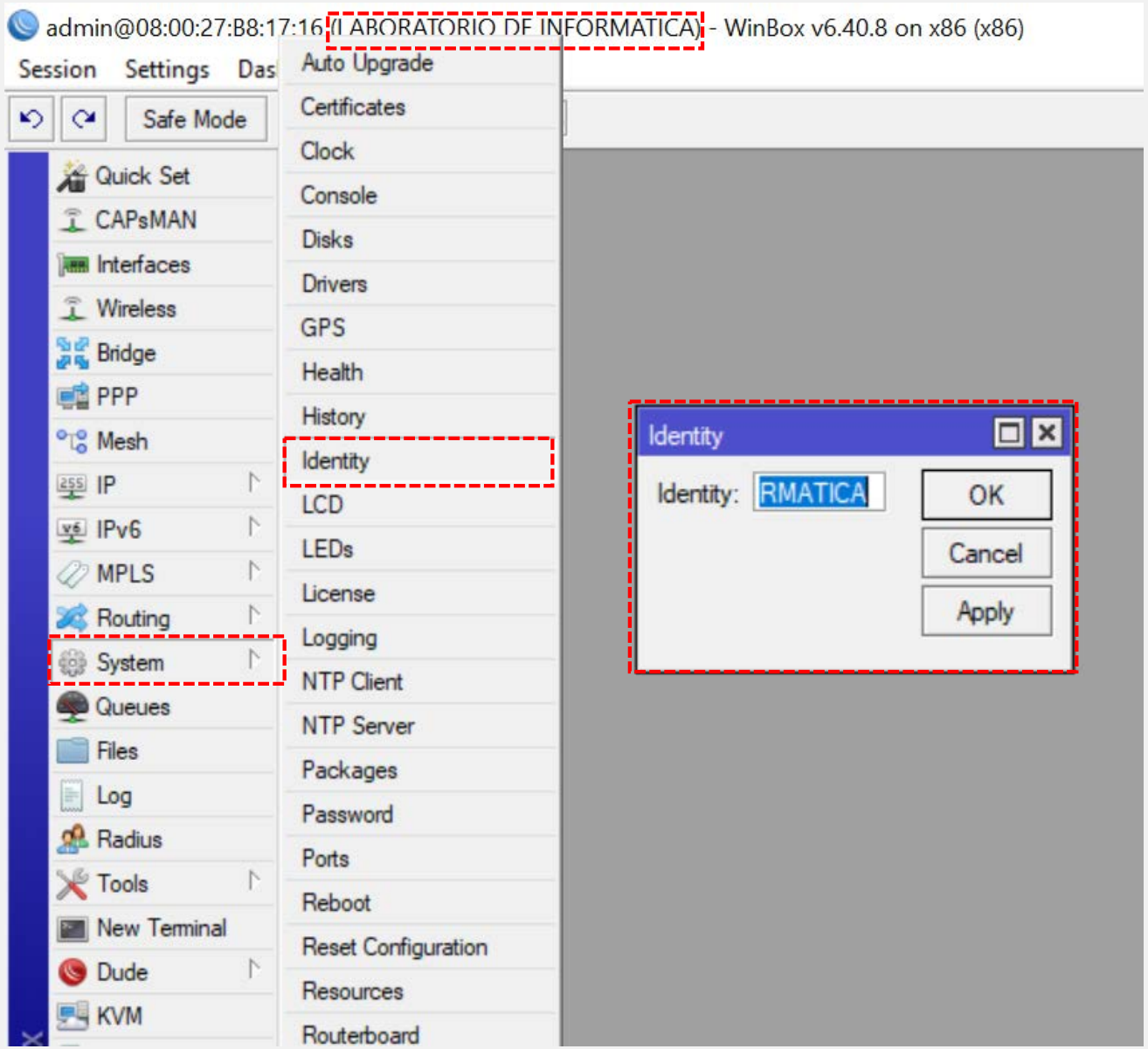
- ✓ Descuidos en los accesos por defecto, dejando la puerta completamente abierta para ingresar al router con las credenciales por defecto.

Usuario	Contraseña
Admin	
Admin	1234
User1	

- ✓ Casos en que a User1 le otorgamos permiso solo de lectura y Admin con permisos Full

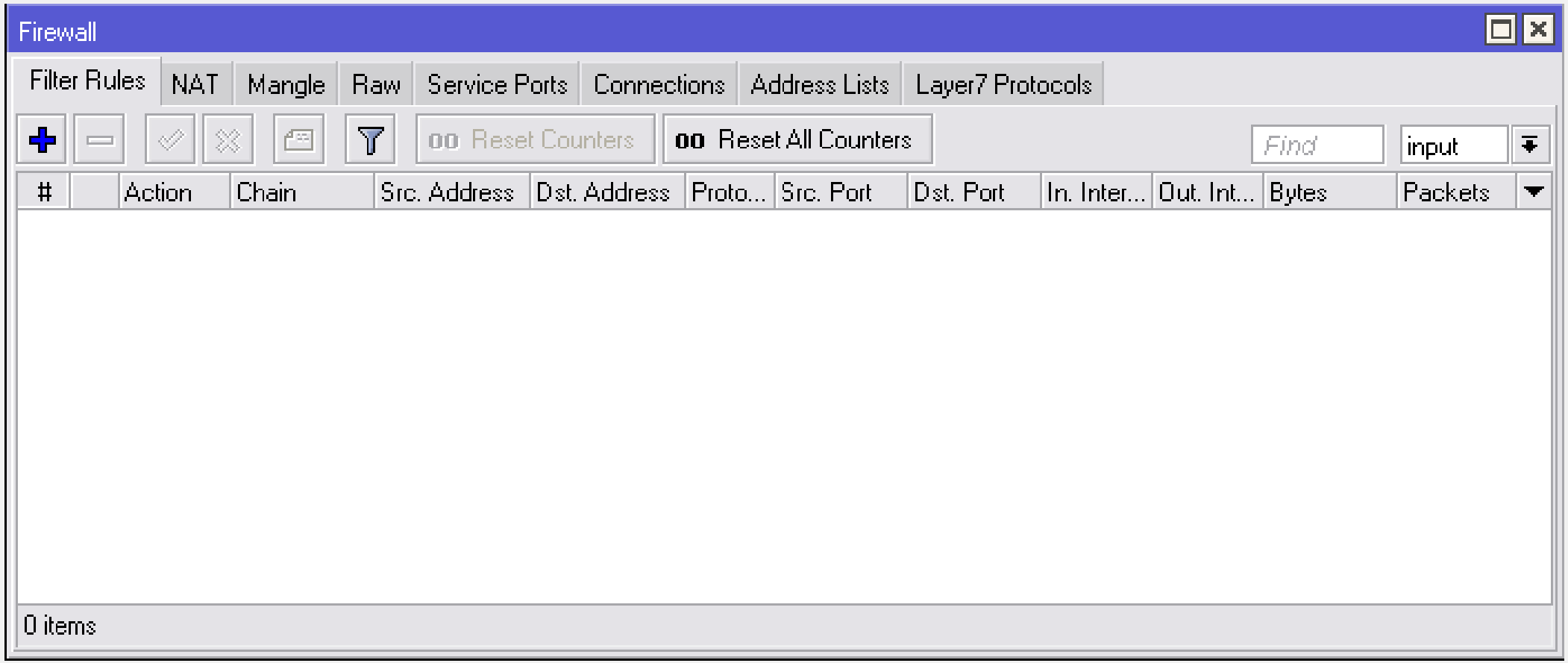


Identifica Tu Equipo



Firewall

- ✓ Una de las primeras acciones a realizar en todo equipo es poner al menos un pequeño firewall para prevenir los ataques más comunes.



