



**UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES**

TITULO DE TRABAJO DE TITULACIÓN:

Implementación de firewall en equipo MikroTik para el fortalecimiento de la seguridad en redes con acceso a Internet.

AUTOR:

Sánchez Cumanicho Gabriel Josué

MODALIDAD DE TITULACIÓN

Trabajo Examen Complexivo

Previo a la obtención del grado académico en

INGENIERO EN TELECOMUNICACIONES

TUTOR:

Ing. Manuel Asdrual Montaña B, M.sc.

LA LIBERTAD – ECUADOR

Año 2024



**UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES**

TRIBUNAL DE SUSTENTACIÓN

Ing. Ronald Róvira Jurado. Ph.D.

DIRECTOR DE LA CARRERA

Ing. Luis Amaya Fariño, Mgtr.

DOCENTE ESPECIALISTA - GUIA UIC II

Ing. Manuel Asdrual Montaña B, MSc

DOCENTE TUTOR

Ing. Corina Gonzabay De La A, Mgtr.

SECRETARIA




**UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES**

DECLARACIÓN DE DOCENTE TUTOR

En mi calidad de docente tutor del componente práctico de examen complejo:
“Implementación de Firewall en equipo MikroTik para el fortalecimiento de la seguridad en redes con acceso a Internet”, elaborado por **Gabriel Josué Sánchez Cumanicho**, estudiante de la Carrera de Telecomunicaciones, Facultad de Sistemas y Telecomunicaciones de la Universidad Estatal Península de Santa Elena, previo a la obtención del título de Ingeniería en Telecomunicaciones, me permito declarar que, tras supervisar el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos. En consecuencia, lo considero apto en todos sus aspectos y listo para ser evaluado por el docente especialista.

Atentamente



Ing. Manuel Asdrual M, MSC

DOCENTE TUTOR



**UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES**

DECLARACIÓN AUTORÍA DE LAS ESTUDIANTES

El presente trabajo práctico de examen complejo con el título **“Implementación de Firewall en equipo MikroTik para el fortalecimiento de la seguridad en redes con acceso a Internet”**, declaro que la concepción análisis y resultados son originales a la actividad educativa en el área de Telecomunicaciones.

Atentamente

Gabriel Josué Sánchez Cumanicho

C.I.: 0706966868



**UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES**

DECLARACIÓN DE DOCENTE ESPECIALISTA

En mi calidad de docente especialista del trabajo práctico de examen complejo, **“Implementación de Firewall en equipo MikroTik para el fortalecimiento de la seguridad en redes con acceso a Internet”**, elaborado por **Gabriel Josué Sánchez Cumanicho**, estudiante de la carrera de Telecomunicaciones, Facultad de Sistemas y Telecomunicaciones de la Universidad Estatal Península de Santa Elena, previo a la obtención del título de Ingeniería en Telecomunicaciones, me permito declarar que, tras supervisar el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos. En consecuencia, lo considero apto en todos sus aspectos y listo para la sustentación del trabajo.

Atentamente

Ing. Luis Amaya Farfán, Mgtr.

DOCENTE ESPECIALISTA



**UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES**

DECLARACIÓN DE RESPONSABILIDAD

Quien se suscribe, **Gabriel Josué Sánchez Cumanicho** con C.I. 0706966868, estudiante de la carrera de Telecomunicaciones, declaro que el trabajo de examen complejo denominado **“Implementación de Firewall en equipo MikroTik para el fortalecimiento de la seguridad en redes con acceso a Internet”** pertenece y es exclusivo responsabilidad del autor y pertenece al patrimonio intelectual de la Universidad Estatal Península de Santa Elena.

Atentamente

Gabriel Josué Sánchez Cumanicho

C.I.: 0706966868

DEDICATORIA

Este proyecto va dedicado Dios, ya que gracias a él con esfuerzo y dedicación pude terminar esta carrera.

A mis padres José y Lupe, tíos Ena, Lisseth Agustín, William y especialmente a mis abuelos Papa Agustín y Mama Victoria quienes desde pequeño me han formado con valores, responsabilidades y respeto gracias a cada uno de ustedes por formar parte de mi vida, gracias a ellos pude alcanzar este logro.

Gracias a mi tía Ena quien ha sido una segunda mamá quien me ayudado no solo económicamente, si no con conocimiento para forjar la persona que soy hoy en día.

Gracias a todo ustedes por impulsarme a seguir estudiando, a ser una persona mejor y por estar conmigo en momentos buenos y malos.

Dedicado a

Ena Cumanicho G.

José Sánchez A. (+)

Ángel Sánchez A. (+)

William Cumanicho G (+)

Gabriel Josué Sánchez C

AGRADECIMIENTOS

Agradezco a Dios por que día a día me protegió y me brindo de su sabiduría para poder terminar esta carrera.

A mi Familia por brindarme todo el apoyo y sustento económico para poder realizar este proyecto, sin ustedes no sería posible este proyecto.

A los docentes por brindar sus conocimientos a lo largo de preparación como profesional, agradecido con el Ing. Manuel Asdrual Montaña Blacio tutor de mi trabajo complejo, por su tiempo, guía, dedicación a este proyecto y por ser una persona muy comprensible, agradecer también al Ing. Fernando Chamba por sus conocimientos y orientación en la carrera, agradecer a mis amigos Anthony, Isaac, Edwin quienes me han apoyado a lo largo de esta carrera profesional.

Agradezco a Erika por estar presente en este trayecto como profesional, dándome apoyo emocional y conocimientos para seguir adelante, a pesar de los momentos difíciles, me ha brindado su apoyo incondicionalmente.

Gracias a todos ustedes por formar parte de mi vida y mi trayecto como profesional.

Gabriel Josué Sánchez C

ÍNDICE GENERAL

DEDICATORIA	VII
AGRADECIMIENTOS	VIII
RESUMEN	1
ABSTRACT	1
1. Capítulo 1	2
1.1 Introducción.....	2
1.2 Objetivo General.....	3
1.3 Objetivos Específicos	3
1.4 Justificación.....	4
1.5 Metodología.....	5
2. Capítulo 2	6
2.1 Fundamentos de seguridad en redes	6
2.1.1 Conceptos básicos de seguridad en redes.....	6
2.1.2 Amenazas comunes en redes con acceso a internet.....	6
2.1.3 Importancia de la seguridad en la infraestructura de red	7
2.2 Firewalls.....	8
2.2.1 Definición y función de un firewall.....	8
2.2.2 Tipos de firewalls.....	9
2.2.3 Arquitecturas de firewall.....	11
2.2.4 Reglas de firewall.....	12
2.3 Equipos mikrotik.....	16
2.3.1 Introducción a mikrotik.....	16
2.3.2 Router os: sistema operativo de mikrotik.....	16
2.3.3 Características de seguridad en equipos mikrotik.....	17
2.3.4 Ventajas y limitaciones de los equipos mikrotik en seguridad de red.....	18
2.4 DoS/DDoS.....	19
2.4.1 Definición y tipos de ataques dos/ddos.....	19
2.4.2 Mecanismos de funcionamiento de los ataques ddos	20
2.4.3 Impacto de los ataques dos/ddos en la infraestructura de redes.....	21
2.4.4 Medidas de mitigación y protección contra dos/ddos.....	21
2.5 Ip Spoofing.....	22
2.5.1 Definición y conceptos básicos de ip spoofing.....	22

2.5.2	Funcionamiento del ip spoofing.....	22
2.5.3	Tipos de ataques basados en ip spoofing	23
2.5.4	Medidas de prevención contra el ip spoofing.....	24
2.5.5	Uso de filtrado de paquetes y firewalls contra ip spoofing.....	25
2.6	Kali Linux	25
2.7	Wireshark.....	26
3.	Capítulo 3.....	26
3.1	Implementación de reglas de filtrado en el firewall.....	26
3.1.1	Configuración desde winbox para las reglas de filtrado en el firewall.....	27
3.1.2	Configuración de la opción forward (tráfico que pasa a través del equipo).....	32
3.2	Protección contra amenazas dos/ddos	38
3.2.1	Configuración contra los ataques ddos	39
3.3	Prevención de ataques de ip spoofing.....	44
4.	Capítulo 4.....	53
4.1	Resultados	53
4.2	Resultados de las reglas del firewall (address list).....	53
4.3	Resultados de las demás reglas de firewall	57
4.4	Resultados de ataques de ddos.....	59
4.5	Resultados de los ataques de ip spoofing.....	60
4.6	Conclusiones	63
4.7	Recomendaciones	64
	Hoja de Guías Prácticas	65
	Bibliografía	101

ÍNDICE DE FIGURAS

Figura 1. Infraestructura de Red.....	8
Figura 2. Funcionamiento de un firewall	9
Figura 3. Función de una DMZ	12
Figura 4. Funcionamiento de las Reglas.....	14
Figura 5. Funcionamiento de Accept	15
Figura 6. Sistema MikroTik.....	17
Figura 7. Firewall en Equipos MikroTik	18
Figura 8. Ingreso al equipo mediante winbox	27
Figura 9. Configuración de las reglas del firewall	27
Figura 10. Primera regla del firewall.....	28
Figura 11. Aceptación de la función input	29
Figura 12. Regla input invalida.....	29
Figura 13. Regla input drop.....	30
Figura 14. Configuración para modo administración	30
Figura 15. Regla para el acceso al equipo	31
Figura 16. Aceptación de la regla.....	31
Figura 17. Cerrando la cadena de input.....	32
Figura 18. Opción denegación	32
Figura 19. Reglas del firewall opción forward	33
Figura 20. Aceptación de establecidas y relacionadas	33
Figura 21. Opción invalid dentro del forward.....	34
Figura 22. Denegación de la opción invalid.....	34
Figura 23. Creación de address list para navegar	35
Figura 24. Address list para navegar	36
Figura 25. Aceptación de ip's para navegar.....	36
Figura 26. Nueva regla para todo lo demás en ip's para navegar.....	37
Figura 27. Aceptación de la opción drop.....	37
Figura 28. Nueva regla para el acceso al winbox.....	38
Figura 29. Creación del address list.....	38
Figura 30. Ingreso al firewall para nueva regla	39
Figura 31. Creación de la nueva regla.....	40

Figura 32. Opción extra-psd	40
Figura 33. Función drop en el escaneo de puertos	40
Figura 34. Nueva regla de denegación	41
Figura 35. Establecer la connection limit	41
Figura 36. Agregar el address list	42
Figura 37. Nueva regla suspensión de ataques ddos	43
Figura 38. Establecer una conexión limite	43
Figura 39. Colocar la opción tarpit y comentario	43
Figura 40. Topología de red para el ataque	45
Figura 41. Ingresar los datos de red dentro de kali linux	45
Figura 42. Ataque a servidor mediante hping3	46
Figura 43. Ingreso de ip suplantas al equipo	46
Figura 44. Visualización del tráfico en el servidor mediante wireshark	47
Figura 45. Intento de conexión a la página web	47
Figura 46. Ataque al servidor con una ip suplantada	48
Figura 47. Monitoreo de la red	48
Figura 48. Monitoreo de la red ingreso de ip's suplantadas	48
Figura 49. Nueva regla para evitar ataques syn flood	49
Figura 50. Agregamos la lista en la ventana advanced	49
Figura 51. Denegamos la regla	50
Figura 52. Segunda regla filtrado de paquetes	51
Figura 53. Establecer el límite de la conexión	51
Figura 54. Selección de Acción de la regla	51
Figura 55. Configuración del filtro ip	52
Figura 56. Configuración de ip para administrar el equipo	53
Figura 57. Ingreso a las redes e internet	54
Figura 58. Selección del recurso del centro de redes	54
Figura 59. Agregamos la dirección ip manualmente	55
Figura 60. Ingreso al equipo mediante winbox	55
Figura 61. Ingreso de paquetes señal de acceso correcto	55
Figura 62. Resultados de la ventana statics	56
Figura 63. Desactivamos la opción del addressList	56
Figura 64. Ingreso al equipo fallido	56

Figura 65. DHCP automático.....	57
Figura 66. Insertamos las dns	57
Figura 67. Estadística de la regla ip's permitidas para navegar.....	57
Figura 68. ingreso de paquetes, acceso para navegar.....	58
Figura 69. Envio y Recibo de paquetes de Navegación.....	58
Figura 70. Desactivamos las ip's de Navegación.....	58
Figura 71. No se observan el ingreso paquetes, no existe conexión.....	58
Figura 72. Ventana de estadísticas de la ip para navegar.....	59
Figura 73. Estadísticas de los packets y bytes antes de empezar el DDoS attack.....	60
Figura 74. Ataque evadido correctamente	60
Figura 75. Activación de la lista de Ip's del ataque	60
Figura 76. Ingreso del ataque al desactivar las reglas	60
Figura 77. Comando para los ataques syn	61
Figura 78. Paquetes que ingresan al servidor dentro del equipo	61
Figura 79. Activación de la regla synflooder	61
Figura 80. Acceso al servicio web.....	62
Figura 81. Envio de IP'S Suplantadas hacia el servidor.....	62
Figura 82. Estadísticas de la Interfaz por donde pasa el ataque ya mitigado	62
Figura 83. Se filtran los paquetes, no se encuentran ingresando	62
Figura 84. Topología de Red Acceso a Internet.....	66
Figura 85. Ingreso mediante el winbox	67
Figura 86. Resetear la configuración.....	67
Figura 87. Nuevo usuario y contraseña.....	68
Figura 88. Agregamos la Interfaz lan y wan	69
Figura 89. Nuevo cliente DHCP.....	69
Figura 90. Agregamos las direcciones IP	70
Figura 91. Configuración de DHCP Server.....	70
Figura 92. Agregamos la dirección ip para la salida del internet	71
Figura 93. Detalles de la conexión de red.....	72
Figura 94. Acceso a internet y ping exitoso	72
Figura 95. Topología de red túnel eoip.....	73
Figura 96. Agregar las direcciones IP a R1.....	73
Figura 97. Agregamos una configuración nueva eoip tunnel.....	74

Figura 98. Agregamos la nueva interface con sus direcciones ip	74
Figura 99. Comunicación entre R2 Y R1	75
Figura 100. Agregamos de nuevo el eoip tunnel	75
Figura 101. Se agregan las siguientes IP	75
Figura 102. Creamos un bridge nuevo	76
Figura 103. Nuevo puerto del bridge.....	76
Figura 104. Se añade nuevo puerto con la interfaz ether2.....	77
Figura 105. añadimos la siguiente ip en address list.....	77
Figura 106. Configuración de dhcp server	78
Figura 107. Colocamos las direcciones DNS.....	78
Figura 108. Configuración de dhcp client	78
Figura 109. Se agrega una nueva bridgel	79
Figura 110. Agregamos un nuevo ports con la bridgel	79
Figura 111. Agregar otra configuración en ports.....	79
Figura 112. Ping desde la computadora red A	80
Figura 113. Ping desde otra computadora conectada	80
Figura 114. Topología de red	81
Figura 115. Ingreso al Equipo mediante winbox.....	81
Figura 116. Configuración de nueva nat	82
Figura 117. Configuración de la pestaña action	82
Figura 118, Visualizamos los paquetes que ingresan.....	83
Figura 119. Ingreso de la dirección Ip en el address list.....	83
Figura 120. Se configuran las dns	84
Figura 121. Realizamos otro dhcp server con otra interfaz ether 3.....	84
Figura 122. Configuración de nat	85
Figura 123. Configuración de la ventana action.....	85
Figura 124. Añadimos la dirección Ip Publica al Gateway.....	85
Figura 125. Ingre hacia el secundario equipo est01	86
Figura 126. Conexión establecida	86
Figura 127. Conexión Exitosa	87
Figura 128. Topología de red bgp.....	88
Figura 129. Configuración de ip´s R1	89
Figura 130. Configuración de ip´s R2	89

Figura 131. Configuración de ip´s R3	90
Figura 132. Configuración Protocolo bgp.....	90
Figura 133. Configuración de protocolo bgp del router R2.....	91
Figura 134 Configuración del BGP.....	91
Figura 135. Configuración del protocolo bgp en router 3 R3	92
Figura 136. Añadir sistema autónomo a R1	92
Figura 137. Añadir sistema autónomo a R2	93
Figura 138. Añadir sistema autónomo a R2	93
Figura 139. Añadir sistema autónomo a R3	93
Figura 140. Configuración de la ventana networks en router1	94
Figura 141. Configuración de la ventana networks en router2	94
Figura 142. Configuración de networks en R3 Imagen elaborada por el autor	94
Figura 143. Configurar dhcp setup R1	95
Figura 144. Configurar dhcp setup R2	95
Figura 145. Configurar dhcp setup R3	96
Figura 146. Tabla de direcciones ip enlazadas R1.....	96
Figura 147. Tabla de direcciones ip enlazadas R2.....	97
Figura 148. Tabla de direcciones ip enlazadas R3.....	97
Figura 149. dhcp de lan-1 y lan-2.....	98
Figura 150. Conexión establecida entre lans	98
Figura 151. dhcp de lan-1 y lan-3.....	99
Figura 152. Conectividad exitosa	99
Figura 153. dhcp de lan-2 y lan-3.....	100
Figura 154 . Conexión establecida	100

RESUMEN

El proyecto se centra en la implementación de reglas de firewall en equipos MikroTik para reforzar la seguridad en redes con acceso a internet, específicamente mediante la protección contra ataques DoS/DDoS y de IP Spoofing, el objetivo principal es establecer configuraciones que permitieran controlar el tráfico de red y mitigar amenazas comunes, para ello, se utilizó un análisis metodológico que incluyó la configuración de reglas específicas en las cadenas input y forward, así como la utilización de herramientas de simulación de ataques para evaluar la efectividad de las medidas, los resultados mostraron que las configuraciones implementadas lograron bloquear con éxito accesos no autorizados, proteger contra ataques DDoS y prevenir ataques de suplantación de IP, las guías didácticas desarrolladas también contribuyeron al fortalecimiento del conocimiento en redes y equipos MikroTik, el proyecto demostró ser efectivo en mejorar la seguridad de las redes mediante configuraciones avanzadas y pruebas prácticas.

Palabras claves: Firewall, Seguridad en la red, Mikrotik

ABSTRACT

This project focuses on the implementation of firewall rules on MikroTik equipment to reinforce security in networks with Internet access, specifically by protecting against DoS/DDoS and IP Spoofing attacks. The main objective is to establish configurations that allow traffic control. network and mitigate common threats, for this, a methodological analysis was used that included the configuration of specific rules in the input and forward chains, as well as the use of attack simulation tools to evaluate the effectiveness of the measures, the results showed that the implemented configurations managed to successfully block unauthorized access, protect against DDoS attacks and prevent IP spoofing attacks, the teaching guides developed also contributed to strengthening knowledge on MikroTik networks and equipment, the project proved to be effective in improving security of networks through advanced configurations and practical tests.

Keywords: Firewall, Network security, Mikrotik

1. Capítulo 1

1.1 Introducción

El aumento de las nuevas redes informáticas o redes de computación y de nuevos servicios de Internet provocan la aparición de un gran número de amenazas cibernéticas que sitúan un riesgo a la integridad de los sistemas de información y los sistemas de información. Las redes que permiten el acceso a la Internet son generalmente víctimas de: intrusión no autorizada, ataques de denegación de servicio y denegación de servicio distribuido “DoS/DDoS” y suplantación de direcciones de origen o también conocida como (IP Spoofing), es importante tener medios de protección adecuados, como firewalls, que permite controlar y filtrar sistemas de tráfico de datos, además de proteger la red contra amenazas. El fabricante MikroTik sobresale en este rubro, puesto que permiten establecer sistemas de firewall robustos y adaptables, que protegen de manera óptima redes con acceso a Internet.

El presente proyecto tiene como objetivo principal implementar un sistema de firewall en dispositivos MikroTik para fortalecer de la seguridad de redes con acceso a Internet, este sistema estará enfocado en el control del tráfico de datos, también contará con la protección contra amenazas externas como son los ataques de denegación de servicio o más conocido como DoS, y la prevención de técnicas maliciosas como el IP spoofing, generadas por atacantes externos que comprometen la seguridad de la red, con esta implementación se busca garantizar un entorno de red confiable y robusta, capaz de responder a las crecientes exigencias de seguridad.

En los objetivos específicos planteados, se implementan las reglas de filtrado dentro del firewall en los equipos MikroTik, estas reglas nos permitirán controlar de una manera adecuada el tráfico de datos entrante y tráfico saliente, garantizando así que solo el acceso autorizado tenga un acceso en la red, esto se conseguirá mediante diversas configuraciones dentro del equipo que serán diferentes entre usuarios, servicios legítimos y aquellos que identifiquen como una amenaza, optimizando así la seguridad sin minimizar el rendimiento.

Adicionalmente se implementarán mecanismos específicos de protección, como la prevención ante ataques DoS/DDoS, estos ataques tienen la capacidad de paralizar una red a través de la saturación del tráfico en la red, su mitigación es fundamental para

garantizar la disponibilidad y estabilidad de los servicios en línea, mediante estas configuraciones avanzadas en el firewall dentro del equipo MikroTik, se buscará detectar y bloquear el paso de estos ataques de forma proactiva, manteniendo la red segura y operativa.

Finalmente, se desarrollará una guía didáctica que servirá como apoyo para realizar futuras actualizaciones del firewall, esta guía permitirá a los administradores de red supervisar la seguridad de manera eficiente, al posibilitar posibles vulnerabilidades en la red y manteniendo el sistema actualizado frente a nuevas y posibles amenazas, esto contribuirá a una gestión proactiva de la seguridad en redes con acceso a Internet.

1.2 Objetivo General

Implementar reglas de firewall en equipos MikroTik para el fortalecimiento de la seguridad en redes con acceso a Internet, mediante un control del tráfico de datos, una protección frente a amenazas externas en la red y por último optimización del rendimiento de la red.

1.3 Objetivos Específicos

- Implementar reglas de filtrado en el firewall de equipos MikroTik para controlar el tráfico entrante y saliente, permitiendo solo el acceso autorizado.
- Implementar mecanismos de protección en el firewall, como la prevención de ataques DoS/DDoS para salvaguardar la red.
- Implementar un mecanismo de prevención de ataques de IP spoofing en el firewall para fortalecer la seguridad de la red.
- Desarrollar una guía didáctica para el fortalecimiento en configuraciones de redes con acceso a Internet y firewall.

1.4 Justificación

La implementación de un firewall en los dispositivos MikroTik representa un paso fundamental para reforzar la protección de las redes con acceso a Internet, especialmente ante el crecimiento de las amenazas cibernéticas; estas son cada vez más sofisticadas y habituales con el paso del tiempo, el creciente uso de las tecnologías de la información y la comunicación ha provocado un aumento rápido en el tráfico de datos, lo que también ha elevado la superficie de ataque para posibles intrusos, es por ello que resulta crucial implementar estrategias avanzadas que protejan la integridad, y disponibilidad de la información.

En la actualidad, el acceso a Internet es primordial para el funcionamiento de empresas y los centros educativos, sin embargo, esta conectividad también cuenta con limitaciones de cobertura, riesgos asociados, como ataques de denegación de servicio DoS y suplantación de IP Spoofing y otros tipos de ciber ataques que ponen en peligro la integridad, confidencialidad de los datos en redes con acceso a Internet.

La implementación de reglas de firewall en equipos MikroTik ofrece una respuesta rápida y eficiente a los problemas de seguridad, ya que permiten gestionar el tráfico entrante y saliente de la red, al aplicar políticas de seguridad avanzadas que nos permitirán contrarrestar con las amenazas en la red, es por ello que este proyecto cuenta con soluciones para el fortalecimiento de la seguridad en redes de Internet mediante la configuración de firewall en dispositivos MikroTik, tomando en cuenta tanto la protección frente a los ataques externos como la optimización del rendimiento de la red.

Finalmente, se realizará el desarrollo de una guía didáctica para estudiantes no solo para fomentar el aprendizaje sobre el uso del firewall en equipos MikroTik, sino que también promover y concientizar sobre la seguridad informática a los estudiantes. Educar a los estudiantes sobre las mejores prácticas y el funcionamiento de máquinas virtuales con sistema operativo Linux frente a los desafíos de la ciberseguridad.

1.5 Metodología

- **Investigación exploratoria:** Inicialmente se realiza una revisión exhaustiva de la literatura técnica y científica sobre firewalls y seguridad en redes, este proceso consistirá en analizar los fundamentos y aplicaciones de los firewalls en equipos MikroTik, destacando los protocolos de seguridad y las configuraciones que han mostrado buenos resultados en entornos similares, con una revisión nos ayudará a comprender la importancia de los firewalls en la defensa contra amenazas comunes y a identificar las mejores configuraciones de políticas de seguridad en redes con acceso a Internet.
- **Investigación experimental:** En este método se llevará a cabo en un entorno de laboratorio controlado, donde se realizarán pruebas de firewall en equipos MikroTik, se diseñarán distintos escenarios de ataque como ataques DDoS, accesos no autorizados y IP Spoofing suplantación de IP, para evaluar la efectividad de las configuraciones de firewall en tiempo real, estas configuraciones serán documentadas y evaluadas en base su impacto en la latencia, el rendimiento y la seguridad de la red, gracias a esto se proporcionarán una base de conocimientos para comprender el impacto que tiene el firewall en diferentes situaciones de amenazas.
- **Pruebas de seguridad:** Se realizarán pruebas de penetración y simulaciones de ataques para evaluar la efectividad de las configuraciones implementadas, también se utilizarán herramientas de análisis de seguridad para identificar posibles vulnerabilidades en la red, permitiendo así una mejora de las medidas de protección.

