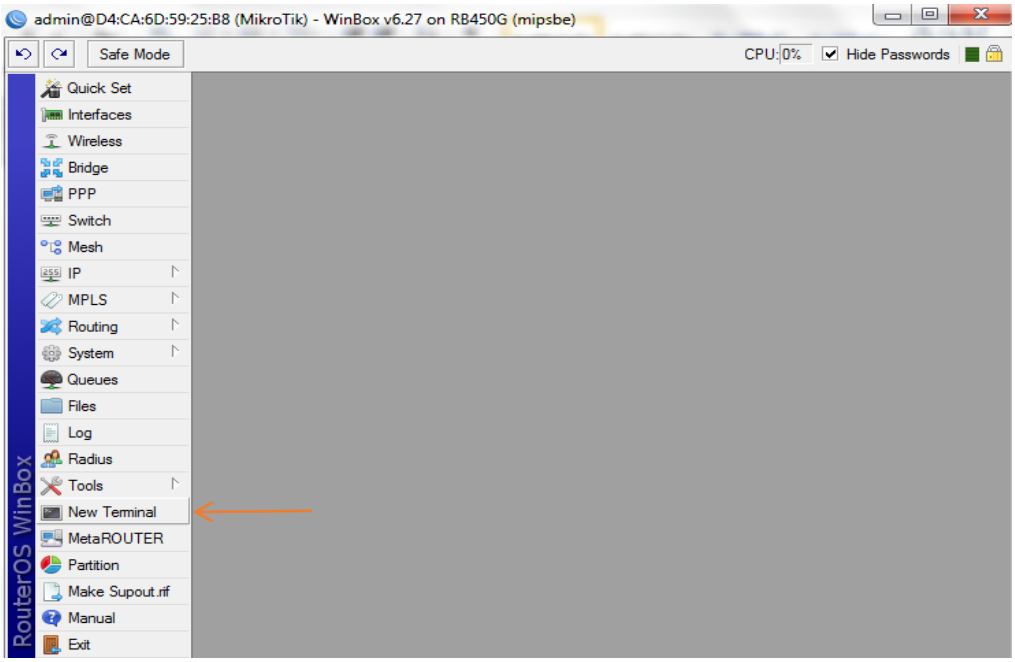
PROCEDIMIENTO DE SEGURIDAD EN LA RED

1. PROCEDIMIENTO DE PREVENCION DE ACCESO AL ROUTER POR FUERZA BRUTA SSH Y FTP

Detener los ataques FTP.

La configuración permite un máximo de 10 intentos de conexión FTP incorrectas por minuto.
Se ingresa a la Routerboard y por new terminal se ingresan las líneas para evitar ataques por FTP:



Desde New Terminal se ingresan las siguientes líneas de configuración:

```
[admin@MikroTik] > ip firewall filter
[admin@MikroTik] /ip firewall filter> add chain=input protocol=tcp dst-port=21 src
-address-list=ftp_blacklist action=drop comment=Bloqueo_Fuerza_Bruta_por_FTP
[admin@MikroTik] /ip firewall filter> add chain=output action=accept protocol=tcp
comment="530 Login Incorrect" dst-limit=1/1m,9,dst-address/1m
[admin@MikroTik] /ip firewall filter> add chain=output action=add-dst-to-address-l
ist protocol=tcp content="530 Loging Incorrect" address-list=ftp_blacklist address
-list-timeout=3h
[admin@MikroTik] /ip firewall filter>
```

Visto desde el New Terminal:

```
[admin@MikroTik] > ip firewall filter
[admin@MikroTik] /ip firewall filter> add chain=input protocol=tcp dst-port=21 src
-address-list=ftp_blacklist action=drop comment=Bloqueo_Fuerza_Bruta_por_FTP
[admin@MikroTik] /ip firewall filter> add chain=output action=accept protocol=tcp
comment="530 Login Incorrect" dst-limit=1/1m,9,dst-address/1m
[admin@MikroTik] /ip firewall filter> add chain=output action=add-dst-to-address-l
ist protocol=tcp content="530 Loging Incorrect" address-list=ftp_blacklist address
-list-timeout=3h
```

Bloqueo de ataques de fuerza bruta por SSH

Esta configurción bloquea por 10 dias la dirección de origen después de intentos repetidos:
[admin@MikroTik] > ip firewall filter
[admin@MikroTik] /ip firewall filter> add chain=input protocol=tcp dst-port=22 src
-address-list=ssh_blacklist action=drop comment="bloqueo de ataques de fuerza brut
a por SSH" disabled=no