Firewall

Los ataques tienen principalmente 2 objetivos:

- ✓ Tomar el control del router.
- ✓ Provocar una denegación de servicios (CPU 100%, consumo de todo el ancho de banda, etc.)

Principales problemas:

- ✓ Ataques por Fuerza Bruta
- ✓ Ataque al DNS

Firewall

Ataque por Fuerza Bruta

```
[rcaire@suyai /home/rcaire]% python3 mkbrutus.py -t 192.168.0.11 -d dictionary2.txt

                Mikrotik RouterOS Bruteforce Tool 1.0.0
          Ramiro Caire (@rcaire) & Federico Massa (@fgmassa)

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

[-] Default RouterOS credentials were unsuccessful, trying with user's password list...

[-] Trying User: admin Pasword: 1234
[-] Trying User: admin Pasword: 12345
[-] Trying User: admin Pasword: 123456
[-] Trying User: admin Pasword: 1234567
[-] Trying User: admin Pasword: 12345678
[-] Trying User: admin Pasword: porsche
[-] Trying User: admin Pasword: dragon
[-] Trying User: admin Pasword: qwerty
[-] Trying User: admin Pasword: 696969
[-] Trying User: admin Pasword: mustang
[-] Trying User: admin Pasword: letmein
[-] Trying User: admin Pasword: baseball
[-] Trying User: admin Pasword: master
[-] Trying User: admin Pasword: michael
[-] Trying User: admin Pasword: football
[-] Trying User: admin Pasword: shadow
[-] Trying User: admin Pasword: monkey
[-] Trying User: admin Pasword: abc123
[-] Trying User: admin Pasword: jordan
[-] Trying User: admin Pasword: pass
[-] Trying User: admin Pasword: password
[-] Trying User: admin Pasword: P@ssw0rd
[+] Login successful!!! User: admin Password: P@ssw0rd
```

Ataque por DNS

Torch (Running)

Basic

Interface: wan

Entry Timeout: 00:00:03 s

Collect

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

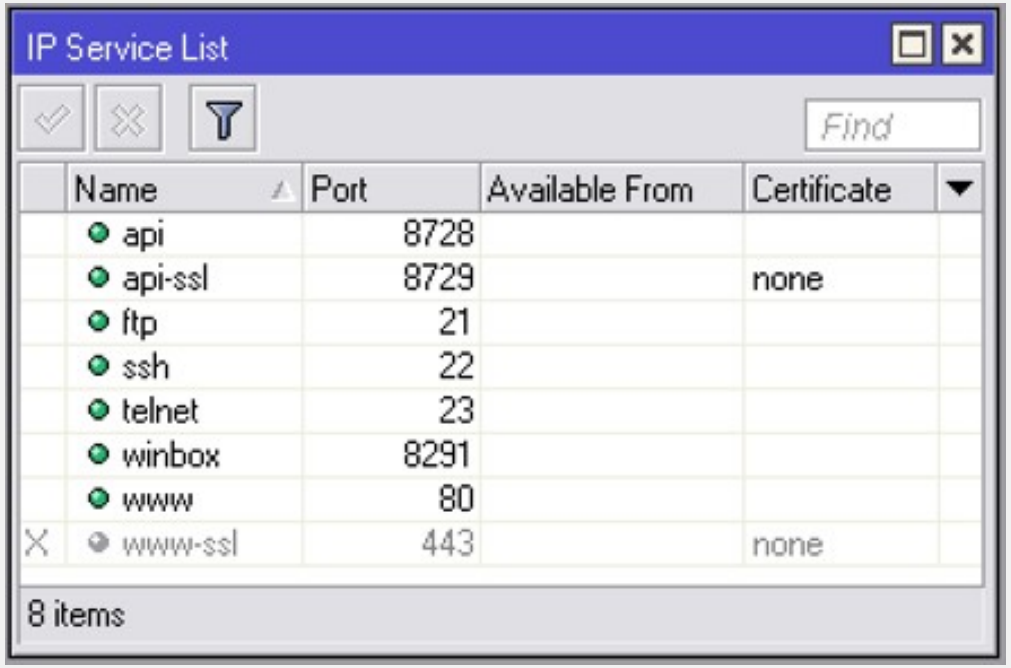
VLAN Id: any

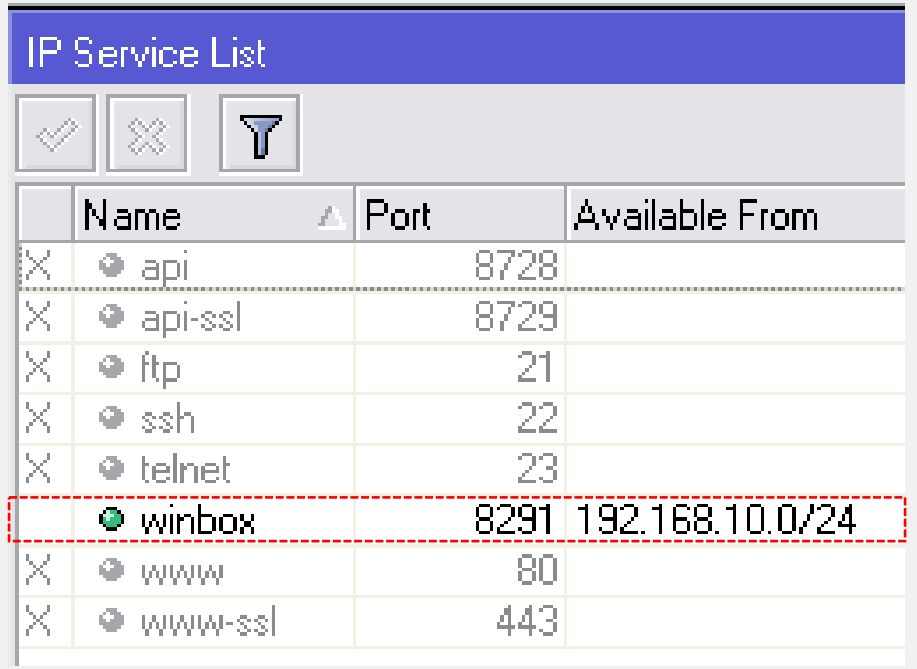
Et...	Prot...	Src.	Dst.	VLAN Id	Tx Rate	Rx Rate	Tx Pack...	Rx Pack
800 (ip)		115.238.184.126:12633	[redacted]53 (dns)		6.0 kbps	344 bps	0	
800 (ip)		115.238.184.125:26701	[redacted]:53 (dns)		6.0 kbps	344 bps	0	
800 (ip)		115.238.184.126:43549	[redacted]:53 (dns)		6.0 kbps	344 bps	0	
800 (ip)		115.238.184.125:16379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

IP -> Service

- ✓ Deshabilita Servicios innecesarios, y proteger los demás con reglas de *firewall* o especificar.





