Configuración inicial router MikroTik para hogar y pequeña empresa

MikroTik

Sobre el expositor

- Juan Manuel Diaz Gómez
- Ingeniero de Telecomunicaciones Universidad Santo Tomás sede Medellín-Colombia
- Experiencia con Mikrotik desde el año 2008
- Certificaciones obtenidas: MTCNA-MTCTCE
- Contacto e-mail: jmdg1104@Gmail.com

Introducción

Hoy en día, muchas personas buscan para los hogares, colegios, empresas, etc., tener una red Wi-Fi, controlar la velocidad, tener una red segura, poder establecer una VPN para acceder a los servicios remotamente, poder tener empleados realizando teletrabajo. Una opción por las que muchos están optando es adquirir un router:

MikroTik

Objetivos

Los objetivos a alcanzar para implementar soluciones en hogar y empresa son:

- Configuración por defecto
- Configuración desde cero de nuestro dispositivo
- Configuración red WAN y LAN (cableada y Wi-Fi)
- Firewall básico
- Calidad de servicio
- DNS
- Backups
- VPN

Configuración por defecto

Configuración por defecto

RouterOS Default Configuration

```
The following default configuration has been installed on your router:

RouterMode:
 * WAN port is protected by firewall and enabled DHCP client
 * Wireless and Ethernet interfaces (except WAN port ether1)
   are part of LAN bridge
wlan1 Configuration:
    mode:          ap-bridge;
    band:          2ghz-b/g/n;
    ht-chains:     0,1;
    ht-extension:  20/40mhz-Ce;
LAN Configuration:
    IP address 192.168.88.1/24 is set on bridge (LAN port)
    DHCP Server: enabled;
WAN (gateway) Configuration:
    gateway:  ether1 ;
    ip4 firewall:  enabled;
    NAT:   enabled;
    DHCP Client: enabled;
    DNS: enabled;
```

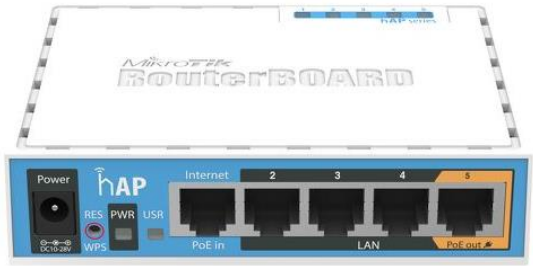
Remove Configuration | Show Script... | OK

Configuración desde cero de nuestro dispositivo

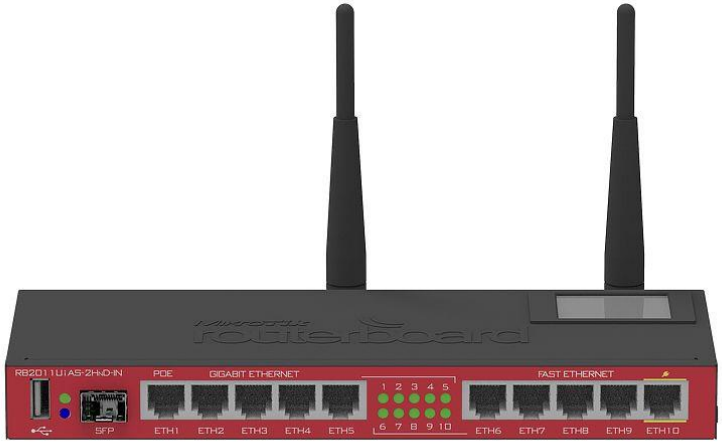
1) Escoger el dispositivo

RB931

RB941



RB952



RB2011

1) Escoger el dispositivo

Product code	RB931-2nD
CPU	QCA9533
CPU nominal frequency	650 MHz
CPU core count	1
Size of RAM	32 MB
10/100 Ethernet ports	3
Wireless	Built-in 2.4 GHz 802.11b/g/n, dual-chain

MikroTik

1) Escoger el dispositivo

Antenna gain	1.5 dBi
Antenna beam width	360°
Wireless chip model	QCA9533
Supported input voltage	5 V (Jack)
Dimensions	48 x 78 x 81mm
License level	4
Operating System	RouterOS

MikroTik

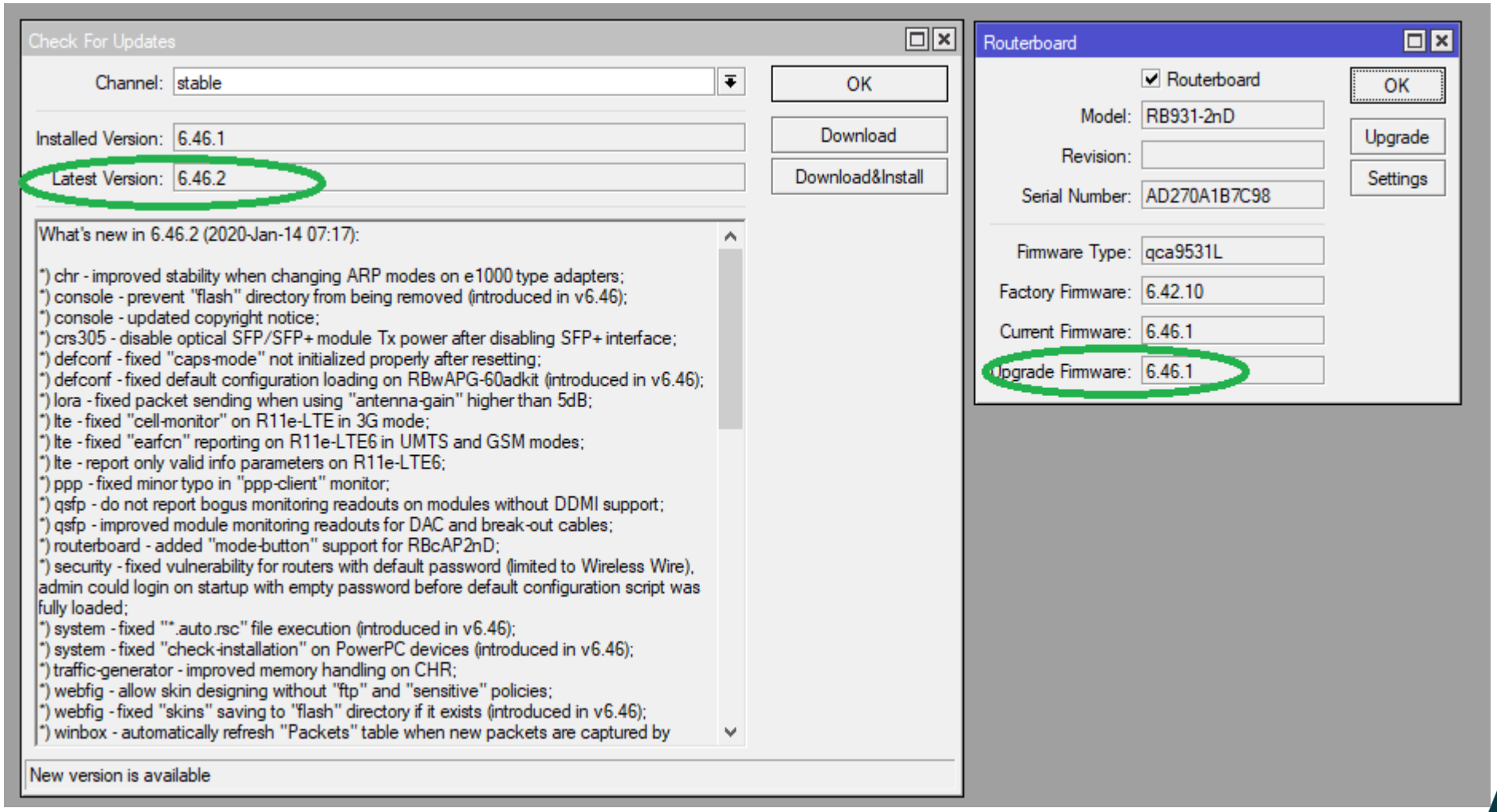
2) Eliminar la configuración por defecto

RouterOS Default Configuration

```
The following default configuration has been installed on your router:

RouterMode:
 * WAN port is protected by firewall and enabled DHCP client
 * Wireless and Ethernet interfaces (except WAN port ether1)
   are part of LAN bridge
wlan1 Configuration:
    mode:          ap-bridge;
    band:          2ghz-b/g/n;
    ht-chains:     0,1;
    ht-extension:  20/40mhz-Ce;
LAN Configuration:
    IP address 192.168.88.1/24 is set on bridge (LAN port)
    DHCP Server: enabled;
WAN (gateway) Configuration:
    gateway:  ether1 ;
    ip4 firewall:  enabled;
    NAT:   enabled;
    DHCP Client: enabled;
    DNS: enabled;
```

Remove Configuration | Show Script... | OK

3) Actualizar versión RouterOS y el firmware



3) Actualizar versión RouterOS y el firmware

Package List

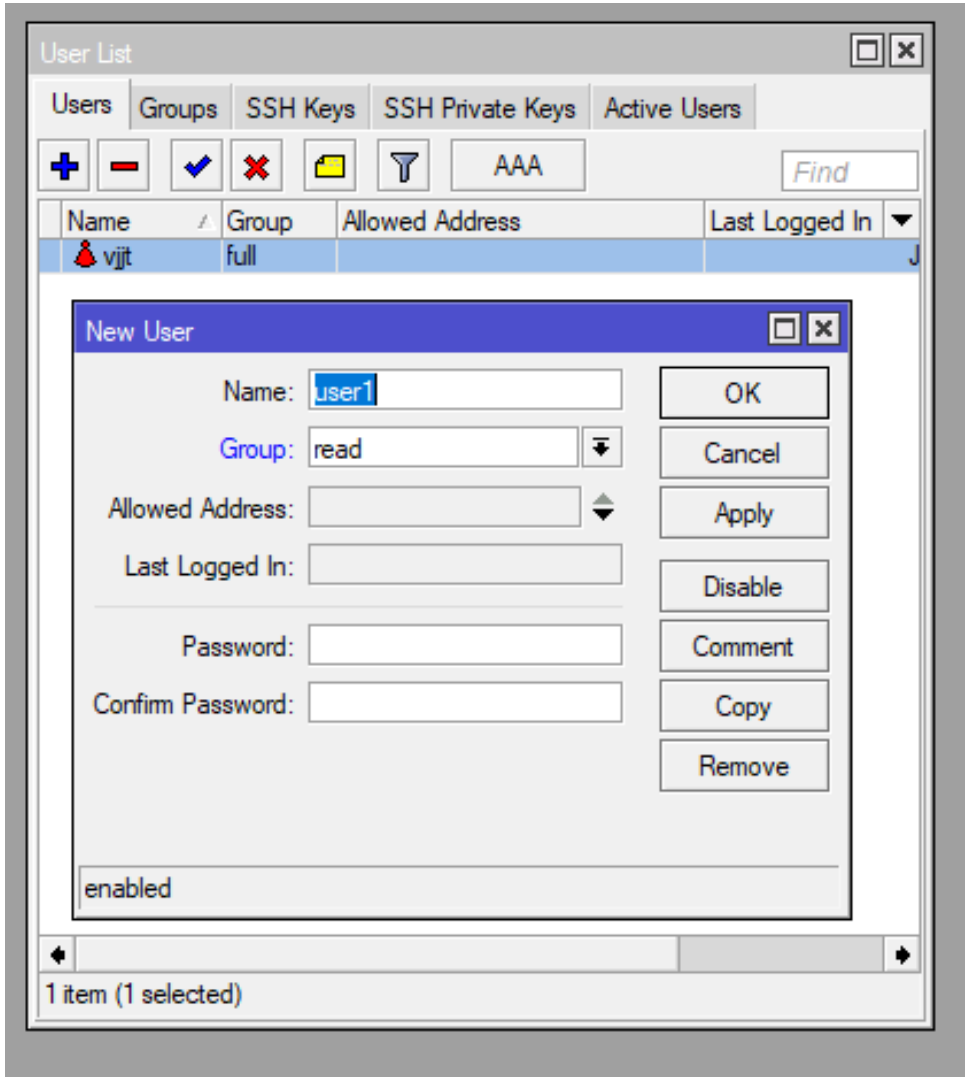
Check For Updates | Enable | Disable | Uninstall | Unschedule | Downgrade | Check Installation | Find