[admin@MikroTik] /ip firewall filter> add chain=input protocol=tcp dst-port=22 con
nection-state=new src-address-list=ssh_stage3 action=add-src-to-address-list addre
ss-list=ssh_blacklist address-list-timeout=10d comment="bloqueo por 10 dias" disab
led=no

[admin@MikroTik] /ip firewall filter> add chain=input protocol=tcp dst-port=22 con
nection-state=new src-address-list=ssh_stage2 action=add-src-to-address-list addre
ss-list=ssh_stage3 address-list-timeout=1m comment="" disabled=no

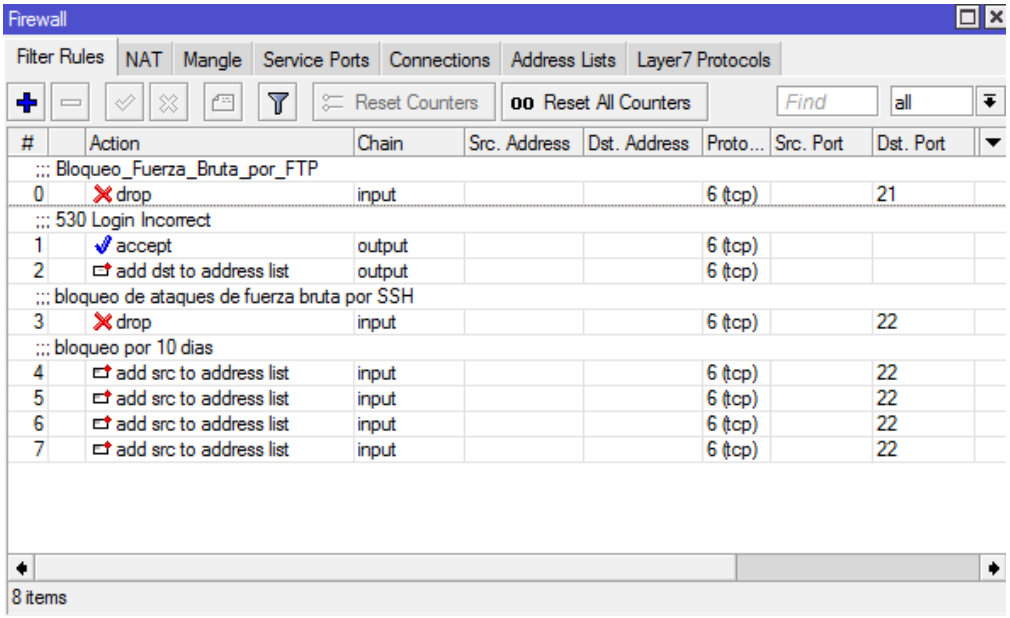
[admin@MikroTik] /ip firewall filter> add chain=input protocol=tcp dst-port=22 con
nection-state=new src-address-list=ssh_stage1 action=add-src-to-address-list addre
ss-list=ssh_stage2 address-list-timeout=1m comment="" disabled=no

[admin@MikroTik] /ip firewall filter> add chain=input protocol=tcp dst-port=22 con
nection-state=new action=add-src-to-address-list address-list=ssh_stage1 address-l
ist-timeout=1m comment="" disabled=no
Visto desde New Terminal:

```
[admin@MikroTik] > ip firewall filter
[admin@MikroTik] /ip firewall filter> add chain=input protocol=tcp dst-port=22 src
-address-list=ssh_blacklist action=drop comment="bloqueo de ataques de fuerza brut
a por SSH" disabled=no
[admin@MikroTik] /ip firewall filter> add chain=input protocol=tcp dst-port=22 con
nection-state=new src-address-list=ssh_stage3 action=add-src-to-address-list addre
ss-list=ssh_blacklist address-list-timeout=10d comment="bloqueo por 10 dias" disab
led=no
[admin@MikroTik] /ip firewall filter> add chain=input protocol=tcp dst-port=22 con
nection-state=new src-address-list=ssh_stage2 action=add-src-to-address-list addre
ss-list=ssh_stage3 address-list-timeout=1m comment="" disabled=no
[admin@MikroTik] /ip firewall filter> add chain=input protocol=tcp dst-port=22 con
nection-state=new src-address-list=ssh_stage1 action=add-src-to-address-list addre
ss-list=ssh_stage2 address-list-timeout=1m comment="" disabled=no
[admin@MikroTik] /ip firewall filter> add chain=input protocol=tcp dst-port=22 con
nection-state=new action=add-src-to-address-list address-list=ssh_stage1 address-l
ist-timeout=1m comment="" disabled=no
[admin@MikroTik] /ip firewall filter>
```