2. Capítulo 2

2.1 Fundamentos de seguridad en redes

2.1.1 Conceptos básicos de seguridad en redes

La seguridad en redes es llega a ser considerada como un pilar fundamental en la infraestructura tecnológica actual, abarcando un conjunto de políticas, procedimientos y prácticas diseñadas para prevenir, detectar y por último responder a amenazas que se puedan comprometer la integridad de los recursos informáticos.

(Santos Chávez, 2024) las amenazas en las redes se clasifican en diversas categorías, incluyendo ataques pasivos, que se intervienen directamente con la interceptación y monitoreo del tráfico de la red, sin modificar los datos y los ataques activos, estos implican la modificación del flujo de datos o la creación de los flujos falsos, para tratar de evitar estas amenazas, se implementan múltiples capas de seguridad en la que incluyen firewalls, los sistemas de detección y la prevención de intrusiones “IDS/IPS”, el control de acceso basado en roles “RBAC”, y los mecanismos de autenticación. Estas medidas de seguridad trabajan agarradas de la mano para crear una defensa que este acorde a los requerimientos del usuario, donde múltiples controles de seguridad se agregan entre sí para proteger los activos de la red [1].

2.1.2 Amenazas comunes en redes con acceso a internet

En las redes con acceso a Internet, existen múltiples amenazas que son comunes que se pueden comprometer con la seguridad de los sistemas y los datos como se muestra en la **Tabla1**, una de las amenazas más extendidas son los ataques de malware, que incluyen virus de gusanos, troyanos, spyware y ransomware.

Estos programas maliciosos pueden ingresar a la red a través de descargas de archivos, correos electrónicos, sitios web comprometidos o dispositivos externos infectados. El malware como sabemos dañar los sistemas, robar información sensible o bloquear el acceso a archivos críticos, exigiendo un rescate “en el caso del ransomware” para restaurar el acceso.

Otra amenaza más común son los ataques de “DoS” y “DDoS”, dichos ataques tienen como objetivo principal saturar los recursos de la red o de los servidores, lo que provoca que los servicios se vuelvan inaccesibles para los usuarios finales, un ejemplo puede ser

que el equipo opere al 100% de su máxima capacidad, en ataques DDoS se utilizan múltiples dispositivos y a menudo comprometidos a través de redes denominadas como bots o también llamadas "botnets", al lanzar un ataque coordinado desde diferentes ubicaciones perjudicando así al servicio [2].

Amenaza	Descripción	Impacto Potencial
Malware	Software malicioso que puede dañar o explotar sistemas.	Pérdida de datos, robo de información, daños en sistemas.
IP Spoofing	Suplantación de dirección IP para ocultar la identidad del atacante.	Acceso no autorizado, ataques de man-in-the-middle.
DDoS	Ataques que buscan saturar un servicio con tráfico excesivo.	Inactividad del servicio, pérdida de ingresos.

Tabla 1. Amenazas en la red

2.1.3 Importancia de la seguridad en la infraestructura de red

La seguridad en la red es primordial para garantizar el funcionamiento continuo y la protección de los sistemas informáticos dentro de cualquier organización con acceso a la red.

Las redes son el medio a través del cual circula mucha información que puede ser sensible, y si no se protegen correctamente pueden convertirse en un blanco muy fácil para los hackers o ciber atacante. Una infraestructura de red segura siempre garantizará la confidencialidad, es decir, que solo las personas autorizadas tengan acceso a la información; la integridad, evitando que los datos sean alterados sin autorización, asegurando que los servicios de red estén siempre accesibles para los usuarios.

Como se observa en la **Figura 1**, la seguridad en la infraestructura de red es importante, por lo que hay que cumplir con normativas y estándares internacionales de seguridad de la información, como el reglamento general de protección de datos “GDPR” o las normativas ISO 27001, estas regulaciones exigen a las diferentes y numerosas organizaciones implementar mecanismos sólidos y fuertes para proteger los datos de sus usuarios, y una infraestructura de red bien protegida es clave para cumplir con estos requisitos. En caso de no cumplir con los requerimientos pueden ocasionar sanciones

severas y comprometer la confianza de los clientes y socios, lo que es de suma importancia la importancia de contar con redes bien resguardadas [3].

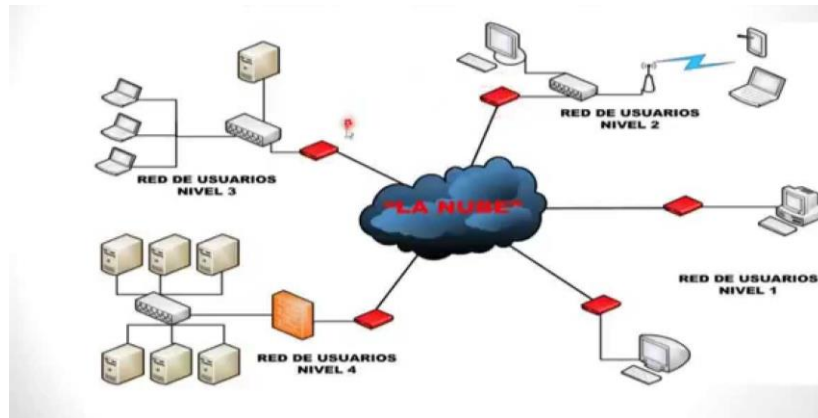


Figura 1. Infraestructura de Red
Imagen obtenida de [4]

2.2 Firewalls

2.2.1 Definición y función de un firewall

Un firewall es un sistema que actúa como una pared de ladrillos entre las redes como se ilustra en la **Figura 2**, este puede ser un tipo de hardware o software o una combinación de ambos, este está diseñado para monitorear y controlar el tráfico entrante y saliente de una red, la principal función es actuar como una barrera entre redes internas seguras y confiables y redes externas como Internet, que pueden ser peligrosas. El firewall determina si se debe permitir o bloquear el tráfico en un conjunto de reglas ya predefinidas, las cuales están configuradas para prevenir accesos no autorizados, ataques y otros tipos de amenazas en la red [5].

El funcionamiento de un firewall comienza en la inspección de paquetes de datos que circulan a través de la red, dentro del firewall el filtrado de paquetes examina cada paquete de datos en función de los siguiente: su origen, destino, puerto y protocolo, este decide si debe ser bloqueado o permitido. Otros tipos de firewalls, como los de inspección de estado y los de próxima generación “NGFW”, son más avanzados y sofisticados, ya que estos analizan tanto el estado como el contenido de las conexiones, brindando así una protección más profunda frente a nuevas amenazas avanzadas. Los NGFW pueden detectar aplicaciones también pueden analizar el contenido de los datos y hasta llegar a defenderse contra ataques complejos [6].

Los firewalls también pueden cumplir con su función de segmentación interna dentro de una red. Esto es especialmente útil para implementar políticas de seguridad dentro de la propia infraestructura de la red, limitando el acceso entre diferentes usuarios o servidores, un firewall también puede registrar eventos de seguridad y hasta generar informes, lo que permite a los administradores de red que puedan identificar patrones de tráfico inusuales o sospechosos.



*Figura 2. Funcionamiento de un firewall
Fuente: imagen obtenida de [7]*

2.2.2 Tipos de firewalls

2.2.2.1 Firewalls de hardware vs software

El firewall de hardware y los firewalls de software son dos tipos de herramientas que cumplen la misma función básica, la cual protegen las redes, los sistemas de accesos no autorizados y ataques cibernéticos, en un firewall de hardware este es un dispositivo físico que se conecta entre la red interna y la conexión a Internet o a otra red externa. Actúa como una barrera en la puerta de enlace o más conocida en como “Gateway” esta filtra todo el tráfico entrante y saliente mediante de las reglas configuradas, los firewalls están presentes en las zonas corporativas y ofrecen una protección a nivel de toda la red, gestionando grandes volúmenes de tráfico sin afectar el rendimiento del dispositivo final.

Los firewalls de software son aplicaciones instaladas directamente en los servidores, computadoras y dispositivos que son individuales, estos se encargan de controlar el tráfico que pasa a nivel de host, eso quiere decir que el tráfico que entra y sale de un dispositivo. Los firewalls de software son altamente configurables y estos ofrecen una protección

personalizada según las necesidades del sistema o red en el que están instalados, aunque su implementación es más sencilla y resulta flexible, uno de los grandes inconvenientes es que consumen recursos del sistema, esto quiere decir que pueden reducir el rendimiento del dispositivo, especialmente si se trata de un equipo con pocos recursos.

Los firewalls de hardware son ideales para proteger redes completas, ya que estas proporcionan una seguridad centralizada y no afectan el rendimiento de los dispositivos conectados, sin embargo, los firewalls de software ofrecen una capa adicional de seguridad en dispositivos que son especiales, lo que es útil para reforzar la protección en zonas con mucho tráfico en redes más pequeñas. En muchos de estos casos, las organizaciones utilizan ambos tipos donde se combinan para obtener una solución de seguridad más completa y robusta [8].

2.2.2.2 Firewalls basados en paquetes vs aplicaciones

Los firewalls en paquetes comienzan inspeccionando cada paquete de datos que pasa a través de la red, y a aquellos deciden permitir o bloquear el tráfico tales como la dirección IP de origen y destino, los puertos, y por último el protocolo utilizado, estos firewalls, también se conocen como firewalls de filtrado de paquetes, ya que se enfocan en la capa de red del modelo OSI la capa 3 y la capa de transporte la capa 4, estas son eficaces para bloquear los ataques básicos como el acceso no autorizado a ciertos puertos y la entrada del tráfico desde direcciones IP maliciosas. Sin embargo, estas tienen limitaciones, ya que no examinan el contenido del tráfico, lo que los deja más vulnerables a ataques más avanzados que se disfrazan como tráfico legítimo [9].

Los firewalls que se basan en aplicaciones estos operan en niveles superiores de la capa del modelo OSI, para ser más concretos en la capa de aplicación la capa 7, a diferencia de los firewalls en paquetes, estos poseen la habilidad de examinar el contenido de los paquetes y reconocen qué tipo de aplicación está generando el tráfico, como ejemplo un navegador web, un cliente de correo electrónico y por último una aplicación de mensajería. Los firewalls de aplicaciones permiten hacer un control mucho más centrado, ya que se pueden bloquear o permitir el tráfico según la aplicación, además de analizar el comportamiento de las aplicaciones para detectar actividades sospechosas o maliciosas, como el envío de datos no autorizados, penetración de ataques y la explotación de vulnerabilidades del software [10].

2.2.3 Arquitecturas de firewall

Las arquitecturas de firewall son diseños empleados para implementar firewalls dentro de una red de manera segura, con su principal objetivo de maximizar la seguridad y disminuir el riesgo de ataques.

Una de sus arquitecturas las más comunes es la del firewall de filtrado de paquetes en una única capa, donde el firewall es el que se coloca entre la red interna y la externa en este caso Internet, controla todo el tráfico que entra o sale, este tipo de configuración se denomina como simple y eficiente para redes pequeñas o medianas, pero puede ser menor para proteger redes extensas, ya que solo filtra el tráfico basado en direcciones IP y puertos, sin inspeccionar el contenido o de donde se originan de las conexiones.

La arquitectura que es comúnmente popular es la zona desmilitarizada o también llamada como DMZ, se utilizan para proporcionar una capa adicional de seguridad, para realizar esta configuración se crea una subred separada conocida como DMZ, entre la red interna segura y la red externa que no es de confianza como se presenta en la **Figura 3**. Los servicios que necesitan ser accesibles públicamente son servidores web y servidores de correo, se colocan dentro de la DMZ, de modo que, si un caso es expuesto, el atacante no tendrá acceso directo a la red interna, un firewall protege tanto la red interna como la DMZ, controlando el tráfico que entra y sale de ambas áreas. Esta implementación del DMZ es común en organizaciones que requieren una mayor separación entre recursos internos y públicos [11].

Las arquitecturas de firewalls en multicapa o en "capa dual" ofrecen un análisis mucho más avanzado y seguro. En este tipo de diseños, se utilizan múltiples firewalls en diferentes puntos de la red para crear unas zonas con diferentes niveles de seguridad, por ejemplo, un primer firewall puede controlar el acceso entre la red externa y también una primera capa de servidores, mientras que un segundo firewall puede proteger los recursos que son los más solicitados en una capa interna.

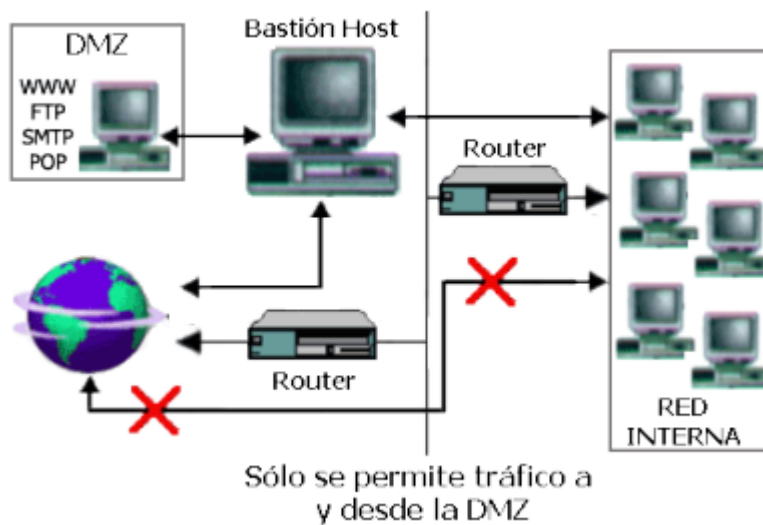


Figura 3. Función de una DMZ
Fuente: Imagen obtenida de [12]

2.2.4 Reglas de firewall

2.2.4.1 Input

La opción Input hace referencia a las reglas y políticas que controlan el tráfico entrante que tiene como destino directo el propio dispositivo del firewall o el sistema donde está implementado; esto significa que el tráfico que se evalúa en la cadena de input es aquel que llega al firewall y no el que simplemente pasa a través de él para dirigirse a otros dispositivos o redes [13].

Los paquetes de datos que contienen solicitudes para gestionar un dispositivo del firewall; como el acceso a su interfaz de administración o el uso de servicios locales, se procesan en la cadena de Input. Así, la configuración de reglas en Input es fundamental para proteger el firewall y los servicios que este dispositivo pueda tener habilitados, evitando accesos no autorizados o ataques directos al dispositivo.

2.2.4.2 Output

La opción Output dentro del firewall se encarga de controlar el tráfico que se origina en el propio dispositivo del firewall y tiene como destino otras redes o dispositivos externos, esto quiere decir que esta opción regula los paquetes de datos que el firewall y los envía hacia el exterior, ya sea como respuesta a solicitudes recibidas o para ejecutar tareas

específicas, como actualizaciones, sincronización de hora o el envío de registros a un servidor de monitoreo [13].

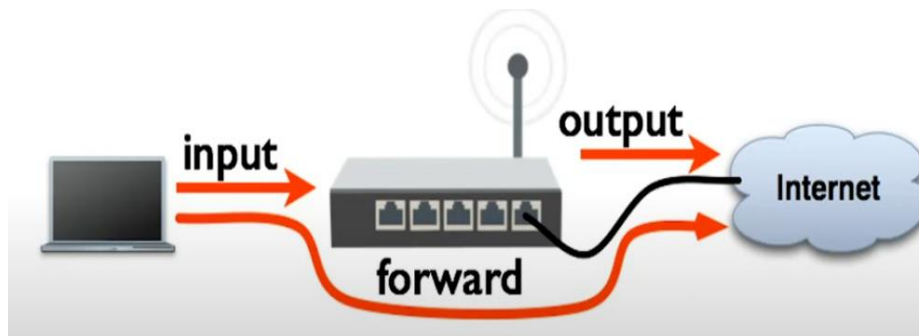
Configurar reglas en la opción Output permite a los administradores de red restringir o permitir qué servicios y aplicaciones del firewall pueden enviar datos al exterior.

Por ejemplo, se puede limitar el acceso a Internet para que el firewall solo se comunique con servidores específicos, evitando conexiones hacia sitios externos no autorizados; como resultado la cadena output contribuye a la seguridad general del sistema, al reducir el riesgo de que el propio dispositivo del firewall pueda ser utilizado para enviar datos a destinos maliciosos en caso de una posible intrusión, manteniendo un control más completo sobre las comunicaciones que salen del sistema.

2.2.4.3 Forward

Forward se encarga de controlar y filtrar el tráfico que atraviesa el dispositivo dentro firewall, es decir el tráfico que tiene origen en una red o dispositivo y destino en otra red u otro dispositivo, sin dirigirse al propio firewall, esta función es fundamental para proteger la red interna de amenazas externas y asegurar que solo el tráfico autorizado pueda ingresar o salir de la red. [13]

Tal como se observa en la **Figura 4** las reglas de la cadena Forward permiten definir qué tipos de conexiones y paquetes pueden pasar a través del firewall hacia otros dispositivos especificando las direcciones IP de origen y destino, protocolos, puertos y servicios permitidos, una configuración adecuada de forward permiten evitar que tráfico no autorizado acceda a recursos internos o que dispositivos de la red envíen datos hacia destinos peligrosos o no permitidos, en combinación las opciones Input y Output de la cadena forward asegura un control fijo sobre el flujo de datos en la red, minimizando riesgos de intrusiones, fugas de información y otros ataques que puedan comprometer la seguridad y eficiencia de la infraestructura de la red.



*Figura 4. Funcionamiento de las Reglas
Fuente: Imagen obtenida de [14]*

2.2.4.4 Establecidos

Esta opción quiere decir que los paquetes que son parte de conexiones ya establecidas, por eso cuando el firewall permite una conexión de entrada o salida, los paquetes asociados a esta conexión se marcan como establecidos y los paquetes establecidos ya han pasado la verificación inicial del firewall, por lo que las políticas configuradas en esta opción permiten atravesar sin necesidad de someterse a reglas de filtrado ya colocadas adicionales, esta configuración ayuda a reducir la carga del firewall y a garantizar una comunicación sea muy fluida, como sesiones HTTPS activas o transferencias de archivos continuas.

2.2.4.5 Relacionado

La opción de relacionado, lo que se puede decir es que permiten el paso de paquetes que no forman parte de una conexión ya establecida, pero que estos están vinculados a una conexión ya previa, como por ejemplo, cuando se establece una conexión FTP se abre una conexión principal en un puerto específico y luego se generan nuevas conexiones adicionales denominadas “relacionadas” para transferir datos, esta opción en el firewall detecta y permite estas conexiones asociadas, permitiendo que el tráfico necesario fluya de acuerdo con las conexiones previas sin tener que configurar reglas nuevas para cada sesión.

2.2.4.6 Aceptar

Indica al firewall que permita el tráfico especificado según los criterios de la regla configurada, cuando el tráfico cumple con los parámetros establecidos en una regla de Accept (como dirección IP, protocolo, o puerto), se le permite pasar a través del firewall

sin restricciones adicionales como se observa en la **Figura 5** del funcionamiento del Accept.

Esta opción se utiliza para definir qué tipos de conexiones o paquetes son seguros y deben ser autorizados, como el acceso de dispositivos confiables o el tráfico de protocolos necesarios para el funcionamiento de la red, la regla de Accept es principal para gestionar el flujo de datos y asegurar que los usuarios y servicios aprobados puedan comunicarse sin interrupciones.

2.2.4.7 Denegación

La opción Drop, bloquea de manera silenciosa el tráfico que coincide con los criterios de la regla configurada, descartando los paquetes sin enviar ningún tipo de notificación al origen, al utilizar Drop, el firewall simplemente ignora el tráfico no autorizado, lo cual es útil para desincentivar posibles ataques, ya que el emisor no recibe confirmación ni mensaje de error, haciéndole creer que el tráfico fue “absorbido” sin respuesta, esta opción es ideal para bloquear conexiones sospechosas o intentos de acceso no autorizado, ya que reduce la visibilidad del sistema ante potenciales atacantes y evita el consumo innecesario de recursos.



*Figura 5. Funcionamiento de Accept
Fuente: Imagen obtenida de [15]*

2.3 Equipos mikrotik

2.3.1 Introducción a mikrotik

El origen de MikroTik es de Letonia de un país soberano de Europa, esta empresa se especializa tanto en el desarrollo de hardware como el desarrollo de software para redes de datos, con un enfoque particular en routers y switches de alto rendimiento, esta empresa fue fundada en 1996, MikroTik ha ganado reconocimiento en el mercado global por ofrecer soluciones de red accesibles y robustas, orientadas tanto a usuarios domésticos como a entornos empresariales, la compañía ha desarrollado una amplia gama de dispositivos que permiten la implementación de infraestructuras de red escalables, con un fuerte enfoque en la relación calidad-precio, entre sus productos más populares se encuentran los routers de la serie Router BOARD y los switches de la línea CRS, que permiten una fácil gestión de redes mediante su software Router OS.

MikroTik ha crecido en popularidad a gran medida debido a que se enfoca en dar soluciones accesibles sin sacrificar el rendimiento, los dispositivos MikroTik, estos permiten a pequeñas y medianas empresas, proveedores de servicios de Internet y administradores de redes crear infraestructuras robustas, con características avanzadas de seguridad y optimización de tráfico de datos, gracias a la flexibilidad y el bajo costo de entrada, MikroTik se ha convertido en una opción competitiva frente a marcas más costosas, consolidándose como una alternativa eficiente para quienes buscan implementar redes con un control avanzado sobre su rendimiento y la seguridad [16].

2.3.2 Router os: sistema operativo de mikrotik

Es un sistema operativo desarrollado por MikroTik que se ejecuta en su mayoría de dispositivos Router BOARD y otros equipos de red, el sistema diseñado para ofrecer un control exhaustivo en la gestión y configuración de redes, Router OS cuenta una amplia gama de funcionalidades que van desde la configuración de enrutamiento básico hasta configuraciones avanzadas de seguridad y gestión de tráfico, su versatilidad lo convierte en una herramienta ideal tanto para redes domésticas como para entornos empresariales, con la capacidad de manejar las tareas complejas como el enrutamiento dinámico, control de ancho de banda, y la creación de túneles VPN.

Router OS también se destaca por su facilidad de uso, gracias a la herramienta de administración gráfica Winbox, permite una configuración sencilla y a su vez rápida de

los dispositivos MikroTik como se puede ilustrar en la **Figura 6**, aunque Router OS puede ser administrado también a través de la línea de comandos, Winbox ofrece una interfaz intuitiva que simplifica la creación de reglas de firewall, configuraciones de VLAN, enrutamiento dinámico, y otros aspectos de la red, esta flexibilidad hace que Router OS, sea accesible tanto para profesionales experimentados en el área de redes como para usuarios menos experiencia técnica que requieren una solución eficiente y personalizable para sus necesidades de conectividad y seguridad [17].



*Figura 6. Sistema MikroTik
Fuente: Imagen obtenida de [18]*

2.3.3 Características de seguridad en equipos mikrotik

Los equipos MikroTik están diseñados con un enfoque sólido en la seguridad, ofreciendo múltiples características que permiten a los administradores de redes implementar políticas avanzadas de protección, una de las principales funcionalidades es su potente firewall, integrado en RouterOS, que permite filtrar y controlar el tráfico de red de manera granular, los administradores pueden establecer reglas específicas para bloquear accesos no autorizados, limitar el tráfico a determinados puertos, y monitorear conexiones sospechosas, además, el firewall de MikroTik para darnos una idea se demuestra en la **Figura 7** el cual soporta “NAT” traducción de direcciones de red, lo que permite ocultar la estructura interna de la red detrás de direcciones IP públicas, mejorando la seguridad de los dispositivos internos, en seguridad MikroTik ofrece herramientas avanzadas para la gestión de autenticación y el control de acceso, como el uso de servidores “RADIUS” para la autenticación centralizada de usuarios y la implementación de listas de control de acceso “ACL “. Estas funcionalidades permiten definir políticas estrictas de acceso basadas en las direcciones IP, rangos de red o puertos específicos, asegurando que solo usuarios autorizados puedan acceder a los recursos de la red [19].