Name	Version	Build Time	Scheduled
routeros-smips	6.46.1	Dec/13/2019 12:44:23	
advanced-t...	6.46.1	Dec/13/2019 12:44:23	
dhcp	6.46.1	Dec/13/2019 12:44:23	
hotspot	6.46.1	Dec/13/2019 12:44:23	
ipv6	6.46.1	Dec/13/2019 12:44:23	
mpls	6.46.1	Dec/13/2019 12:44:23	
ppp	6.46.1	Dec/13/2019 12:44:23	
routing	6.46.1	Dec/13/2019 12:44:23	
security	6.46.1	Dec/13/2019 12:44:23	
system	6.46.1	Dec/13/2019 12:44:23	
wireless	6.46.1	Dec/13/2019 12:44:23	

Free HDD Space: 7.6 MiB

Total HDD Size: 16.0 MiB

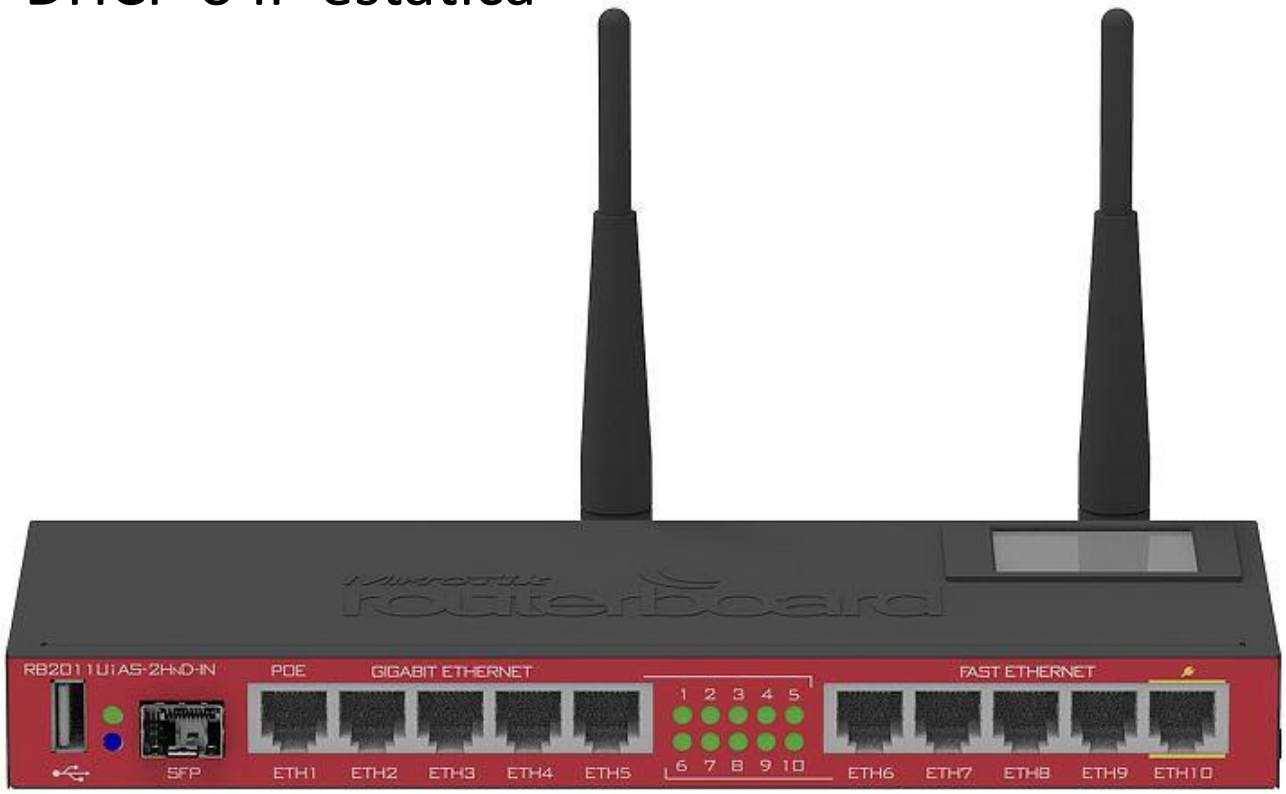
4) Asignar un usuario y contraseña



Configuración WAN y LAN (cableada y Wi-FI)

1) Definir los puertos a utilizar

- Recomendación para el puerto WAN usar cualquiera diferente al ETH1, por DHCP o IP estática



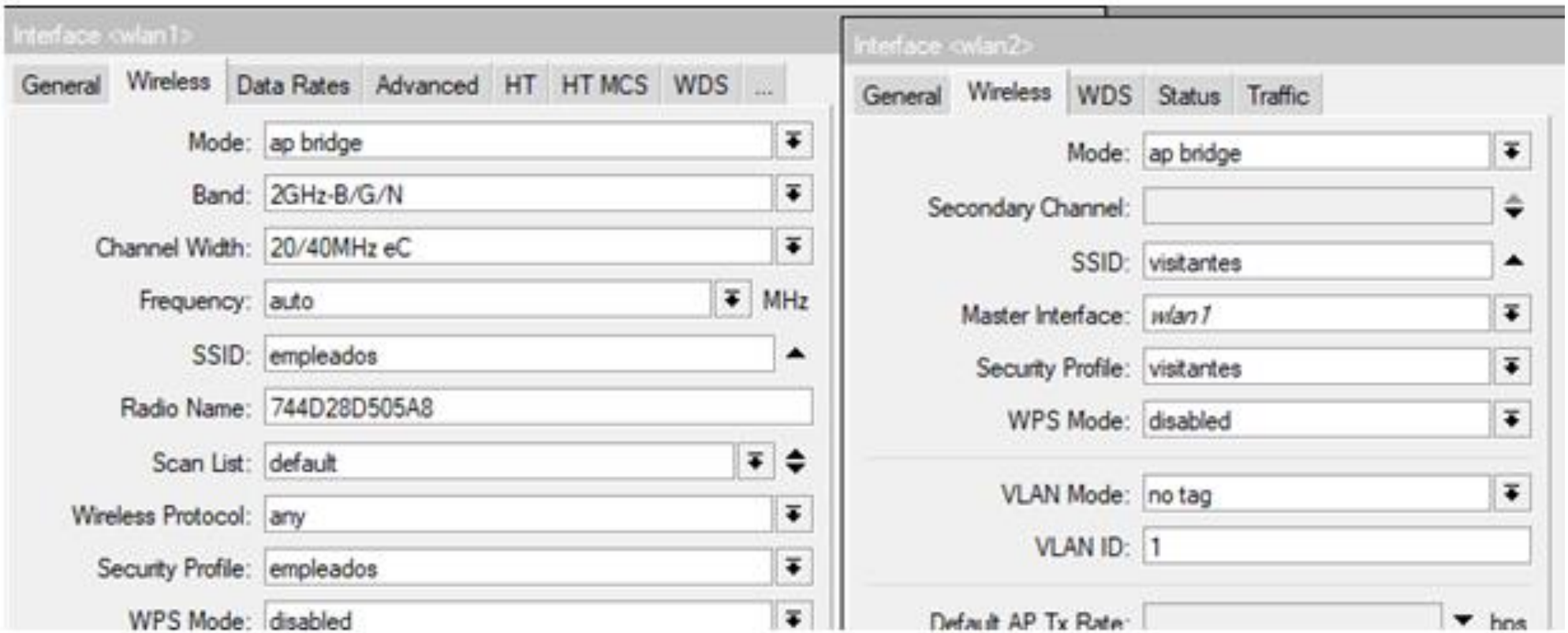
2) Especificar los servicios requeridos en la LAN

- Cámaras de seguridad
- Automatización del hogar u oficina
- Servidores (telefonía, crm, etc.)
- Número de sedes (VPN)
- Visitantes (opción hotspot con trial)
- Dispositivos a conectar
- Ancho de banda total
- Servidor NTP

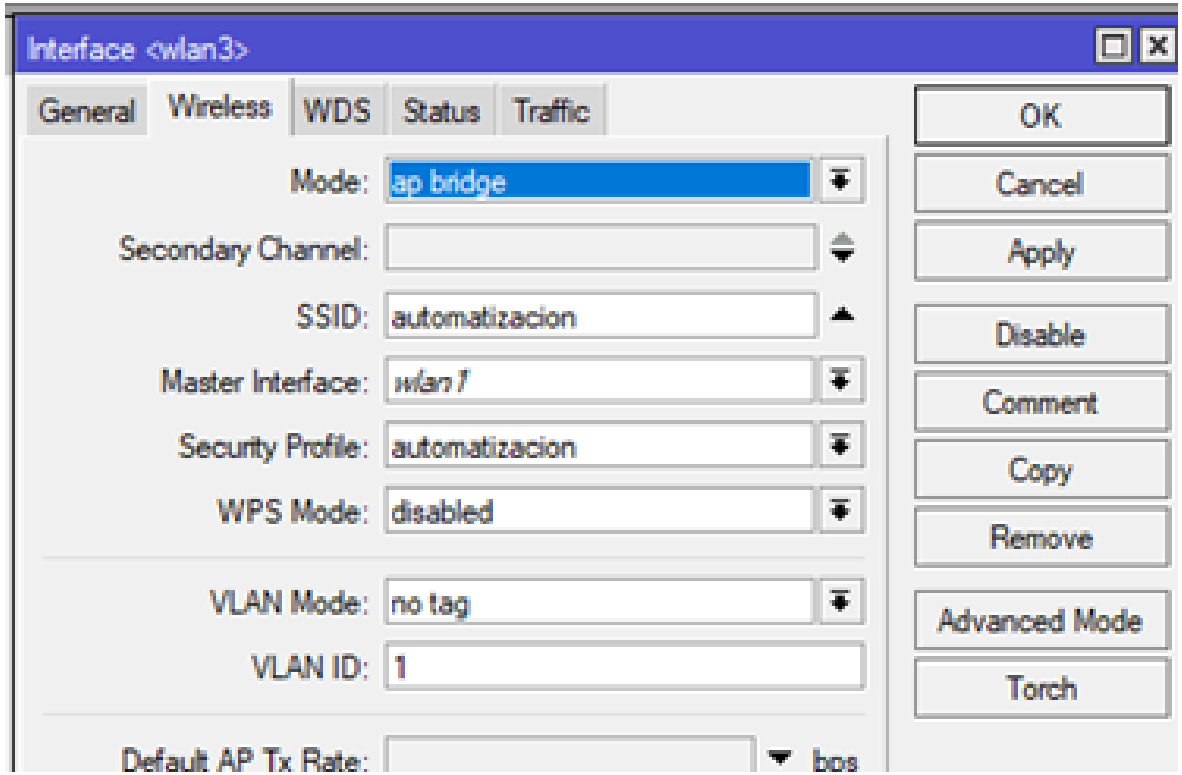
3) Ejemplo

- Oficina con 5 empleados, servidor VOIP, cámaras, alarma, automatización de luces, 2 sedes remotas, 2 empleados por teletrabajo, computador de escritorio por empleado, dispositivo Wi-Fi por empleado, visitantes diariamente llegan a la oficina, ancho de banda de 40 Mbps dedicados
- Por cable red empleados: 192.168.20.0/24 (5 puertos ethernet)
- Por cable servidor, cámaras, alarma red 192.168.50.0/28 (3 puertos ethernet)
- Por wifi 3 redes: empleados 192.168.10.0/24 – visitantes 192.168.15.0/24 – automatización de luces 192.168.30.0/28