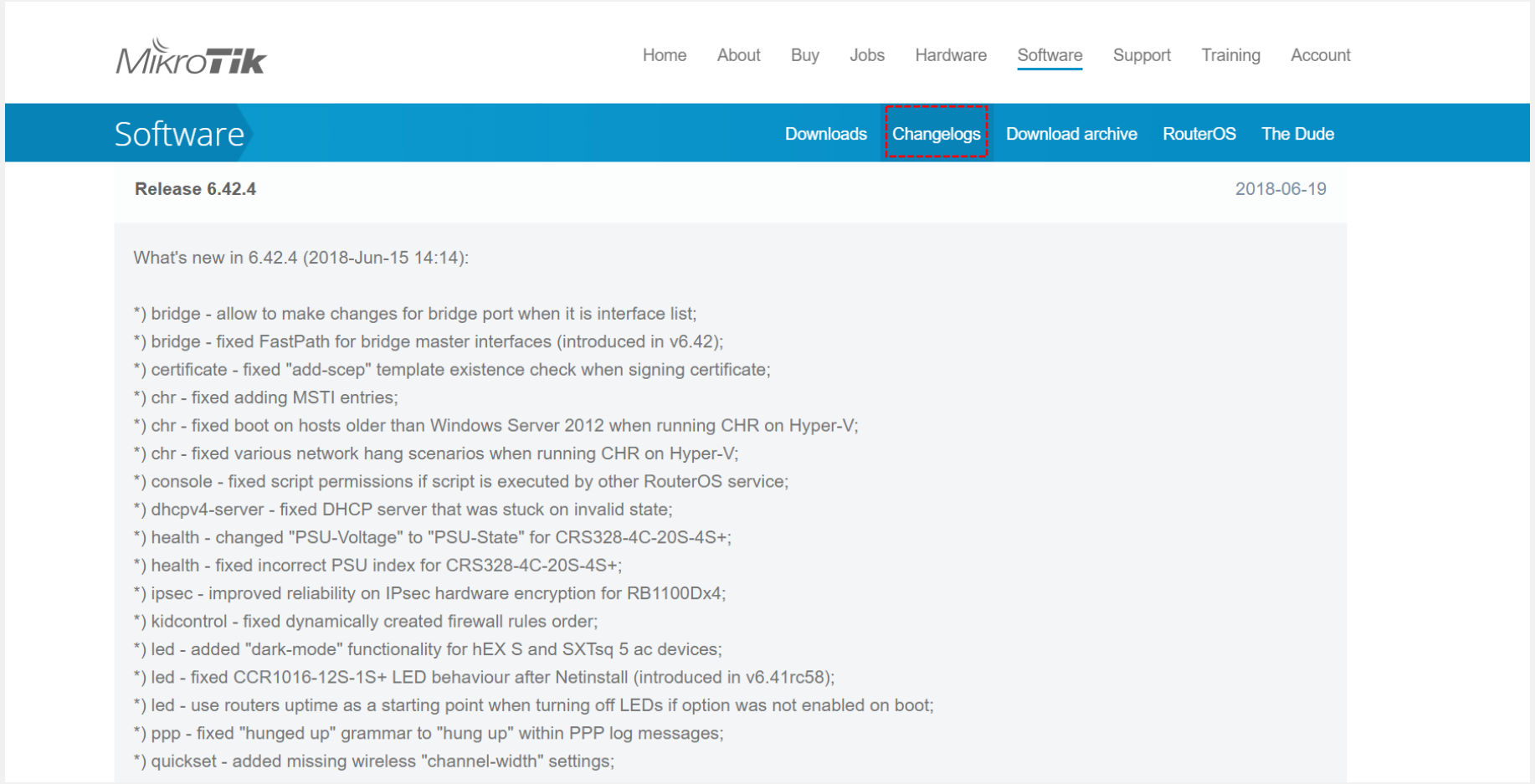
Servicios Principales a Proteger

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
1701	UDP	L2tP
1723	TCP	PPtP
1812,1813	UDP	User Manager

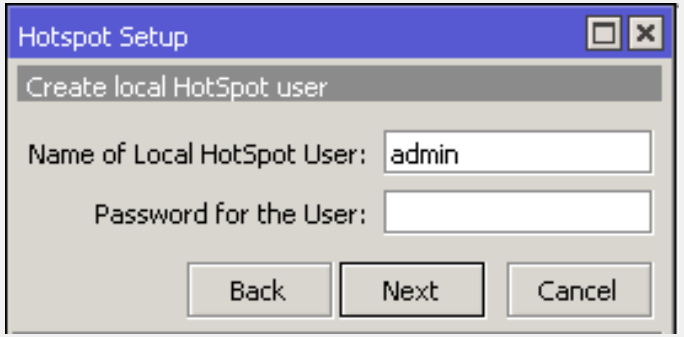
Actualización de Equipos

- ✓ NUNCA actualizar solo porque si
- ✓ Leé

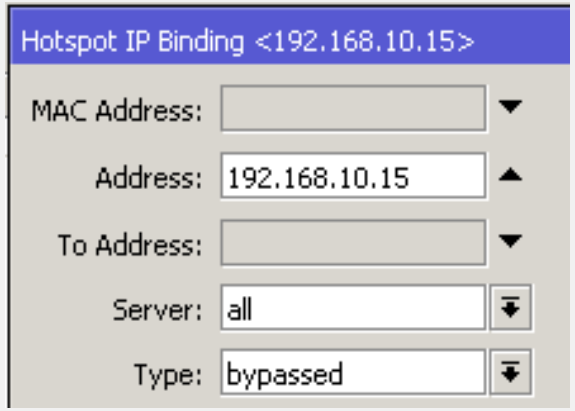


HotSpot

- ✓ No dejar el usuario como “admin” en el HotSpot sin contraseña



- ✓El bypass oculta el HotSpot, pero no controla el ancho de banda!

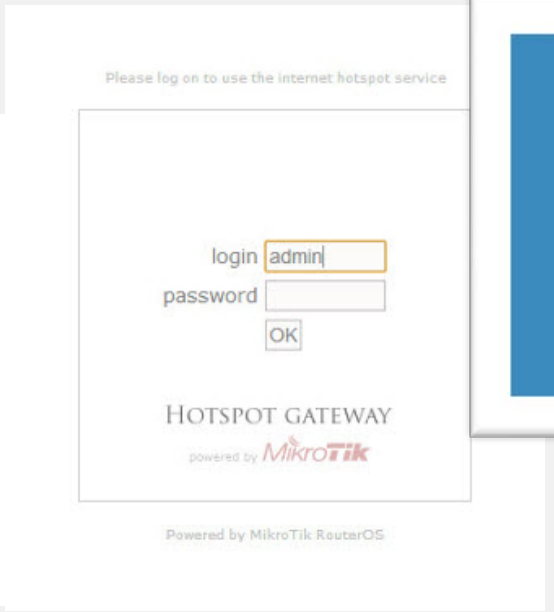


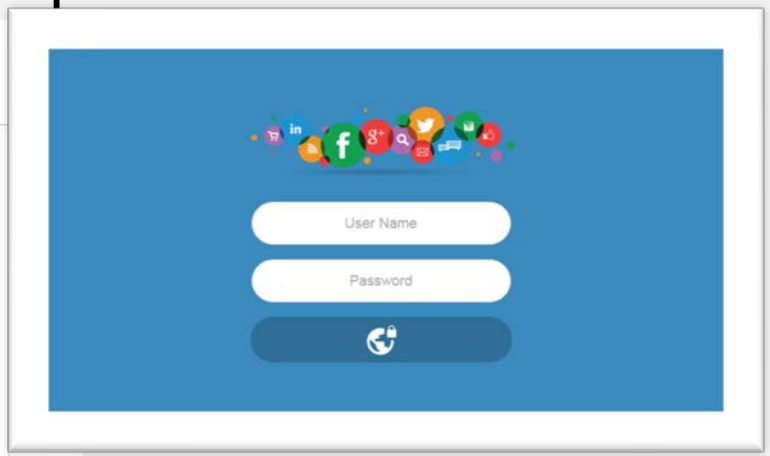
Introducción & Objetivos

Integración de HotSpot con User Manager

¿Que es un HotSpot?

