

MODULO 12

Automatización con scripts

1. Configuraciones para automatización de tareas con Scripts.
 - 1.1. Creación de Script para crear Backup de todo el MikroTik.

Vamos a crear dos scripts para la creación de Backup de tipo binario y export con ayuda de la consola de MikroTik.

Primero: vamos a crear Backup's del tipo binario y export desde consola con el fin de asegurarnos de que por consola se crean los Backup sin ningún problema.



Binario:

```
/system backup save dont-encrypt=yes name="BKP-all-Configuration"
```

Export:

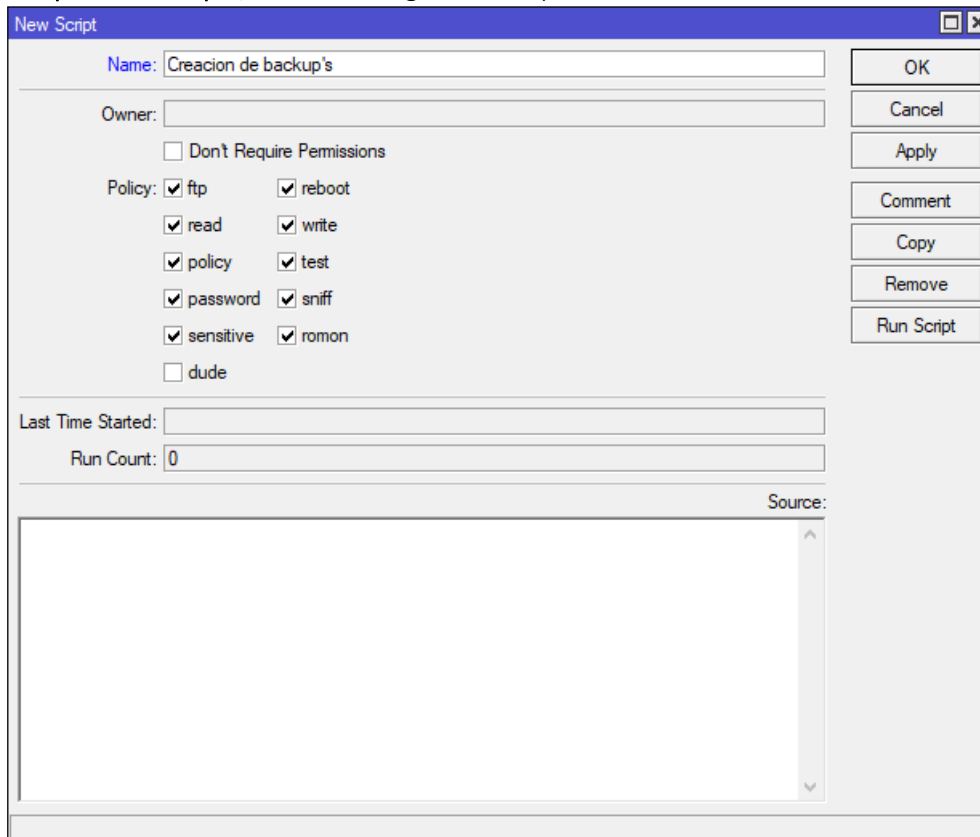
```
/export file="EXP-all-Configuration"
```

Segundo: Verificamos que los Backup se han generado sin ningún problema.

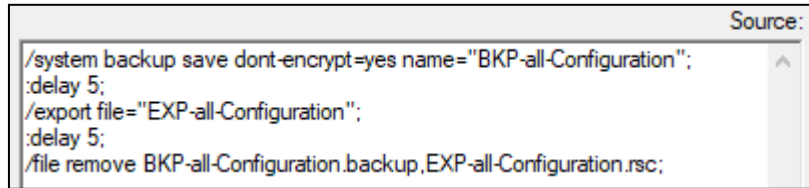
 All-Configuration.backup	backup
 All-Configuration.rsc	script

Luego de verificar los eliminamos.

En **System -> Scripts**, creamos el siguiente script.



Ahora agregamos los comandos usados para generar los Backup a la sección Source del script que estamos creando, finalizando la instrucción con un “;” y agregando un delay de unos cuantos segundos para que el script se ejecute con calma. Quedando de la siguiente forma.



```
Source:
/system backup save dont-encrypt=yes name="BKP-all-Configuration";
:delay 5;
/export file="EXP-all-Configuration";
:delay 5;
/file remove BKP-all-Configuration.backup,EXP-all-Configuration.rsc;
```

Ahora podemos dar clic en RunScript para dar seguimiento en Files, si todo va bien podemos automatizar ese script.