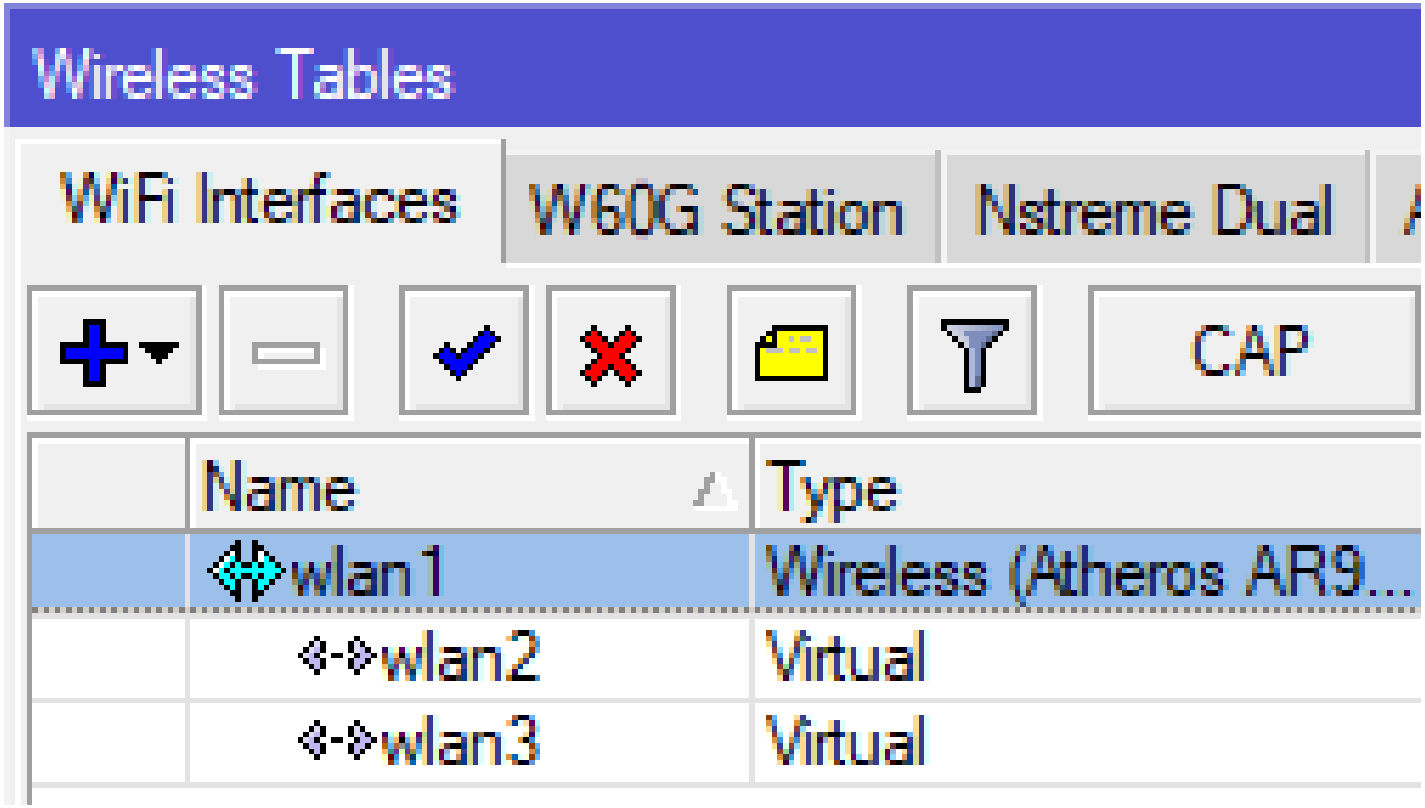
4) Configuración red Wi-Fi usando virtual AP



4) Configuración red Wi-Fi usando virtual AP



4) Configuración red Wi-Fi usando virtual AP



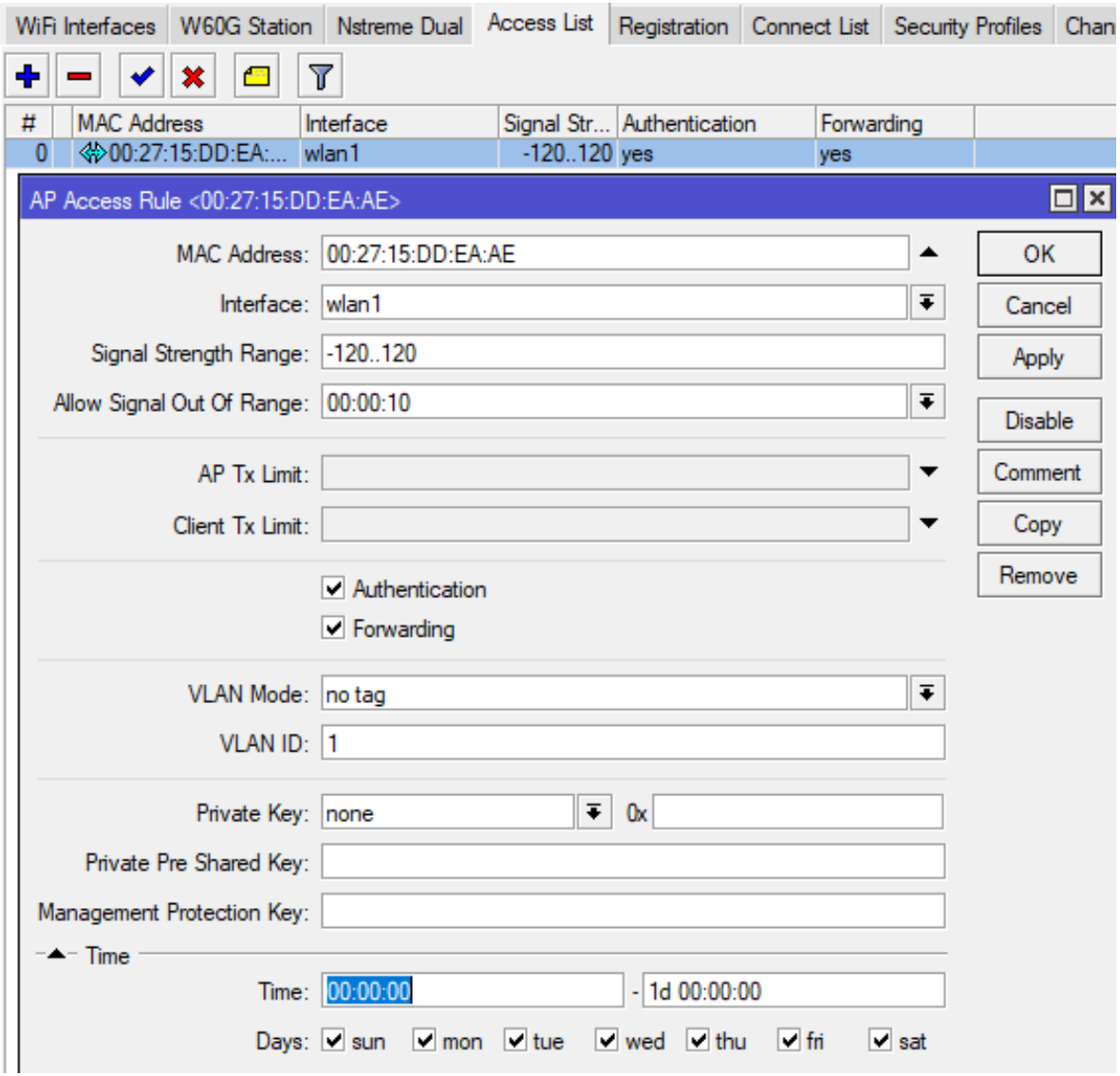
4) Configuración red Wi-Fi usando virtual AP

Wireless Tables

WiFi Interfaces | W60G Station | Nstreme Dual | Access List | Registration | Connect List | Security Profiles | Channels

Name	Mode	Authenticatio...	Unicast Ciphers	Group Ciphers	WPA Pre-Shared ...	WPA2 Pre-Shared...
visitantes	dynamic keys	WPA2 PSK	aes ccm tkip	aes ccm tkip		qwerty123
empleados	dynamic keys	WPA2 PSK	aes ccm tkip	aes ccm tkip		abcd1234
* default	none					
automatizacion	dynamic keys	WPA2 PSK	aes ccm tkip	aes ccm tkip		qazxswedc

4) Configuración red Wi-Fi usando Access-List



Firewall Básico

1) Cambiar puertos por defecto desactivar los no utilizados

IP Service List

Find

	Name	Port	Available From	Certificate
	api	8728	157.245.190.83	
X	api-ssl	8729		none
X	ftp	21		
	ssh	49722		
X	telnet	49723		
	winbox	8291		
	www	49780		
X	www-ssl	443		none