Por interfaz gráfica se pueden observar las líneas configuradas:

En ip firewall filter> print



Listado completo para pegar desde Terminal:

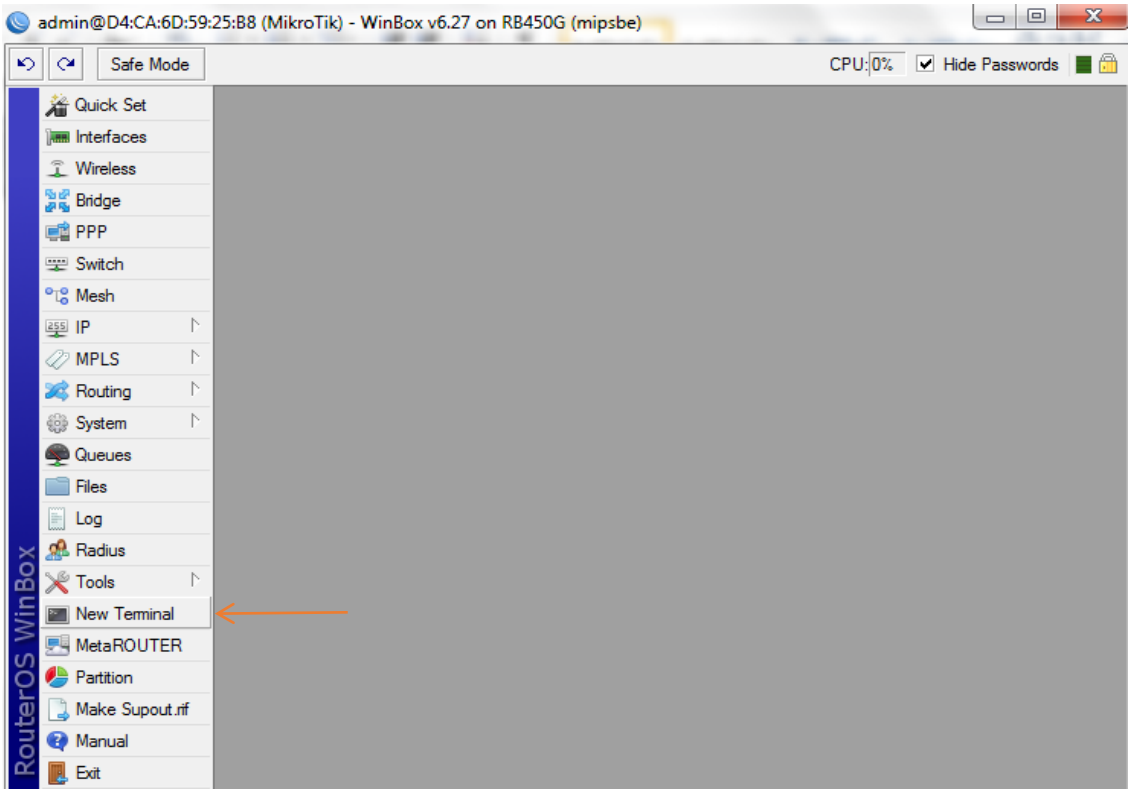
```
/ip firewall filter
add action=drop chain=input comment="fuerza bruta" disabled=no dst-port=21 \
    protocol=tcp src-address-list=ftp_blacklist
add action=accept chain=output content="530 login incorrect" disabled=no \
```

```
    dst-limit=1/1m,9,dst-address/1m protocol=tcp
add action=add-dst-to-address-list address-list=ftp_blacklist \
    address-list-timeout=3h chain=output content="530 login incorrect" \
    disabled=no protocol=tcp
add action=drop chain=input comment="ssh fuerza bruta" disabled=no dst-port=\
    22 protocol=tcp src-address-list=ssh_blacklist
add action=add-src-to-address-list address-list=ssh_blacklist \
    address-list-timeout=1w3d chain=input connection-state=new disabled=no \
    dst-port=22 protocol=tcp src-address-list=ssh_stage3
add action=add-src-to-address-list address-list=ssh_blacklist \
    address-list-timeout=1w3d chain=input connection-state=new disabled=no \
    dst-port=22 protocol=tcp src-address-list=ssh_stage3
add action=add-src-to-address-list address-list=ssh_stage3 \
    address-list-timeout=1m chain=input connection-state=new disabled=no \
    dst-port=22 protocol=tcp src-address-list=ssh_stage2
add action=add-src-to-address-list address-list=ssh_stage2 \
    address-list-timeout=1m chain=input connection-state=new disabled=no \
    dst-port=22 protocol=tcp src-address-list=ssh_stage1
add action=add-src-to-address-list address-list=ssh_stage1 \
    address-list-timeout=1m chain=input connection-state=new disabled=no \
```