MIKROTIK firewall

ip firewall Mtu add chain=input src-address=33.230.158.1 protocol=tcp dst-port=8281 in-interface=ovpn-sinip action=accept

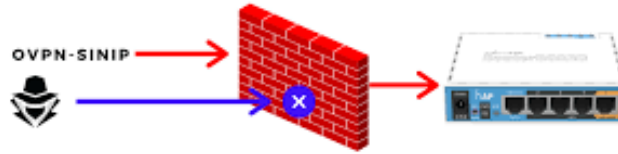


Figura 7. Firewall en Equipos MikroTik
Fuente: Imagen Obtenida de [20]

2.3.4 Ventajas y limitaciones de los equipos mikrotik en seguridad de red

Ventajas

1. **Firewall avanzado y flexible:** Los equipos MikroTik integran un firewall robusto y altamente configurable a través de Router OS, permitiendo así a los administradores de red crear reglas detalladas para controlar el tráfico, filtrar paquetes sospechosos y proteger la red contra accesos no autorizados.
2. **Soporte de múltiples protocolos VPN:** MikroTik soporta una amplia gama de protocolos VPN, incluyendo tales como: IPsec, L2TP, PPTP y OpenVPN, lo que permite la creación de túneles seguros entre ubicaciones remotas y el acceso seguro a la red interna.
3. **Control granular de acceso y autenticación:** MikroTik proporciona herramientas avanzadas como el uso de servidores RADIUS y listas de control de acceso (ACL), lo que facilita la implementación de políticas estrictas de acceso para usuarios y dispositivos.
4. **Relación costo-beneficio:** Una de las mayores ventajas de los equipos MikroTik es su accesibilidad en términos de precio, ofreciendo una solución de seguridad robusta a un costo mucho menor que otras marcas, esto es especialmente beneficioso para pequeñas y medianas empresas que necesitan proteger sus redes sin necesidad de hacer grandes inversiones.

Limitaciones

5. **Curva de aprendizaje empinada:** Aunque MikroTik ofrece una amplia gama de funciones de seguridad, la configuración de sus equipos puede ser compleja para algunos usuarios menos experimentados, las funcionalidades avanzadas de RouterOS requieren un conocimiento avanzado para ser aprovechadas plenamente, lo que puede representar una limitación para pequeñas organizaciones sin personal especializado en esta área de configuraciones de redes.
6. **Ausencia de actualizaciones automáticas:** A diferencia de otros fabricantes, MikroTik no cuenta con un sistema de actualizaciones automáticas de seguridad, el personal administrativo debe realizar manualmente las actualizaciones de firmware y parches de seguridad, lo que incrementa el riesgo si no se mantienen al día las versiones más recientes del sistema operativo.
7. **Funcionalidades avanzadas sujetas a licencias:** Aunque MikroTik nos ofrece muchas características dentro de sus equipos, algunas funciones avanzadas, como ciertos tipos de VPN o QoS, requieren una adquisición de licencias adicionales para poder ser desbloqueadas completamente, esto puede incrementar el costo total si se ocupan estas funciones en una empresa grande.

2.4 DoS/DDoS

2.4.1 Definición y tipos de ataques dos/ddos

Un ataque de denegación de servicio “DoS” es un ciberataque, su objetivo principal es que en un sistema, servidor o red se convierta inaccesible para sus usuarios finales, esto da como resultado que se saturen los recursos del sistema, como el ancho de banda o la capacidad de procesamiento del equipo recibiendo el ataque en cuestión, con una gran cantidad de solicitudes falsas o maliciosas. Dentro de un ataque DoS, el ciber atacante utiliza un solo dispositivo o servidor para realizar el ataque, y como resultado, los servicios que muestra el sistema ya afectado se colapsan, lo que puede causar pérdida de productividad, daños económicos y una mala reputación de la organización afectada [21].

El ataque denominado denegación de servicio distribuido “DDoS”, por otro lado, es una versión mucho más avanzada y sofisticada y dañina del ataque DoS, en este caso, el

ataque proviene de múltiples dispositivos o ubicaciones al mismo tiempo, esto hace que sea más difícil de detectar y mitigar. Con estos dispositivos, casi comprometidos a través de malware, conforman lo que se conoce como una "botnet", el ataque DDoS es mucho más fuerte que un DoS tradicional debido al volumen grande de tráfico generado por los dispositivos que son involucrados, además, resulta difícil de identificar el origen un ataque, ya que proviene de varios puntos en lugar de un solo atacante [22].

2.4.2 Mecanismos de funcionamiento de los ataques ddoS

Los mecanismos funcionan al aprovechar múltiples dispositivos conectados a Internet para generar una cantidad masiva de tráfico hacia un objetivo específico, con el principal propósito es de saturar sus recursos, en este caso elevar el porcentaje del CPU y hacer que sus servicios se vuelvan inaccesibles, los dispositivos utilizados en estos ataques comúnmente son denominados como "botnets", son equipos que se comprometen previamente a través de malware que los hackers controlan de una forma remota. Los atacantes envían varios comandos a estos dispositivos para que simultáneamente se inicien solicitudes de conexión o envíen grandes cantidades de datos hacia el servidor o red víctima, desbordando su capacidad de procesamiento o ancho de banda.

Uno de los mecanismos más utilizados en los ataques DDoS es el flooding, consiste en saturar una red mediante el envío masivo de solicitudes de conexión o paquetes de datos, este tipo de ataque se realiza a través de técnicas como el UDP Flood o el SYN Flood, que generan una sobrecarga en la red al bombardearla con paquetes UDP o intentos de conexión TCP incompletos lo que provoca un agotamiento de los recursos del servidor y un aumento en el uso del CPU, otro mecanismo común es la amplificación DNS, en el cual los atacantes envían solicitudes a servidores DNS legítimos, pero falsifican la dirección IP de origen para redirigir las respuestas hacia la víctima, esto amplifica el volumen de tráfico dirigido al objetivo, incrementando significativamente el impacto del ataque sin la necesidad de emplear una gran cantidad de dispositivos [23].

2.4.3 Impacto de los ataques dos/ddos en la infraestructura de redes

El impacto de los ataques DoS/DDoS puede ser considerable tanto para la seguridad y la reputación de la organización afectada, una interrupción prolongada del servicio puede disminuir la confianza de los clientes y usuarios, lo que lleva a una pérdida de credibilidad y posibles sanciones contractuales o regulatorias, además, los ataques DDoS pueden ser utilizados como distracción para ejecutar otras formas de ciberataques, como el robo de datos o el ingreso de malware en la red. Este doble impacto, que afecta tanto en la disponibilidad como en la integridad de los sistemas, refuerza la necesidad de implementar estrategias robustas de defensa para mitigar los riesgos y las consecuencias de estos ataques [24].

Los ataques DoS/DDoS, tienen un impacto significativo en la infraestructura de redes, ya que su principal objetivo es interrumpir el acceso a servicios críticos al sobrecargar los recursos del sistema, el primer efecto visible de un ataque de este tipo es la saturación del ancho de banda, que impide que el tráfico legítimo llegue a su destino, esto provoca la caída de sitios web, aplicaciones o servicios de red, lo que resulta en una interrupción del servicio para los usuarios finales, para las empresas, esto puede significar pérdidas económicas por inactividad, pérdida de ingresos en plataformas de comercio electrónico, o la interrupción de servicios vitales en industrias como la banca o la salud [25].

2.4.4 Medidas de mitigación y protección contra dos/ddos

Las medidas de prevención para la mitigación y protección contra ataques DoS/DDoS son fundamentales para garantizar la disponibilidad y la seguridad de la infraestructura de red, una de las defensas iniciales consiste en la implementación de firewalls y sistemas de detección y prevención de intrusiones (IDS/IPS), los cuales son capaces de filtrar y bloquear tráfico malicioso al identificar patrones de ataque, como un elevado número de solicitudes o conexiones provenientes de una única dirección IP, además, la configuración de reglas específicas en los firewalls permite limitar el tráfico dirigido a servicios primordiales, lo que contribuye a evitar que un ataque DoS afecte la red antes de que alcance el punto de saturación [26].

Las herramientas para mitigar el impacto de ataques DDoS resulta esencial para una protección eficaz, estas herramientas pueden estar disponibles a través de servicios en la nube o mediante dispositivos de hardware dedicados, diseñados para detectar y

neutralizar ataques de manera inmediata, su funcionamiento se basa en el análisis del tráfico entrante diferenciando entre tráfico legítimo, malicioso, y aplicando contramedidas automáticas como el bloqueo de direcciones IP sospechosas o la limitación de conexiones provenientes de fuentes no son confiables, al integrar estas soluciones con una planificación proactiva y al realizar de pruebas periódicas a las defensas de la red, permitirá reducir significativamente el impacto de los ataques "DoS/DDoS", asegurando una mayor resiliencia y continuidad operativa.

2.5 Ip Spoofing

2.5.1 Definición y conceptos básicos de ip spoofing

El IP Spoofing es una técnica maliciosa utilizada en ciberataques, en la que el atacante falsifica la dirección IP de origen de los paquetes de datos que envía, haciéndolos parecer como si provinieran de una fuente confiable o legítima, el propósito principal de este ataque es ocultar la identidad real del atacante y engañar a los sistemas de defensa de la red permitiendo que el tráfico no autorizado ingrese o salga sin ser detectado, este tipo de ataque puede ser empleado en distintos escenarios, como la ejecución de ataques de denegación de servicio "DoS/DDoS" o la obtención de acceso no autorizado a los recursos de la red.

El IP Spoofing consiste en la manipulación de los encabezados de los paquetes de datos transmitidos a través de la red, en cada paquete, la dirección IP de origen es reemplazada por una dirección falsa o suplantada, de manera que, al llegar al destino, el sistema receptor considera que el paquete proviene de una fuente confiable, los sistemas de red, como los firewalls y enrutadores, confían en estas direcciones IP para decidir qué tráfico debe ser permitido o bloqueado, esto hace que el IP Spoofing sea una técnica eficaz para evadir los mecanismos de seguridad, frecuentemente, este tipo de ataque se combina con otros vectores, como el ARP Spoofing o el envenenamiento de caché DNS, con el propósito de incrementar su efectividad. [27].

2.5.2 Funcionamiento del ip spoofing

El funcionamiento del IP Spoofing se basa en la manipulación del encabezado de los paquetes de datos que se envían a través de una red, en cada paquete contiene información clave en su cabecera, incluida la dirección IP de origen, que identifica de dónde proviene el paquete, en un ataque de IP Spoofing, el atacante altera manualmente esta dirección IP

de origen para que el paquete parezca proceder de una fuente legítima o confiable, en lugar de la verdadera dirección desde la que se envió, este engaño permite al atacante evitar mecanismos de autenticación o medidas de seguridad que normalmente filtrarían o bloquearían el tráfico no autorizado [28].

Uno de los aspectos más importantes del IP Spoofing es que los sistemas de red, como firewalls, enrutadores o sistemas de detección de intrusiones (IDS), confían en las direcciones IP para determinar si el tráfico es seguro o legítimo, si la dirección IP de origen en los paquetes ha sido falsificada, estos sistemas pueden aceptar el tráfico como seguro, permitiendo que el atacante se infiltre en la red, en algunos casos, el atacante puede enviar paquetes de respuesta falsificados o utilizar esta técnica para redirigir el tráfico a otros servidores, realizando ataques como los de Man-in-the-Middle (MitM), donde el tráfico se intercepta, se modifica o se roba sin que las partes legítimas se den cuenta. [29]

2.5.3 Tipos de ataques basados en ip spoofing

Existen diversos tipos de ataques basados en IP Spoofing, cada uno con diferentes propósitos y niveles de sofisticación, uno de los más comunes es el ataque de denegación de servicio "DoS/DDoS", el atacante falsifica múltiples direcciones IP para enviar grandes cantidades de tráfico malicioso hacia un servidor o red objetivo, al utilizar IP'S falsificadas, el atacante puede evadir las defensas de la red y dificultar que las medidas de mitigación bloqueen correctamente el tráfico, en los ataques DDoS, es particularmente efectivo, ya que el volumen masivo de solicitudes saturadas desde múltiples direcciones IP falsas provoca la caída del servicio, haciendo que el sistema se torne inaccesible para los usuarios auténticos [30].

El ataque Man-in-the-Middle, se basa en la interceptación y manipulación del tráfico entre dos partes que creen estar comunicándose de manera directa y segura, en este tipo de ataque, se representa como el atacante utiliza técnicas como el IP Spoofing para posicionarse entre las partes, logrando que los paquetes de datos pasen por su máquina o equipo antes de alcanzar su destino real, al falsificar la dirección IP, del atacante engaña a una o ambas partes, lo que le permite interceptar, modificar o incluso inyectar datos en la comunicación sin ser detectado por los involucrados, este ataque representa un riesgo

significativo en entornos donde se transmiten datos sensibles, como transacciones bancarias o sesiones de autenticación [31].

Un tercer tipo de ataque relacionado con el IP Spoofing es la suplantación de identidad de servidores (server Spoofing); donde el atacante utiliza IP Spoofing para hacerse pasar por un servidor legítimo, ya que al falsificar la dirección IP del servidor; los atacantes pueden engañar a los usuarios o a otros sistemas para que envíen datos sensibles, como credenciales o información financiera, creyendo que están interactuando con un servidor de confianza.

2.5.4 Medidas de prevención contra el ip spoofing

Las medidas de prevención contra el IP Spoofing son esenciales para proteger la integridad y seguridad de la red, ya que estos ataques pueden evadir fácilmente controles básicos de filtrado y autenticación, una de las primeras estrategias de prevención es la implementación de filtrado de paquetes de entrada y salida en los dispositivos de red; este enfoque permite verificar que los paquetes que ingresan o salen de la red tengan direcciones IP de origen legítimas y coherentes, por ejemplo el filtrado de entrada ayuda a bloquear paquetes provenientes de direcciones IP que no deberían acceder a la red, mientras que el filtrado de salida garantiza que los paquetes que salen de la red tengan direcciones IP válidas de origen, previniendo que la red sea utilizada para enviar tráfico Spoofing hacia otros sistemas [32].

El uso de protocolos como IPsec "Internet Protocol Security", para la seguridad de red, es esencial para autenticar y cifrar el tráfico a nivel de IP, este protocolo permite la verificar y validar el origen de los paquetes de datos, asegurando que los paquetes falsificados sean detectados y bloqueados, además, la implementación de firewalls avanzados y sistemas de detección y prevención de intrusiones "IDS/IPS" es primordial ya que se identifica y mitiga los posibles ataques de IP Spoofing, dichos sistemas son capaces de analizar el tráfico en la busca de patrones que no son normales y señales de suplantación de IP, como las solicitudes inusuales o direcciones IP duplicadas, los IDS/IPS, además de bloquear automáticamente el tráfico sospechoso, pueden alertar a los administradores de red sobre incidentes potenciales de Spoofing, fortaleciendo así la seguridad dentro de la red.

2.5.5 Uso de filtrado de paquetes y firewalls contra ip spoofing

Al implementar un filtrado de paquetes de entrada y salida, las redes pueden identificar y rechazar los paquetes cuyos IP de origen no coincidan con las reglas predefinidas de tráfico legítimo, por ejemplo, mediante el filtrado de entrada, se bloquean los paquetes que provienen de direcciones IP sospechosas o externas que no deberían tener acceso a la red interna, de igual manera, que el filtrado de salida asegura que solo los paquetes con direcciones IP de origen legítimas puedan salir de la red, previniendo que los dispositivos internos sean utilizados para generar ataques de suplantación hacia otros sistemas [33].

Sistemas de detección y prevención de intrusiones "IDS/IPS" complementan el filtrado de paquetes, y los firewalls al monitorear la actividad de la red en tiempo real para identificar comportamientos anómalos que podrían indicar un ataque de suplantación de IP, estos sistemas están diseñados para analizar el tráfico en busca de discrepancias en el origen de los paquetes y alertar o bloquear las amenazas potenciales antes de que puedan causar daño. Combinando el filtrado de paquetes, firewalls y herramientas de IDS/IPS, las organizaciones pueden establecer un enfoque de seguridad integral que dificulte el éxito de ataques de IP Spoofing, protegiendo así la integridad y confiabilidad de su infraestructura de red [34].

2.6 Kali Linux

(Alex Vinueza, 2021) comenta que Kali Linux es una distribución que está dirigida hacia la seguridad informática ya sea para pruebas de ataques avanzados. Este software cuenta con una gran cantidad de herramientas que se utilizan para realizar tareas en cuestión a la seguridad informática como ejemplo: cuál realizar ataques hacking ético e investigación forense, este software ha sido desarrollado por la empresa Offensive Security esta es una compañía de entrenamiento para la seguridad de la información.

También nos describe que este software fue una reconstrucción de otro llamado Back Track, cómo es la diferencia que nos comenta que el Back Track está basado en el sistema Ubuntu mientras que Kali Linux opera en los estándares de Debian, por último, incluye las herramientas necesarias para realizar pruebas de penetración cómo se realizan en los ataques de IP Spoofing [35].

2.7 Wireshark

(María Elizabeth Narváez, 2015) Nos habla sobre Wireshark que este es primer de los software más populares libres de código abierto en lo que respecta a analizadores de protocolos de red, este ideal para la red solución de problemas en la red y análisis del tráfico mismo de la red, esta es una herramienta que nos permite monitorear el tráfico de objetivos primordiales con el objetivo de que captura las credenciales del origen de sesión, también nos comenta que al abrir Wireshark se procede a iniciar la captura del tráfico y seleccionamos el tipo de captura o las interfaces disponibles, Wireshark capturará todo el tráfico disponible que circula por el cable de red este tráfico se puede filtrar mediante la selección de di datos en específico también podemos filtrar los protocolos direcciones IP [36].

3. Capítulo 3

3.1 Implementación de reglas de filtrado en el firewall

Se implementaron reglas específicas en las cadenas input y forward, las cuales son esenciales para gestionar el tráfico dentro del router, la cadena input se encarga de controlar todo el tráfico dirigido directamente al router, mientras que la cadena forward administra el tráfico que atraviesa el router hacia otras redes, en la configuración de la cadena input, se establecieron reglas que permiten únicamente las conexiones establecidas y relacionadas, garantizando así la respuesta a solicitudes legítimas, por otro lado, las conexiones inválidas se bloquean mediante la acción drop, adicionalmente, se definieron direcciones IP autorizadas para la administración del equipo, restringiendo el acceso a usuarios no permitidos, todo el tráfico restante es rechazado para reforzar la seguridad del dispositivo, en la cadena forward, se permitió el tráfico correspondiente a conexiones establecidas y relacionadas, asegurando la continuidad del tráfico legítimo, las conexiones inválidas fueron bloqueadas para mitigar riesgos asociados a ataques o tráfico sospechoso, además, se autorizó el acceso a la red a usuarios específicos mediante direcciones IP, permitiendo la navegación según las políticas definidas. Finalmente, se bloqueó todo el tráfico restante en la cadena forward, garantizando que únicamente las conexiones previamente autorizadas puedan transitar a través del router.

3.1.1 Configuración desde winbox para las reglas de filtrado en el firewall

Paso 1: Conectamos el Cloud Router Switch 310-1G-5S-4S+ de MikroTik con un cable de red al puerto de consola (ETH/POE), y el otro extremo al computador Admin para acceder a su interfaz Winbox, en el computador nos dirigimos a Winbox para seleccionar nuestro equipo y proceder con las respectivas configuraciones, una vez dentro de Winbox seleccionamos el equipo mediante la dirección Mac del CRS310 procedemos a colocar un usuario (Login) y contraseña (Password) y damos clic en el apartado de (Connect) para acceder al mismo.

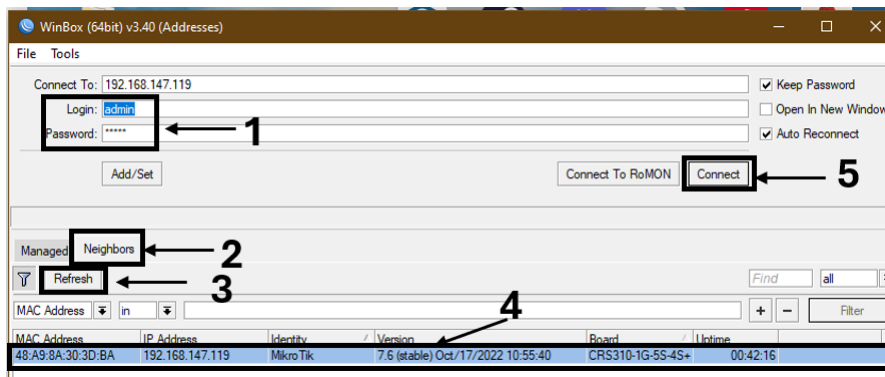


Figura 8. Ingreso al equipo mediante winbox
Imagen elaborada por el autor

Paso 2: Nos dirigimos a la pestaña IP, luego damos clic en la opción Firewall para comenzar con las reglas de filtrado, se nos despliega una ventana donde vemos distintas opciones que vamos a utilizar con la que vamos a comenzar es Filter Rules dando clic a botón (+), empezamos con las reglas básicas para comenzar con la estructura de menor a mayor.

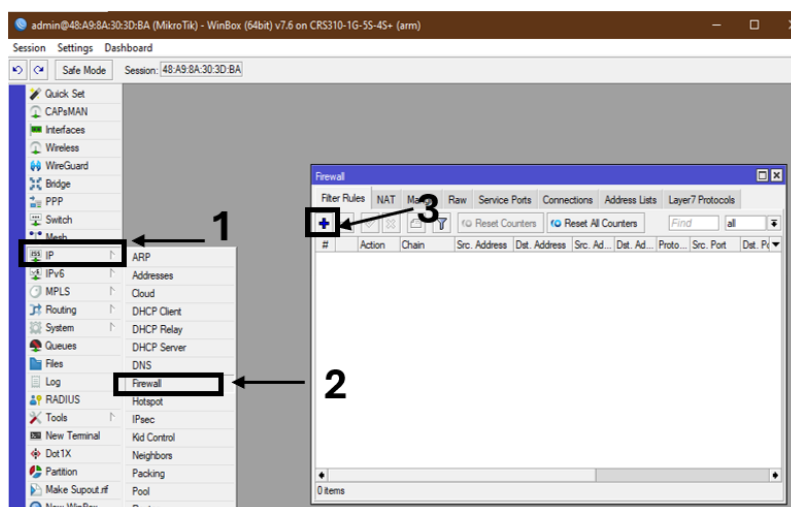

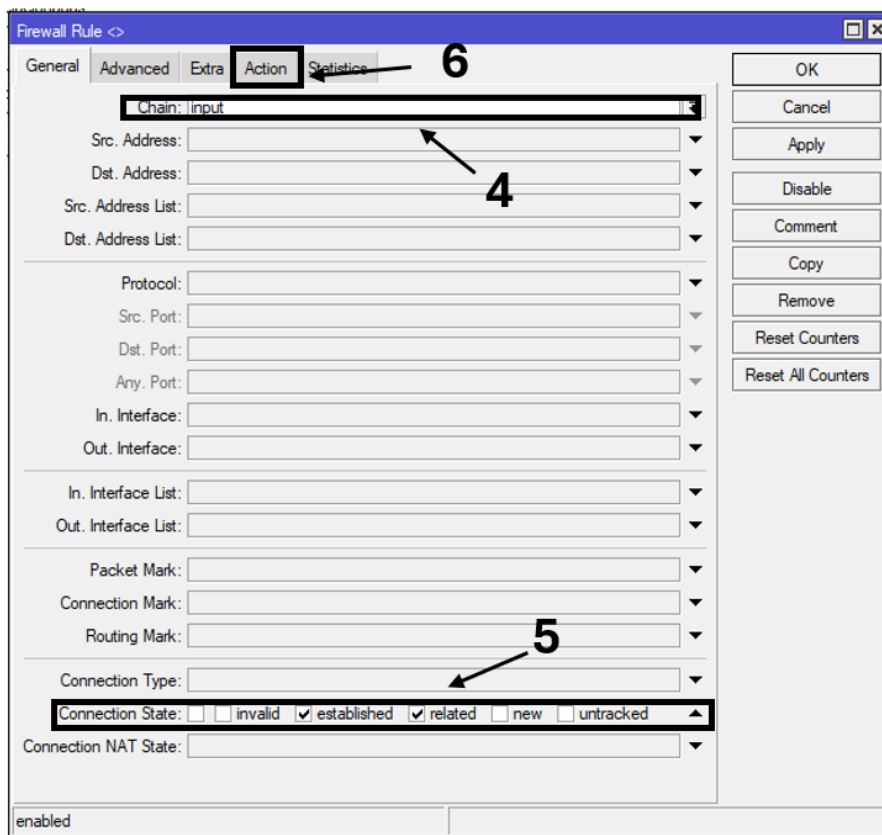


Figura 9. Configuración de las reglas del firewall
Imagen elaborada por el autor

Paso 3: Luego en la ventana emergente, damos clic en la opción Chain y en la pestaña se desplegarán 3 opciones para esta primera parte de las reglas de filtrado empezamos con la opción Input porque con la opción Input ver (2.2.4 Reglas del firewall) teniendo en cuenta su función proseguimos con la siguiente opción dentro de la misma ventana nos dirigimos a Connection State y en la pestaña  luego seleccionamos las 2 casillas correspondientemente estas son establecido (established) y relacionado (related) ver (2.2.4.4 y 2.2.4.5), como siguiente nos colocamos en la opción Action y en la pestaña seleccionamos Accept y damos clic en Apply por ultimo nos dirigimos a la opción Comment para establecerse un comentario y separar las reglas que colocamos y le damos clic en Ok.