8 items

2) Port knocking

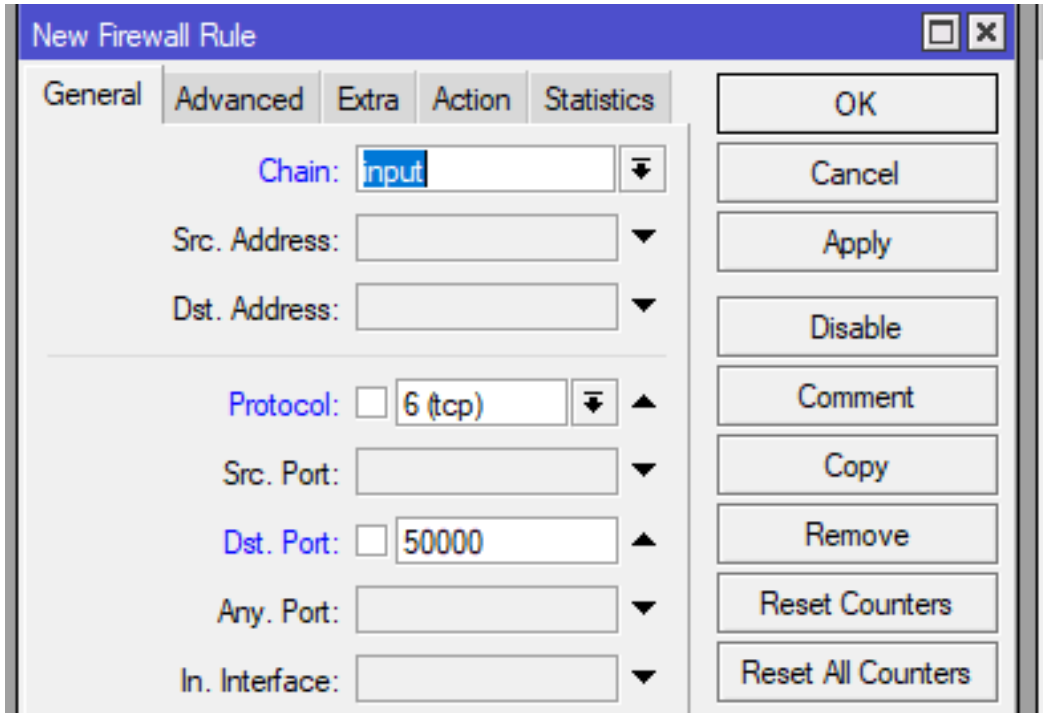
Firewall

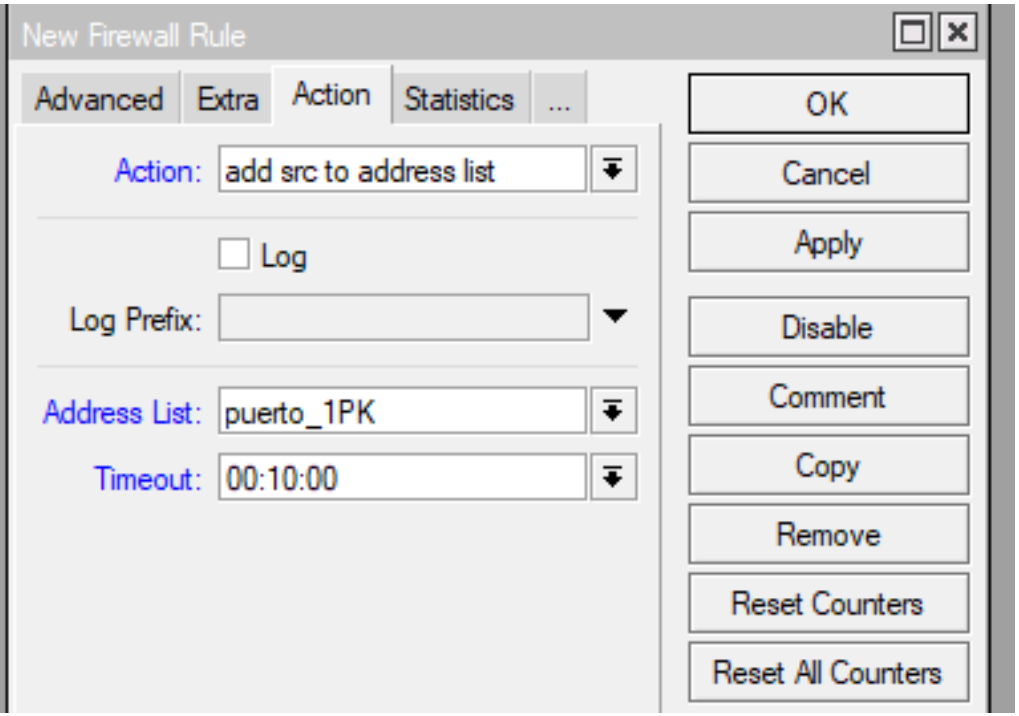
Filter Rules | NAT | Mangle | Raw | Service Ports | Connections | Address Lists | Layer7 Protocols

Reset Counters | Reset All Counters

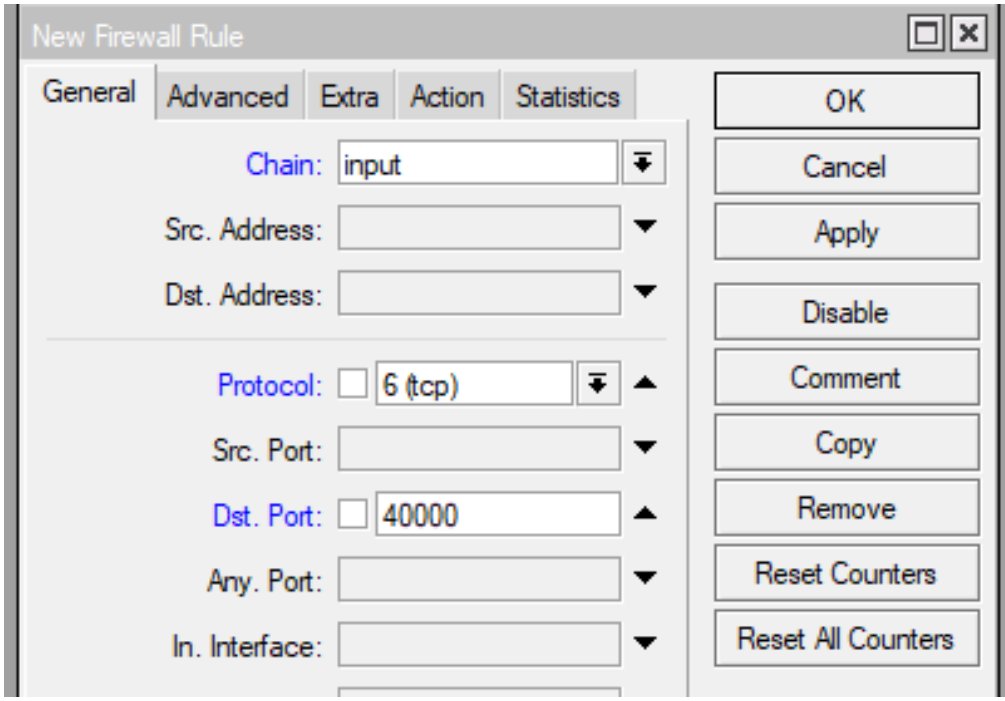
#		Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	In. Inter...	Out. Int...	Src. Ad...	Dst. Ad...	Bytes	Packets
0		add...	input			6 (tcp)		20567							640 B	12
1		add...	input			6 (tcp)		31678					reten1		580 B	11
2		add...	input			6 (tcp)		42789					reten2		580 B	11
3		drop	input			6 (tcp)		8291,49780,49722					!reten3		197.9 KiB	4 714
4		tarpit	input			6 (tcp)		22-23	ether3						6.4 MiB	162 254
;;; VPN PPTP																
5		acc...	input			6 (tcp)		1723							78.5 KiB	1 131
;;; VPN PPTP																
6		acc...	input			47 (g...									2985.9 KiB	34 074
;;; VPN L2TP																
7		acc...	input			17 (u...		1701							7.8 MiB	87 942
;;; CONEXIONES SIMULTANEAS POR CLIENTE																
8	X	drop	forward			6 (tcp)									0 B	0
;;; BLOQUEO CONEXIONES INVALIDAS																
9		drop	input												46.6 MiB	746 533
10		drop	output												129.3 KiB	308
11		drop	forward												144.1 MiB	2 680 672