- ✓ Sistema de autentificación de clientes mayormente por un USUARIO Y CONTRASEÑA al abrir el navegador.
- ✓ Comúnmente utilizados para dar acceso en lugares públicos.





Introducción & Objetivos

¿Que es UserManager ?

- ✓ Es una aplicación RADIUS desarrollada por MikroTik que cumple con los estándares de AAA (Autorización, Autenticación y Contabilización). A través de el es posible administrar servicios PPP, HotSpot, DHCP, Wireless y RouterOS

Ventajas de utilizar UserManager

- ✓ Sin costo adicional.
- ✓ Administración centralizada de toda la red.
- ✓ Única base de datos (o réplicas) aislada de la configuración del server principal.
- ✓ Permite crear usuarios por lotes y generar Boucher o exportarlos a un archivo en CSV para una posterior impresión de tarjetas prepagas.

Requerimientos y Consideraciones

- ✓ Se debe tener la misma versión de RouterOS y del paquete UserManager.
- ✓ Funciona en arquitectura X86, MIPS, PowerPC y Tile.
- ✓ Hardware Mínimo: 32MB de RAM y 2MB de HDD.
- ✓ Software: RouterOS.
- ✓ Licencia MikroTik RouterOS de UserManager.
  - Nivel 3: 10 sesiones activas.
  - Nivel 4: 20 sesiones activas.
  - Nivel 5: 50 sesiones activas.
  - Nivel 6: sesiones ilimitadas.