2. PROCEDIMIENTO BLOQUEO DE SPAMMER

El siguiente procedimiento detecta y bloquea virus SMTP más conocidos como SPAMMER.

Se requieren crear dos reglas de Firewall Forward:



Configuración por líneas de comando:

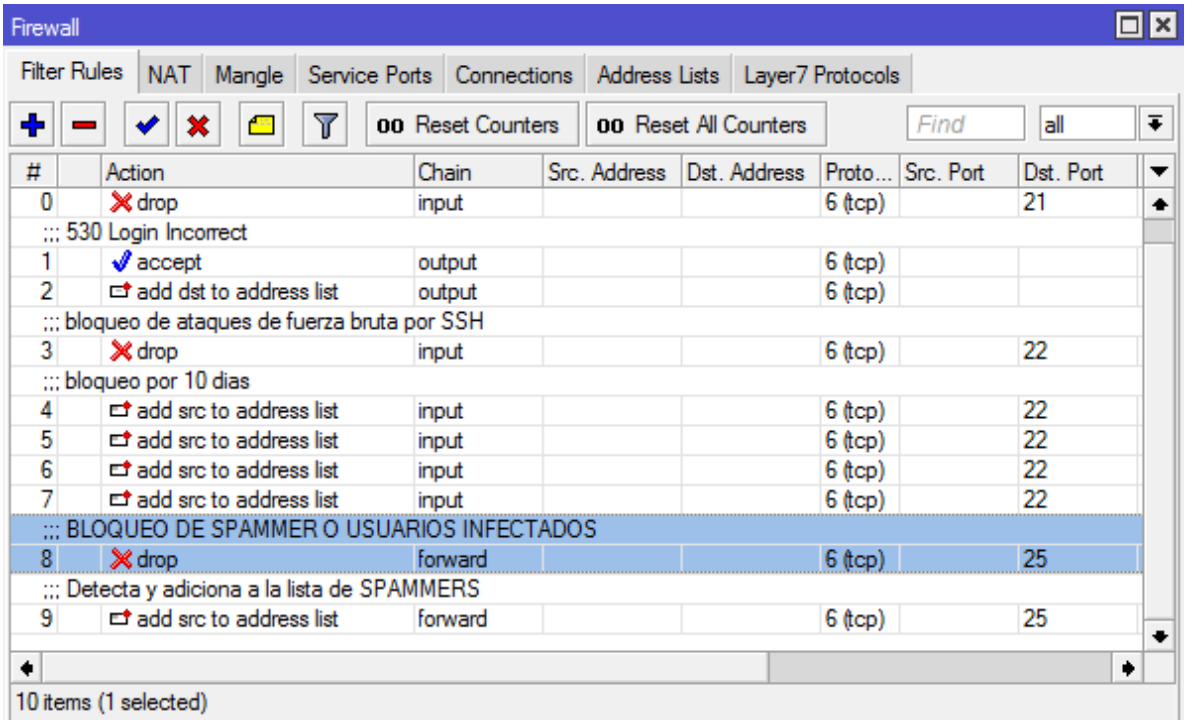
[admin@MikroTik] > ip firewall filter
[admin@MikroTik] /ip firewall filter> add chain=forward protocol=tcp dst-port=25 src-address-list=spammer action=drop comment="BLOQUEO DE SPAMMER O USUARIOS INF
ECTADOS"

[admin@MikroTik] /ip firewall filter> add chain=forward protocol=tcp dst-port=25 c onnection-limit=30,32 limit=50,5 action=add-src-to-address-list address-list=spamm

pammer address-list-timeout=1d comment="Detecta y adiciona a la lista de SPAMMERS"
[admin@MikroTik] /ip firewall filter>

Cuando un usuario infectado, es detectado con un virus, gusano o hacer correo no deseado, el usuario se agrega a una lista spammer y bloquear el saliente SMTP por 1 día. Normalmente, los ataques de spamming al no tener respuesta descartan la ip del usuario.