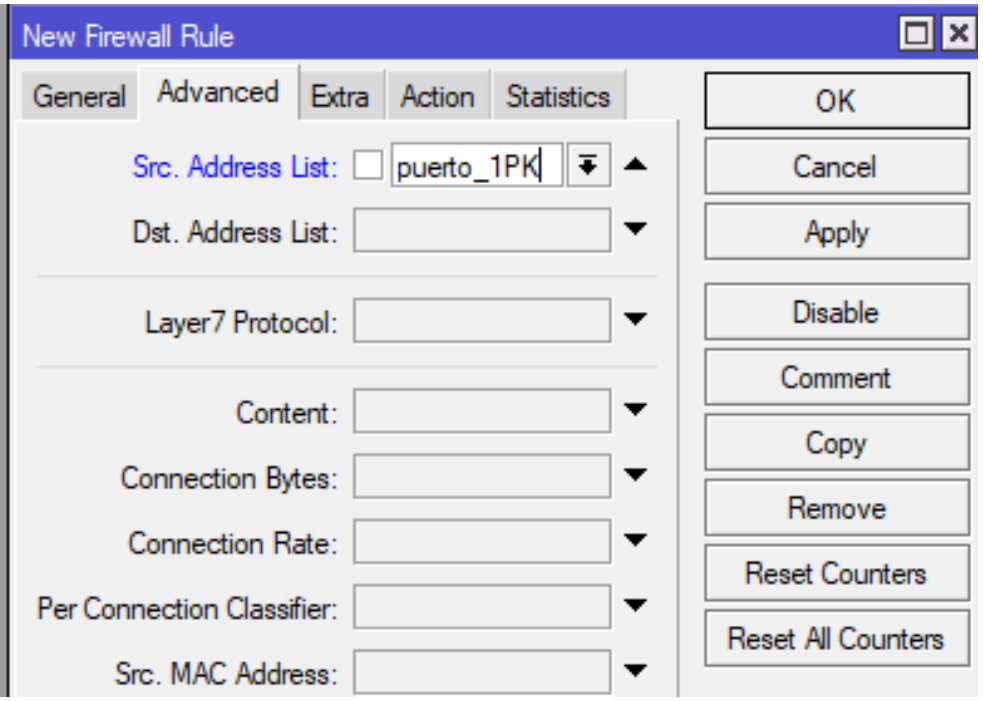
2) Port knocking



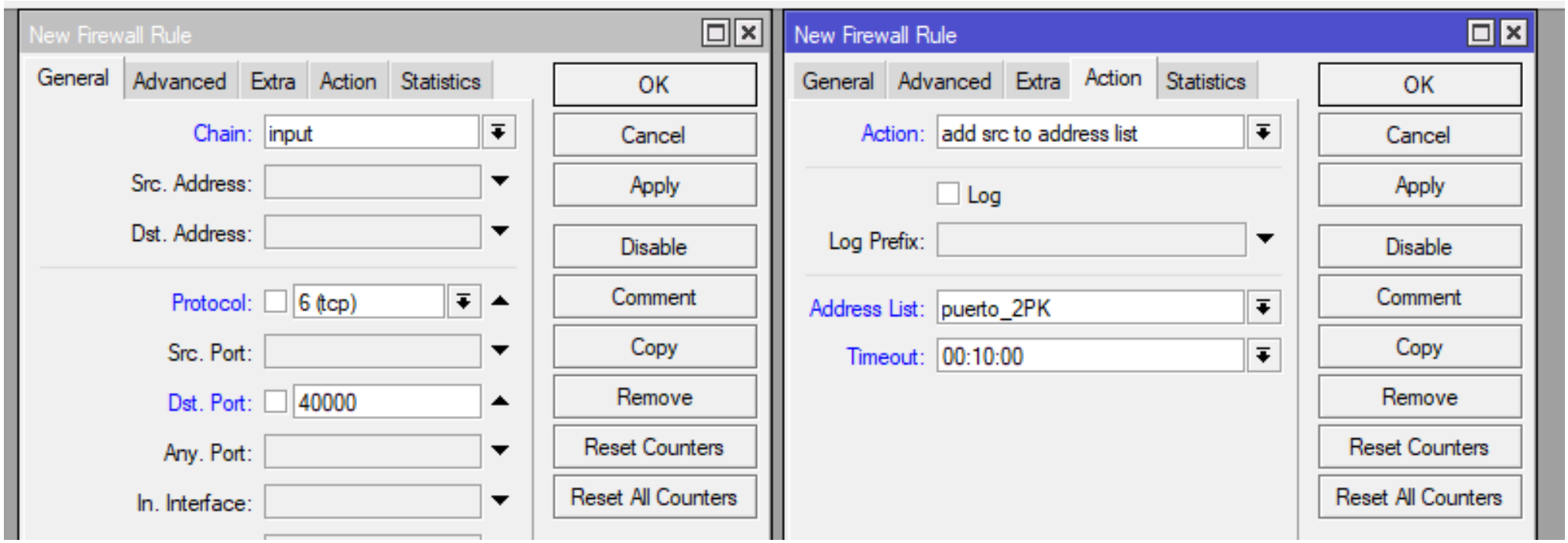


2) Port knocking

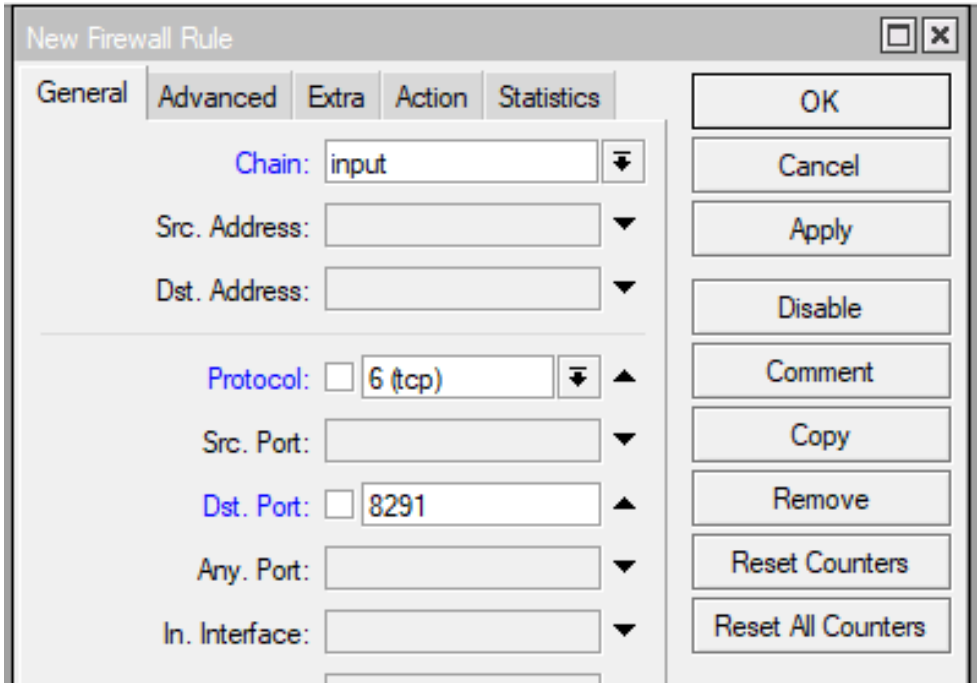


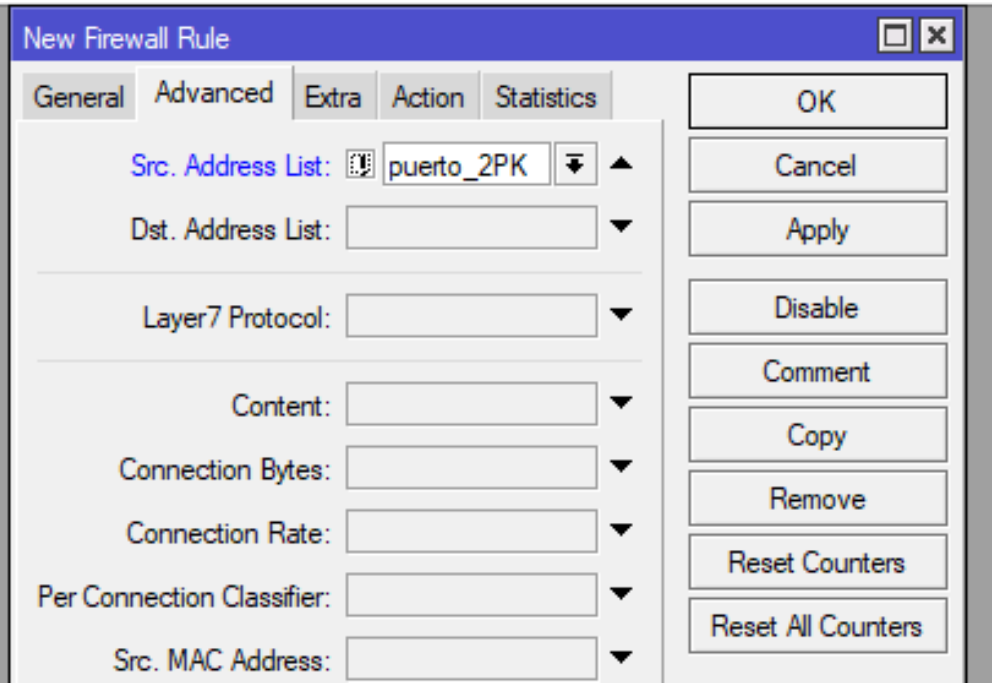


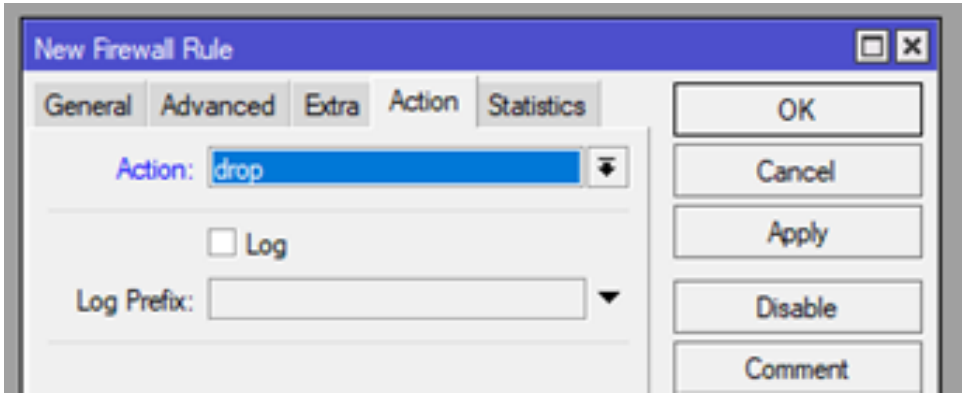
2) Port knocking



2) Port knocking







3) Bloquear peticiones de DNS externo

Firewall

Filter Rules | NAT | Mangle | Raw | Service Ports | Connections | Address Lists | Layer7 Protocols

00 Reset Counters | 00 Reset All Counters

#		Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Ou
0		drop	prerouting			17 (u...		53	ether3	
1		drop	prerouting			6 (tcp)		53	ether3	

4) Servicios pagos para listas

Firewall

Filter Rules | NAT | Mangle | Raw | Service Ports | Connections | Address Lists | Layer7 Protocols

00 Reset Counters | 00 Reset All Counters

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	In. Inter...	Out. Int...	Src. Ad...	Dst. Address List	Bytes	Packets
0	drop	input			17 (u...		53	ether1						7.6 KiB	120
1	drop	input			17 (u...		53	ether2						3968 B	61
2	drop	input			17 (u...		53	ether12						3678 B	56
::: AX001 - Packet Trap															
3	tarpit	input			6 (tcp)							blocke...		0 B	0
::: AX002 - Connection Limit															
4	add...	input			6 (tcp)									0 B	0
::: AX004 - Add Syn Flood IP to the list															
5	add...	input			6 (tcp)									0 B	0
::: AX005 - Drop to syn flood list															
6	drop	input										Syn_Fl...		0 B	0
::: AX006 - Port Scanner Detect															
7	add...	input			6 (tcp)									3280 B	82

[Información tomada de https://axiomcyber.com/shield/](https://axiomcyber.com/shield/)

4) Servicios pagos para listas

;;; AX008 - Drop to port scan list															
8	drop	input										Port_S...		41.9 KiB	1 104
;;; AX007 - Drop Access to WebUI															
9	drop	output			6 (tcp)	80								0 B	0
;;; AX011 - Block all access to Winbox - except to support list # DO NOT ENABLE THIS RULE BEFORE ADD YOUR SUBNET IN THE SUPPORT ADDRESS LIST															
10	drop	input			6 (tcp)		8291					!support		734.3 KiB	18 704
;;; AX036 - Drop to ransomware list															
11	drop	forward											ransomware	2264 B	50
;;; AX037 - Drop to TOR list															
12	drop	forward											tor_nodes	90.5 KiB	1 219
;;; AX041 - Drop invalid/malformed packets															
13	drop	forward												1983.4 KiB	37 737
;;; AX014 - Add Spammers to the list for 3 hours															
14	add...	forward			6 (tcp)		25,587							0 B	0
;;; AX015 - Avoid spammers action															
15	drop	forward			6 (tcp)		25,587					spamm...		0 B	0

[Información tomada de https://axiomcyber.com/shield/](https://axiomcyber.com/shield/)

4) Servicios pagos para listas

- Ransomware (Nodes, Sites, IP addresses)
- Malware (Nodes, Sites, IP addresses)
- Command & Control servers
- Known spammers and spam servers
- TOR Exit Nodes (DarkWeb)
- Layer 7 Regular Expression blocking

Información tomada de https://axiomcyber.com/shield/

Calidad de Servicio

1) Velocidad por red

Queue List

Simple Queues | Interface Queues | Queue Tree | Queue Types

00 Reset Counters | 00 Reset All Counters

#	Name	Target	Dst.	Upload Max Limit	Download Max Limit	Upload Queue Type	Download Queue Type
0	Red_empleados	192.168.20.0/24	ether10	20M	20M	pcq-upload-default	pcq-download-default
1	servidor_camaras_alarma	192.168.50.0/24	ether10	10M	10M	pcq-upload-default	pcq-download-default
2	wifi_empleados	192.168.10.0/24	ether10	5M	5M	pcq-upload-default	pcq-download-default
3	wifi_visitantes	192.168.15.0/24	ether10	2M	2M	pcq-upload-default	pcq-download-default
4	wifi_automatizacion	192.168.30.0/24	ether10	4M	4M	pcq-upload-default	pcq-download-default

Simple Queue <servidor_camaras_alarma>

General | Advanced | Statistics | Traffic | Total | Total Statistics

Name: servidor_camaras_alarma
Target: 192.168.50.0/24
Dst.: ether10

	Target Upload	Target Download	
Max Limit:	10M	10M	bits/s
Burst			
Burst Limit:	unlimited	unlimited	bits/s
Burst Threshold:	unlimited	unlimited	bits/s
Burst Time:	0	0	s
Time			

OK | Cancel | Apply | Disable | Comment | Copy | Remove | Reset Counters | Reset All Counters | Torch

enabled

Simple Queue <Red_empleados>

General | Advanced | Statistics | Traffic | Total | Total Statistics

Packet Marks:

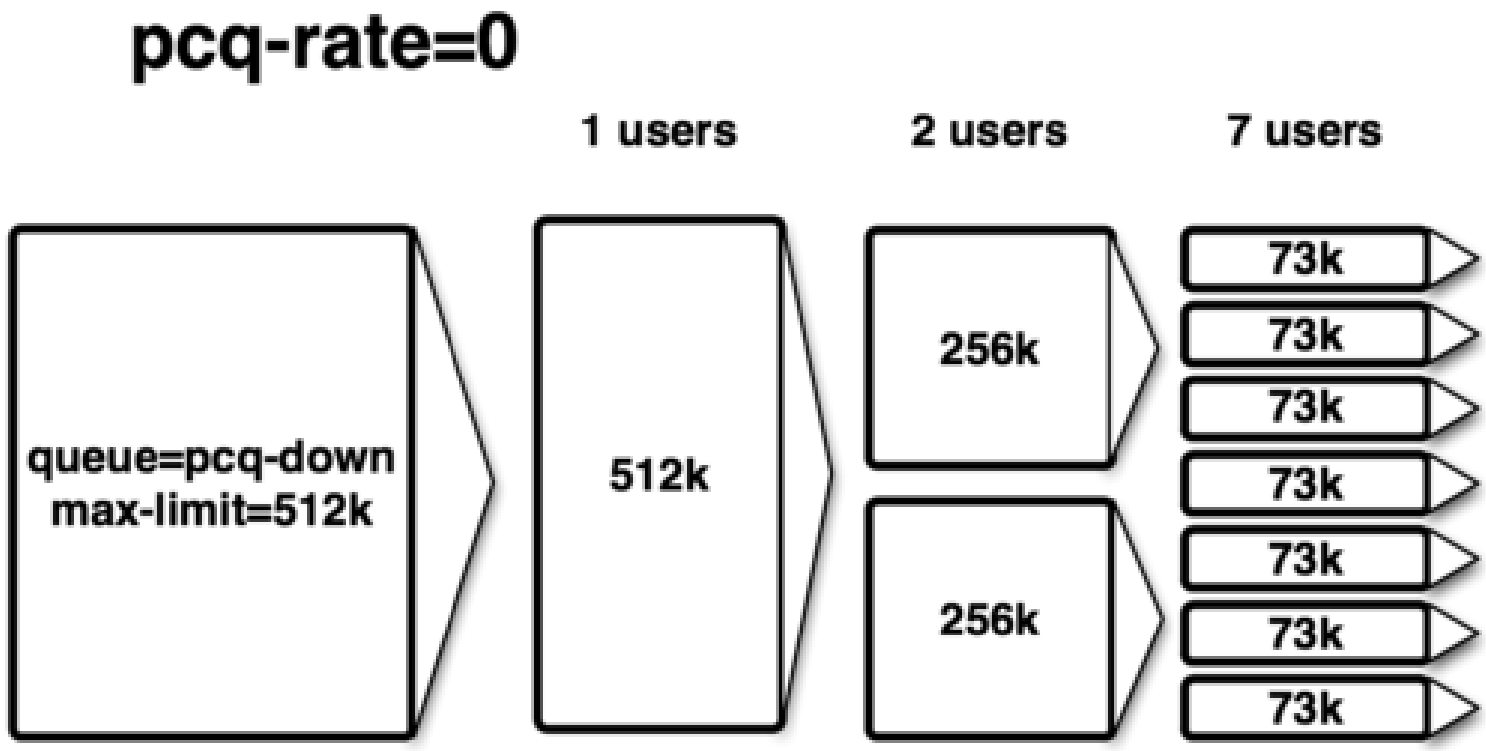
	Target Upload	Target Download	
Limit At:	unlimited	unlimited	bits/s
Priority:	8	8	
Bucket Size:	0.100	0.100	ratio
Queue Type:	pcq-upload-default	pcq-download-default	

Parent: none

OK | Cancel | Apply | Disable | Comment | Copy | Remove | Reset Counters | Reset All Counters | Torch

enabled

2) QoS usando PCQ



3) Mangle (marcado de conexiones

Firewall

Filter Rules | NAT | Mangle | Raw | Service Ports | Connections | Address Lists | Layer7 Protocols

Reset Counters | Reset All Counters

#		Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inte
0	X	mar...	prerouting						
1	X	mar...	prerouting						
2		jump	forward						
3		jump	forward						
;;; voip									
4		mar...	conmark			17 (u...		5060-506...	
;;; YOUTUBE									
5		mar...	conmark			6 (tcp)			
;;; http-https									
6		mar...	conmark			6 (tcp)		80,443	
;;; PING									
7		mar...	conmark			1 (ic...			
;;; DNS									
8		mar...	conmark			17 (u...		53	
;;; rest									
9		mar...	conmark						
10		return	conmark						
;;; VOIP									
11		mar...	pktmark						
;;; YOUTUBE									
12		mar...	pktmark						
;;; HTTP-HTTPS									
13		mar...	pktmark						
;;; PING									
14		mar...	pktmark						
;;; DNS									
15		mar...	pktmark						
;;; SIN MARCA									
16		mar...	pktmark						

4) Queue Tree (asignar prioridades a los servicios marcados)

Queue List

Simple Queues | Interface Queues | Queue Tree | Queue Types

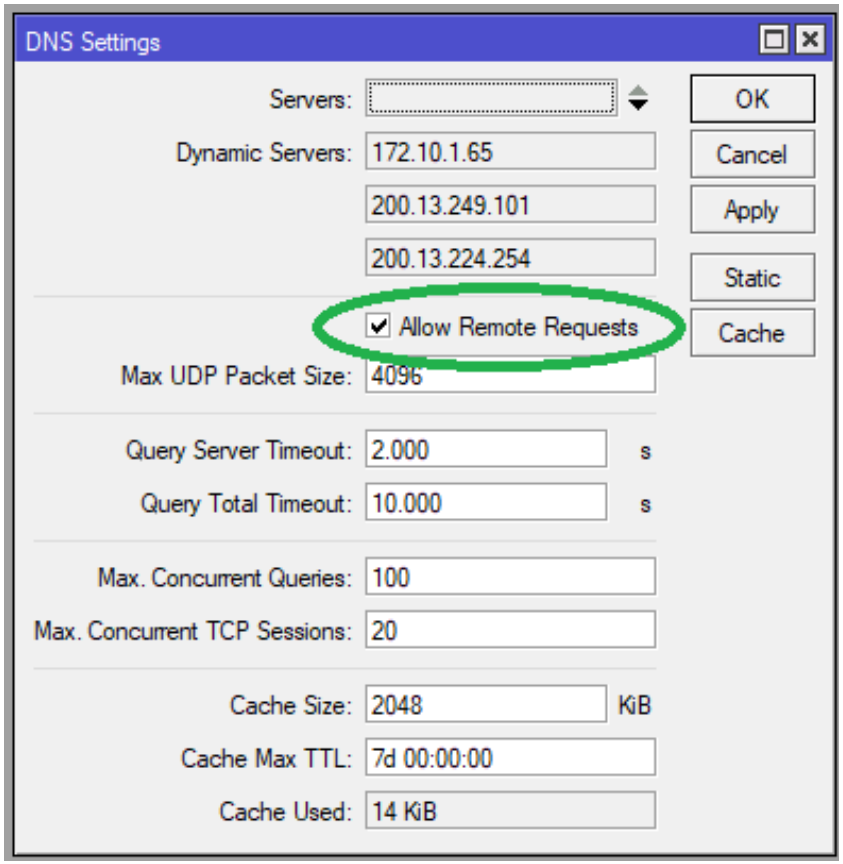
Reset Counters | Reset All Counters

Name	Parent	Packet Marks	Priority	Limit At (b...	Max Limit ...
Download-1	ether2		8		400M
DNS	Download-1	DNS	3	10M	20M
HTTP	Download-1	HTTP	5	150M	300M
PING	Download-1	ICMP	3	10M	20M
TRAFREST	Download-1	SINMARCA	8	100M	150M
VOIP	Download-1	VOIP	2	30M	50M
YOUTUBE	Download-1	YOUTUBE	3	100M	150M
Download-2	ether7		8		400M
DNS-2	Download-2	DNS	3	10M	20M
HTTP2	Download-2	HTTP	5	150M	300M
PING2	Download-2	ICMP	3	10M	20M
TRAFREST2	Download-2	SINMARCA	8	100M	150M
VOIP2	Download-2	VOIP	2	30M	50M
YOUTUBE2	Download-2	YOUTUBE	3	100M	150M
Upload	sfp1		8		800M
DNS-UP	Upload	DNS	3	20M	40M
HTTPUP	Upload	HTTP	5	300M	600M
PINGUP	Upload	ICMP	3	20M	40M
TRAFRESTUP	Upload	SINMARCA	8	200M	300M
VOIPUP	Upload	VOIP	2	60M	100M
YOUTUBEUP	Upload	YOUTUBE	3	200M	300M

DNS

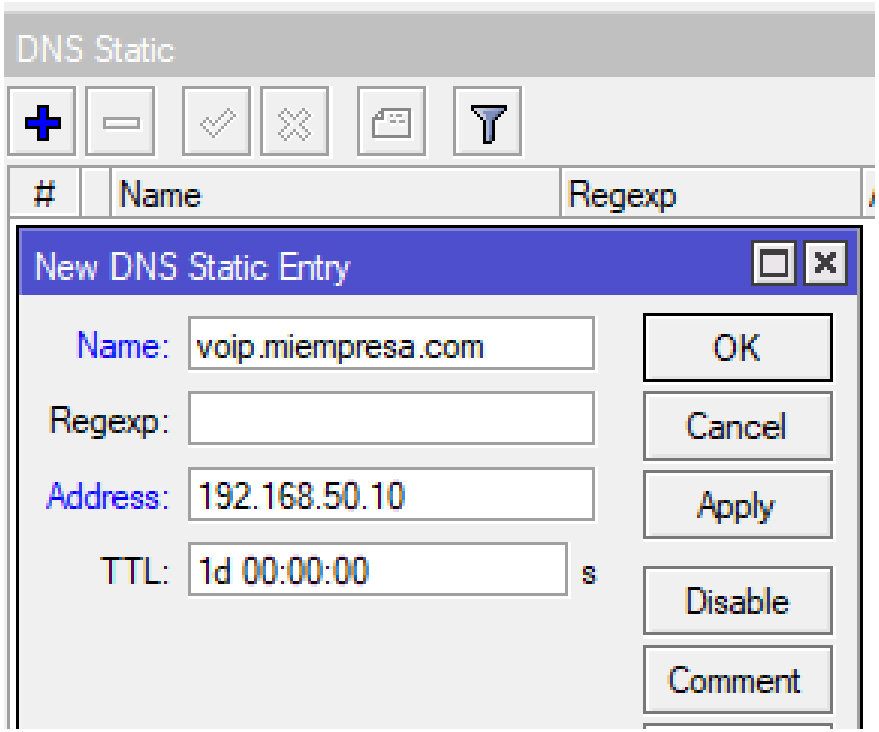
1) Usar Router como servidor DNS

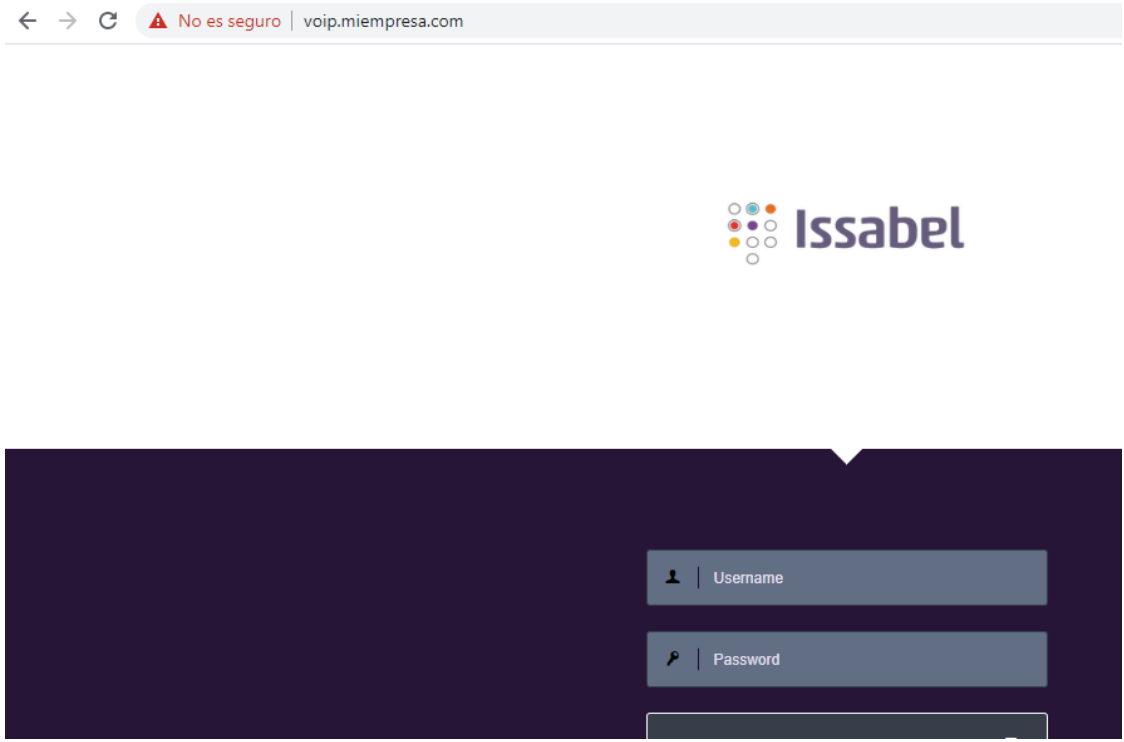
- Podemos configurar el Router como un servidor DNS