1.2. Automatizar el script creado anteriormente.

En **System** -> **Scheduler** vamos a crear una tarea automatizada.

Name:	Nombre de la tarea programada
Start Date:	Fecha de inicio de la tarea programada
Start Time:	Hora de inicio de la tarea programada
Interval:	Intervalo de ejecución para la tarea programada (En un entorno real se pondrá cada 7d 00:00:00).
On Event:	El nombre del script que creamos anteriormente

MODULO 13

Configuración de calidad de servicio

2. Configuraciones de calidad de servicio.

QOS = calidad de servicio es un método empleado para tener el control del tráfico de datos dentro de una red de computadoras y otros dispositivos, de esa forma podemos tener el control sobre el ancho de banda que un dispositivo pueda tener, existen dos métodos los cuales son:

Simple.

Avanzado.

2.1. Método de control simple.

En **Queues** -> **SimpleQueues**, podemos crear reglas de control de ancho de banda

Name = Nombre del QoS

Target = El objetivo a donde queremos controlar

Target Up load, target Down load = velocidades asignadas para subida y bajada de datos

2.2. Método de control avanzado.

2.2.1. Creación de reglas de subida y bajada

En **Queues** -> **QueueTypes**, creamos dos reglas para bajada y subida

Type Name: DOWN
Kind: pcq
Classifier: Src. Address

Type Name: UP

Kind: pcq
Classifier: Dst. Address

2.2.2. Creación de reglas mangle en Firewall.

- REGLAS PARA UPLOAD (subida)

En IP -> Firewall -> Mangle, creamos reglas de control para UPLOAD para los dispositivos a controlar

GENERAL

configuramos el tipo de **chain:prerouting** y la IP en **Src. Address** a quien queremos controlar la subida, El resto lo dejamos en blanco.

ACTION

configuramos el **marcado de paquete** y su **nombre** como tal para identificarlo y asignarle una velocidad de subida.

- REGLAS PARA DOWNLOAD (descarga)

En IP -> Firewall -> Mangle, creamos reglas de control para DOWNLOAD para los dispositivos a controlar.

GENERAL

Configuramos el tipo de **chain:postrouting** y la IP en **Dst. Address** a quien queremos controlar la descarga, El resto lo dejamos en blanco.

ACTION

Configuramos el **marcado de paquete** y su **nombre** como tal para identificarlo y asignarle una velocidad de subida.

2.2.3. Creación de reglas parents (PADRES)

Debemos crear nuevas reglas parents de subida y bajada para grupos en general dando una velocidad límite para cada grupo.

- Grupo parent de descarga

En **Queues** -> **Queue Tree** Creamos nuevas reglas parents donde una velocidad límite de Descarga para un grupo.

Name: DOWN-G1
Parent: La interface objetivo o globalmente
QueueType: Seleccionamos Down ya creada en (QueueType)
MaxLimit: Maxima velocidad de descarga en el padre

- Grupo parent de subida

En **Queues** -> **Queue Tree** Creamos nuevas reglas parents donde una velocidad límite de subida para un grupo.

Name: UP-G1

Parent: La interface objetivo o globalmente

QueueType: Seleccionamos UP ya creada en (QueueType)

MaxLimit: Maxima velocidad de descarga en el padre

The screenshot shows the 'Queue <UP-G1>' configuration window. The 'General' tab is active. The 'Name' field is 'UP-G1', 'Parent' is 'ether8', 'Queue Type' is 'UP', 'Priority' is '8', and 'Bucket Size' is '0.100'. The 'Limit At' field is set to 'bits/s'. The 'Max Limit' is '5M', 'Burst Limit' is 'bits/s', 'Burst Threshold' is 'bits/s', and 'Burst Time' is 's'. The 'enabled' checkbox is checked. On the right, there are buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', 'Remove', 'Reset Counters', and 'Reset All Counters'.

Quedando de la siguiente forma

The screenshot shows the 'Queue List' window. It has tabs for 'Simple Queues', 'Interface Queues', 'Queue Tree', and 'Queue Types'. The 'Queue Tree' tab is active. The table shows the following data:

Name	Parent	Packet	Limit At (b...)	Max Limit	Avg. R...	Queued Bytes	Bytes	Packets
DOWN	ether8			10M	0 bps	0 B	0 B	0
UP-G1	ether8			5M	0 bps	0 B	0 B	0

At the bottom, it shows '2 items', '0 B queued', and '0 packets queued'.