Wifi Normal

Fuente:www.4ipnet.com

Wifi HotSpot

Fuente:www.4ipnet.com

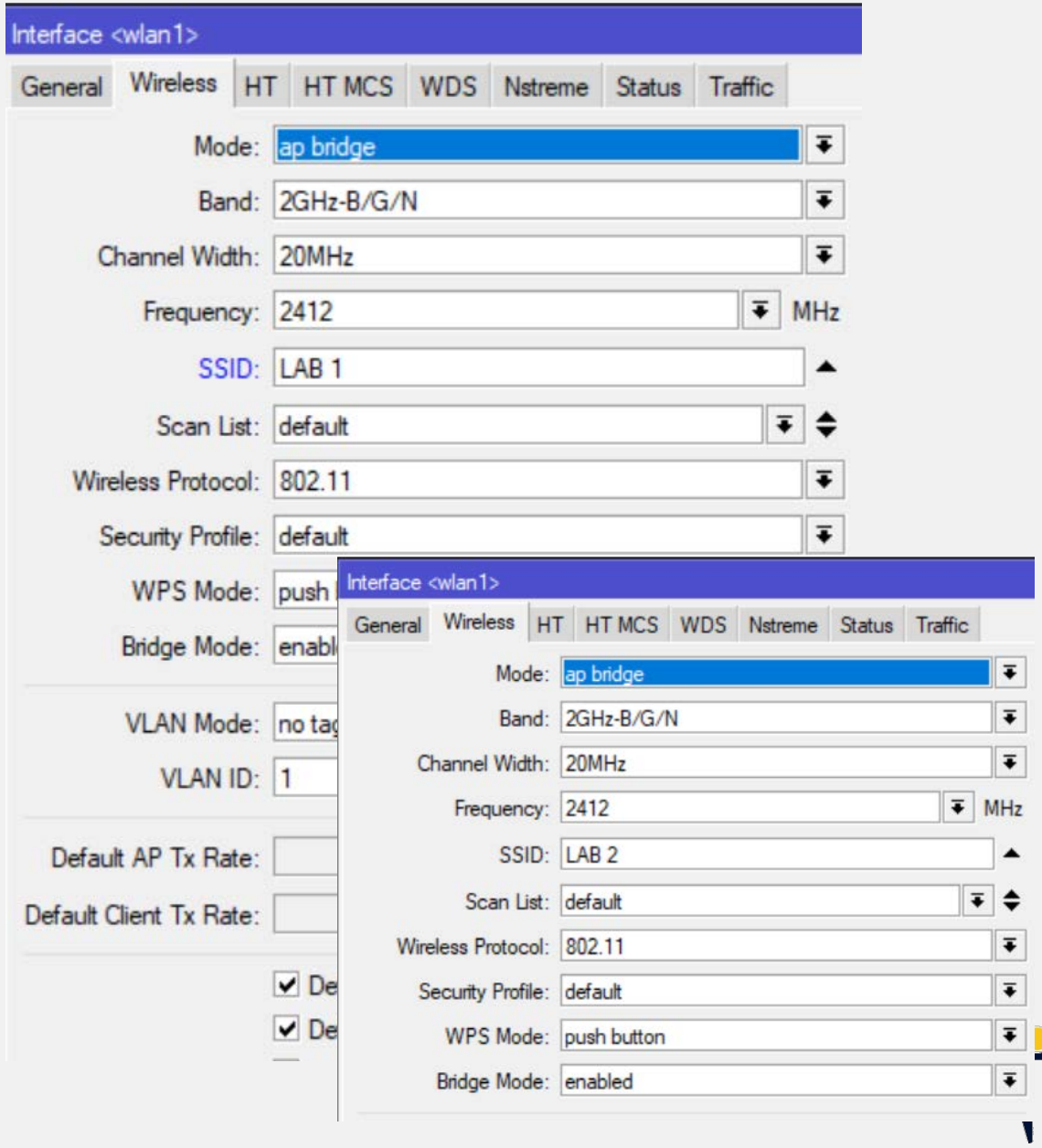
Esquema


INTERNET
HOTSPOT
USERMANAGER
USERMANAGER
DISPOSITIVOS
INALAMBRICOS

Laboratorio

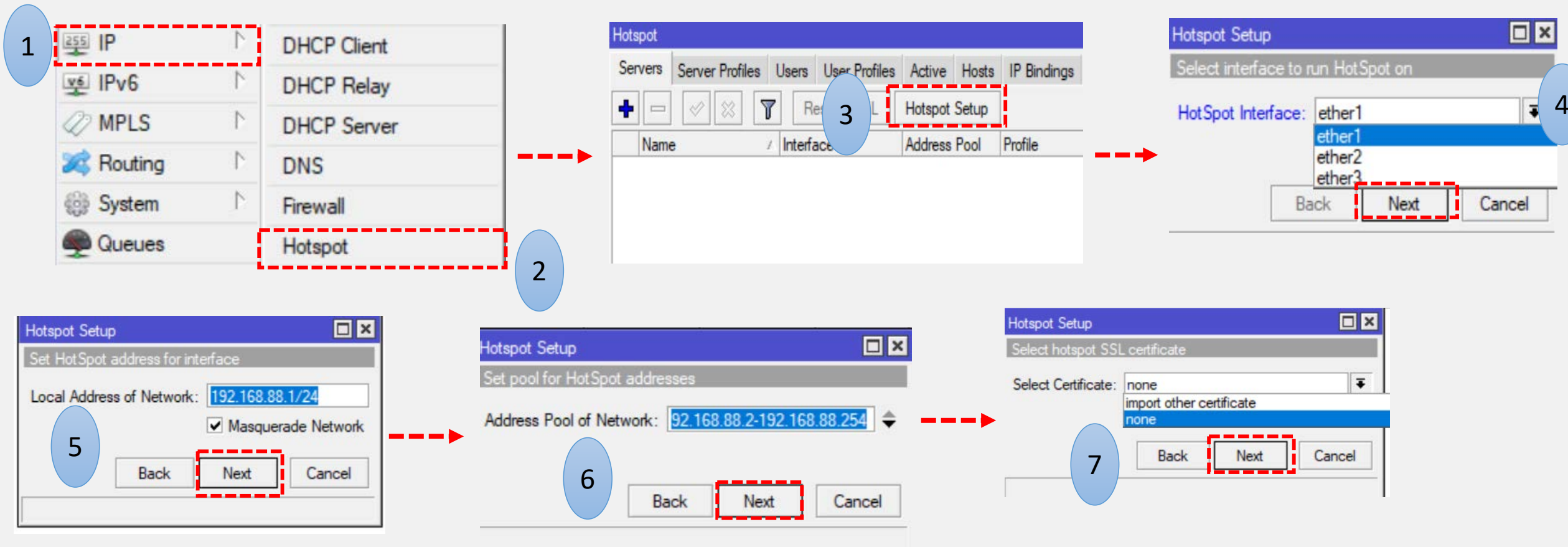
Paso 1: Configuración Básica De Wifi

- ✓ Después de crear nuestra red WIFI, configuramos de las misma **AP1 LAB 1 Y AP2 LAB,** configuramos de la misma forma, de tal manera que no tenga que pedir autenticación (Password) al momento de registranos.

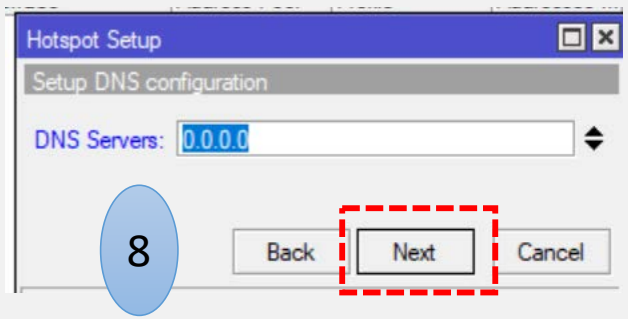


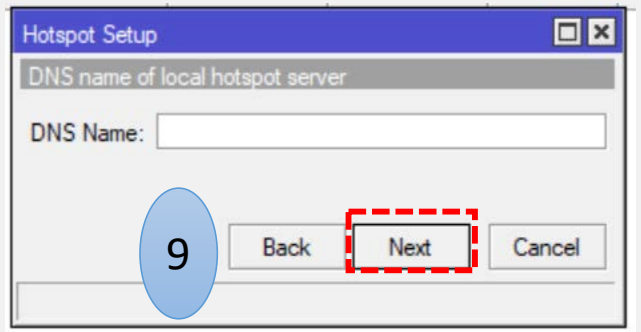
Laboratorio

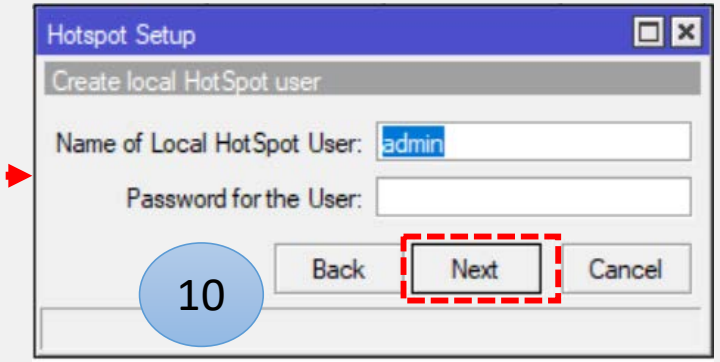
Paso 2: Configuración Básica De HotSpot

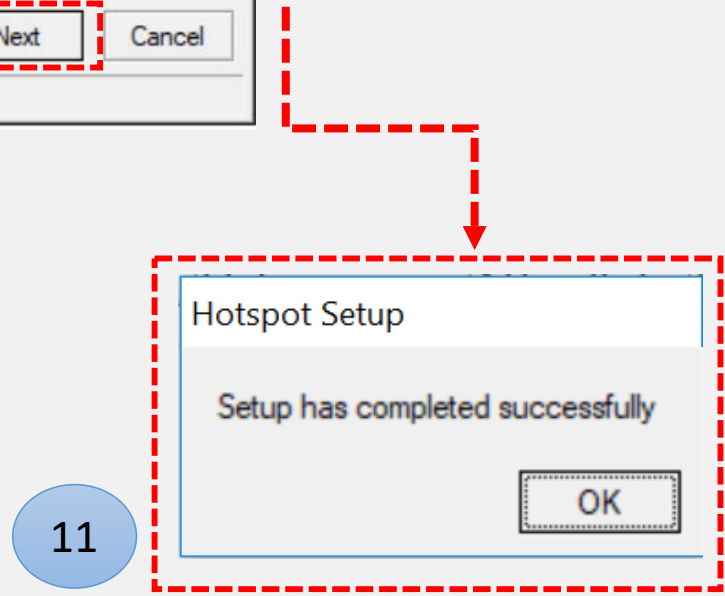


Laboratorio









Laboratorio

Paso 3: Configuración del User Manager

admin@4C:5E:0C:60:5A:8D (MikroTik) - WinBox v6.40.8 on RB750 (mipsbe)