Finalmente para ver las reglas en el router se puede revisar por interfaz gráfica:

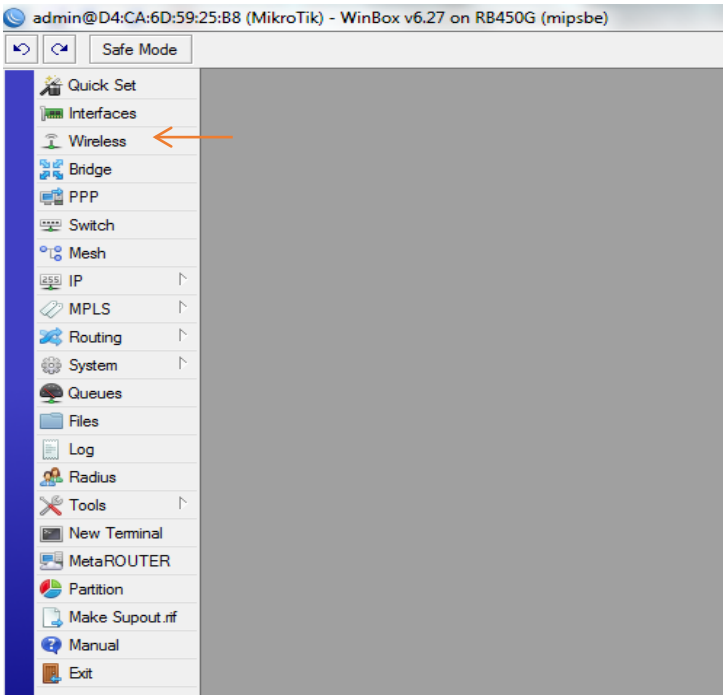


3. PROCEDIMIENTO DE SEGURIDAD PARA LAS CONEXIONES INALAMBRICAS

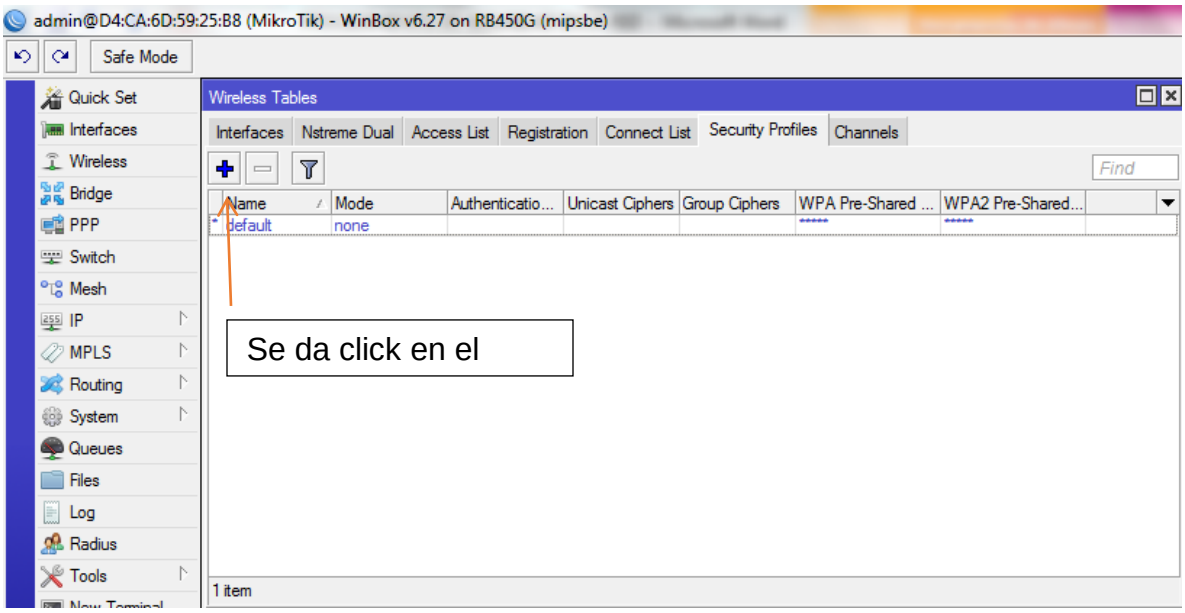
Con este procedimiento se impiden conexiones inalámbricas no autorizadas.