2) Entradas estáticas

- Es posible configurar nombres para acceder servicios de nuestra LAN

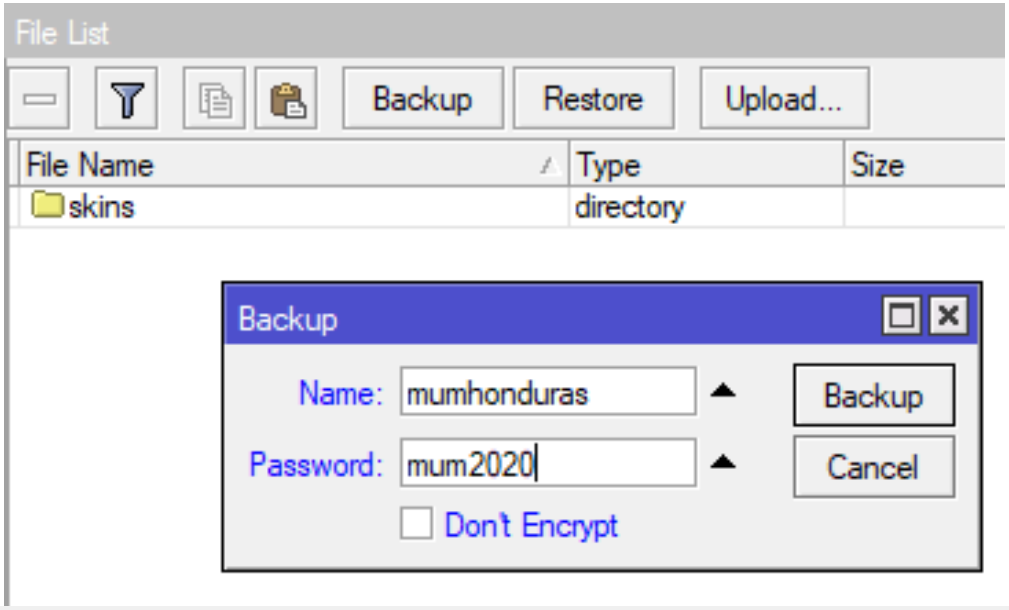


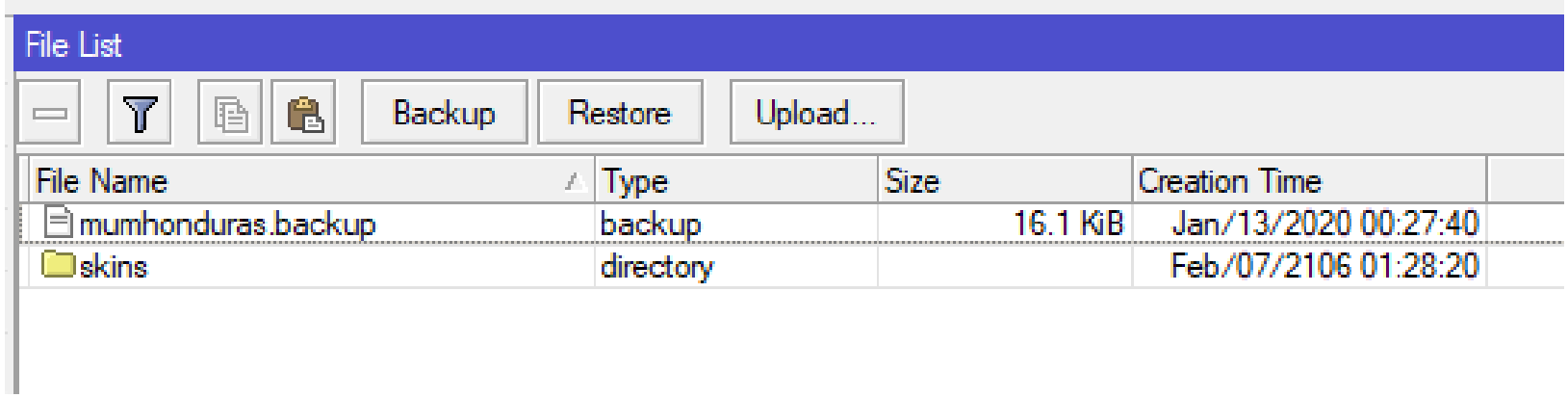


Backups

1) .backup

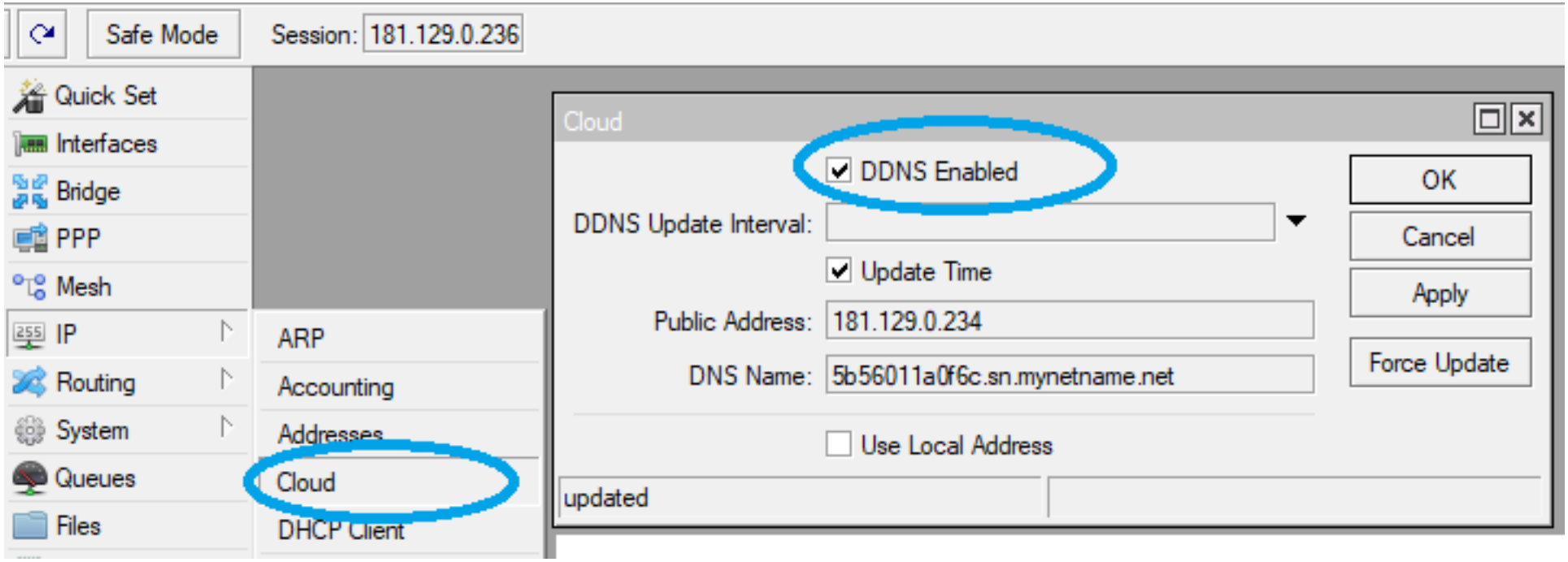
- En files → Backup (extensión .backup)





1) .backup

Cloud backup. Desde la versión 6.14 se tiene disponible, versiones anteriores a 6.43 **cloud.mikrotik.com** versiones de 6.43 en adelante se comunican con **cloud2.mikrotik.com**



1) .backup

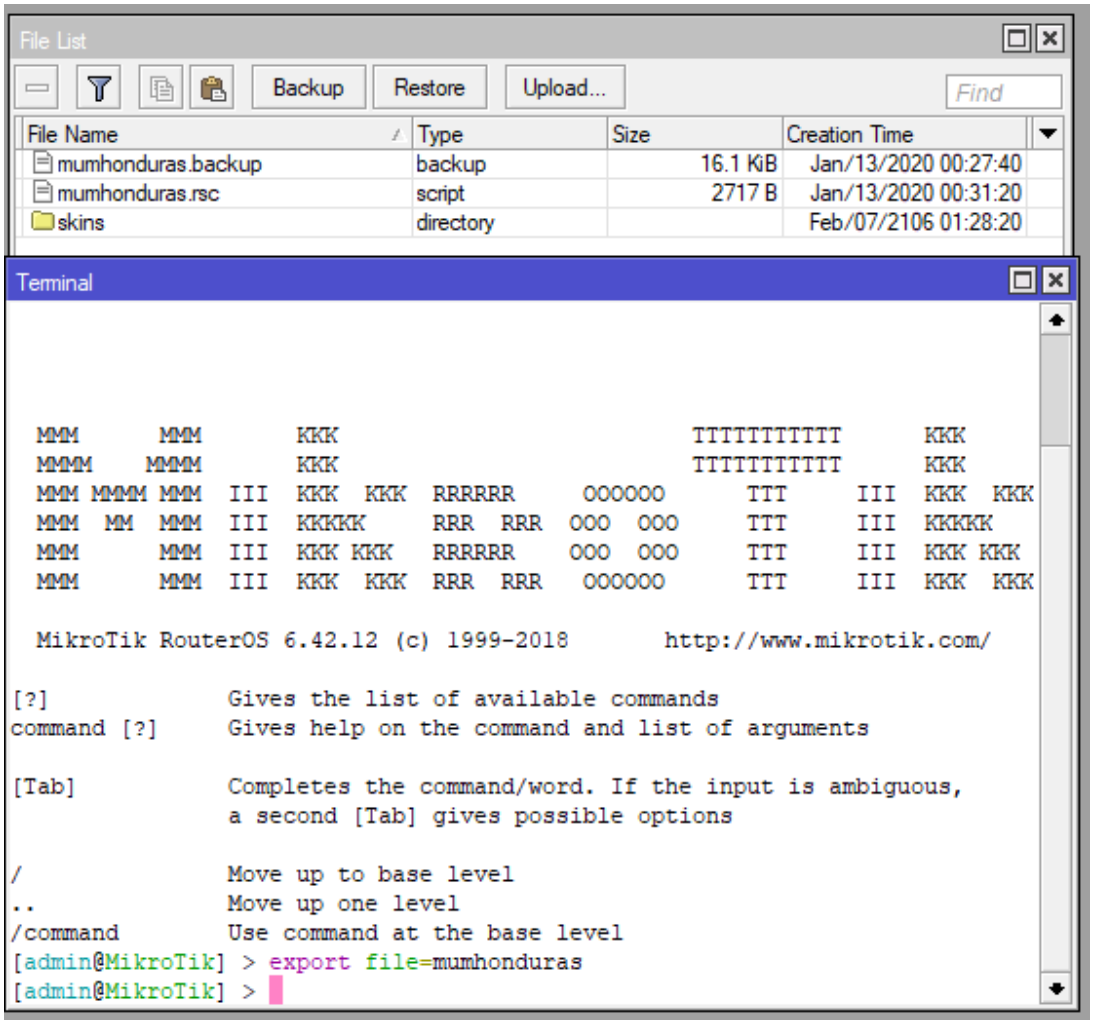
Cloud backup. Desde la versión 6.14 se tiene disponible, versiones anteriores a 6.43 **cloud.mikrotik.com** versiones de 6.43 en adelante se