2.2.4. Agregando hijos a los grupos parents.

- Agregando PC's al grupo de descarga

En **Queues** -> **Queue Tree** Creamos nuevas reglas Hijos donde agregaremos PC's al grupo de Descarga

Name: PC-objetivo Down

Parent: Seleccionamos en parent ya creado (DOWN)

PacketMarks: seleccionamos la PC creada en mangle de firewall

QueueType: Seleccionamos DOWN ya creada en QueueType

MaxLimit: Asignamos una velocidad para esta PC

- Agregando PC's al grupo de subida
En **Queues** -> **Queue Tree** Creamos nuevas reglas Hijos donde agregaremos PC's al grupo de Subida

Name: PC-objetivo UP
Parent: Seleccionamos en parent ya creado (UP)
PacketMarks: seleccionamos la PC creada en mangle de firewall
QueueType: Seleccionamos UP ya creada en QueueType
MaxLimit: Asignamos una velocidad para esta PC

Quedando de la siguiente forma

Name	Parent	Packet	Limit At (b...)	Max Limit ...	Avg. R...	Queued Bytes	Bytes	Packets
DOWN	ether8			10M	0 bps	0 B	0 B	0
PC-obj...	DOWN	PC obj...		3M	0 bps	0 B	0 B	0
UP-G1	ether8			5M	0 bps	0 B	0 B	0
PC-obj...	UP-G1	PC obj...		1M	0 bps	0 B	0 B	0

MODULO 14

Manejo de la herramienta Torch

3. Monitoreo con la herramienta Torch.

3.1. ¿Qué es Torch?

Es una herramienta para monitorear nuestras redes y observar cómo se va cursando el tráfico que procesa nuestro MT, podemos ver orígenes y destinos que van pasando por nuestro MT y ver que ancho de banda se va llevando cada uno.

3.2. Ejemplos de monitoreo con Torch.

- Para ver un ejemplo que como podemos monitorear nuestras redes vamos a realizar la descarga de un paquete de internet con el fin de monitorear el tráfico de datos, para este ejemplo usaremos <http://sps.prima.com.ar>
- En Tools -> Torch, aquí vamos a realizar el monitoreo
- Vamos a seleccionar la interface donde queremos realizar el monitoreo, damos clic en Start

Et...	Prot...	Src.	Dst.	VLAN Id	DSCP	Tx Rate	Rx Rate	Tx Pack...
-------	---------	------	------	---------	------	---------	---------	------------

0 items Total Tx: 0 bps Total Rx: 0 bps Total Tx Packet: 0 Total Rx Packet: 0

- Inmediatamente nos da un informe del monitoreo

Torch (Running)

Basic

Interface: ether3

Entry Timeout: 00:00:03 s

Collect

☒ Src. Address ☒ Src. Address6

☒ Dst. Address ☒ Dst. Address6

☐ MAC Protocol ☐ Port

☐ Protocol ☐ VLAN Id

☐ DSCP

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: any

VLAN Id: any

DSCP: any

Et...	Prot...	Src.	Dst.	VLAN Id	DSCP	Tx Rate	Rx Rate	Tx Pack...
800 (ip)		192.168.30.254	200.49.147.100			9.4 Mbps	258.6 kbps	784
800 (ip)		255.255.255.255	0.0.0.0			32.8 kbps	0 bps	6
800 (ip)		192.168.30.254	192.168.30.255			0 bps	3.8 kbps	0
800 (ip)		192.168.30.254	52.109.108.25			0 bps	0 bps	0
800 (ip)		192.168.30.254	52.108.36.29			696 bps	480 bps	1
800 (ip)		192.168.30.254	157.240.197.17			1088 bps	1168 bps	2
800 (ip)		192.168.30.254	52.209.61.82			0 bps	0 bps	0
800 (ip)		192.168.30.254	212.102.60.232			0 bps	0 bps	0
800 (ip)		192.168.30.254	13.227.200.81			0 bps	0 bps	0

9 items Total Tx: 9.4 Mbps Total Rx: 264.1 kbps Total Tx Packet: 793 Total Rx Packet: 526

- Si queremos un informe detallado sobre un solo equipo seleccionamos la IP del equipo y volvemos a dar en Start, para no escuchar la transmisión de datos de otros equipos si hubiese más equipos conectados.