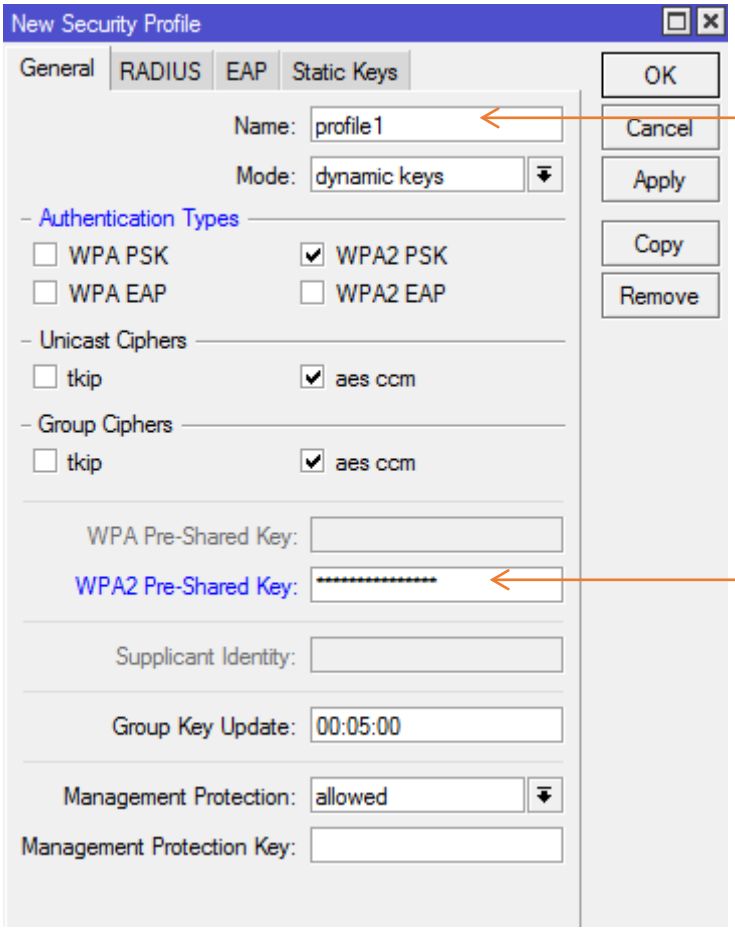
PROCEDIMIENTO PARA ENLACES MIKROTIK

Se realiza acceso por el software propietario Winbox:



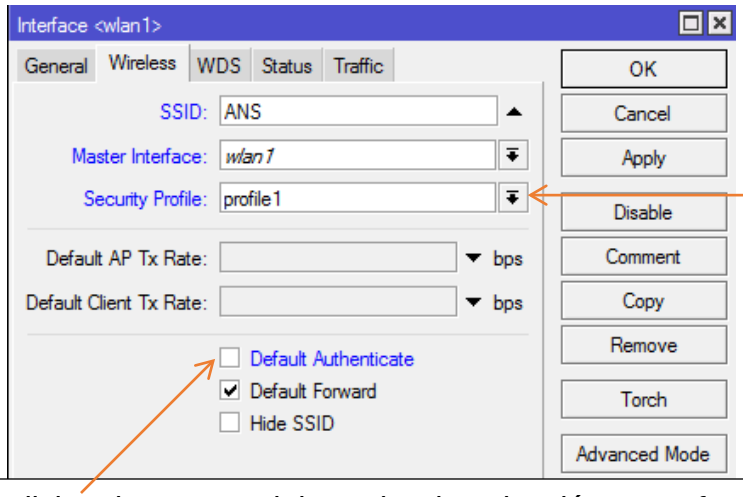
Se ingresa al menú de Wireless y se selecciona la pestaña Security Profile:





Se puede dejar por defecto este nombre, el cual se usara a la hora de aplicarlo a la