*Figura 10. Primera regla del firewall
Imagen elaborada por el autor*

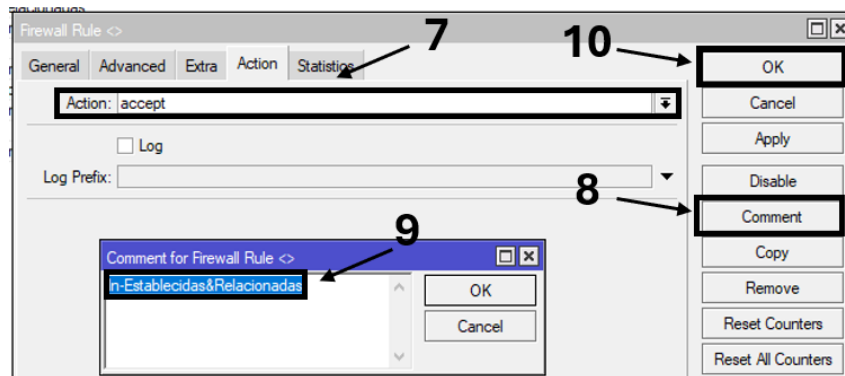


Figura 11. Aceptación de la función input
Imagen elaborada por el autor

Paso 4: Como siguiente dentro de File Rules le damos a (+) para colocar la siguiente regla en la que decimos que todas aquellas conexiones que no se han permitido en la regla anterior son consideradas como invalidas y dentro de ellas tenemos que todas aquellas nuevas y sin seguimiento son consideradas como invalidas, ver opción drop (2.2.4.7), continuando se desplegara una ventana donde en la opción chain damos clic a la pestaña y seleccionamos input, como siguiente nos dirigimos más abajo donde Connection State para seleccionar la casilla invalid luego continuamos y nos dirigimos a Action opción Drop donde damos clic a la pestaña y seleccionamos la opción drop por ultimo colocamos un comentario y damos a la opción Apply y OK.

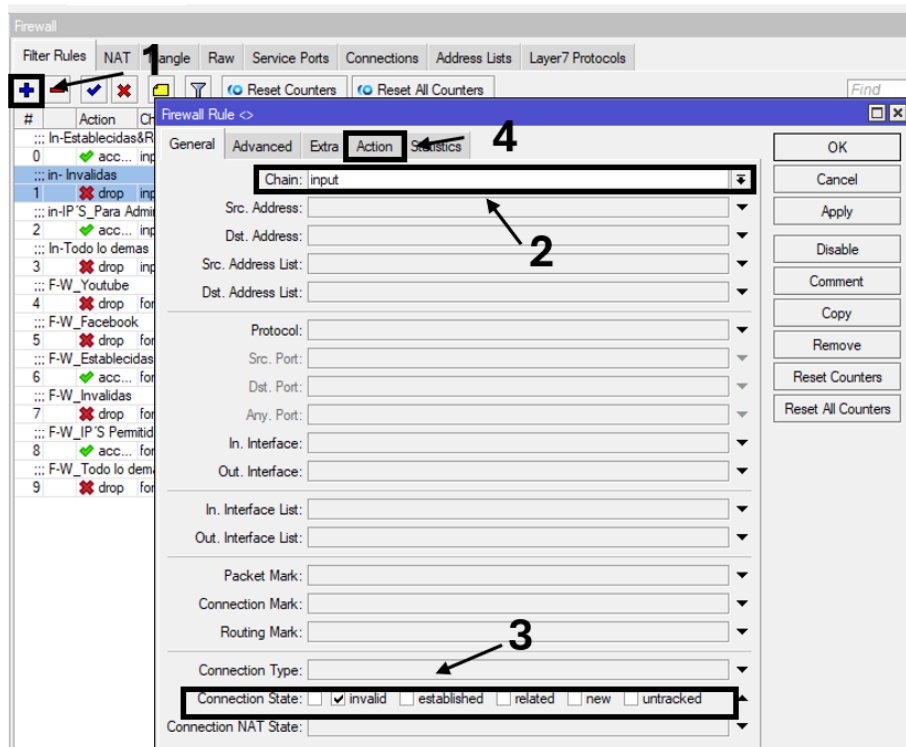


Figura 12. Regla input invalida
Imagen elaborada por el autor

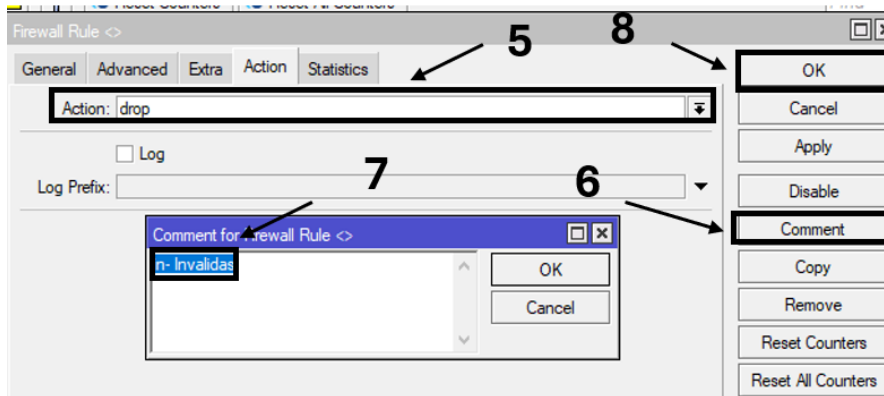


Figura 13. Regla input drop
Imagen elaborada por el autor

Paso 5: Nos dirigimos a la pestaña Address List dentro del firewall para darle un nombre y una dirección ip para el administrador con esto decimos que solo las IP colocadas en el Address List pueden administrar al router y acceder a sus servicios, cuando creamos una lista direcciones lo primero que colocamos es el nombre de la lista, damos clic en (+) para crear el Address List, damos clic en Name para colocar Ip's_Aministracion luego en Address colocamos una dirección IP 192.168.2.0/24 con la que se pueda acceder al router para poder administrarlo por ultimo damos clic en OK.

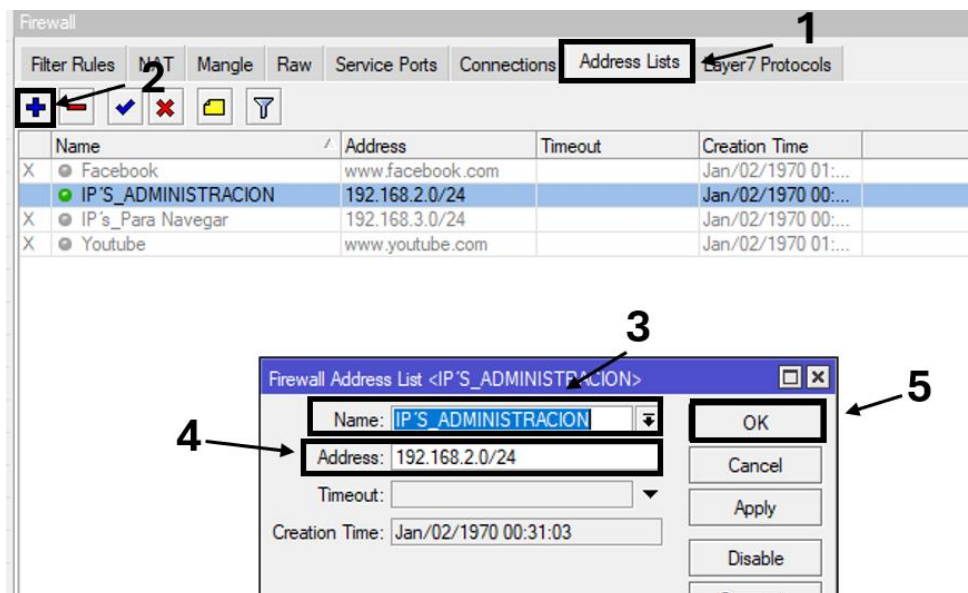


Figura 14. Configuración para modo administración
Imagen elaborada por el autor

Paso 6: Después de haber creado el Address list abrimos y cerramos, comenzamos colocando una nueva regla damos clic en (+) se desplegará una ventana y dentro de Chain colocamos la opción input, en esta nueva regla definimos el Address List de las direcciones IP que hemos creado para que puedan ser permitidas una vez que estas intenten ingresar al Cloud Router Switch este las detecte y mediante la regla las deje ingresar para que se pueda administrar el equipo, en la regla colocamos la opción de Src. Address List dando clic a la pestaña seleccionamos IP'S_ADMINISTRACION, luego nos dirigimos a la pestaña Action dando clic en la pestaña seleccionamos la opción accept y por últimos agregamos un comentario que identifique la regla.

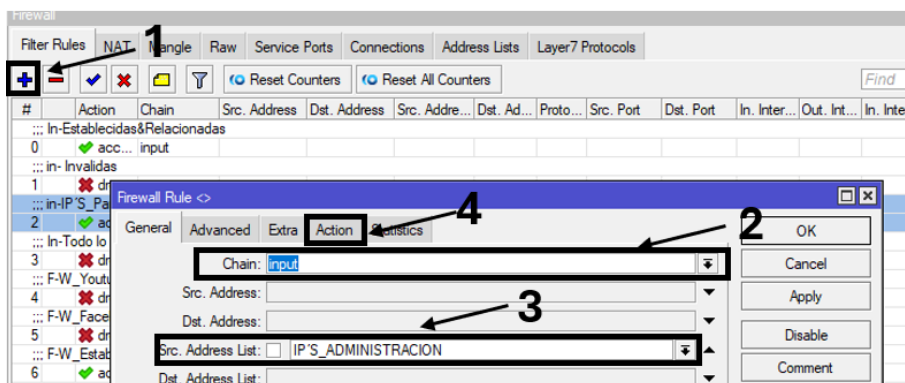


Figura 15. Regla para el acceso al equipo
Imagen elaborada por el autor

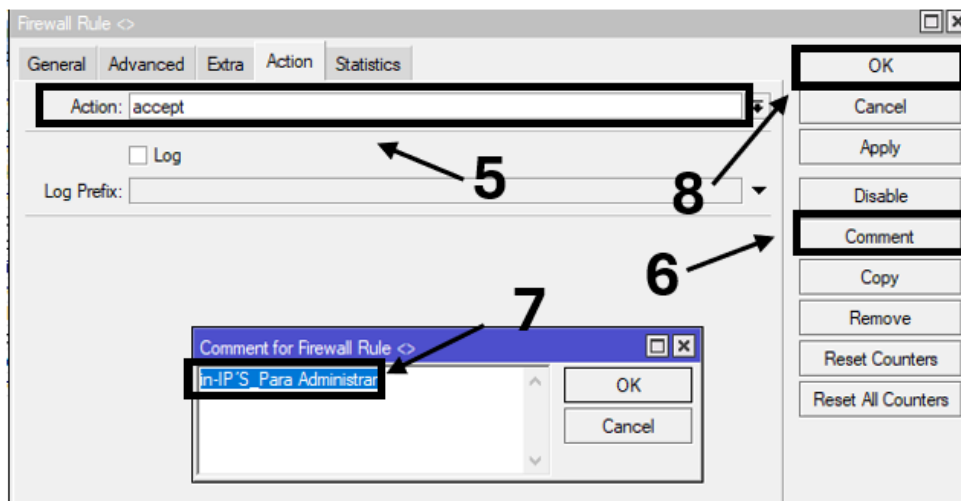
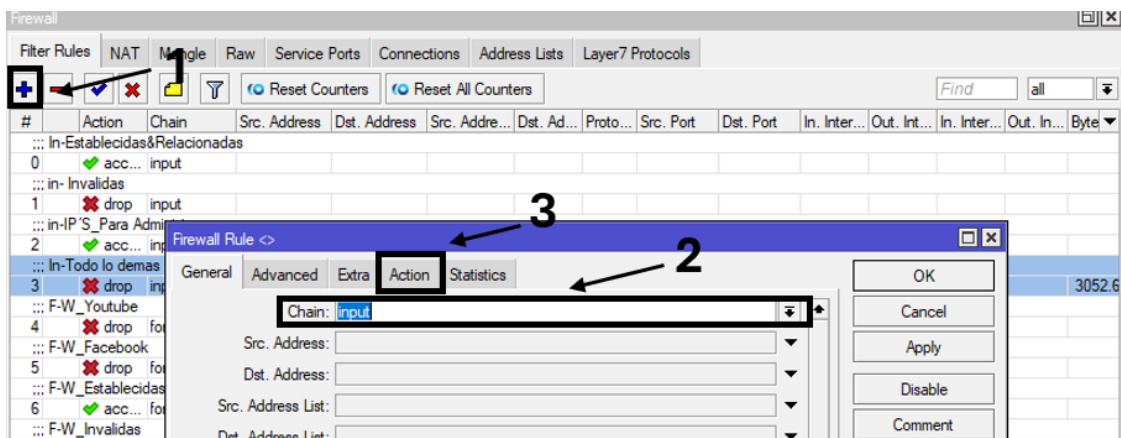
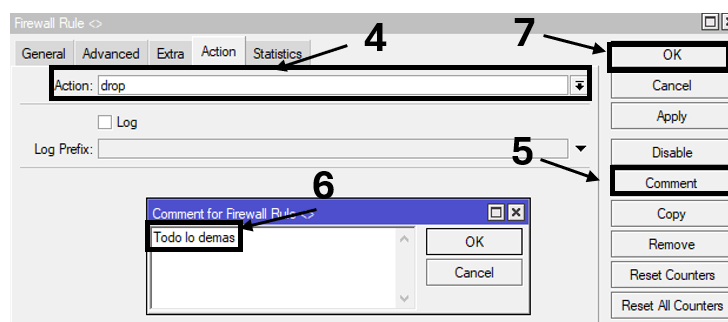


Figura 16. Aceptación de la regla
Imagen elaborada por el autor

Paso 7: Continuamos, como ya hemos agregamos el origen para que pueda acceder al router ahora agregamos lo de más para que pueda cerrarse esto se considera cerrar un nivel de forma distintiva utilizando el drop para entender mejor decimos que todo lo demás que esté relacionado a un protocolo, a puerto, aun origen, a un destino y a una conexión que no se haya permitido en ese instante se lo denominara drop o dropeado. Comenzamos dando clic en (+) para agregar esta regla en la opción Chain colocamos la opción Input, como siguiente nos dirigimos a Action para seleccionar la opción Drop damos clic en la pestaña y escogemos drop, por últimos agregamos otro comentario y damos clic en Ok.



*Figura 17. Cerrando la cadena de input
Imagen elaborada por el autor*



*Figura 18. Opción denegación
Imagen elaborada por el autor*

3.1.2 Configuración de la opción forward (tráfico que pasa a través del equipo)

Paso 8: El Firewall de MikroTik es conocido como state full ya que MikroTik nos da la posibilidad a través de este firewall generar un seguimiento de conexión, como siguiente regla vamos a establecer una seguridad de red privada hacia la red pública y viceversa, es por esto que vamos a administrar las conexiones, para eso comenzamos colocando las conexiones que inicialmente queremos permitir, primero creamos nuestra red inicial en

forward ver (2.2.4.3), abrimos un nueva ventana de reglas dando clic en (+) y en casilla Chain damos clic en la pestaña colocamos la opción forward y en el apartado de Connection State seleccionamos las conexiones establecidas y relacionadas, nos dirigimos a la pestaña de Action en el apartado de Action damos clic en la pestaña escogemos la opción de accept, como ultimo dejamos un comentario para dejar identificado la regla.

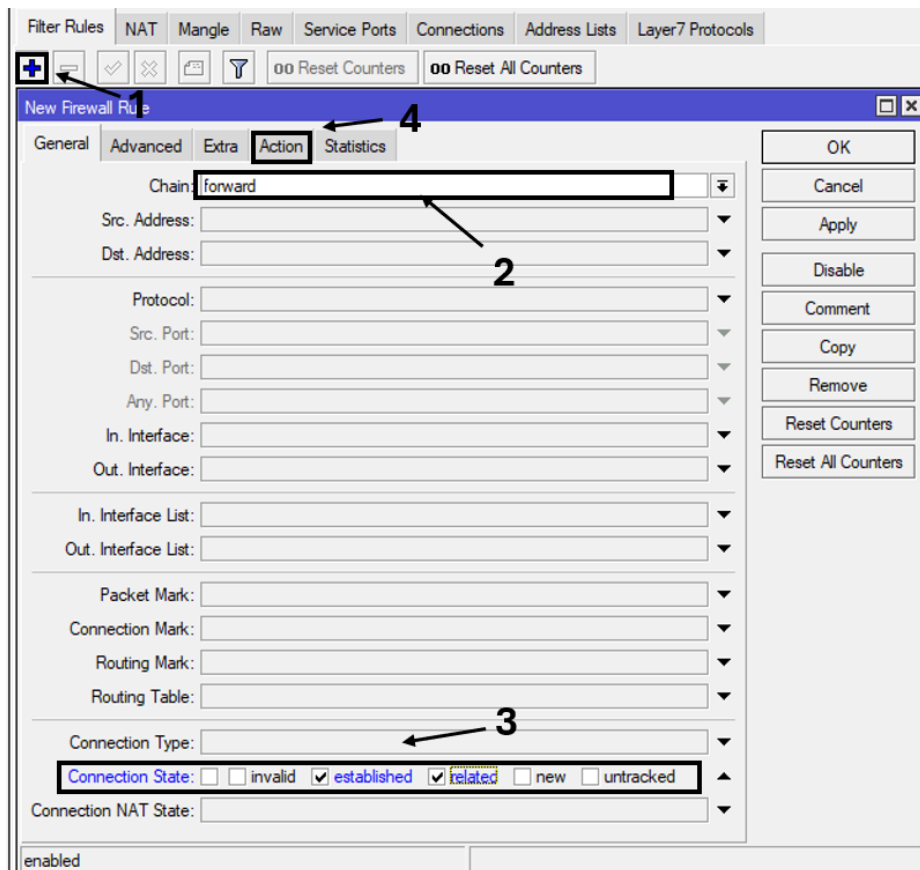


Figura 19. Reglas del firewall opción forward
Imagen elaborada por el autor

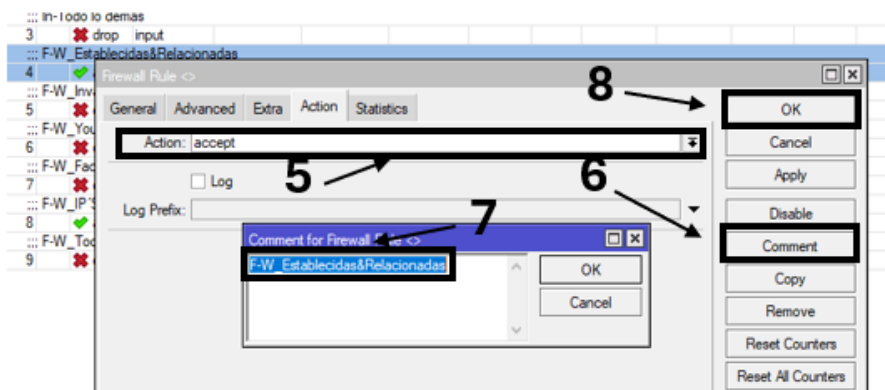
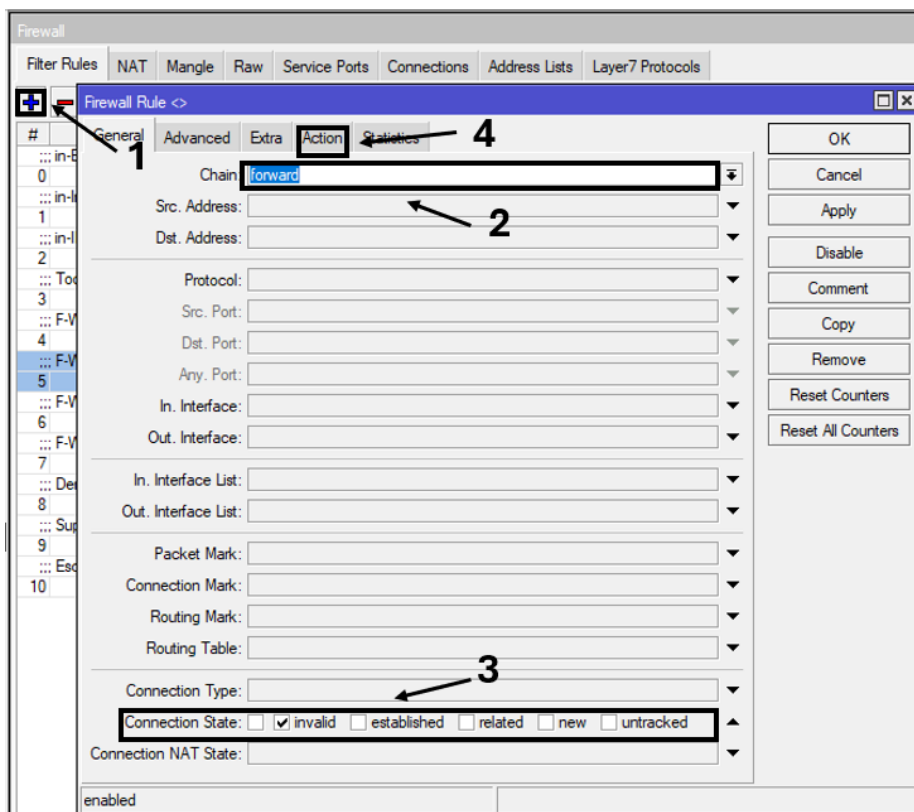
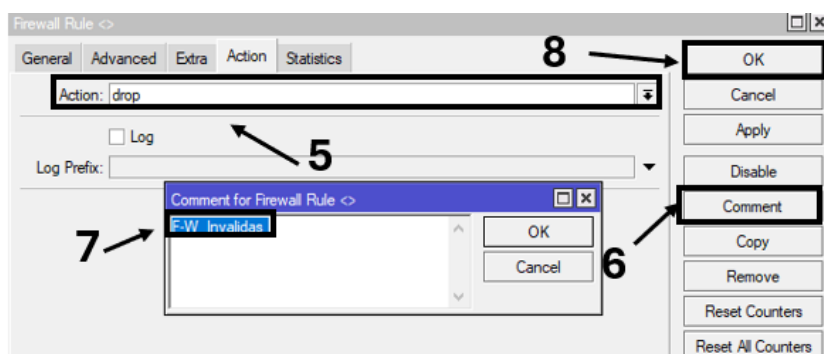


Figura 20. Aceptación de establecidas y relacionadas
Imagen elaborada por el autor

Paso 9: Una vez colocadas las condiciones establecidas y relacionadas tenemos que ir cerrando la condición que inicialmente hemos permitido, todas a aquellas conexiones que no hemos permitido en establecidas y relacionadas van a quedar como invalidadas con la opción drop, comenzamos agregando otra regla dando clic en (+), en el apartado de Chain colocamos la opción Forward, en la sección Connection State damos clic en la pestaña y ➡ seleccionamos la opción invalid, luego nos dirigimos pestaña Action y en la sección del mismo nombre dando clic a colocamos la opción drop por último agregamos un comentario.

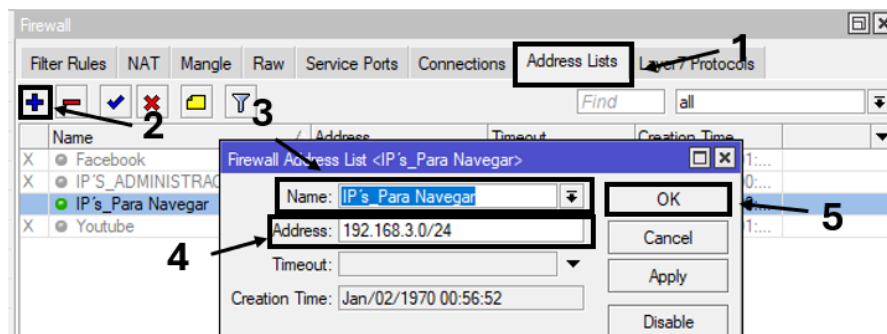


*Figura 21. Opción invalid dentro del forward
Imagen elaborada por el autor*




*Figura 22. Denegación de la opción invalid
Imagen elaborada por el autor*

Paso 10: Vamos a generar otra regla para estructurar aquellas peticiones que queremos permitir que salgan o que puedan ser procesadas por router. Para ello nos dirigimos a la pestaña Address List para colocar ip permitidas para poder navegar, damos clic en (+) para agregar un nuevo Address List donde también especificamos un segmento local, se nos despliega una ventana donde en la opción de Name damos clic para creamos un nombre y en el apartado de Address damos clic para ingresar una dirección ip: 192.168.3.0/24 para que se pueda navegar atreves de esta dirección por último damos OK.



*Figura 23. Creación de address list para navegar
Imagen elaborada por el autor*

Paso 11: Luego aperturar las conexiones en done todo lo que pase por router de aquel origen ya creado Ip's_ParaNavegar van a hacer aceptadas, procedemos a abrir otra regla donde damos clic en (+), se desplegara una ventana y en Chain damos clic a la pestaña  colocamos el forward, para luego dirigimos al apartado de Src.Address List donde damos clic en seleccionamos: Ip's_ParaNavegar, luego nos vamos a pestaña Action y en la Opción Action damos clic en el icono colocando la opción accept, y por último dejamos un comentario.

