FIREWALL MANGLE

DANIEL ESTIVEN GUANCHA

KENIN ANDRES GUERRERO

EDWARD ALBEIRO MALTE



FACULTAD DE INGENIERÍA

INGENIERÍA DE SISTEMAS

NARIÑO-COLOMBIA

2021

FIREWALL MANGLE

DANIEL ESTIVEN GUANCHA

KENIN ANDRES GUERRERO

EDWARD ALBEIRO MALTE

INVESTIGACIÓN SOBRE EL FIREWALL MANGLE

DOCENTE

EDGAR DULCE

TELMATICA III

UNIVERSIDAD DE NARIÑO

FACULTAD DE INGENIERÍA

INGENIERÍA DE SISTEMAS

NARIÑO-COLOMBIA

2021

|  |
| --- |
| Nota de Aceptación |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
| Docente |
|  |
|  |

|  |
| --- |
| Nariño - Colombia, 15 de septiembre del año 2021 |
|  |
|  |

CONTENIDO

.

Pág.

[1. INTRODUCCIÓN 6](#_Toc83496082)

[2. ANTECEDENTES 7](#_Toc83496083)

3. JUSTIFICACION………………………………………………………………………………8

[4. OBJETIVOS 9](#_Toc83496084)

[4.1 OBJETIVO GENERAL 9](#_Toc83496085)

[4.2 OBJETIVOS ESPECÍFICOS 9](#_Toc83496086)

[5. MARCO TEÓRICO 10](#_Toc83496087)

[6 BIBLIOGRAFÍA 15](#_Toc83496088)

RESUMEN

El presente documento mostrará los informes y detalles de los procedimientos sobre la investigación del Firewall Mangle, estudiaremos las funcionalidades que tiene un Firewall y el uso especifico del Firewall Mangle que es una herramienta muy importante que nos permitirá entender y ver como se realiza el marcado de los paquetes en el enrutador, con el que principalmente podremos darles prioridad a unos paquetes para poder controlar el tráfico o el ancho de banda en

una red.

# INTRODUCCIÓN

La expansión de las redes a través del mundo como lo es Internet ha permitido la posibilidad de acceder a diferentes tipos de comunicación y transferencias de información que ha permitido el desarrollo de los diferentes sectores hasta la sociedad actual. Como la expansión de las redes va en aumento es de vital importancia que estos medios permitan tener seguridad y un control al momento de transferir la información a través de la red, lo que hace un firewall común principalmente es tener el control de la transferencia de información y proteger los equipos individuales, servidores o equipos conectados en red contra accesos no deseados de intrusos que pueden robar datos confidenciales, hacer perder información valiosa o incluso denegar servicios en nuestra red.

# ANTECEDENTES

Desde la creación de Internet en 1983, la sociedad ha ido evolucionando a una gran velocidad. Los diferentes sectores económicos, educativos, entre otros se han tenido que ir adaptando a todos estos cambios para no quedarse atrás, las diferentes organizaciones involucradas que desarrollan o que utilizan estos servicios necesitaban poder controlar el tráfico de la información y los medios de comunicación, entre varias de estas, una empresa que nos enfocaremos es MikroTik que es un fabricante de hardware y software de routers que son usados mundialmente en millones de redes de todas las escalas. Esta empresa se fundó en 1995 en Latvia al norte de Europa y ya cuenta con varios miles de técnicos en todo el mundo brindando el apoyo para desarrollo de conmutadores de red, puntos de acceso, así como sistemas operativos y software auxiliar para enrutamientos.

Una característica importante Mikrotik es su sistema operativo o RouterOS que es un sistema operativo stand-alone basado en el kernel de Linux2.6, de gran potencia y capaz de ejecutar cualquier configuración de red, las configuraciones más populares son de Firewall, Routing, Forwarding, MPLS, VPN, Wireless, HotSpot y Web Proxy, entre otras.

Los dispositivos Mikrotik se pueden configurar en capa 2 o capa 3 por medio de la herramienta propietaria WINBOX, específicamente el poder configurar el Firewall con estas herramientas permiten realizar el proceso y entender el funcionamiento del control de la transferencia de paquetes.

# JUSTIFICACIÓN

Con la creciente incorporación de Internet y las redes a la forma de vida actual en todas sus facetas, se han generado diversas clases de aplicaciones, y con ellas existen en la actualidad múltiples tipos de tráfico que demandan diferente ancho de banda para circular a través de la red.