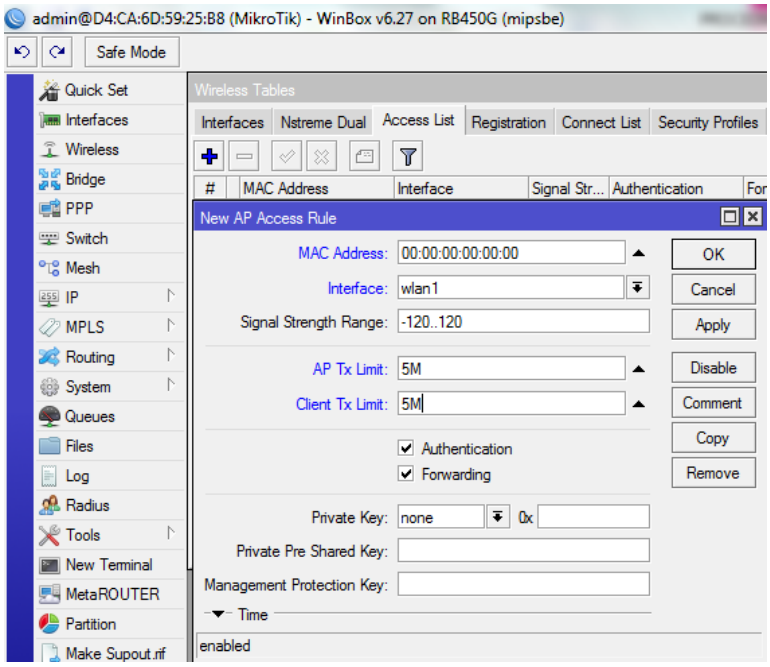
Se configura el key de seguridad inalámbrica asignado por parte



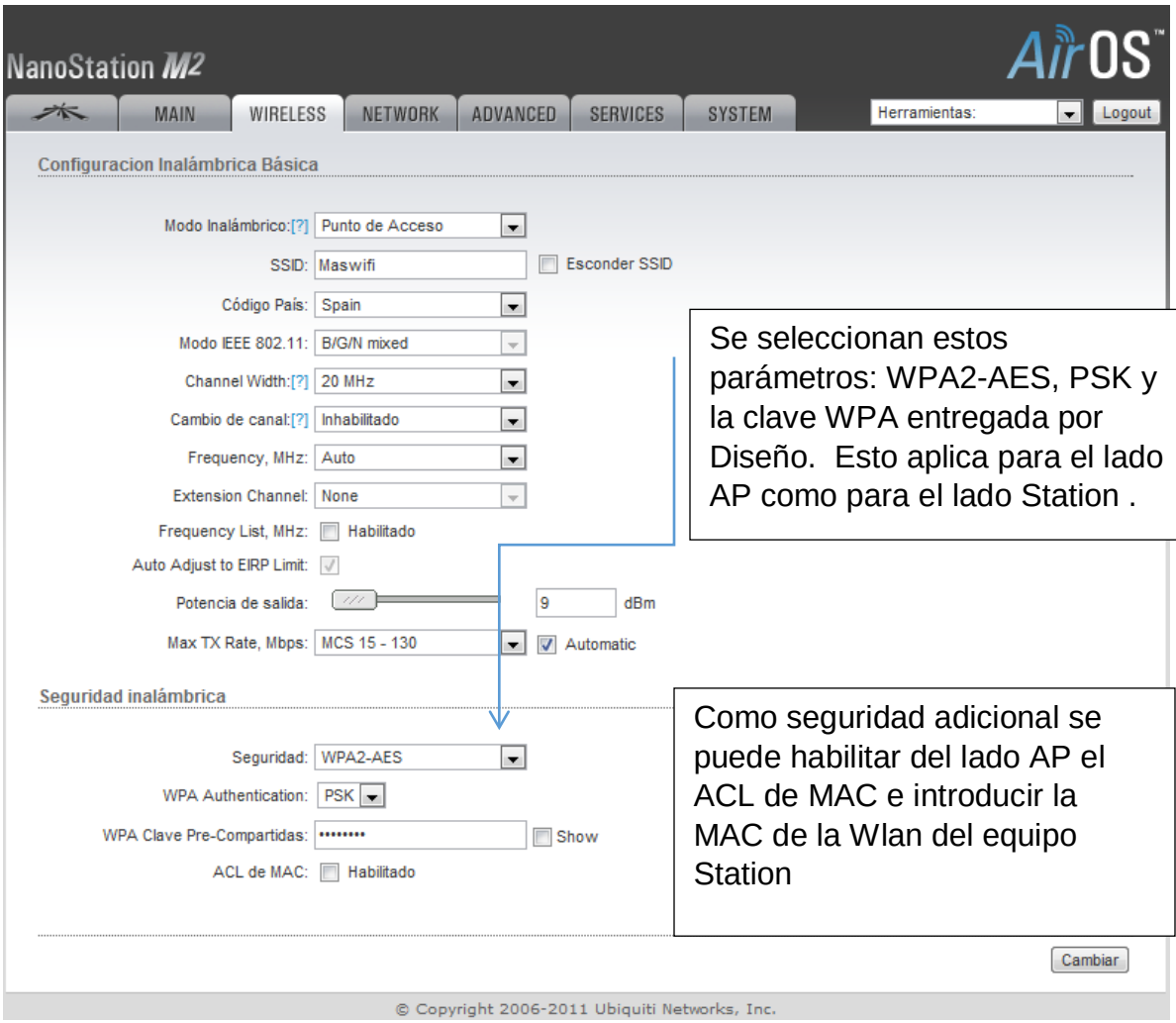
Sobre la tarjeta inalámbrica en Security Profile se selecciona el profile 1 que previamente se configuro