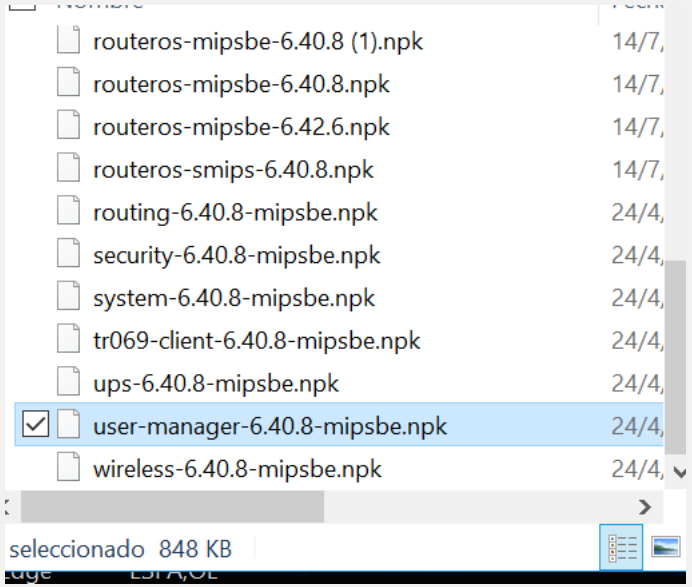
1

https://mikrotik.com/dowload

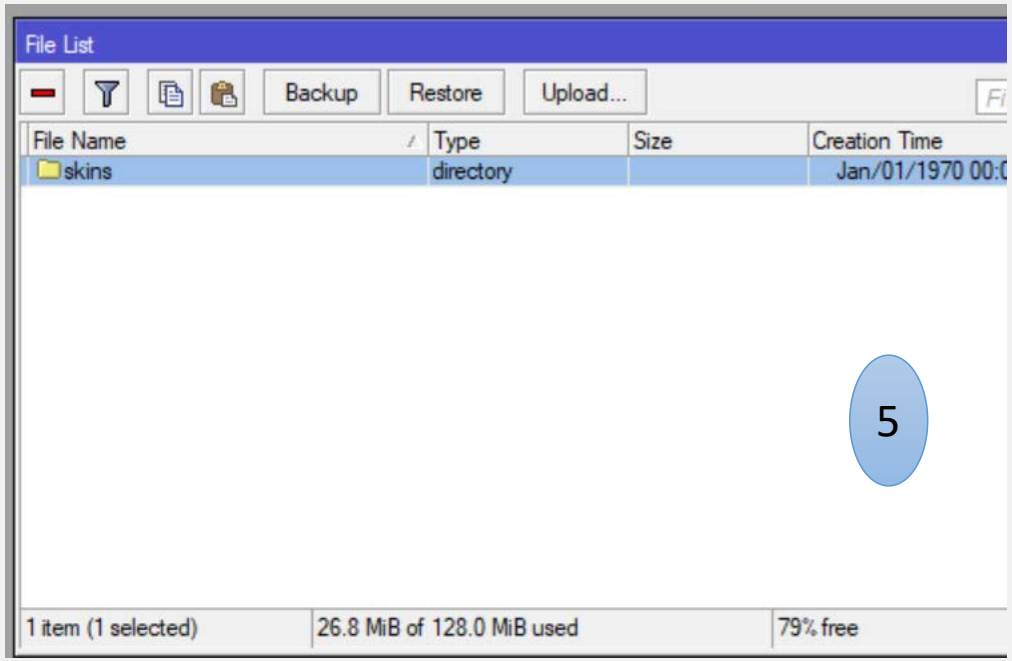
2

```
[admin@AULA ] > system reboot
```