Puesto que siempre se exige el máximo la capacidad de las redes, especialmente la conexión a Internet, es que termina siendo importante controlar el tráfico de los paquetes para administrarlo adecuadamente según nuestras necesidades. Para estos fines, diversas herramientas que hasta hace poco estaban reservadas a entornos corporativos, ahora se hacen accesibles como Firewall Mangle de MikroTik que nos permitirá estudiar sus funcionalidades probando con nuestros routers domésticos y entornos virtuales para así comprender como funciona el marcado de los paquetes para su procesamiento futuro con marcas especiales basadas en reglas, por lo que resulta interesante comprender en general cómo funcionan para poder obtener el máximo provecho de ellas.

Diariamente por la red circulan diferentes tipos de datos, muchos de ellos son privados, como transacciones bancarias, mensajería instantánea, documentos, etc. y aun mas hoy en día que se a optado por la virtualización, es por ende que la seguridad de la información se ha convertido en un factor indispensable, ya que ciber atacantes pueden acceder de forma inescrupulosa y hacer mal uso de nuestros datos, por tanto, es de imprescindible para ISP (proveedores de internet) , administradores de una red, o incluso para una persona que desee proteger su datos dentro de su propia red, blindarla para proteger los datos de los usuarios y así tener un comportamiento adecuado del tráfico que transita por ella.

# 4. OBJETIVOS

## 4.1 OBJETIVO GENERAL

* Investigar las utilidades del Firewall Mangle de MikroTik y entender su funcionamiento en la práctica.

## 4.2 OBJETIVOS ESPECÍFICOS

* Estudiar las funciones de un Firewall.
* Entender la importancia de poder controlar la transferencia de información a través de una red.
* Comprender como funciona el marcado de paquetes.
* Realizar la práctica para comprobar y entender su funcionamiento.

# 5. MARCO TEÓRICO

**5.1. Historia**

Mikrotik es una [empresa](https://www.ecured.cu/Empresa) letona que fue fundada en 1996 para desarrollar routers y sistemas inalámbricos ISP. Mikrotik ahora proporciona [hardware](https://www.ecured.cu/Hardware) y [software](https://www.ecured.cu/Software) para la conexión a Internet en la mayoría de los países de todo el mundo. Su experiencia en el uso de la industria de [hardware](https://www.ecured.cu/Hardware) de PC estándar y sistemas de enrutamiento completas permitió en 1997 para crear el sistema de [software](https://www.ecured.cu/Software) RouterOS que proporciona una amplia estabilidad, controles, y la flexibilidad para todo tipo de interfaces de datos y enrutamiento. En 2002, se decidió hacer su propio [hardware](https://www.ecured.cu/Hardware), y surge la marca RouterBOARD. Existen distribuidores y clientes en la mayoría de las partes del mundo. La empresa se encuentra en Riga, la capital de Letonia y tiene más de 140 empleados.

**5.2. RouterOS**

Mikrotik RouterOS es un [software](https://www.ecured.cu/Software) que funciona como un Sistema Operativo para convertir un PC o una placa Mikrotik RouterBOARD en un router dedicado. MikroTik se dedica principalmente a la venta de productos de [hardware](https://www.ecured.cu/Hardware) de red como routers denominados routerboards y [switches](https://www.ecured.cu/Switch) también conocidos por el software que lo integra, denominado RouterOS y SwOS. Está basado en el [núcleo](https://www.ecured.cu/N%C3%BAcleo) [Linux](https://www.ecured.cu/Linux), el cual implementa funcionalidades que los NSP e [ISP](https://www.ecured.cu/index.php?title=ISP&action=edit&redlink=1) tienden a implementar, como por ejemplo BGP, IPv6, OSPF o MPLS.

RouterOS es un sistema versátil, con un gran soporte por parte de MikroTik, proporcionando una amplia variedad de ejemplos de configuración. La venta de RouterOS, combinado con su línea de [productos](https://www.ecured.cu/Productos) de [hardware](https://www.ecured.cu/Hardware) conocida como MikroTik RouterBOAR.

**5.3. Wimbox**

Es una pequeña utilidad que permite la administración de MikroTik RouterOS utilizando una GUI rápida y sencilla. Es un binario nativo de Win32, pero se puede ejecutar en Linux y MacOS (OSX) usando Wine. Todas las funciones de la interfaz de Winbox están lo más cerca posible de reflejar las funciones de la consola, es por eso que no hay secciones de Winbox en el manual. Algunas de las configuraciones críticas avanzadas y del sistema no son posibles desde winbox, como el cambio de dirección MAC en un registro de cambios de la interfaz de Winbox

**5.4. Firewall Mangle**

Mangle es una especie de “Marcador” que etiqueta/marca paquetes para un futuro procesamiento con marcas especiales. Muchas facilidades/opciones en RouterOS hacen uso de estas marcas como por ejemplo Queue Trees, NAT Routing. Las marcas de mangle únicamente existen dentro del mismo Router y estas marcas no son transmitidas a través de la red.