Filters

Src. Address: 192.168.30.254

Dst. Address: 0.0.0.0/0

Start

Stop

Close

Et...	Prot...	Src.	Dst.	VLAN Id	DSCP	Tx Rate	Rx Rate	Tx Pack...
800 (ip)		192.168.30.254:64496	200.49.147.100:80 (http)			9.1 Mbps	183.0 kbps	762
800 (ip)		192.168.30.254:50402	192.168.30.255:20561			0 bps	4.5 kbps	0
800 (ip)		192.168.30.254:61739	239.255.255.250:1900			0 bps	1432 bps	0
800 (ip)		192.168.30.254:64143	13.227.205.132:443 (https)			0 bps	0 bps	0
800 (ip)		192.168.30.254:58954	157.240.197.17:443 (https)			0 bps	0 bps	0
800 (ip)		192.168.30.254:64338	157.240.197.10:443 (https)			0 bps	0 bps	0
800 (ip)		192.168.30.254:58949	157.240.197.10:443 (https)			0 bps	0 bps	0
800 (ip)		192.168.30.254:64412	52.108.36.29:443 (https)			0 bps	0 bps	0
800 (ip)		192.168.30.254:64102	52.209.61.82:443 (https)			0 bps	0 bps	0
800 (ip)		192.168.30.254:64398	13.107.42.12:443 (https)			32.4 kbps	1292.1 kbps	75

- A continuación, se puede aplicar alguna penalización QoS con dirección al dispositivo objetivo.

MODULO 15

Control parental

4. Configuraciones de control parental (Bloqueo de páginas web).

4.1. Creación de reglas para el bloqueo de páginas web.

En IP -> Firewall, ingresamos a la pestaña **Layer7 Protocols** y creamos una nueva regla, para bloquear Facebook, por ejemplo, respetando los caracteres especiales.

4.2. Creación del marcado de conexión.

En IP -> Firewall, ingresamos a **Mangle** y creamos una nueva regla.

GENERAL

Indicamos que tipo de cambio se hará además indicamos que no habrá ninguna marca de conexión.

ADVANCED

Establecemos el nombre marca de conexión e indicamos e indicamos que pagina queremos bloquear.

ACTION

En acción seleccionamos marca de conexión y ponemos un nombre para reconocer la marca de conexión

Mangle Rule <>

General Advanced Extra Action Statistics

Action: mark connection

☐ Log

Log Prefix:

New Connection Mark: facebook_conn

☒ Passthrough

OK Cancel Apply Disable Comment Copy

4.3. Creación del marcado de paquetes.

En IP -> **Firewall**, ingresamos a **Mangle** y creamos una nueva regla.

GENERAL

En connection mark ponemos la regla que creamos hace un momento.

Mangle Rule <>

General Advanced Extra Action Statistics

Chain: prerouting

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

In. Interface:

Out. Interface:

In. Interface List:

Out. Interface List:

Packet Mark:

Connection Mark: ☐ facebook_conn

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

ADVANCED

Sin cambios

ACTION

En acción establecemos la marca de paquetes e indicamos el nombre del paquete objetivo.

Mangle Rule <>

General Advanced Extra Action Statistics

Action: mark packet

☐ Log

Log Prefix:

New Packet Mark: facebook_pack

☐ Passthrough

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

4.4. Creación del filtro de reglas.

En IP -> Firewall, ingresamos a Filter Rules y creamos una nueva regla

GENERAL

Establecemos en tipo de cambio en forward

Agregamos la regla creada en MANGLE dentro de packer mark, el resto en blanco

ACTION

Denegamos toda conexión para esta regla.

4.5. Agregando dispositivos a las reglas.

En IP -> Firewall ingresamos a Addresses List

Aquí Seleccionamos un nombre que ya creamos anteriormente.

Agregamos una IP o un conjunto de IP's a donde queremos aplicar las restricciones

MODULO 16

Bloqueo de juegos móviles (caso FreeFire)

4. Configuración para bloqueo de juegos móviles.

4.1. Tener el conocimiento de la IP del móvil objetivo.

Para este ejemplo vamos a usar un teléfono móvil con una conexión WiFi directamente al MikroTik.

En el MikroTik ya debemos tener una subred en la interface inalámbrica para que el teléfono móvil pueda conectarse

Podemos identificar al teléfono móvil en el menu DHCP-server en el servidor instalado en la interface inalámbrica.