6



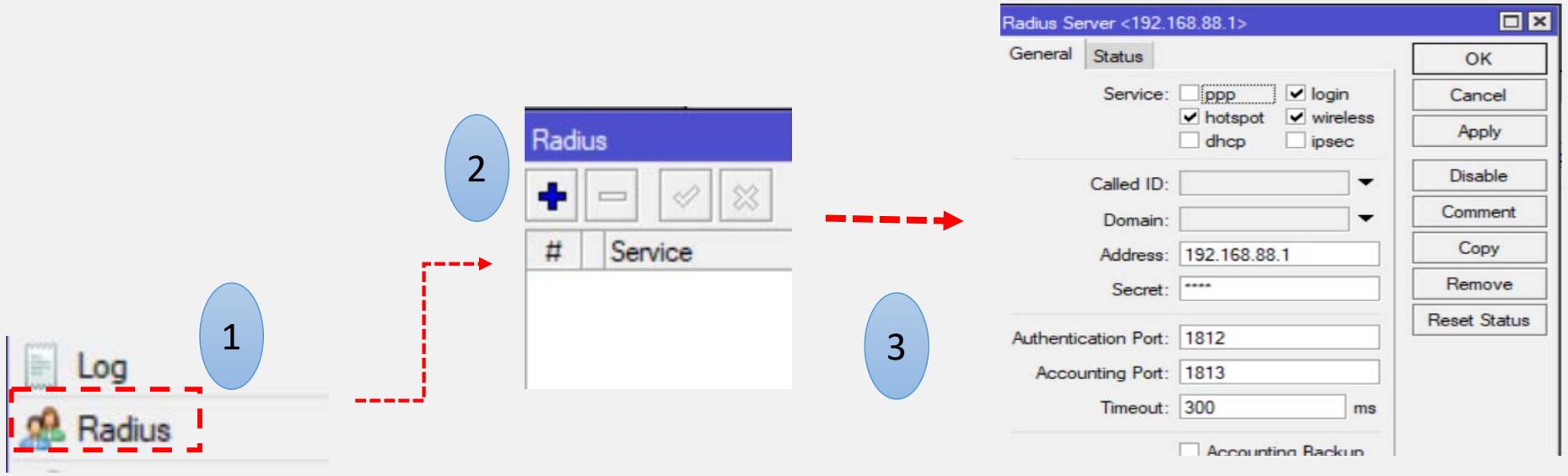
4



5

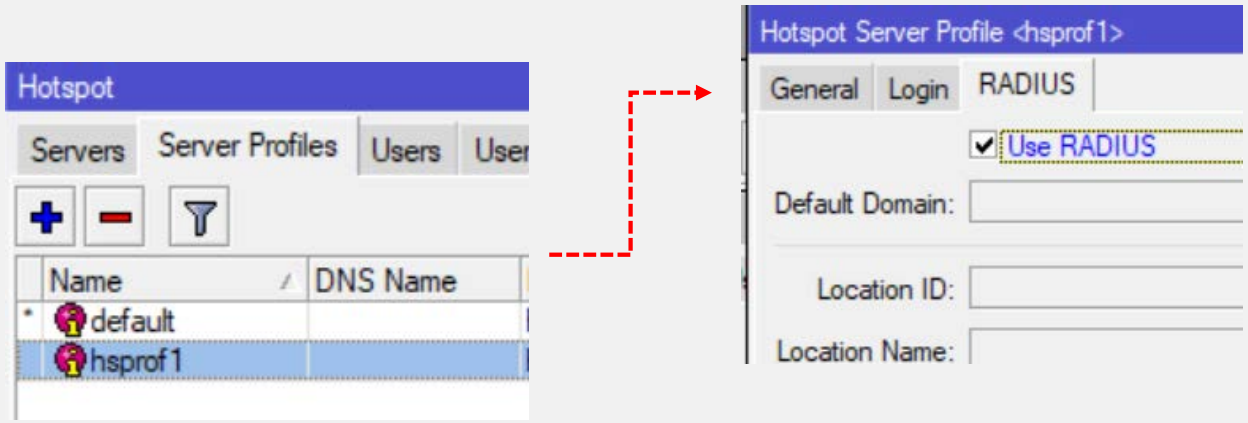
Laboratorio

Paso 4: Configuración del Hostpot y User manager



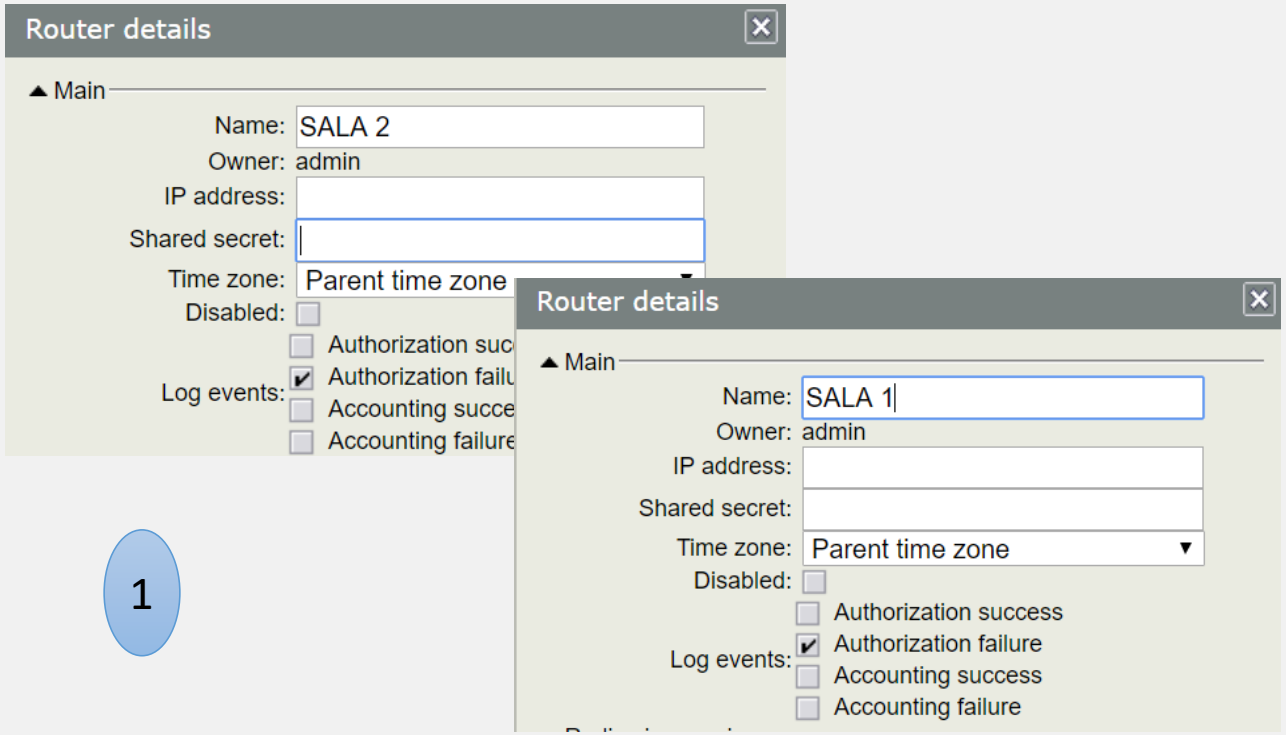
IP 192.168.87.1
IP 192.168.87.2

RADIUS 192.168.88.1



Laboratorio

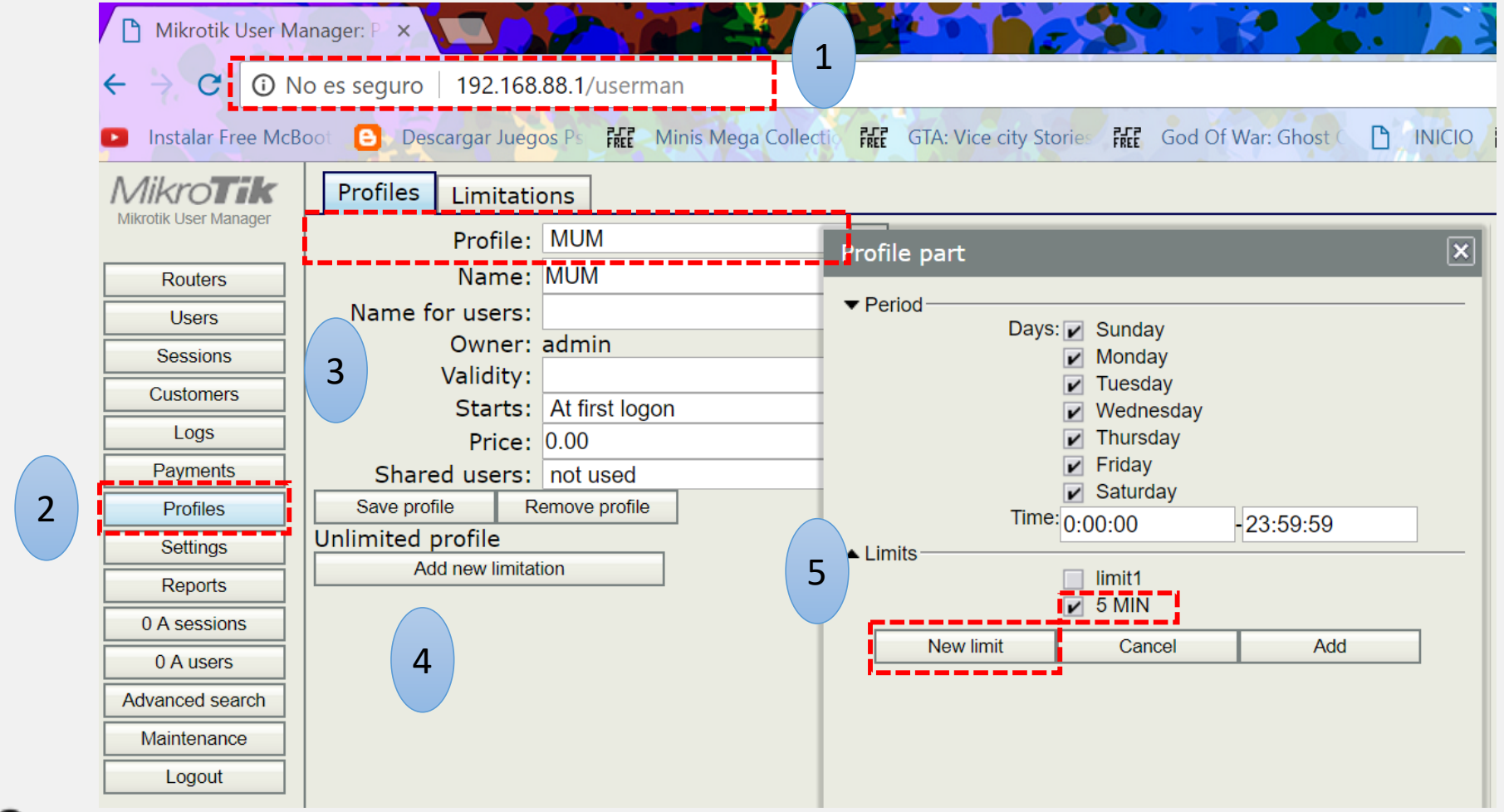
Paso 4: Configuración del Hostpot y User manager