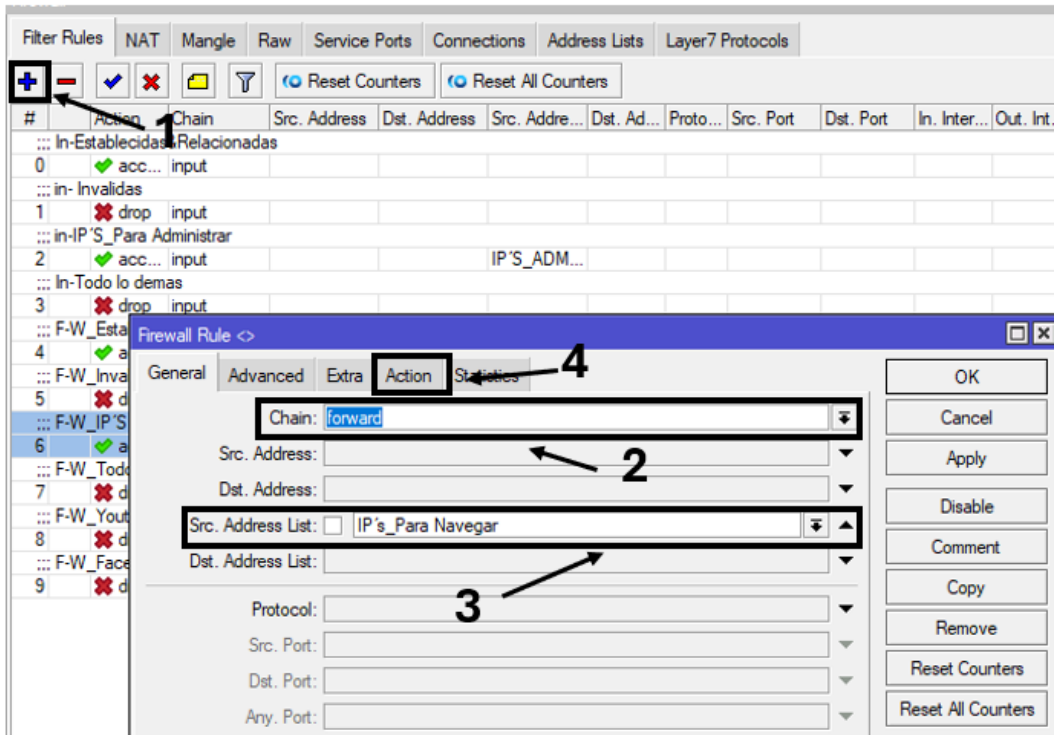


Figura 24. Address list para navegar
Imagen elaborada por el autor

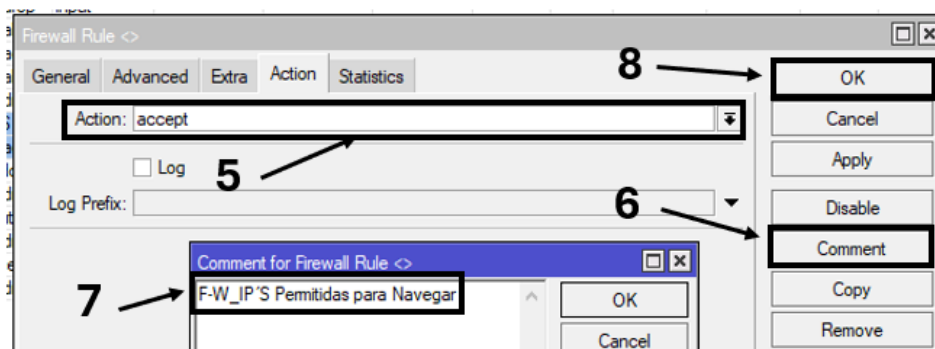



Figura 25. Aceptación de ip's para navegar
Imagen elaborada por el autor

Paso 12: Una vez permitido lo que necesitamos es importante ir cerrando las cadenas con la opción drop, Empezamos colocando una nueva regla, comenzamos dando clic en (+) nos dirigimos a Chain y le damos clic en  y escogemos la opción a la opción de forward para después ir a la opción Action en donde nos colocaremos en la opción del mismo nombre después damos clic en la pestaña y seleccionamos el apartado drop y como parte final de agregamos un comentario.

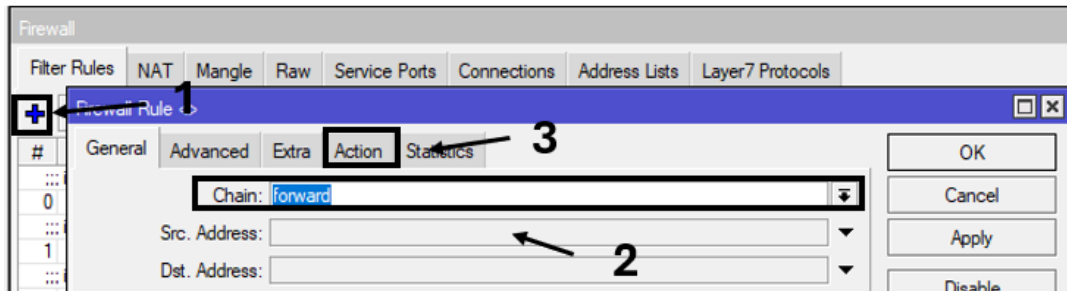


Figura 26. Nueva regla para todo lo demás en ip's para navegar
Imagen elaborada por el autor

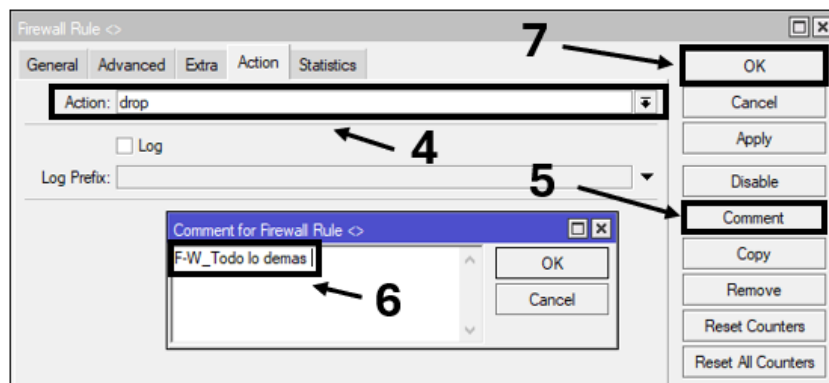


Figura 27. Aceptación de la opción drop
Imagen elaborada por el autor

Paso 13: En este paso vamos a crea un Address List dinámico para identificar aquellos dispositivos que están accediendo al CRS a través del winbox, comenzamos dando clic (+) para crea una nueva regla donde nos enfocamos en la cadena denominada Chain le damos clic en la pestaña y seleccionamos la opción de input, luego nos enfocamos en la condición ya que necesitamos identificar aquellos dispositivos que intenten generar una conexión al equipo a través del puerto por defecto del Winbox que es 8921 entonces decimos que todo lo que ingrese al equipo con Protocolo Tcp del puerto por defecto sea ejecutada la acción de agregar a estos orígenes de agregar a un Address List y este Address List tendrá un nombre con el cual identificamos el acceso al Winbox, luego de seleccionar input seleccionamos la casilla de protocol y seleccionamos (TCP), continuando en el opción Dst. Port colocamos el valor del puerto de acceso al Winbox, luego nos dirigimos a Action y damos clic en la pestaña y seleccionamos Add src Address List continuando colocamos un nombre Address List denominado Acceso al Winbox por último damos clic en Ok.

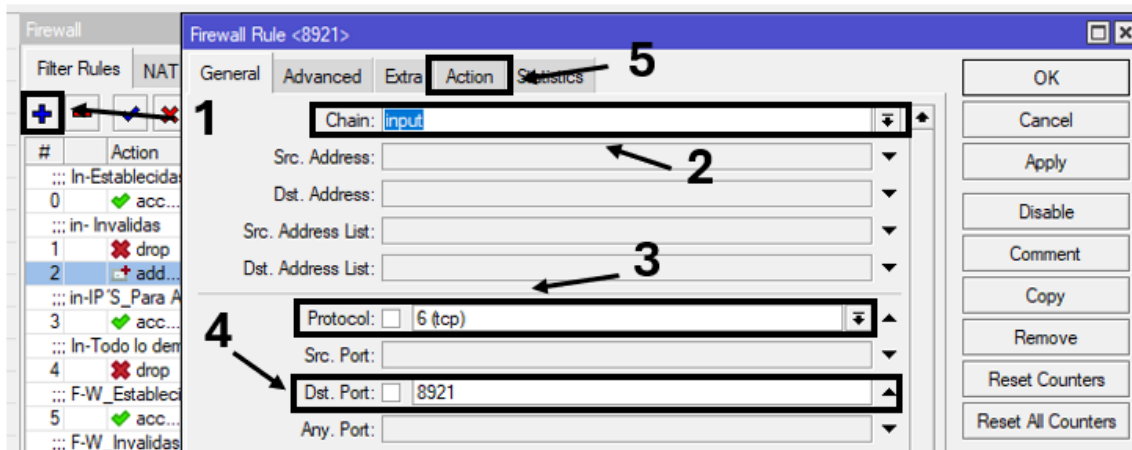


Figura 28. Nueva regla para el acceso al winbox
Imagen elaborada por el autor

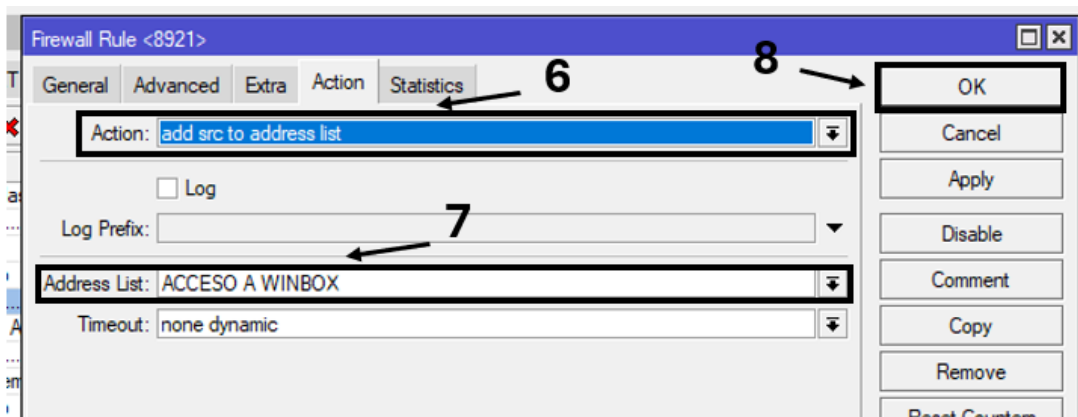




Figura 29. Creación del address list
Imagen elaborada por el autor

3.2 Protección contra amenazas dos/ddos

Los ataques DoS y DDoS son amenazas significativas estos ataques afectan la seguridad y estabilidad de las redes, en esta práctica se implementaron medidas de protección en el equipo MikroTik mediante el desarrollo de reglas de firewall diseñadas para mitigar estos riesgos, en primer lugar, se configuraron 3 reglas la primera para bloquear puertos no utilizados, reduciendo así la superficie de ataque, posteriormente, se implementó una regla para evitar los ataques DDoS, basada en la detección y limitación de solicitudes extrañas provenientes de múltiples orígenes, finalmente se configuró una regla adicional para contrarrestar ataques DoS, esta se centra en bloquear intentos de saturación desde un único origen, para evaluar la efectividad de estas configuraciones, se utilizó una herramienta que generaba tráfico malicioso simulando ataques DoS y DDoS, esta prueba práctica permitió validar que las reglas implementadas cumplieran con su propósito de proteger la red contra estas amenazas.

3.2.1 Configuración contra los ataques ddos

Paso 1: Lo que vamos a realizar es un bloqueo de los puertos del equipo para que estos no sean inseguros en nuestra red, comenzamos ingresando al Winbox del equipo en la opción de Ip nos dirigimos a Firewall, dentro del mismo damos clic a (+) donde se muestra una ventana nos colocamos en General, en la opción de Chain damos clic a la pestaña  y seleccionamos la opción de input seguido nos dirigimos a la opción Protocol donde escogemos el (TCP), continuando nos colocamos en la pestaña Extra luego nos centramos en el apartado de PSD (PORT SCAN DETECTION) damos clic a la pestaña  y no aparcen 4 opciones que las dejaremos por defecto (Weight Threshold) es el peso total de los últimos paquetes del TCP y UDP precedentes de un mismo host o host atacante el equipo lo detecta como una secuencia de escaneo de puertos, (Delay Threshold) es el retardo de los paquetes precedentes del mismo host con una secuencia del mismo ataque (Low Port Weight) es el peso del paquete con un puerto de destino que maneja privilegios que corresponde de los puertos del 1 hasta el 1024 y por ultimo (High Port Weight) es el peso del paquetes compuestos de destino que no maneja privilegios, luego de tener en cuenta para que sirven los parámetros nos dirigimos a la pestaña de Action y damos clic Drop para reducir y eliminar todas esas conexiones que manejen esas características y por ultimo colocamos un comentario para identificar la regla.

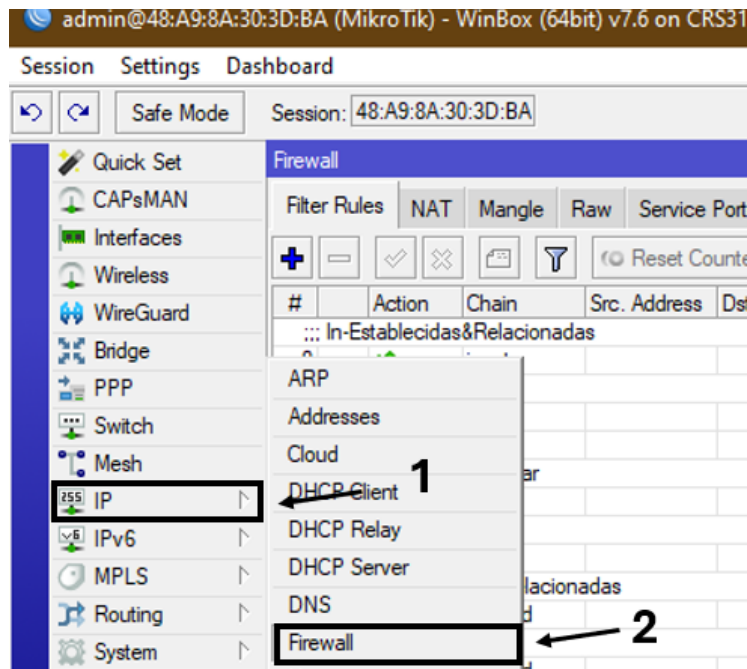


Figura 30. Ingreso al firewall para nueva regla
Imagen elaborada por el autor

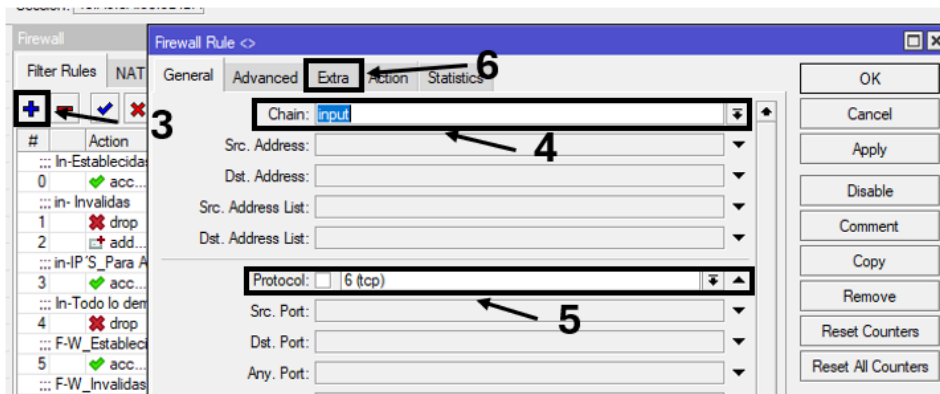


Figura 31. Creación de la nueva regla
Imagen elaborada por el autor

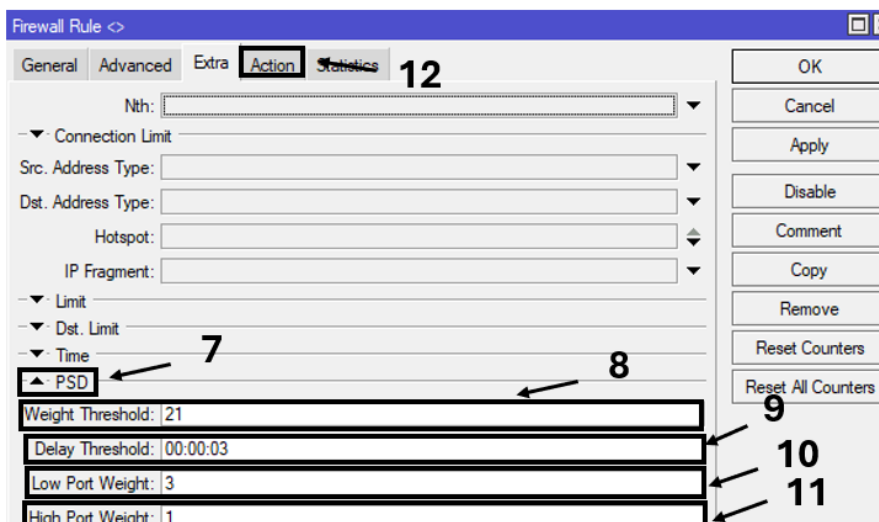


Figura 32. Opción extra-psd
Imagen elaborada por el autor

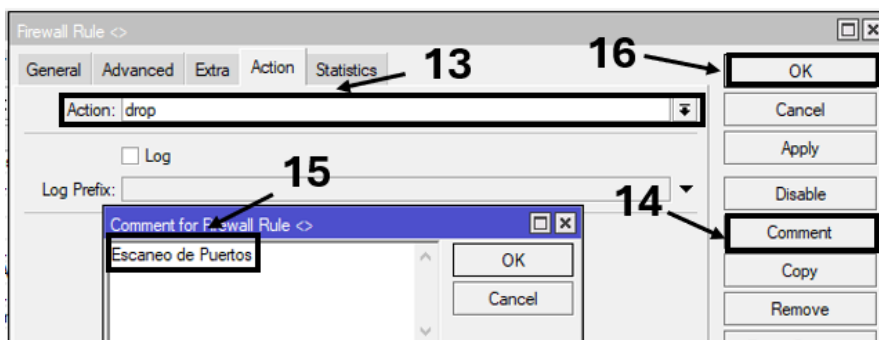


Figura 33. Función drop en el escaneo de puertos
Imagen elaborada por el autor

Paso 2: Continuamos y vamos a crear una regla para evitar los ataques DDoS, nos dirigimos a Filter Rules luego damos clic en (+), se desplegará una ventana, nos enfocamos en la pestaña General nos colocamos en Chain luego damos clic a la pestaña seleccionamos la opción Input, luego en el apartado de Protocol damos clic en la misma

pestaña ➡ y seleccionamos la opción (TCP), luego damos clic en la pestaña EXTRA, como siguiente nos centramos en la opción Connection Limit donde indicamos la cantidad de conexiones que vamos a emplear por host es decir por dirección IP o por un sub red donde permitimos 10 conexiones limite, luego nos situamos en la pestaña Action y en la sección del mismo nombre damos clic en la pestaña ➡ y seleccionamos la opción Add src Address List, luego nos centramos en Address List damos clic y colocamos un nombre en este caso Lista_Negra por ultimo colocamos un comentario y damos Ok.

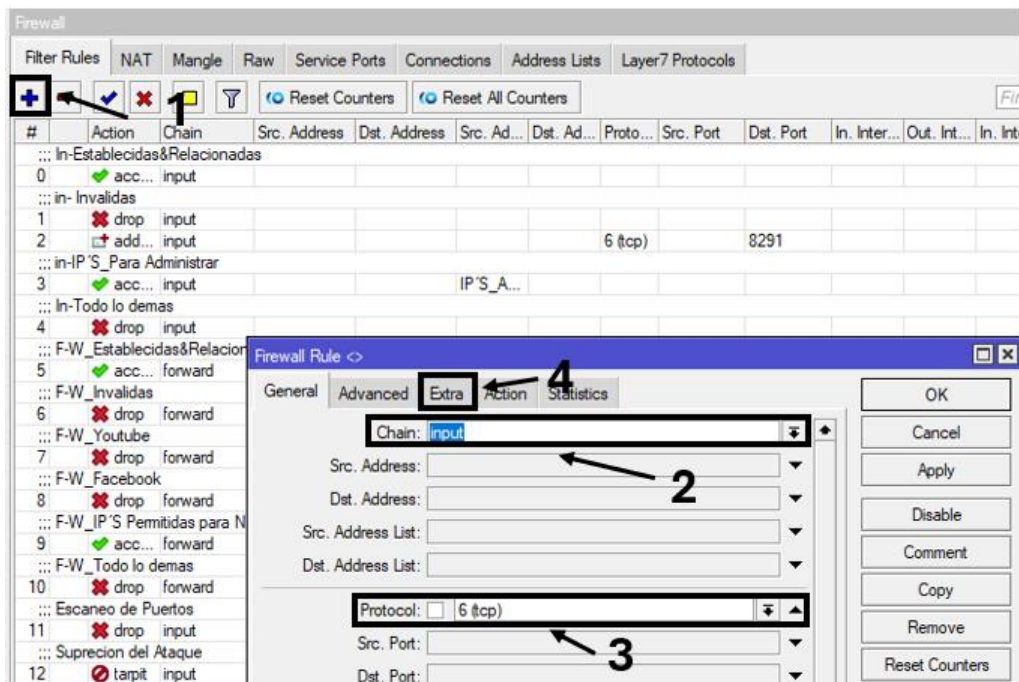


Figura 34. Nueva regla de denegación
Imagen elaborada por el autor

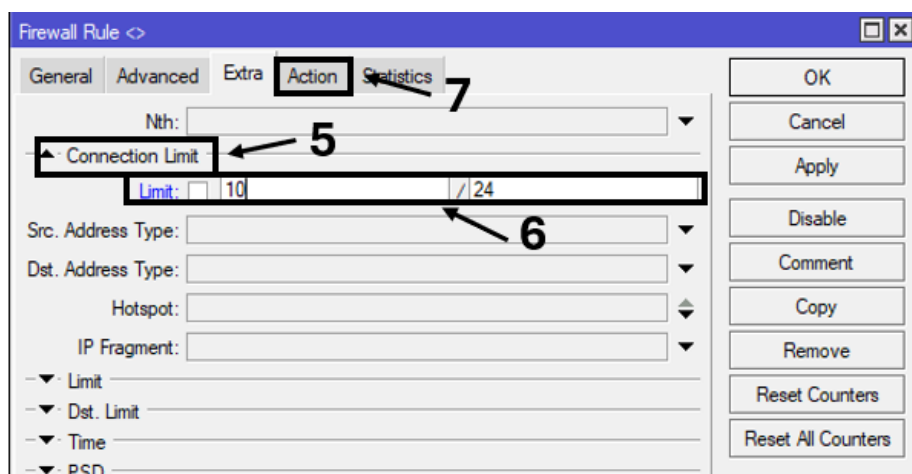
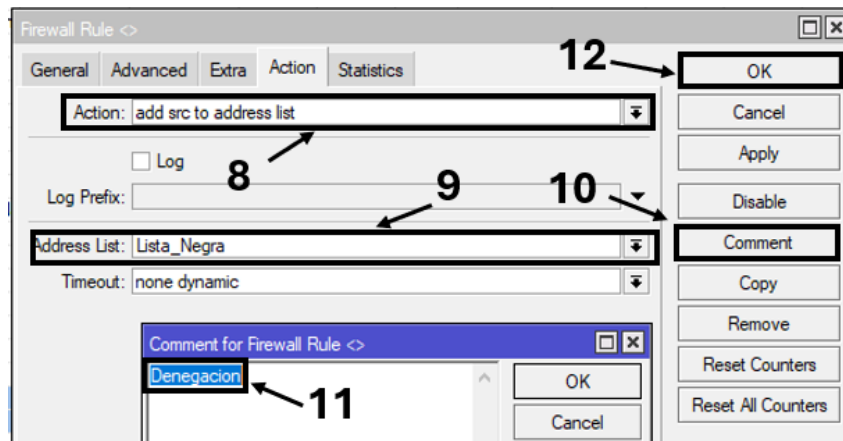





Figura 35. Establecer la connection limit
Imagen elaborada por el autor



*Figura 36. Agregar el address list
Imagen elaborada por el autor*

Paso 3: Continuamos con otra regla para suprimir el ataque para ello damos clic en (+) se desplegará una ventana donde nos dirigimos a Chain luego damos clic a la pestaña  y seleccionamos la opción input, luego en la sección de Protocol damos clic en la pestaña  y escogemos la opción (TCP), continuando nos centramos en Src. Address list y seleccionamos la lista que creamos recientemente Lista_Ngera, luego nos dirigimos a la pestaña Extra y en la opción Connection limit colocamos 10 por ip, continuando nos dirigimos a Action luego dando clic a la siguiente pestaña  seleccionamos la opción Tarpit colocamos Tarpit por que Tarpit nos permite mantener en suspender este ataque ya que al colocar drop se bloquea la conexión y como el ataque de DDoS es recurrente se vuelve a activar una vez que se bloqueó luego colocamos un comentario y damos OK.