Adicionalmente se debe retirar la selección en Default Authenticate del lado del Radio AP con esto es necesario registrar en el Access Lista la MAC Address de la tarjeta inalámbrica del esquipo Station

Para ingresar la MAC Address de la tarjeta inalámbrica del equipo Station , vamos por el menú de wireless y la pestaña Access Lista allí adicionamos con el icono e ingresamos el dato de la MAC Address, adicionalmente se selecciona la interfaz inalámbrica y se puede limitar el ancho de banda del enlace.



4. PROCEDIMIENTO EN ENLACES UBIQUITI



A continuación los nodos donde se tienen equipos de seguridad para la red:

CLIENTES	NODO	DEPARTAMENTO	MUNICIPIO
COMPASS SERVICES SAS -- PTO NUEVO	FUEGO STEREO	MAGDALENA	SANTA MARTA
AUSTING INGENIEROS SAS -- PTO NUEVO	FUEGO STEREO	MAGDALENA	SANTA MARTA
MEDIA COMMERCE -- PEAJE NEGUANJE	LA LLORONA	MAGDALENA	SANTA MARTA
AUSTING INGENIEROS SAS -- LA JAGUA	LA LOMA	CESAR	LA JAGUA DE IBIRICO
COMPASS SERVICES SAS -- MINA LA JAGUA	LA LOMA	CESAR	LA JAGUA DE IBIRICO
AUSTING INGENIEROS SAS -- CALENTURITAS	LA LOMA	CESAR	EL PASO
CHM MINERIA SAS -- MINA DRUMOND	LA LOMA	CESAR	EL PASO
KOMATSU COLOMBIA SAS -- MINA DRUMMOND	LA LOMA	CESAR	EL PASO
MECANICOS ASOCIADOS SAS -- MINA DRUMMOND	LA LOMA	CESAR	EL PASO
CHM MINERIA SAS -- MINA EL DESCANSO	LA LOMA	CESAR	EL PASO
COMPASS SERVICES SAS -- MINA CALENTURITAS	LA LOMA	CESAR	EL PASO
PETROLEUM BLENDING S.A -- OMEGA RAMIRIQUI	YOPAL	CASANARE	YOPAL
PETROLEUM BLENDING S.A -- OMEGA RANCHO HERMOSO	YOPAL	CASANARE	YOPAL
PETROLEUM BLENDING S.A -- OMEGA CAMPO POINTER	YOPAL	CASANARE	YOPAL
GEOPARK COLOMBIA	VILLANUEVA	CASANARE	VILLANUEVA
AGROPECUARIA ALIAR S.A -- PUERTO GAITAN	PUERTO GAITAN	META	PUERTO GAITAN
MEDIA COMMERCE -- CAFABA	YONDO	SANTANDER	BARRANCABERMEJA
ESCUELAS ARAUCA	ARAUCA	ARAUCA	ARAUCA
	ARAUQUITA	ARAUCA	ARAUQUITA
	SARAVENA	ARAUCA	SARAVENA
	TAME	ARAUCA	TAME
	FORTUL	ARAUCA	FORTUL
	PUERTO RONDON	ARAUCA	PUERTO RONDON