DHCP Server						
DHCP	Networks	Leases	Options	Option Sets	Vendor Classes	Alerts
<div><div><div><div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div></div></div><div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div></div></div><div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div> <div><div></div><div></div><div></div><div></div></div>						

4.2. Análisis de puertos de conexión.

Para hacer en análisis debemos tener en el teléfono móvil ejecutando el juego FreeFire

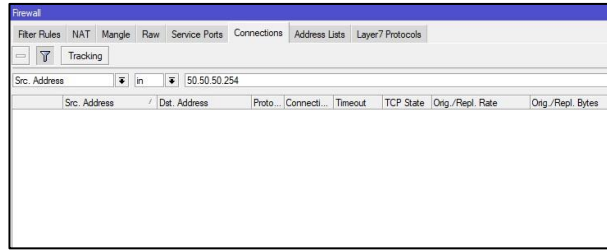


Seguidamente en IP -> Firewall -> Connections observamos todas las conexiones que todos los dispositivos en todas las subredes están realizando.

Podemos filtrar la información de un solo dispositivo, activando el filtrado solo para el dispositivo objetivo.

<input type="button" value="Filter"/>	<input type="button" value="Tracking"/>
Src. Address	in 50.50.50.254

Debemos limpiar todas las conexiones que este realizando nuestro teléfono móvil



A continuación, se generarán nuevas conexiones, y si el juego está ejecutándose podremos ver sus conexiones con puertos diferentes a 443 y 80, como podemos observar.

Firewall								
Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols								
Tracking								
Src. Address in 50.50.50.254								
	Src. Address	/	Dst. Address	Proto...	Connecti...	Timeout	TCP State	Orig./Repl. Rate
C	50.50.50.254:68		50.50.50.1:67	17 (u...		00:00:06		0 bps/0 bps
SACs	50.50.50.254:33710		129.227.127.54:443	6 (tcp)		23:59:57	established	0 bps/0 bps
SACs	50.50.50.254:37789		129.227.127.37:39698	6 (tcp)		23:59:52	established	0 bps/0 bps
SACs	50.50.50.254:42759		107.155.5.220:8130	17 (u...		00:02:52		0 bps/0 bps
SCs	50.50.50.254:44379		192.168.0.1:53	17 (u...		00:00:03		0 bps/0 bps
SCs	50.50.50.254:45117		192.168.0.1:53	17 (u...		00:00:03		0 bps/0 bps
SACs	50.50.50.254:45719		129.227.127.141:39800	6 (tcp)		23:59:59	established	848 bps/424 bps
SACs	50.50.50.254:47808		152.199.54.7:443	6 (tcp)		23:59:59	established	1088 bps/23.7 kbps
SACs	50.50.50.254:53832		64.233.186.95:443	6 (tcp)		23:59:53	established	0 bps/0 bps
SACs	50.50.50.254:53834		64.233.186.95:443	6 (tcp)		23:59:54	established	0 bps/0 bps

4.3. Crear reglas firewall para bloquear esos puertos en el dispositivo objetivo

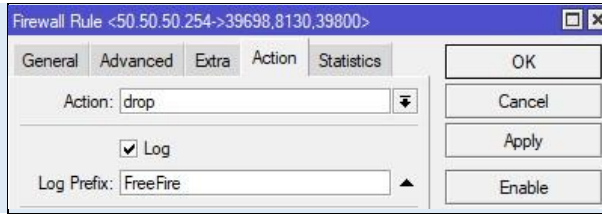
En IP -> Firewall, en la pestaña FilterRules creamos una nueva regla.

GENERAL

Chain : forward
Src. Address : 50.50.50.254
Protocol : 6(tcp)
Dst. port : aquí ponemos los puertos que queremos bloquear.

ACTION

Action : drop
log : habilitado
log Prefix : FreeFire => para controlar el registro de log's



✖ drop	forward	50.50.50.254	6 (tcp)	39698,81...
--------	---------	--------------	---------	-------------

4.4. Verificar los que se están denegando

En Log podemos ver el tráfico que está pasando la dirección IP objetivo bajo el prefijo

firewall, info	FreeFire forward: in:Wlan1 out:ether1, src-mac 34:7e:00:cb:15:44, prot...
firewall, info	FreeFire forward: in:Wlan1 out:ether1, src-mac 34:7e:00:cb:15:44, prot...
firewall, info	FreeFire forward: in:Wlan1 out:ether1, src-mac 34:7e:00:cb:15:44, prot...

4.5. Verificar bloqueo en el teléfono móvil.

Como podemos observar en el teléfono móvil aún tenemos acceso al juego, pero la transferencia de datos desde las conexiones que demanda el juego ya se está bloqueando.