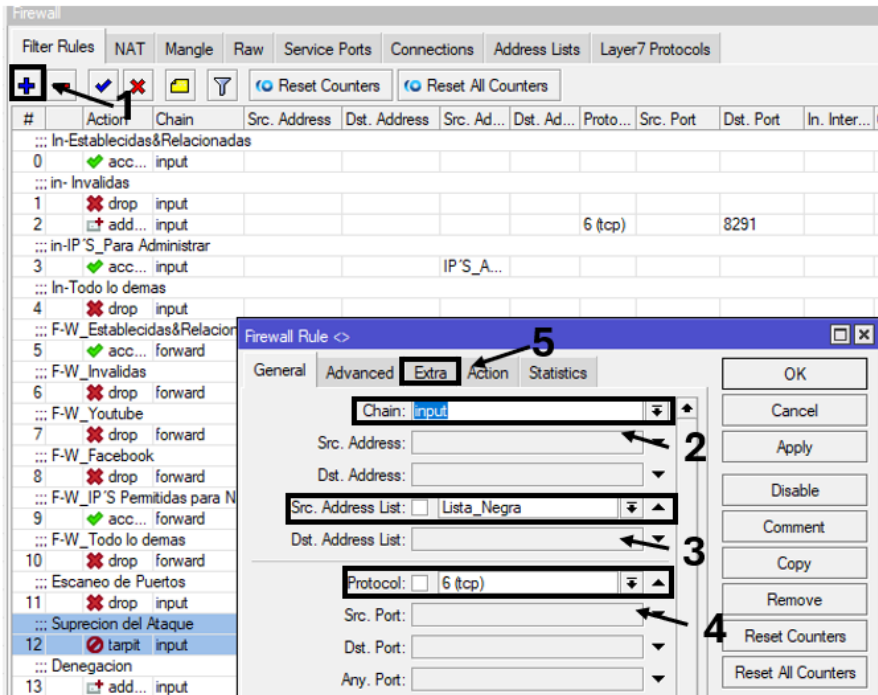


Figura 37. Nueva regla suspensión de ataques ddos
 Imagen elaborada por el autor

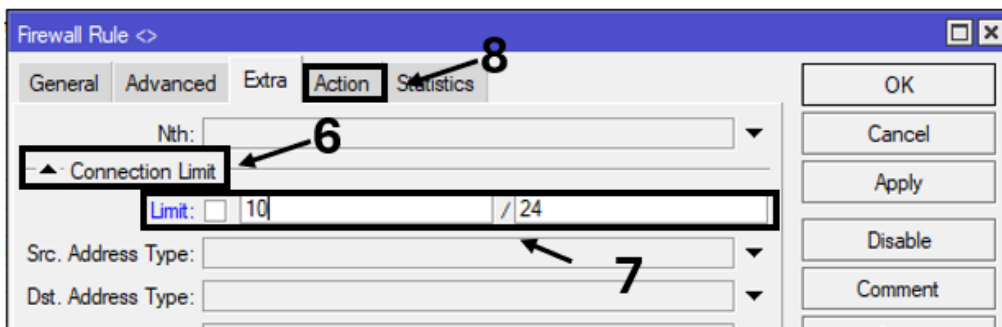


Figura 38. Establecer una conexión límite
 Imagen elaborada por el autor

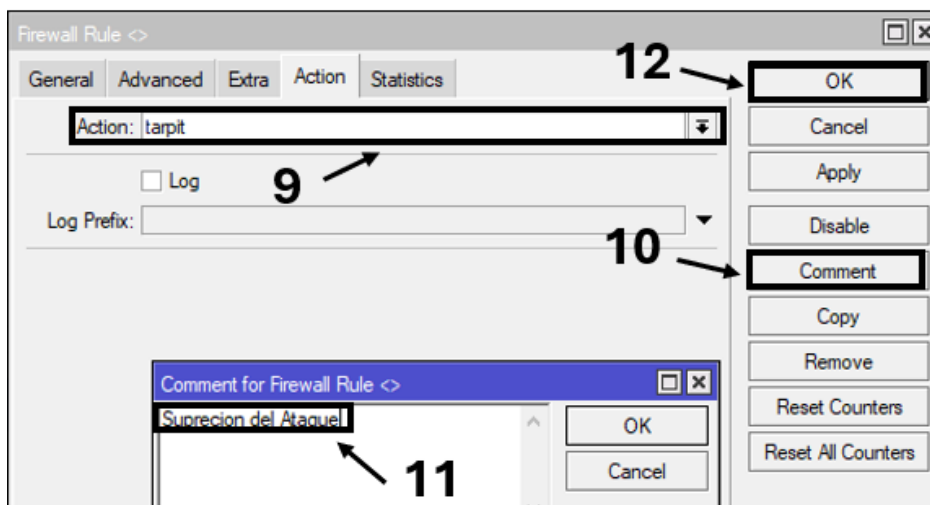


Figura 39. Colocar la opción tarpit y comentario
 Imagen elaborada por el autor

3.3 Prevención de ataques de ip spoofing

El IP Spoofing es una técnica empleada por atacantes para enviar paquetes de datos utilizando direcciones IP falsas, con el objetivo de ocultar su identidad real o suplantar a otro dispositivo en la red, para evitar este tipo de ataques en equipos MikroTik, se implementaron configuraciones específicas en el firewall y ajustes avanzados en la configuración del equipo, en primer lugar se desarrollaron dos reglas de firewall para mitigar intentos de IP Spoofing, una de estas reglas se encargó de filtrar los paquetes entrantes, permitiendo únicamente aquellos provenientes de usuarios legítimos, además, se realizaron ajustes avanzados en la sección IP Settings del dispositivo para reforzar la protección frente a este tipo de ataques, la validación de estas configuraciones se realizó simulando ataques de IP Spoofing mediante el uso de la herramienta hping3 en un entorno de prueba configurado en Kali Linux dentro de VirtualBox, generando tráfico malicioso, adicionalmente, se utilizó Wireshark para monitorear la red, analizando tanto los intentos iniciales de ataque como la efectividad de las reglas implementadas, comprobando su capacidad para prevenir este tipo de amenazas.

Para realizar la siguiente prevención de ataques primero los generamos mediante la ayuda de una máquina virtual que tenga instalado el sistema Operativo Kali Linux luego los ataques los generamos con los siguientes comandos explicados en los pasos 1-8 para entender un poco mejor se utilizó la siguiente topología de red entre un cliente y un atacante intentando ingresar al equipo y al servidor por defecto, para los ataques de SYN FLOOD este ataque aprovecha un enlace de 3 vías para establecer una conexión TCP, el ataque consiste en enviar una gran cantidad de segmentos TCP con el pronombre SYN habilitada y direcciones de origen falsos para abrir conexiones con un servidor (ver paso 4).

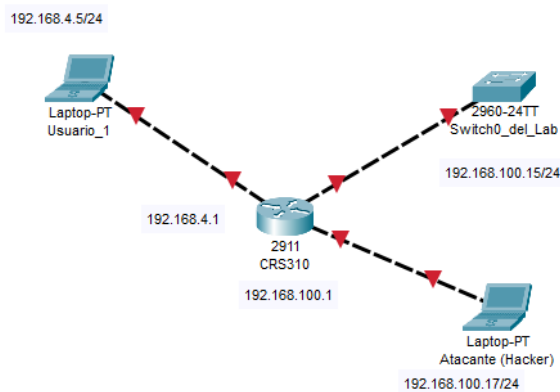


Figura 40. Topología de red para el ataque
Imagen elaborada por el autor

Paso 1: Para poder realizar los ataques de ip spoofing es necesario tener instalado una máquina virtual, y dentro de la máquina virtual debemos instalar el sistema operativo Kali Linux ya que este nos permitirá realizar los ataques de suplantación de ip al equipo, continuamos ingresando a Kali Linux y nos dirigimos al apartado de **settings**, luego daremos clic en la opción de **Advance Network Configuration**, se desplegara una ventana donde hacemos clic en **Wired conection1** continuando nos colocamos en la siguiente pestaña **IPV4 Settings**, hacemos clic en Add para agregar la siguiente dirección ip estática para poder acceder el router, **192.168.100.15**, en **Netmask** se coloca la máscara en este caso se coloca automáticamente como **/24**, en la casilla **Gateway** colocamos la ip con la que se conecta al equipo **192.168.100.1**, y por ultimo damos clic en **Save** para guardar la configuración, se procede reiniciar la máquina virtual para que ya parezcan los cambios realizados.

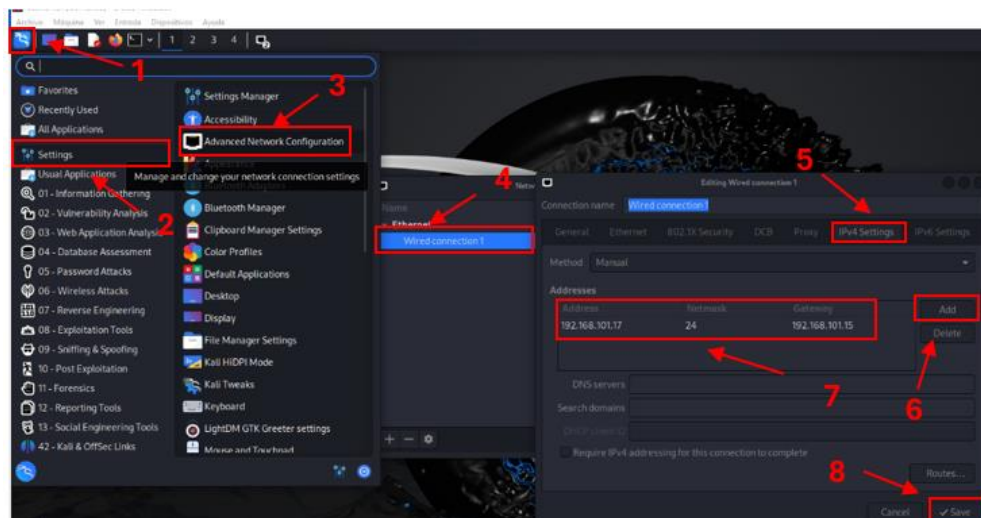
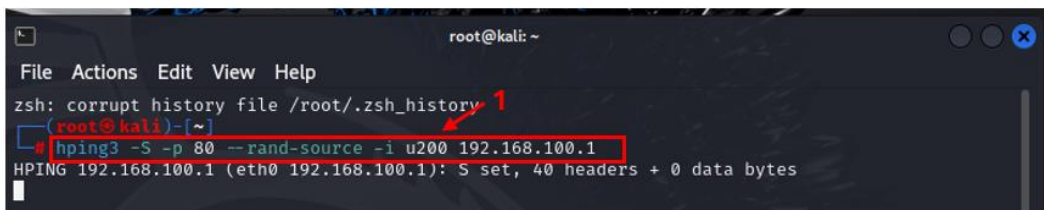


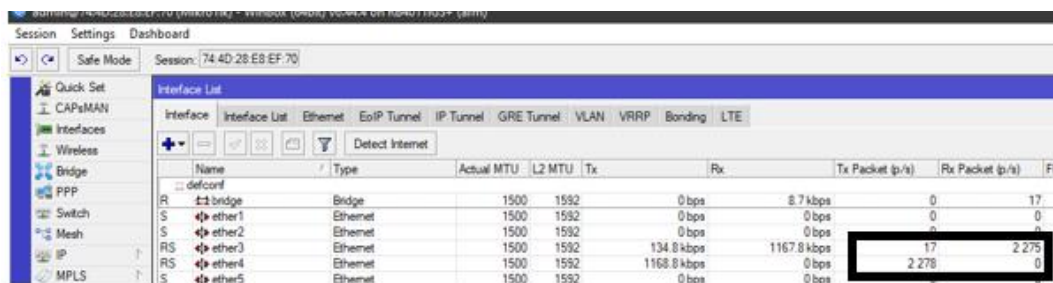
Figura 41. Ingresar los datos de red dentro de kali linux
Imagen elaborada por el autor

Paso 2: Para realizar la técnica del ip spoofing dentro de Kali Linux tenemos herramientas con las que nos podemos ayudar para generar estos tipos de ataques, ya que necesitamos una creación de paquetes de Ip, para esto dentro de Kali hacemos uso de la herramienta **hping3**, dentro del Kali accedemos al terminal root@kali y procedemos digitar un comando que nos ayudaran con el ataque **hping3 -S -p 80 --rand-source -i u200 192.168.100.1**, --rand-source: nos sirve para que los paquetes se envían con direcciones IP de origen aleatorias, • -p: Puerto de destino, X es el número de puerto, -S: la identificación del ataque SYN, -i: Es el Intervalo de tiempo en el que se envía cada paquete, como se puede observar en la siguiente imagen se digita el comando y directamente desde la computadora ingresando al winbox, podemos notar como existe una cantidad grande que se transmite que es de 2,278(p/s) y recibe paquetes 2,275(p/s), entre el puerto eth3, eth4.



*Figura 42. Ataque a servidor mediante hping3
Imagen elaborada por el autor*

hping3 es una herramienta dentro de Kali Linux de comandos en línea utilizada principalmente para realizar pruebas de redes y análisis de seguridad entre sus usos más principales encontramos pruebas de conectividad y rendimiento gestión de tráfico personalizado pruebas de seguridad en este caso la utilizamos para simular diversos ataques SYN flood estos ataques saturan un servidor con las soluciones TSPSYN también realiza escaneo de puertos con técnicas avanzadas similar a nmap.



*Figura 43. Ingreso de ip suplantas al equipo
Imagen elaborada por el autor*

Paso 3: Abrimos el Wireshark y escaneamos la interfaz de ethernet donde se pueden ver los ataques dirigidos al equipo como se observa en la siguiente imagen las direcciones ip suplantadas, los paquetes SYN que están siendo enviados al equipo, esto quiere decir que el ataque está funcionando correctamente.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	39.162.128.4	192.168.100.1	TCP	60	13520 → 80 [SYN] Seq=0 Win=512 Len=0
2	0.000256	99.254.77.100	192.168.100.1	TCP	60	13521 → 80 [SYN] Seq=0 Win=512 Len=0
3	0.000560	148.162.229.130	192.168.100.1	TCP	60	13522 → 80 [SYN] Seq=0 Win=512 Len=0
4	0.000806	78.65.97.161	192.168.100.1	TCP	60	13523 → 80 [SYN] Seq=0 Win=512 Len=0
5	0.001062	123.253.77.39	192.168.100.1	TCP	60	13524 → 80 [SYN] Seq=0 Win=512 Len=0
6	0.002058	106.245.212.149	192.168.100.1	TCP	60	13525 → 80 [SYN] Seq=0 Win=512 Len=0
7	0.002298	124.186.99.41	192.168.100.1	TCP	60	13526 → 80 [SYN] Seq=0 Win=512 Len=0
8	0.002544	188.224.115.250	192.168.100.1	TCP	60	13527 → 80 [SYN] Seq=0 Win=512 Len=0

*Figura 44. Visualización del tráfico en el servidor mediante wireshark
Imagen elaborada por el autor*

Paso 4: Desde otra computadora con la dirección IP 192.168.4.5, intentamos ingresar al equipo mediante el navegador web con la siguiente dirección IP 192.168.100.1, pero no hay acceso a la página por la negación, abrimos WireShark y nos dirigimos a analizar el ethernet donde podemos observar que se envía el paquete SYN, pero no se percibe que recibe el paquete SYN-ACK, Porque cada segmento SYN recibido, el servidor responde con un segmento SYN-ACK y genera una conexión a media abierta esperando un acuse de recibo por parte del cliente.

No.	Time	Source	Destination	Protocol	Length	Info
1322	71.784389	192.168.4.5	192.168.100.1	TCP	66	49816 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1325	72.034928	192.168.4.5	192.168.100.1	TCP	66	49817 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1342	72.784948	192.168.4.5	192.168.100.1	TCP	66	[TCP Retransmission] 49816 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 ...
1345	73.037344	192.168.4.5	192.168.100.1	TCP	66	[TCP Retransmission] 49817 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 ...
1380	74.792097	192.168.4.5	192.168.100.1	TCP	66	[TCP Retransmission] 49816 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 ...
1383	75.041869	192.168.4.5	192.168.100.1	TCP	66	[TCP Retransmission] 49817 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 ...
1458	78.793064	192.168.4.5	192.168.100.1	TCP	66	[TCP Retransmission] 49816 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 ...
1461	79.042265	192.168.4.5	192.168.100.1	TCP	66	[TCP Retransmission] 49817 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 ...

*Figura 45. Intento de conexión a la página web
Imagen elaborada por el autor*

Paso 5: Se hará otra prueba para demostrar que se puede acceder al servidor al usar una dirección de ip de suplantación, nos dirigimos la máquina virtual Kali Linux para enviar paquetes a la dirección ip origen 192.168.4.2 al puerto 80 de la dirección IP 192.168.100.1, para ello nos dirigimos a Root@Kali y se desplegará una ventana donde procedemos a colocar el siguiente comando **hping3 -S -p 80 -a 192.168.4.2 --fast 192.168.100.1**, luego damos enter, continuando nos dirigimos al winbox del equipo ingresamos y nos

colocamos en la pestaña de interfaces, donde podemos ver que la interfaz de eth3 recibe los paquetes y estos se transmiten en la otra interfaz eth4 esto nos indica que el equipo nos permite el acceso a los paquetes de ip suplantadas.

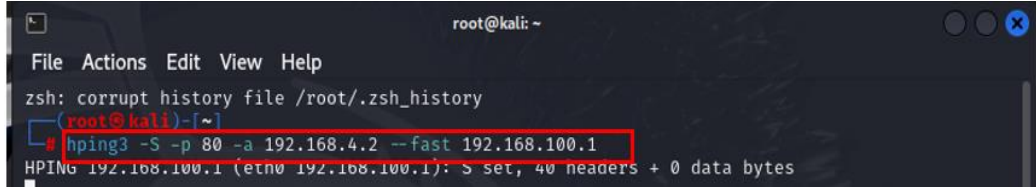


Figura 46. Ataque al servidor con una ip suplantada
 Imagen elaborada por el autor

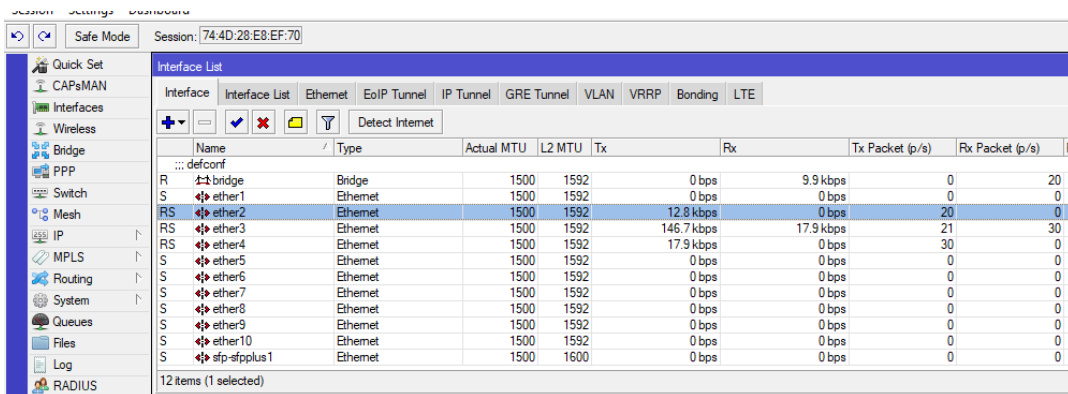


Figura 47. Monitoreo de la red
 Imagen elaborada por el autor

Paso 6: Para comprobar que están suplantando la direcciones IP abrimos el Wireshark para ver que ip ingresan al equipo una vez ingresamos al apartado de ethernet para examinar el puerto podemos observar las direcciones IP que ingresan al equipo por el puerto 80.

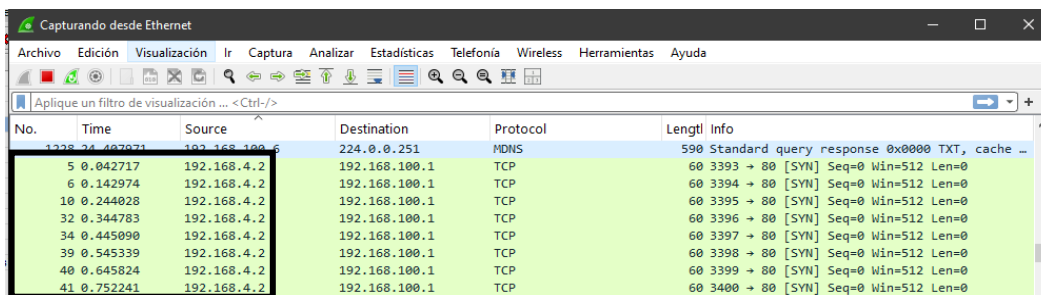


Figura 48. Monitoreo de la red ingreso de ip's suplantadas
 Imagen elaborada por el autor

Una vez comprendidos los conceptos de ataques a ahora nos dirigimos al equipo para prevenir estos ataques mediante reglas de firewall y el uso de IP Settings de la siguiente manera.

Paso7: Para prevenir los ataques de IP spoofing necesitamos colocar las siguientes reglas dentro del equipo para que no exista la suplantación de direcciones IP, comenzamos dirigiéndonos al equipo mediante winbox ingresamos con un usuario y contraseña, ya dentro del equipo nos dirigimos a la pestaña de IP y seleccionamos la pestaña de firewall donde se desplegara una ventana y damos clic en (+) nos abrirá una nueva ventana donde nos centramos en Chain damos clic y seleccionamos la opción de forward seguido en la pestaña de Advanced damos clic en la sección de **Src.Address List** y colocamos un nombre para identificar el ataque que recibe el equipo luego hacemos clic en la sección Action seguido de la misma sección damos clic y seleccionamos la opción drop por ultimo lo identificamos con un comentario para guardarlo con Ok.

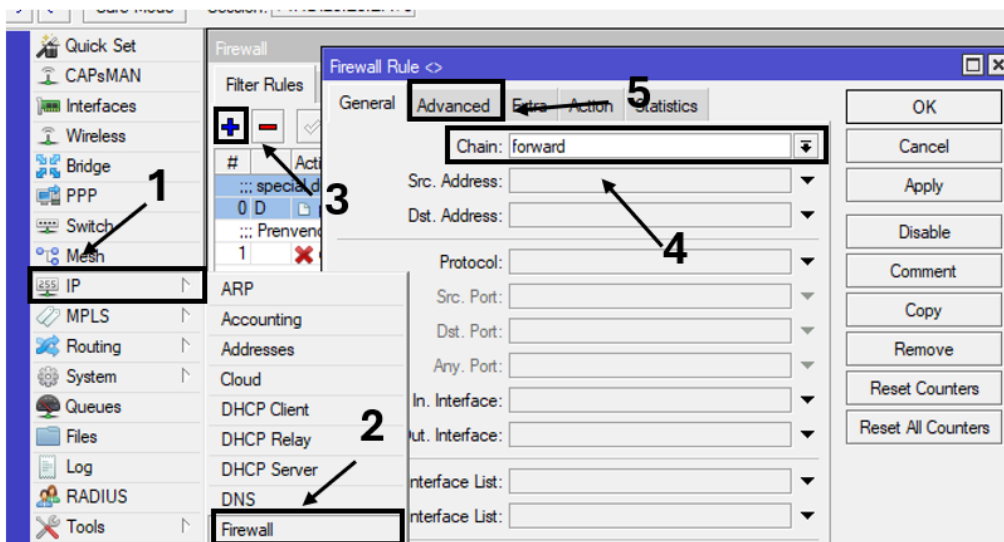


Figura 49. Nueva regla para evitar ataques syn flood
Imagen elaborada por el autor

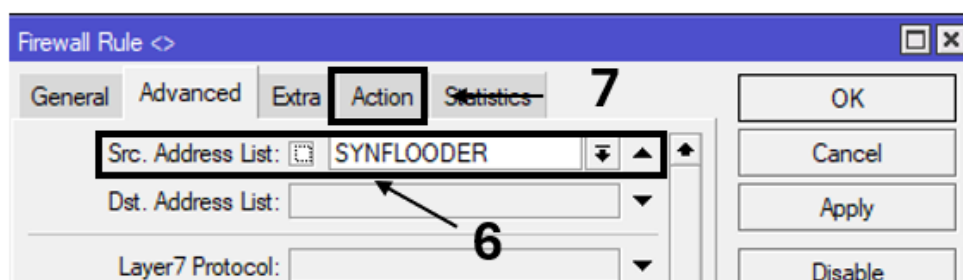
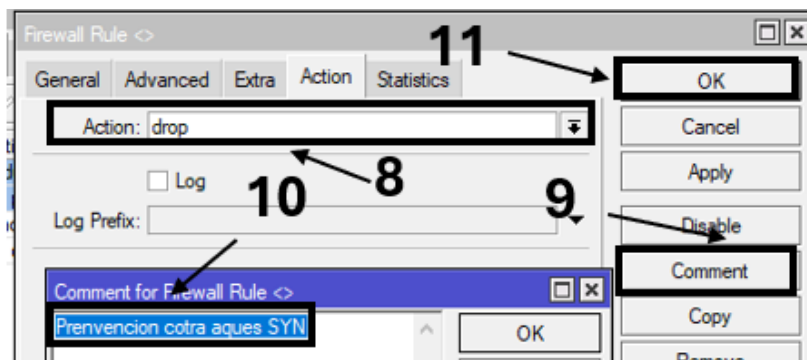


Figura 50. Agregamos la lista en la ventana advanced
Imagen elaborada por el autor



*Figura 51. Denegamos la regla
Imagen elaborada por el autor*

Paso 8: Continuando agregamos otra regla esta regla está destinada para realizar un filtrado de paquetes, determinando si los paquetes son TCP correspondientes a una nueva conexión, si ingresan de un misma IP y el número de quetes que se recibe de forma instantánea en un límite, al momento de que este límite se supere se agregara a una lista de bloqueo. Agregamos una nueva regala (+), damos clic en Chain y escogemos la opción de forward ya que los paquetes que ingresan deben estar dirigidos al equipo, luego el protocolo seleccionamos el TCP, en apartado de abajo la opción Connection State seleccionamos la casilla new, por lo que son conexiones nuevas, continuando damos clic en la pestaña de Extra nos centramos en la opción Connection Limitid donde establecemos el límite de paquetes SYN en esta caso 150, por último nos colocamos en la pestaña de Action y damos clic en la opción del mismo nombre y seleccionamos add src addres list, en la siguiente pestaña colocamos el Address lista nates creado y el opción de Timeout digitamos la numeración de un día y guardamos al dar clic en ok.