Adicionalmente, Mangle se utiliza para modificar algunos campos en la cabecera IP como los campos TOS (DSCP) y TTL

**5.4.1. Estructura del Mangle**

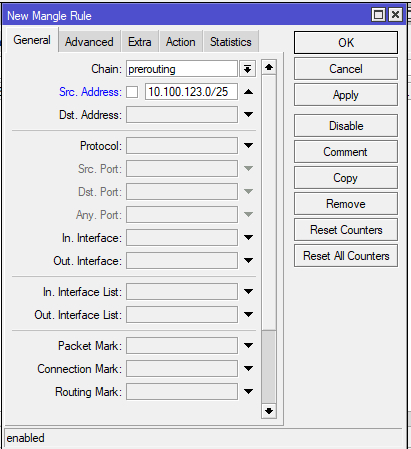
Las reglas del mangle están organizadas en cadenas, y existen 5 cadenas predeterminadas.

* **Prerouting:** hace una marca antes del Queue Global-in
* **Postrouting:** hace una marca antes del Queue Global-out
* **Input:** hace una marca antes del filtro Input
* **Output:** hace una marca antes del filtro Output
* **Fordward:** hace una marca antes del filtro Fordward

**5.4.2 Marcado de Conexiones**

Se usa mark-connection para identifica uno o un grupo de conexiones

* Las marcas de conexiones son almacenadas en la tabla de connection tracking.
* Solo puede haber una marca de conexión para una conexión.
* Connection Tracking ayuda a asociar cada paquete a una conexión especifica (Connection Mark).

*figura 1: regla de marcado de conexión*

*fuente: los autores*

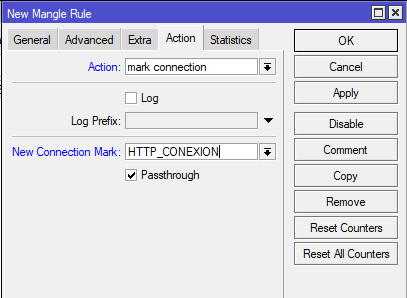


figura 2: regla de marcado de conexión

Fuente: los autores

**5.4.3 Marcado de Paquetes**

Los paquetes pueden ser marcados de la siguiente manera:

* **Indirectamente:**  usando el recuro Connection Tracking, basado en Connection marks creados previamente (más rápido)
* **Directamente:** sin el Connection Tracking, No se necesitan Connection marks, el Router comparará cada paquete en una base a una conexión dada. Este proceso imita algo de las características del Connection Tracking. El Router utiliza más capacidad de procesamiento del CPU.

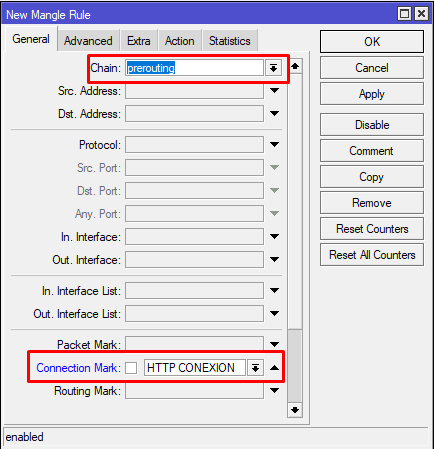
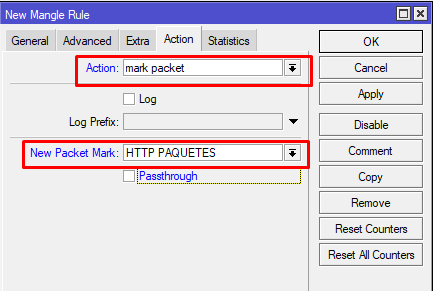


Figura 3: regla de marcado de paquetes

Fuente: los autores

figura 4: regla de marcado de paquetes

fuente los autores

# 6 BIBLIOGRAFÍA

EcuRed

Empresa MikroTik, Que Hace MikroTik Articulo, 18 junio 2016

https://www.ecured.cu/Mikrotik

MikroTik Página Oficial

Introducción a Mangle, Ultima actualización 12 marzo del 2020

<https://help.mikrotik.com/docs/display/ROS/Mangle>

RouterOS

Control de tráfico, Firewall y QoS con MikroTik RouterOS

Autor – Mauro Escalante