Terminal

```
  MMM      MMM       KKK                          TTTTTTTTTTT      KKK
  MMMM    MMMM       KKK                          TTTTTTTTTTT      KKK
  MMM MMMM MMM  III  KKK  KKK  RRRRRR     OOOOOO      TTT     III  KKK  KKK
  MMM  MM  MMM  III  KKKKK     RRR  RRR  OOO  OOO     TTT     III  KKKKK
  MMM      MMM  III  KKK KKK   RRRRRR    OOO  OOO     TTT     III  KKK KKK
  MMM      MMM  III  KKK  KKK  RRR  RRR   OOOOOO      TTT     III  KKK  KKK

  MikroTik RouterOS 6.46.1 (c) 1999-2019       http://www.mikrotik.com/

[?]             Gives the list of available commands
command [?]     Gives help on the command and list of arguments

[Tab]           Completes the command/word. If the input is ambiguous,
                a second [Tab] gives possible options

/               Move up to base level
..              Move up one level
/command        Use command at the base level
[vjjt@CCR PPAL HOTEL] > /system backup cloud upload-file action=create-and-upload password=mumhonduras
  status: finished

[vjjt@CCR PPAL HOTEL] > /system backup cloud print
 0 name="cloud-20200113-004748" size=6.7MiB ros-version="6.46.1" date=jan/13/2020 00:47:56 status="ok"
   secret-download-key="w3SLd3QHMO8borYtX07zSKt"
[vjjt@CCR PPAL HOTEL] >
```

2) .rsc

Por línea de comandos → export file=mumhonduras (extensión .rsc)



2) .rsc

ccr1036tol: Bloc de notas

Archivo Edición Formato Ver Ayuda

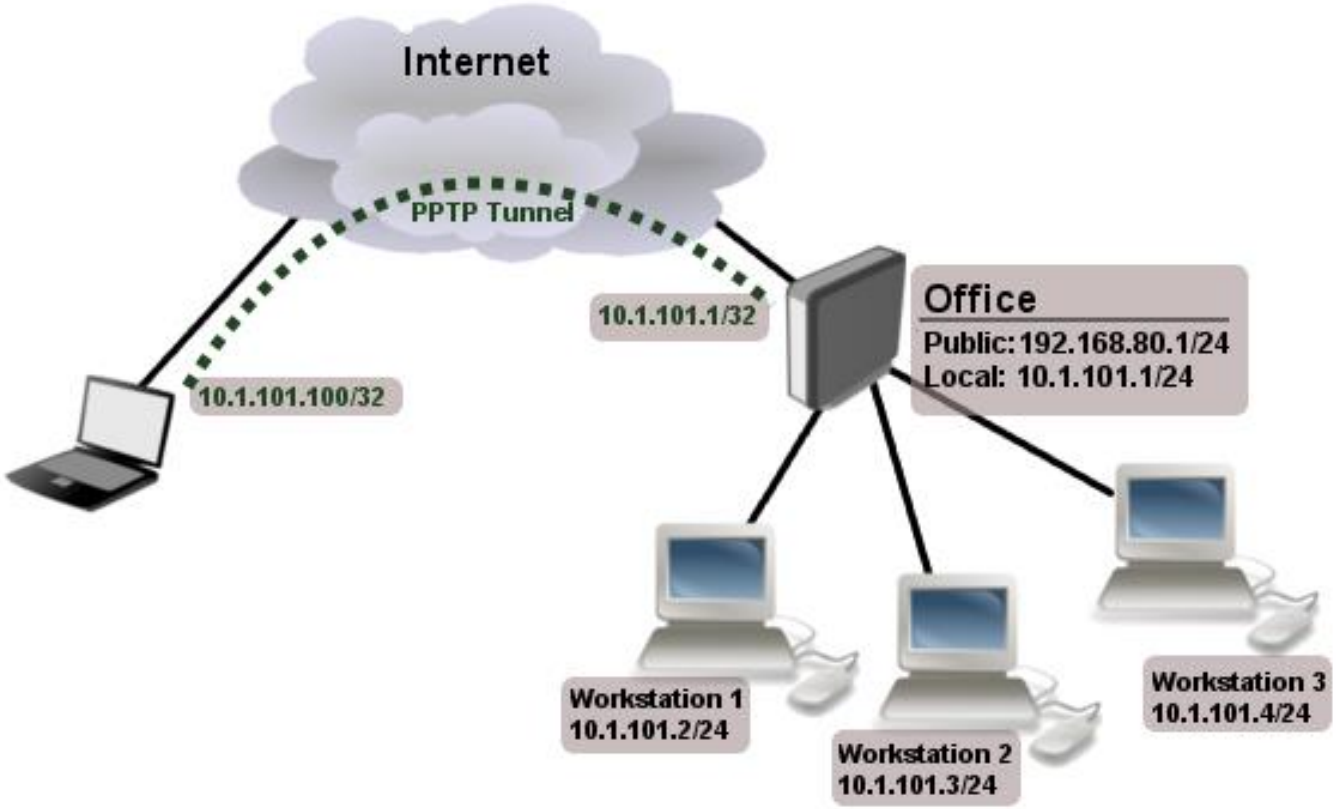
```
# jan/16/2020 12:02:28 by RouterOS 6.46.1
# software id = ZMS5-WZT4
#
# model = CCR1036-12G-4S
# serial number = 5B56011A0F6C
/interface ethernet
set [ find default-name=ether1 ] advertise=\
    10M-half,10M-full,100M-half,100M-full,1000M-half,1000M-full speed=100Mbps
set [ find default-name=ether2 ] comment="PADRE AMAYA" speed=100Mbps
set [ find default-name=ether3 ] comment=WAN speed=100Mbps
set [ find default-name=ether4 ] comment=SERGIO speed=100Mbps
set [ find default-name=ether5 ] speed=100Mbps
set [ find default-name=ether6 ] advertise=10M-full,100M-full comment=\
    "HOTEL CM" speed=100Mbps
set [ find default-name=ether7 ] advertise=\
    10M-half,10M-full,100M-half,100M-full,1000M-half,1000M-full comment=\
    "PADRE AMAYA 2" speed=100Mbps
set [ find default-name=ether8 ] comment=ZARZAL speed=100Mbps
set [ find default-name=ether9 ] speed=100Mbps
set [ find default-name=ether10 ] comment="CLIENTE APTO 402" speed=100Mbps
set [ find default-name=ether11 ] comment="DVR EDIFICIO" speed=100Mbps
set [ find default-name=ether12 ] advertise=\
    10M-half,10M-full,100M-half,100M-full,1000M-half,1000M-full comment=CS
```

VPN´s

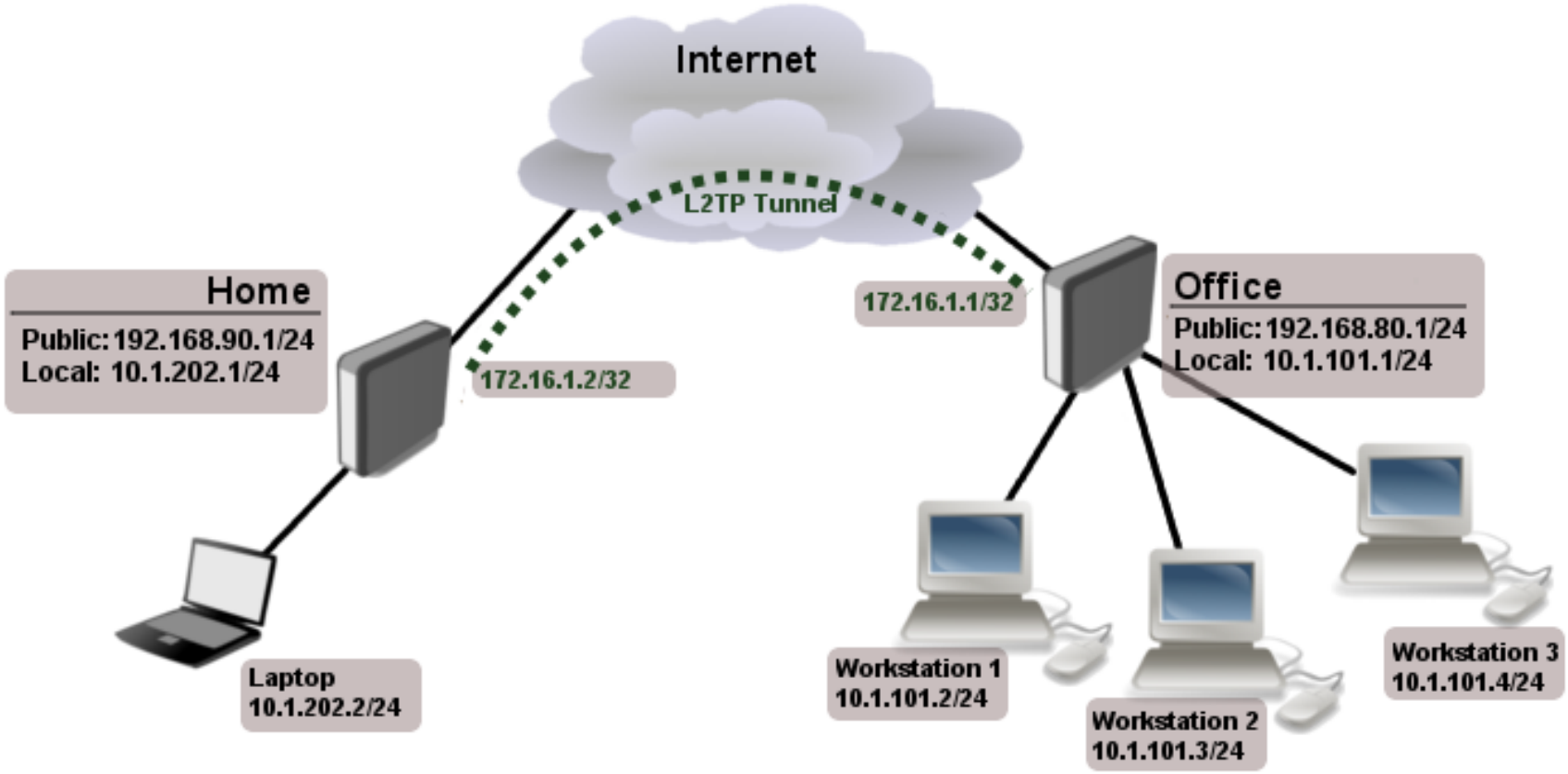
1) Múltiples opciones de VPN

fuente: https://es.vpnmentor.com/blog/comparacion-de-protocolos-de-vpn-pptp-vs-l2tp-vs-openvpn-vs-sspt-vs-ikev2/

2) Conexión cliente - Servidor



3) Site to Site



¿PREGUNTAS?

LINKS DE REFERENCIA

- https://wiki.mikrotik.com/wiki/Manual:Queue
- https://wiki.mikrotik.com/wiki/Manual:Queues_-_PCQ
- https://wiki.mikrotik.com/wiki/Manual:System/Backup
- https://wiki.mikrotik.com/wiki/Tunnels
- https://axiomcyber.com/shield/

Los esperamos en Colombia!!!

Gracias