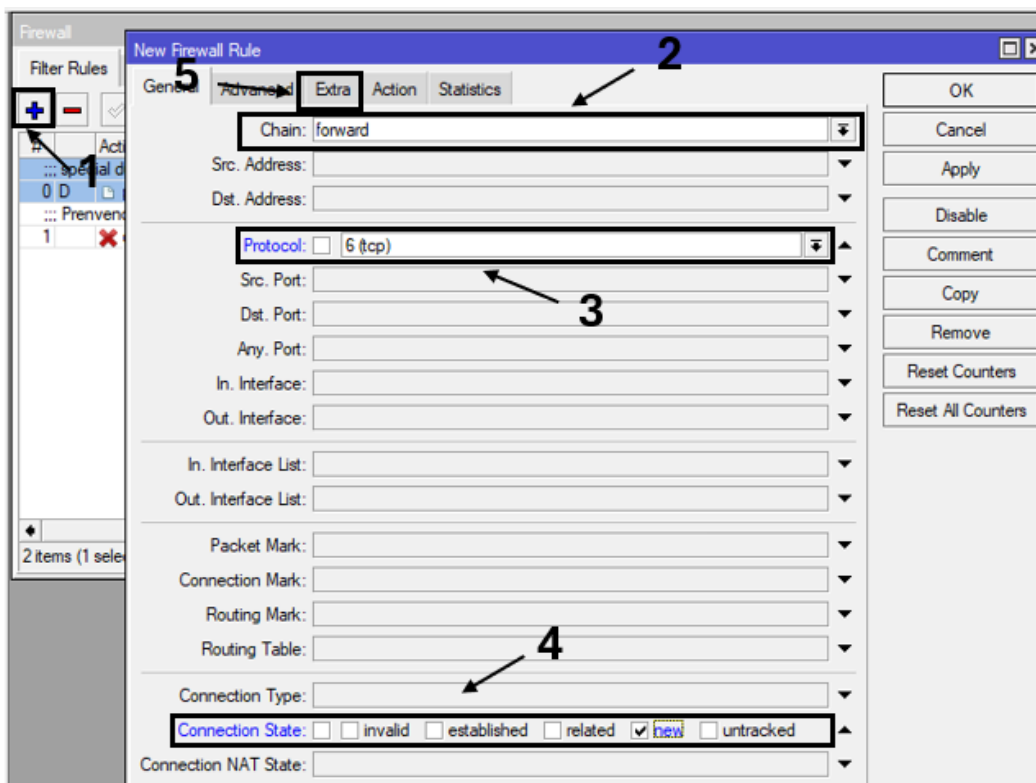


Figura 52. Segunda regla filtrado de paquetes
Imagen elaborada por el autor

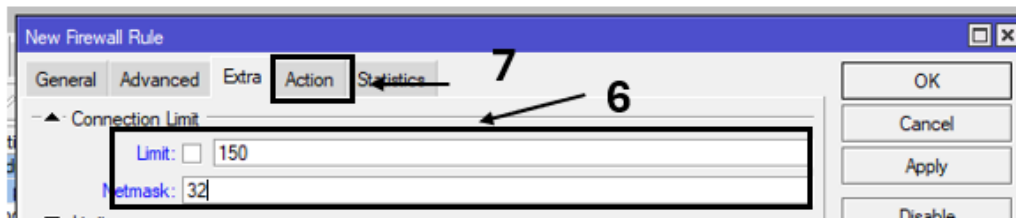


Figura 53. Establecer el límite de la conexión
Imagen elaborada por el autor

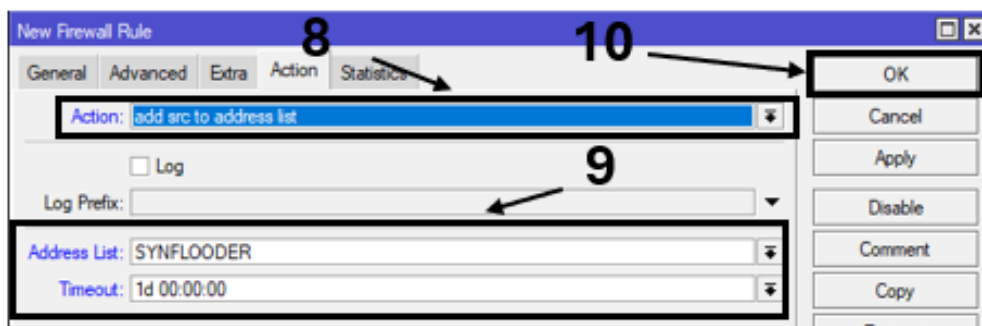


Figura 54. Selección de Acción de la regla
Imagen elaborada por el autor

Paso 9: Como último paso para prevenir los ataques utilizamos el Reverse Path Forwarding esta opción nos permite limitar el impacto sobre el uso del spoofing en los ataques DDoS, esta herramienta evita que el tráfico tome una vía de salida diferente a la vía que utilizo para el ingreso, en otras palabras si un usuario 1 se intenta comunicar con otro usuario 2 a través de la interfaz de usuario 1, la respuesta se deberá realizarse a través de la misma interfaz, caso contrario no se permitirá la conexión, dentro del winbox nos dirigimos a la pestaña IP y seleccionamos la opción **Settings**, se desplegará una ventana, donde seleccionaremos la opción IP Forward, luego Send Redirects, también Secure Redirects, y por último Allow Fast Path, al finalizar Route Cache, en la casilla de RP Filter seleccionamos la opción de strict por que seleccionamos la opción de strict, La IP de origen se verifica en la FIB (Forwarding Information Base), una tabla que almacena datos necesarios para el reenvío de paquetes. Además, se asegura que el paquete llegue a través de la misma interfaz que se emplearía para responder a esa IP específica, por últimos dejamos lo demás por defecto y damos en OK.

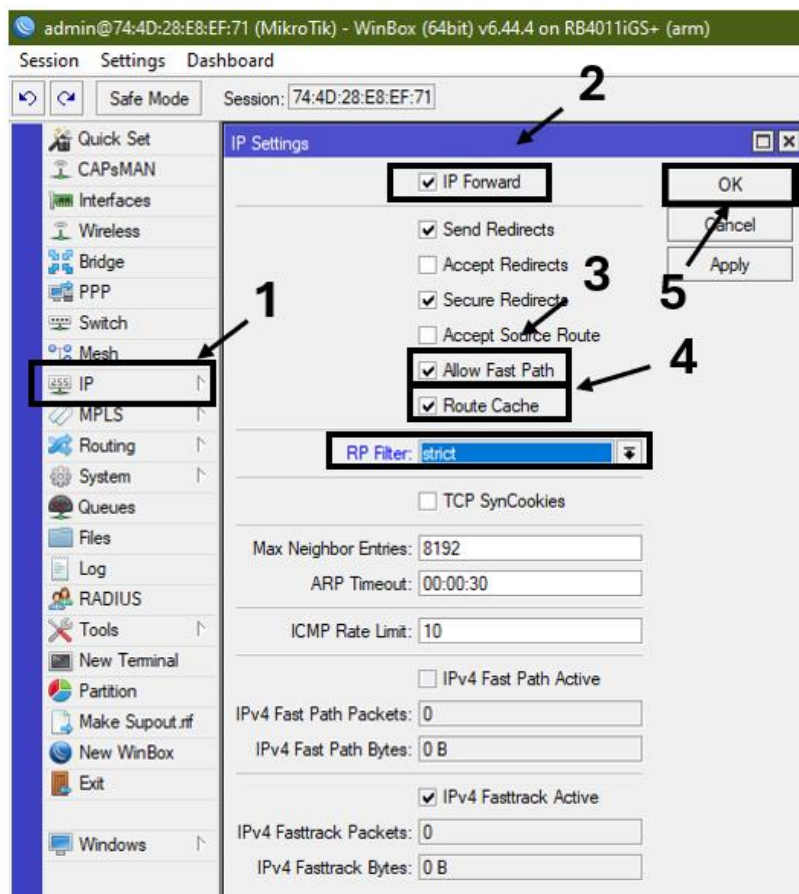


Figura 55. Configuración del filtro ip
Imagen elaborada por el autor

4. Capítulo 4

4.1 Resultados

4.1.1. Resultados de las reglas del firewall (address list)

Para comprobar que se puede acceder al equipo mediante la el Address List (**IP'S_PARA_ADMINISTRAR**) con la siguiente dirección IP: **192.168.2.0** para el acceso nos dirigimos dentro del equipo en el winbox accedemos al apartado de IP luego a Address damos clic (+) se desplegará un ventana donde agregamos la dirección ip:192.168.2.0 antes colocada en las reglas para administrar el equipo esto lo digitamos en la opción network, luego Address colocamos un dirección ip con el mismo dominio 192.168.2.5/24 y por ultimo seleccionamos la interface por el cual se pueda acceder para administrar el equipo de la siguiente manera.

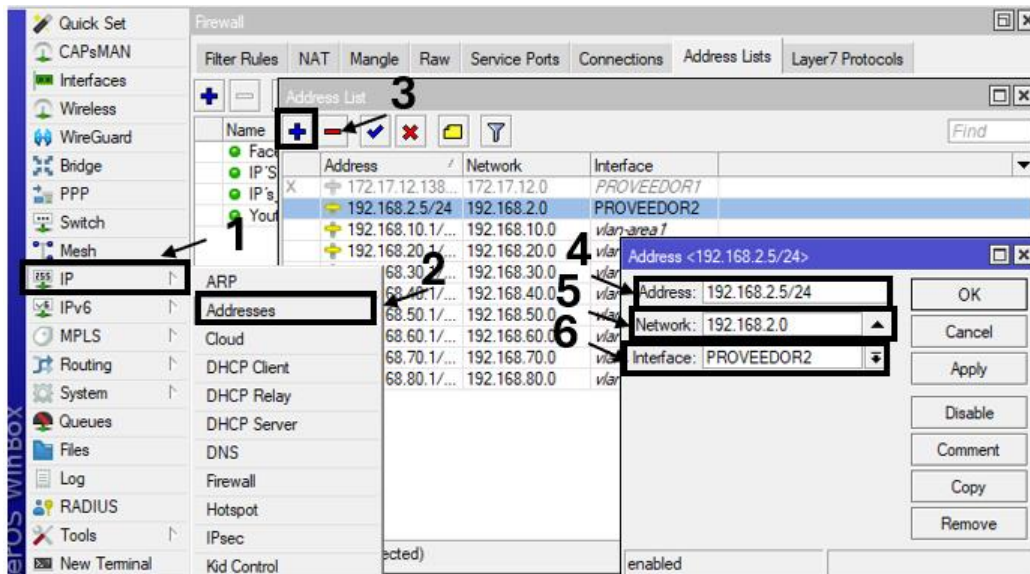
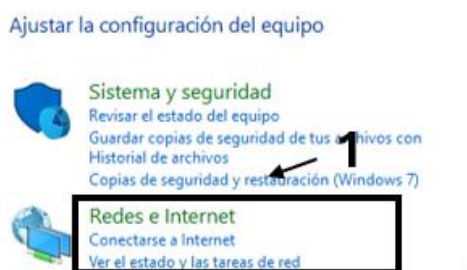


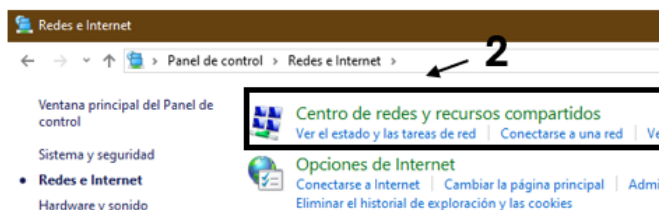
Figura 56. Configuración de ip para administrar el equipo
Imagen elaborada por el autor

Continuando con el acceso nos dirigimos al panel de control y damos clic en Redes e Internet, luego a centro de redes y recursos compartidos es aquí donde seleccionamos la red a las que estamos conectado en este cosa una red cableada Ethernet dando clic se despliega un ventana donde seleccionaremos la opción de detalles como siguiente damos doble clic en habilitar el protocolo de Internet versión 4(TCP/IPV4), se desplegara una ventana y daremos clic usar la siguiente dirección ip y ahí digitaremos con dirección ip entramos para administrar el equipo en este caso le damos la ip **192.168.2.7** automáticamente se colocara la máscara de subred y en la puerta de enlace

predeterminada colocamos la dirección del Address que anteriormente colocamos, luego desde la computadora con la dirección asignada en el panel de control nos dirigimos al winbox para verificar si tenemos acceso al equipo, seleccionamos la dirección ip para acceder y cómo podemos observar en la Figura 64 vemos que contamos con datos recibidos indicando que existe un ingreso al dar doble clic se mostrara una ventana donde daremos clic en la pestaña de **Statistics** donde podemos ver los Bytes y Packets recibidos indicando un acceso correcto, para probar de otra forma en la parte de Firewall del equipo nos dirigimos al Address List y desactivamos la opción de IP'S_ADMINISTRACION, cerramos y abrimos otro winbox para ingresar mediante la dirección ip del equipo y cómo podemos observar no nos da acceso.



*Figura 57. Ingreso a las redes e internet
Imagen elaborada por el autor*



*Figura 58. Selección del recurso del centro de redes
Imagen elaborada por el autor*

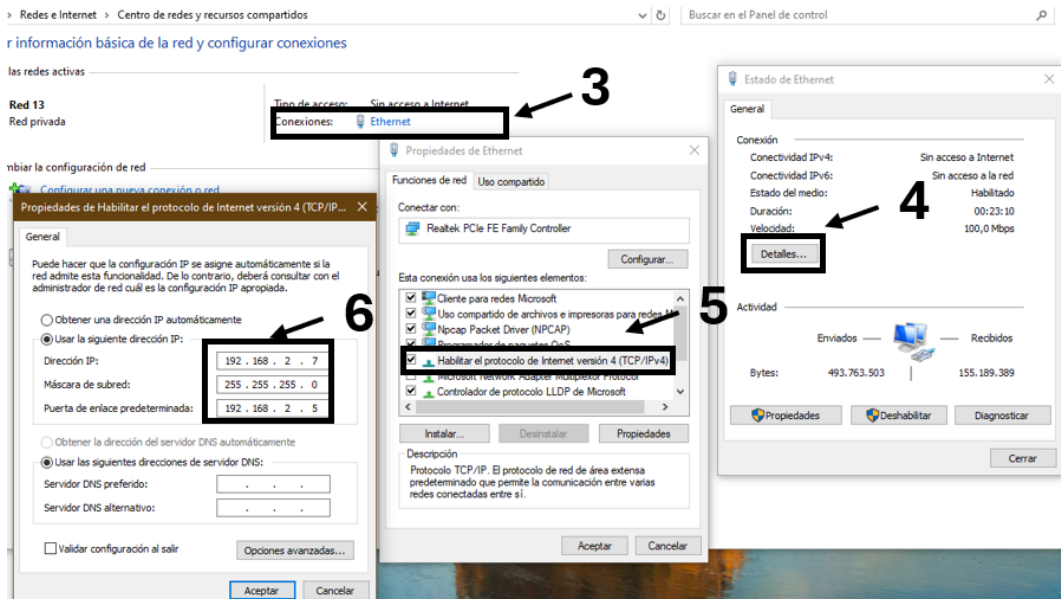


Figura 59. Agregamos la dirección ip manualmente
Imagen elaborada por el autor

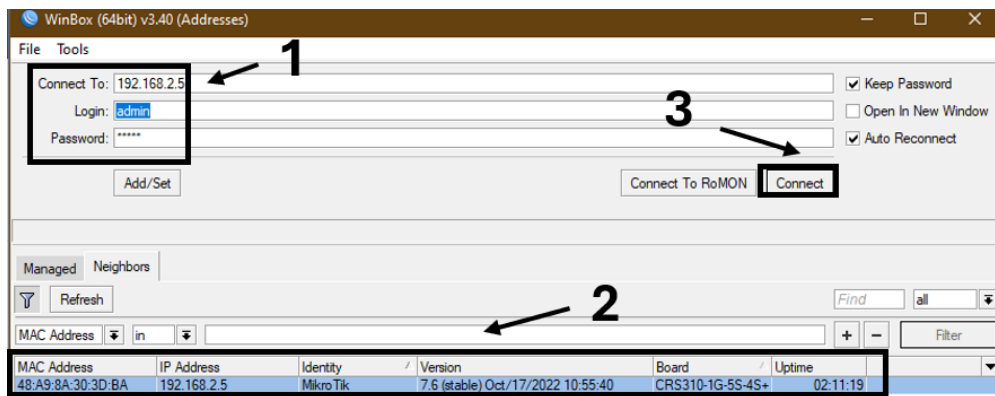


Figura 60. Ingreso al equipo mediante winbox
Imagen elaborada por el autor

Como podemos observar ingresan paquetes lo que significa que el acceso fue exitoso.

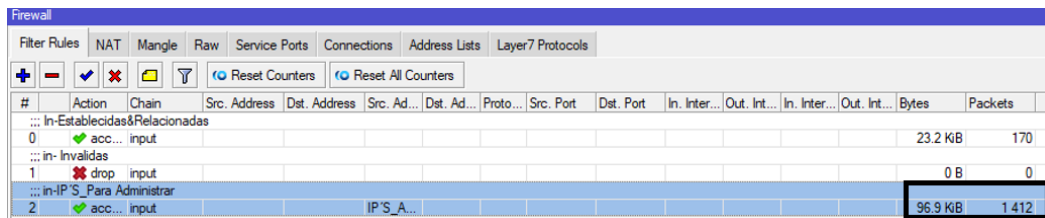


Figura 61. Ingreso de paquetes señal de acceso correcto
Imagen elaborada por el autor

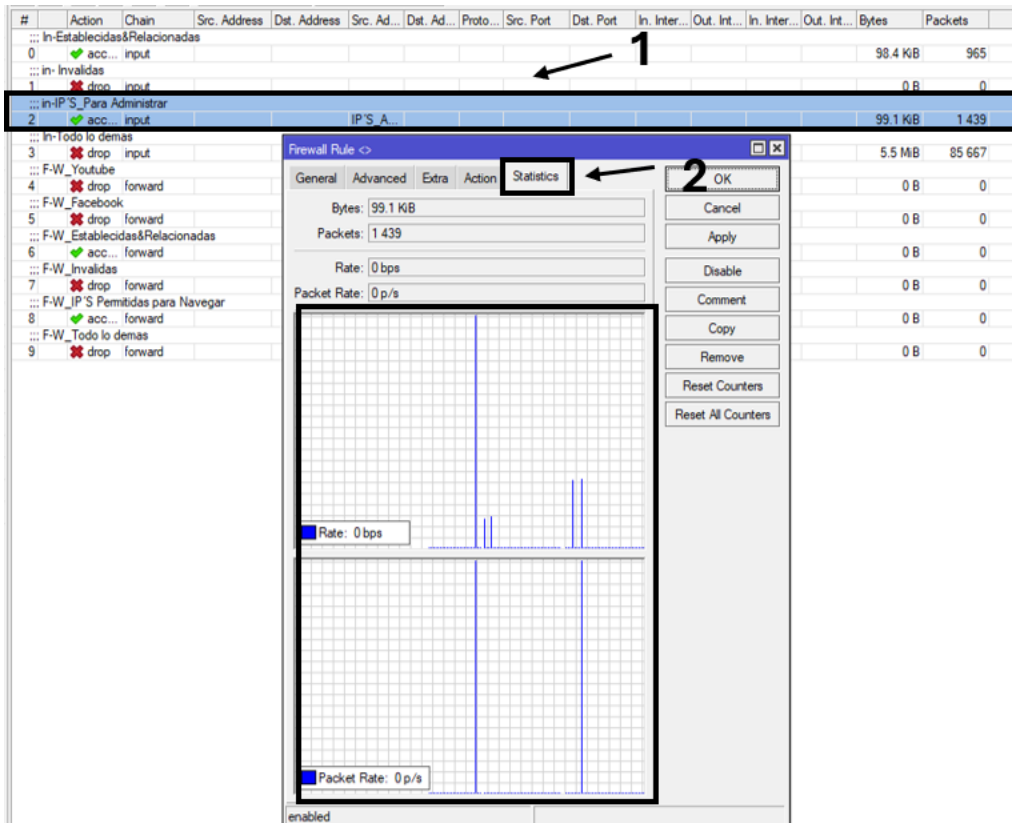


Figura 62. Resultados de la ventana statics
Imagen elaborada por el autor

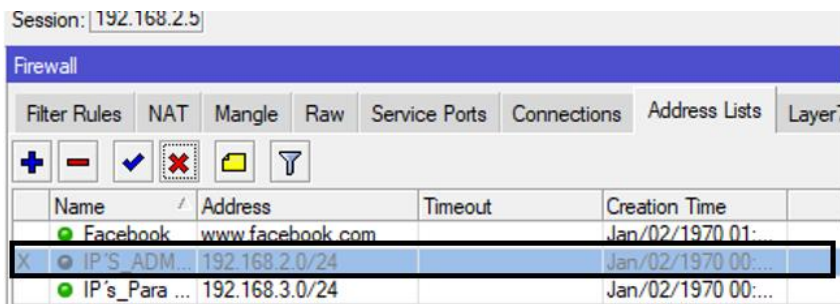


Figura 63. Desactivamos la opción del addressList
Imagen elaborada por el autor

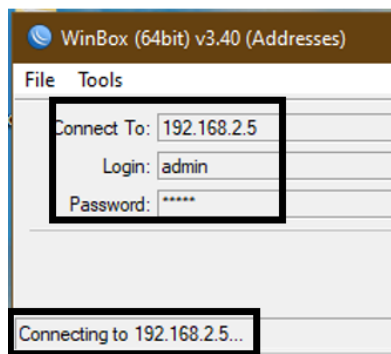


Figura 64. Ingreso al equipo fallido
Imagen elaborada por el autor

4.1.2. Resultados de las demás reglas de firewall

Para la comprobación de las **IP'S_Para_Navegar**, nos dirigimos al panel de control para colocar por defecto el DHCP, ya que el equipo nos una ip automáticamente sin necesidad de colocar una dirección estática, antes de poder confirmar la navegación colocamos los DNS que nos brinda nuestro proveedor en este caso 9.9.9.9, 1.1.1.1, 8.8.4.4, 1 procedemos a ingresar a YouTube para demostrar conectividad, en tora ventana abrimos el winbox para ver la regla dentro del firewall y cómo podemos observar cuenta con envío bytes y paquetes, otra manera de verificar que funcione es desactivando la opción de **IP'S_Para_Navegar** dentro del Address List, una vez desactivada ingresamos nuevamente y podemos observar que no tenemos registro de Bytes y Packets esto quiere decir que la regla está cumpliendo con su función.