LADO SERVIDOR

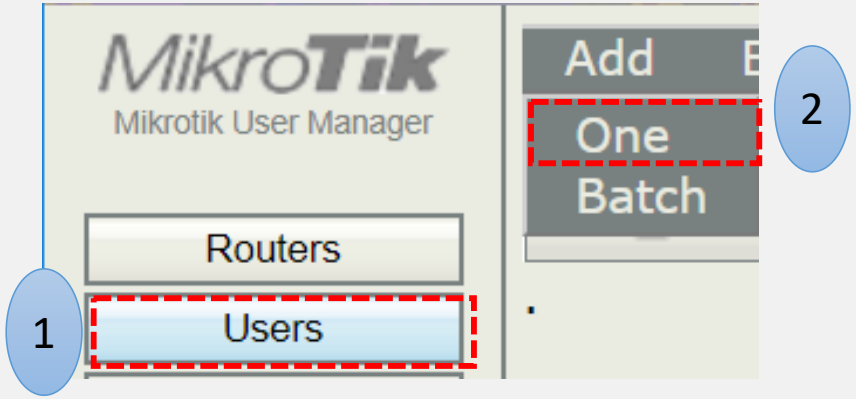
Laboratorio

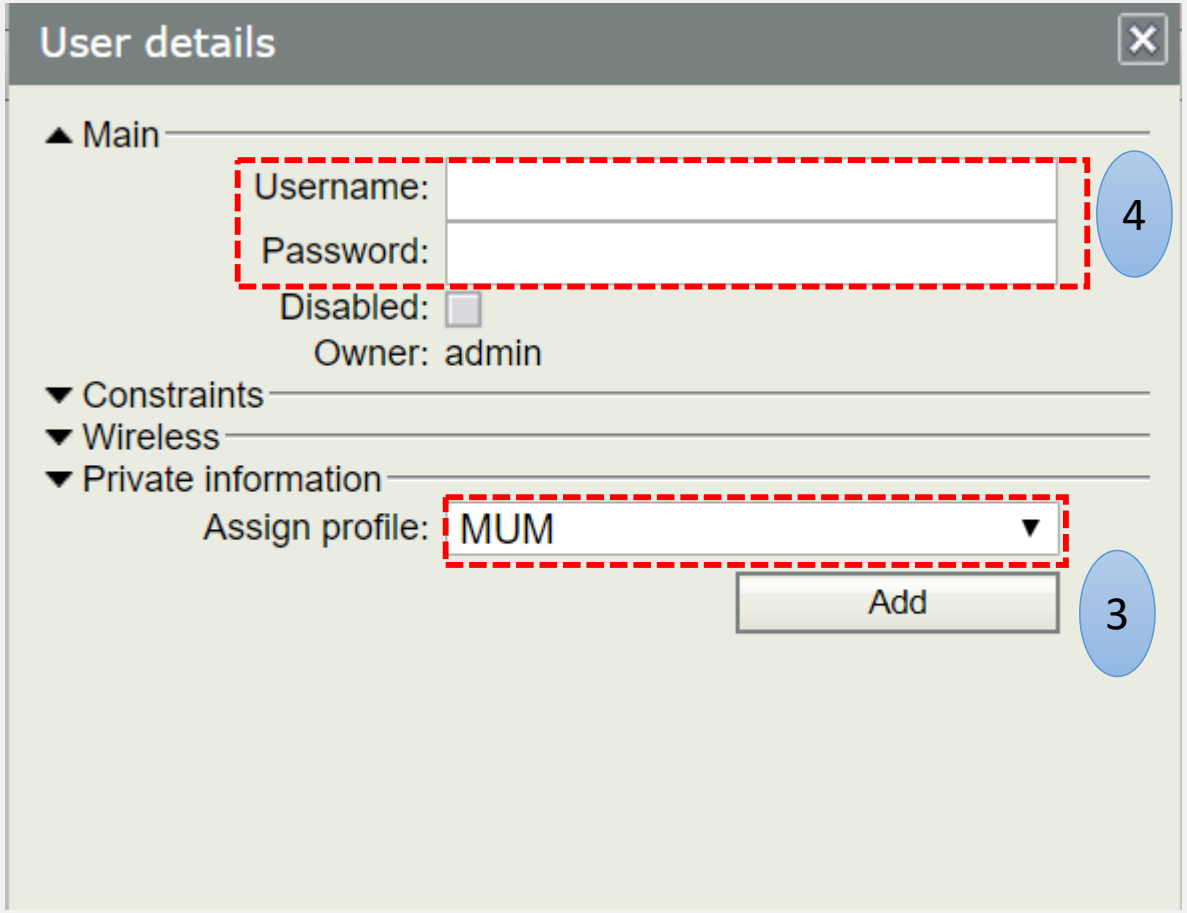
Paso 5: Configuración User manager (PERFIL)



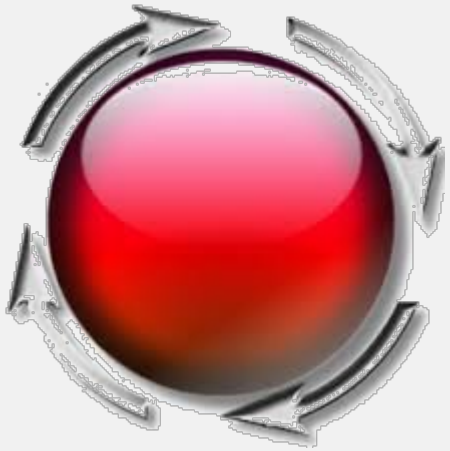
Laboratorio

Paso 6 : Configuración User manager (Usuarios)





Laboratorio



DUDE

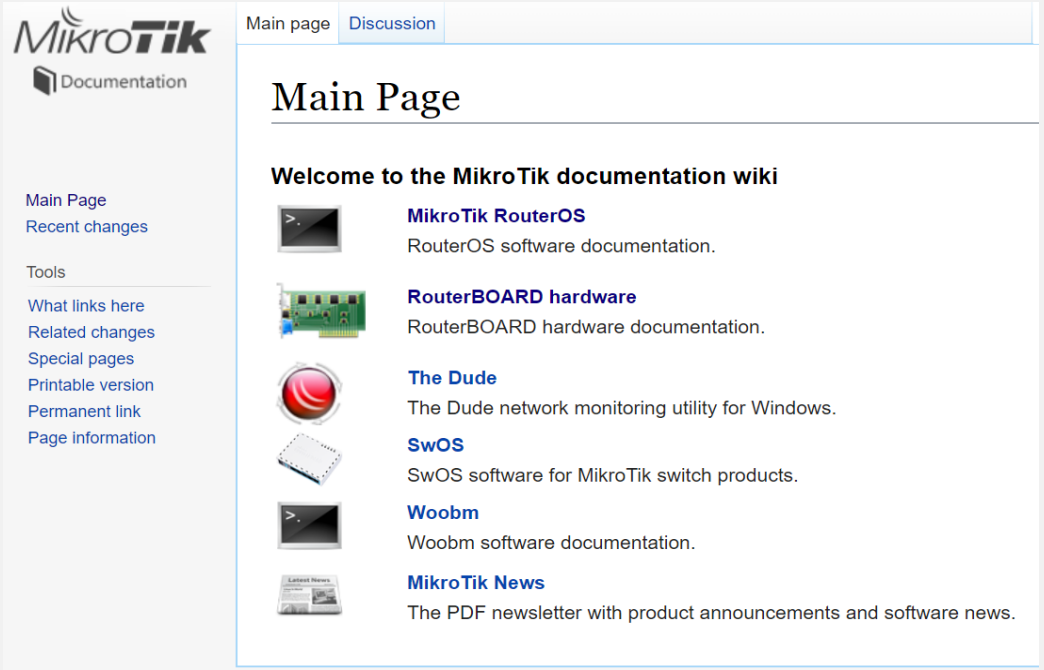
+

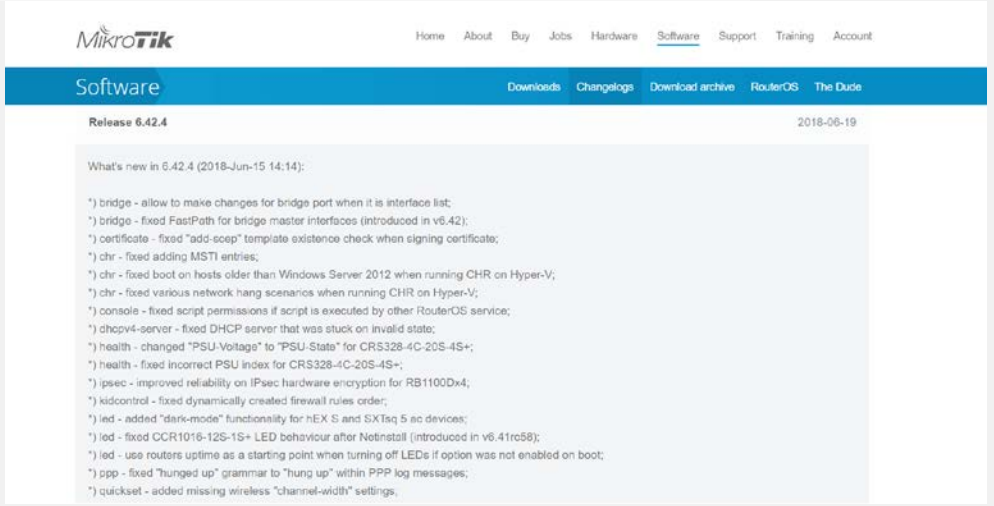
VPN

Virtual Private Network

Recomendaciones

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





¿PREGUNTAS?

¡MUCHAS GRACIAS!

"El verdadero progreso es el que pone la tecnología al alcance de todos" … Henry Ford

Armando Cartagena
ITDES

MUM HONDURAS 2018