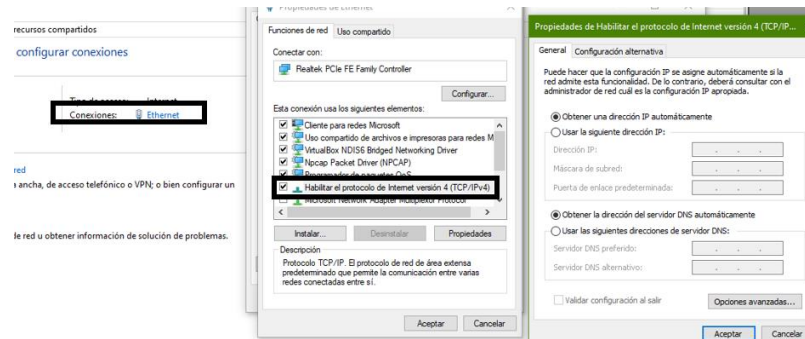


Figura 65. DHCP automático
Imagen elaborada por el autor

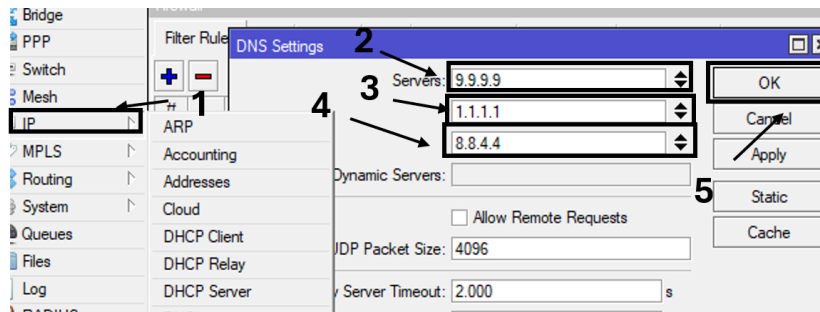


Figura 66. Insertamos las dns
Imagen elaborada por el autor

#	Action	Chain	Src. Address	Dst. Address	Proto	Src. Port	Dst. Port	In. Inter...	Out. Int...	In. Inter...	Out. Int...	Src. Address List	Dst. Ad...	Bytes	Packets
0	acc...	input												0 B	0
1	drop	input												0 B	0
2	acc...	input										IP'S_ADMINISTRACION		0 B	0
3	drop	input												366 B	5
4	acc...	forward												0 B	0
5	drop	forward												0 B	0
6	acc...	forward										IP'S_Para Navegar		0 B	0
7	drop	forward												0 B	0

Figura 67. Estadística de la regla ip's permitidas para navegar
Imagen elaborada por el autor

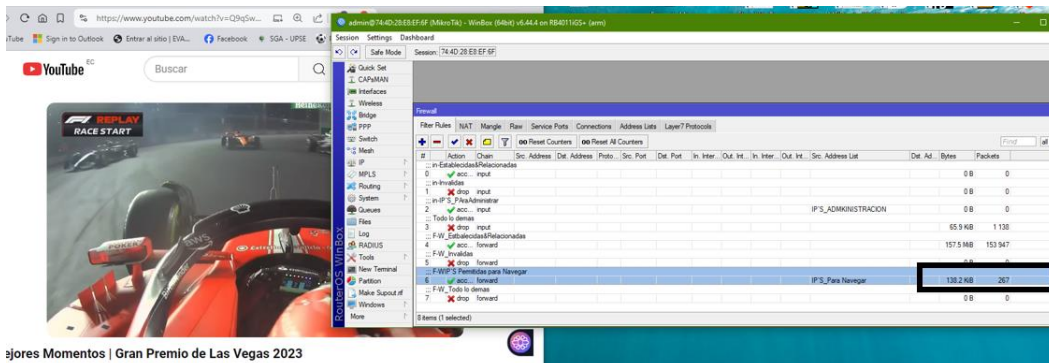


Figura 68. ingreso de paquetes, acceso para navegar
Imagen elaborada por el autor

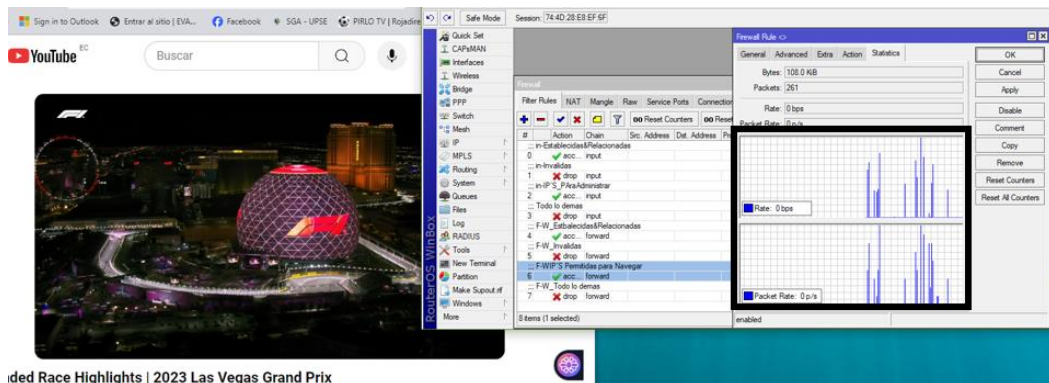


Figura 69. Envio y Recibo de paquetes de Navegación
Imagen elaborada por el autor

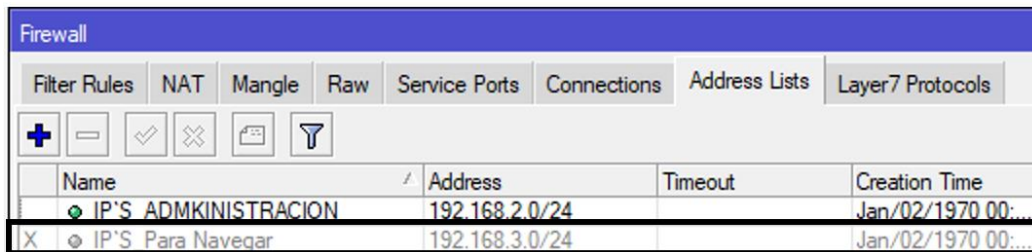


Figura 70. Desactivamos las ip's de Navegación
Imagen elaborada por el autor

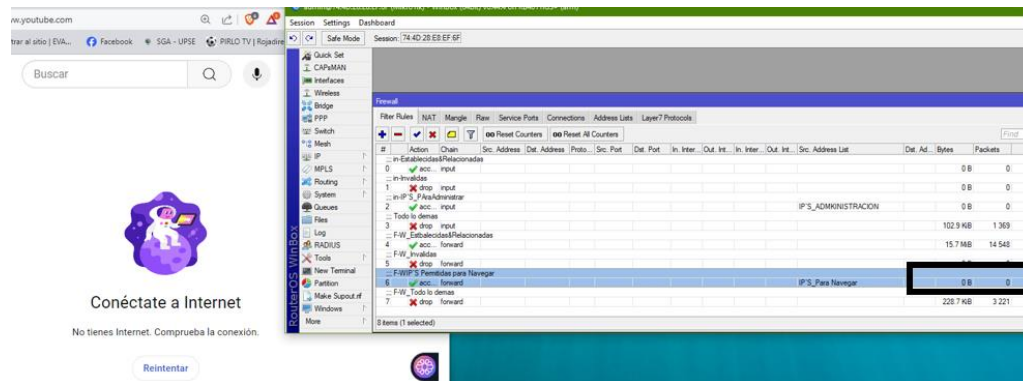


Figura 71. No se observan el ingreso paquetes, no existe conexión
Imagen elaborada por el autor

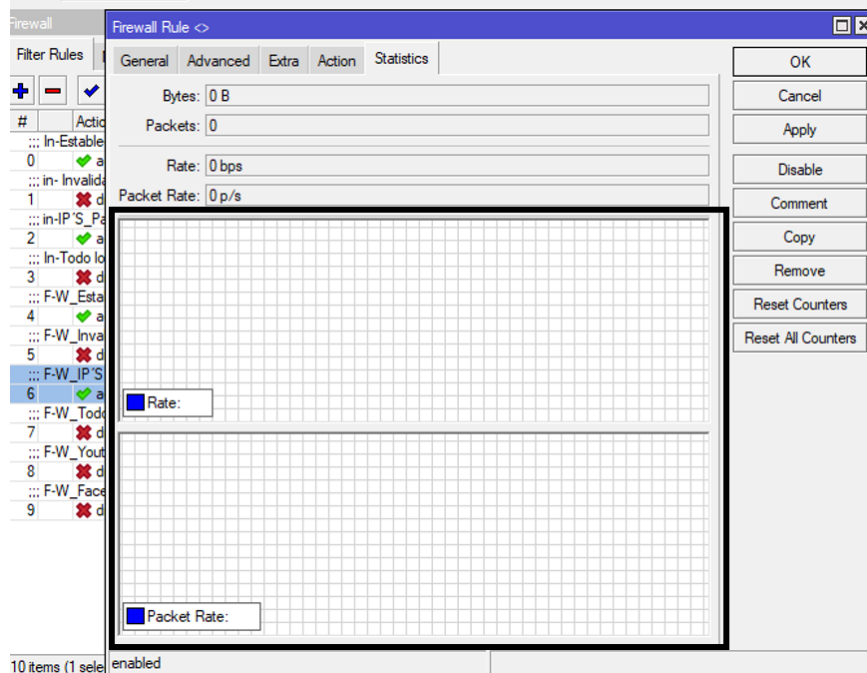


Figura 72. Ventana de estadísticas de la ip para navegar
 Imagen elaborada por el autor

4.1.3. Resultados de ataques de ddos

Para poder demostrar que el equipo está recibiendo ataques de denegación de servicio (DDoS), procedemos a descargar una herramienta que nos ayuda a enviar paquetes al equipo, esta herramienta se llama **Fastream Web Stress**, una vez descargada la abrimos como primer paso en el apartado de **url** colocamos la dirección Ip del router **192.168.2.5**, en la opción **Threads** colocamos un valor de 30 y más abajo la opción de **Clients per Thread** le damos un valor de 10 y por ultimo damos clic en **Run** para empezar con el ataque donde podemos observar que claramente se activa la regla en el apartado de **Bytes** y **Packets** también observando el estado del CPU que se encuentra en un **2%** demostrando que correctamente está funcionando la prevención de los ataques, en la sección de **Hits/sec** vemos que se encuentra en 0 esto quiere decir que no está enviado paquetes al equipo, al momento de desactivar la regla y comenzar de nuevo con el envío de paquetes en la herramienta, podemos observar un aumento en la CPU del **55%** dentro del winbox y en la herramienta en la sección de **Hits/sec** podemos ver el valor de 459 que el número de paquetes que ingresan al equipo cuando la regla se encuentra desactivada.

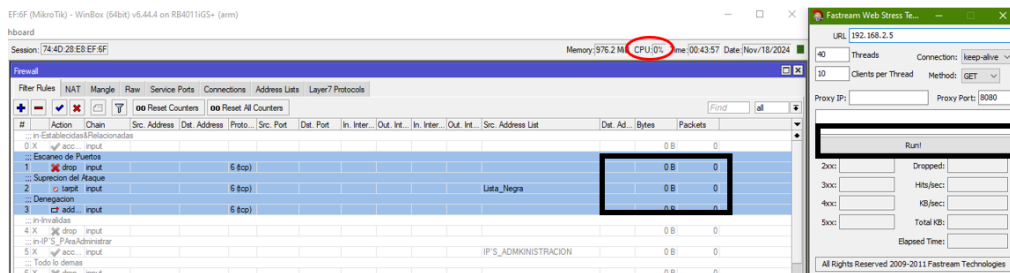


Figura 73. Estadísticas de los packets y bytes antes de empezar el DDoS attack
Imagen elaborada por el autor

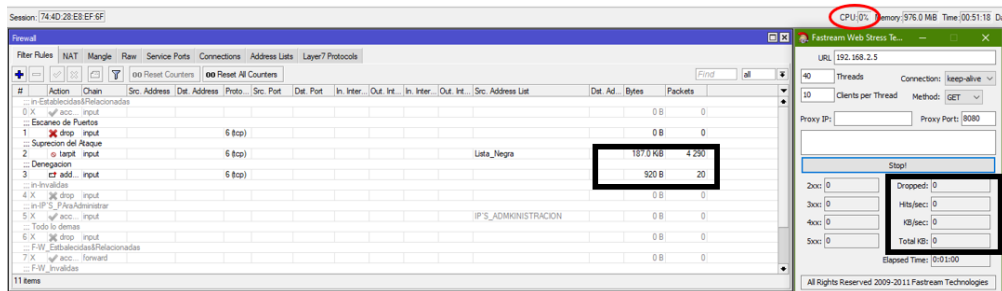


Figura 74. Ataque evadido correctamente
Imagen elaborada por el autor

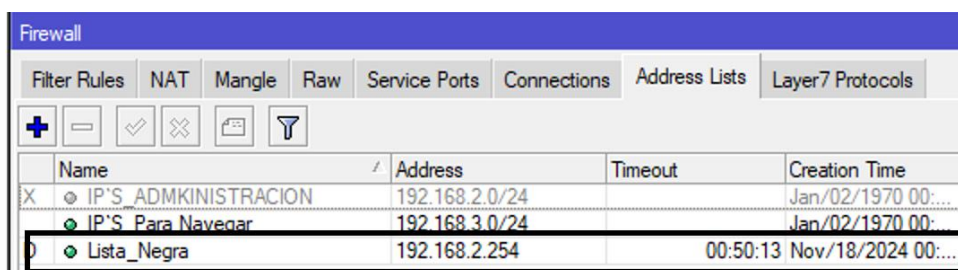


Figura 75. Activación de la lista de Ip's del ataque
Imagen elaborada por el autor

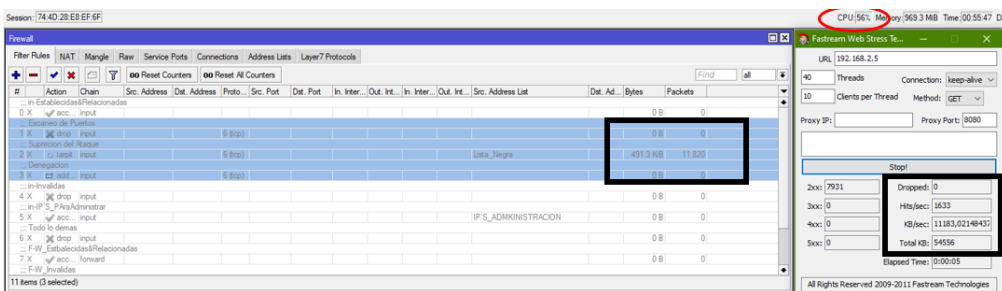
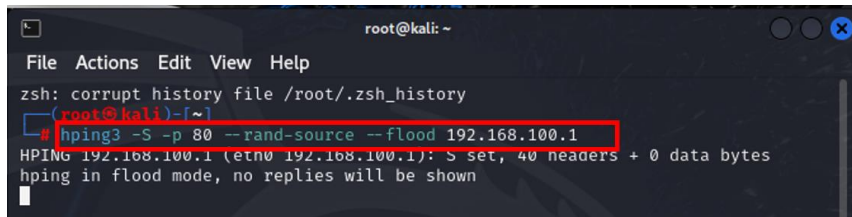


Figura 76. Ingreso del ataque al desactivar las reglas
Imagen elaborada por el autor

4.1.4. Resultados de los ataques de ip spoofing

Comenzamos realizando 2 pruebas, para esta primera prueba utilizaremos dentro del equipo las configuraciones ya realizadas para mitigar estos ataques mediante el Firewall, además usamos el Reverse Path Forwarding, el equipo contesta a las solicitudes de conexión, se contrarresta el spoofing y por consiguiente se reduce el ataque SYN FLOOD.

Para comenzar nos dirigimos a nuestra máquina virtual y abrimos el Kali Linux para realizar el ataque SYN FLOOD que genera paquetes con ips aleatorias al puerto 80 de la siguiente dirección ip **192.168.100.1** la velocidad que se transmite es la máxima posible y varía dependiendo del tiempo, abrimos el terminal y nos colocamos en la terminal de ROOT@KALI, luego digitamos el siguiente comando **hping3 -S -p 80 --rand-source --flood 192.168.100.1**, una vez realizado el ataque procedemos a ingresar la winbox, una vez ingresados nos dirigimos a la pestaña de interfaces donde se puede observar el monitoreo de las interfaces del equipo al dar clic en la ventana interfaces List podemos observar que la interfaz ethernet 3 recibe los paquetes con una velocidad de 49453(p/s) los mismos no se transmiten por la interfaz ethernet 4, esto nos confirma que el equipo descarta los paquetes de ip suplantadas.



*Figura 77. Comando para los ataques syn
Imagen elaborada por el autor*

Interface	Type	MTU	Actual MTU	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)
ether1	Ethernet	1500	1500	1592	0 bps	0 bps	0	0
ether2	Ethernet	1500	1500	1592	0 bps	0 bps	0	0
ether3	Ethernet	1500	1500	1592	220.2 kbps	25.3 Mbps	25	49 453
ether4	Ethernet	1500	1500	1592	16.5 kbps	512 bps	24	1
ether5	Ethernet	1500	1500	1592	0 bps	0 bps	0	0
ether6	Ethernet	1500	1500	1592	0 bps	0 bps	0	0

*Figura 78. Paquetes que ingresan al servidor dentro del equipo
Imagen elaborada por el autor*

Name	Address	Timeout	Creation Time
SYNFLOODER	192.168.4.5	23:59:55	Dec/02/2024 09:...

*Figura 79. Activación de la regla synflooder
Imagen elaborada por el autor*

Para realizar otra comprobación nos dirigimos a Wireshark y desde una computadora con la dirección ip 192.168.4.5 intentamos acceder al equipo mediante un navegador web de preferencia, y se puede evidenciar como se establece la conexión de forma correcta en la siguiente imagen se verifican los paquetes que conforman el enlace de 3 vías.

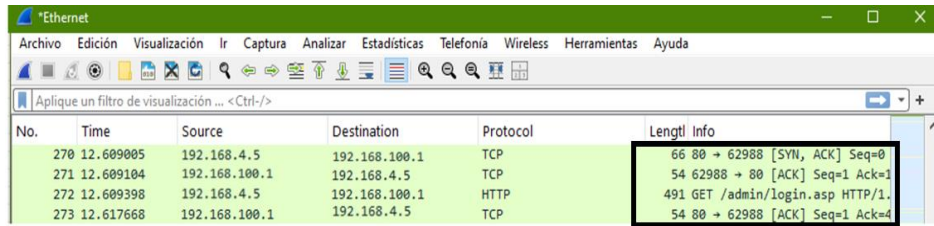


Figura 80. Acceso al servicio web
Imagen elaborada por el autor

Para la segunda prueba comprobaremos que mediante el uso del Reverse Path Forwarding el atacante no podrá conectarse al equipo con una dirección ip suplantada, desde el mismo terminal de root@Kali enviamos paquetes con la siguiente dirección ip suplantada en el terminal digitamos el siguiente comando **hping3 -S -p 80 -a 192.168.4.4 -fast 192.168.100.1**, luego nos dirigimos al winbox del equipo y damos clic a interfaces para monitorear, donde observamos que la interfaz ethernet 3 recibe los paquetes y estos no se transmiten por la interfaz ethernet 4 lo que nos da como resultado que el equipo no permitirá más el paso de paquetes con Ip de suplantación, por ultimo nos dirigimos a Wireshark, procedemos a captura Ethernet y observamos la interfaz de ethernet que no ingresan los paquetes a través del equipo.

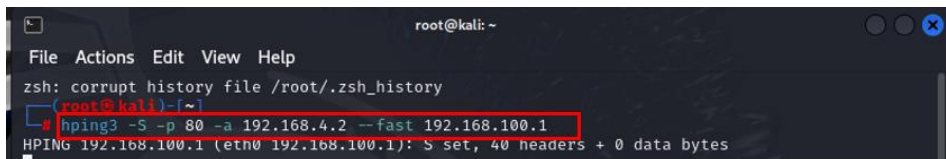


Figura 81. Envío de IP'S Suplantadas hacia el servidor
Imagen elaborada por el autor

Name	Type	MTU	Actual MTU	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)
S ether1	Ethernet	1500	1500	1592	0 bps	0 bps	0	0
S ether2	Ethernet	1500	1500	1592	0 bps	0 bps	0	0
RS ether3	Ethernet	1500	1500	1592	232.7 kbps	22.1 kbps	27	36
RS ether4	Ethernet	1500	1500	1592	0 bps	0 bps	0	0
S ether5	Ethernet	1500	1500	1592	0 bps	0 bps	0	0

Figura 82. Estadísticas de la Interfaz por donde pasa el ataque ya mitigado
Imagen elaborada por el autor

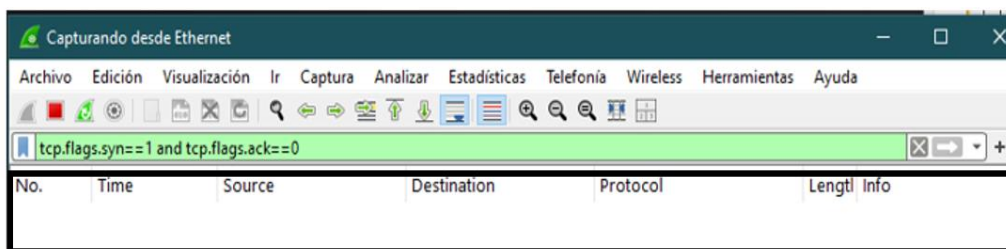


Figura 83. Se filtran los paquetes, no se encuentran ingresando
Imagen elaborada por el autor

4.2 Conclusiones

- Las configuraciones del firewall en los equipos MikroTik mejoró la seguridad en redes con acceso a internet, previniendo accesos no autorizados y protegiendo así la red contra diversas amenazas.
- Se implementaron reglas específicas en las cadenas input y forward para gestionar el tráfico autorizado y bloquear accesos no permitidos, estas configuraciones garantizaron que el tráfico legítimo tuviera continuidad mientras se rechazaron conexiones inválidas y no autorizadas, las pruebas realizadas confirmaron una efectividad del 90% en la restricción de accesos no autorizados al sistema mediante la lista de direcciones IP configuradas.
- Las reglas diseñadas para mitigar ataques DoS y DDoS demostraron ser altamente efectivas, durante las simulaciones con una herramienta especializada, como *Fastream Web Stress*, se evidenció que las medidas implementadas limitaron el impacto del ataque, con las reglas activadas, el uso del CPU se mantuvo en un 2%, mientras que al desactivarlas el consumo ascendió al 55%, además, los *hits/sec* se redujeron de 459 a 0, confirmando que los paquetes maliciosos no alcanzaron el equipo.
- La configuración del *Reverse Path Forwarding* y las reglas avanzadas de firewall bloquearon eficazmente intentos de suplantación de identidad IP, durante las pruebas de ataques SYN Flood generados con *hping3* desde un entorno simulado en Kali Linux, se verificó que los paquetes maliciosos no eran reenviados entre las interfaces del equipo, validando un bloqueo del 100% de este tipo de tráfico, el monitoreo con Wireshark corroboró la ausencia de paquetes no deseados.
- Se elaboraron cuatro guías con éxito, diseñadas para mejorar el aprendizaje de estudiantes en configuraciones avanzadas de redes y dispositivos MikroTik, recalcando conceptos clave como reglas de firewall, protocolos de conexión y optimización de recursos.

4.3 Recomendaciones

- En las configuraciones del firewall siempre se debe de tener un orden y tener comentada cada regla, ya que al no tener algún comentario podríamos deshabilitarla y que la misma no funcione correctamente, el orden de las reglas es primordial ya que el equipo analiza las reglas desde principio a fin, al momento que ingresa el tráfico el equipo compara cada regla en el orden que están establecidas después que la regla coincide con el tráfico se aplica la acción que se define en permitir o denegar y por ende no se evalúan el resto de las reglas.
- Para las reglas del firewall se recomienda realizar un listado de las direcciones IP que se van a permitir para navegar, para acceder al equipo y hasta para poder bloquear el ingreso a por los protocolos SSH, telnet y el más conocido el puerto 80.
- Tener previo conocimiento en redes de datos para poder realizar las configuraciones IP en una red de área local, se recomienda investigar a profundidad acerca de las herramientas que tienen los equipos MikroTik.
- Para poder instalar una máquina virtual se recomienda tener un mínimo de 80 GB apartados para el sistema operativo que deseamos utilizar en este caso Kali Linux.
- Para entender un poco más sobre los ataques de IP Spoofing dentro de Kali Linux es recomendable saber hacia dónde dirigimos el ataque teniendo en cuenta los comandos para realizarlo, porque de lo contrario podríamos hacer un mal uso de esta herramienta y afectar a un servidor con el ataque mencionado.
- Este proyecto trata de concientizar al estudiante sobre el uso de las reglas del firewall y los ataques denegación de servicio y de suplantación de identidad es por esto que este material tanto nos ayuda a prevenir estos ataques cómo también nos ayuda a generarlo en el sentido del uso de una máquina virtual teniendo instalado Kali Linux esta es una herramienta para realizar escaneos de vulnerabilidades, analizadores de redes e instrucciones en la red, por ende se trató de realizar un ataque hacia un servidor y también cómo contrarrestar dicho ataque.

Hoja de Guías Prácticas

Practica N°1

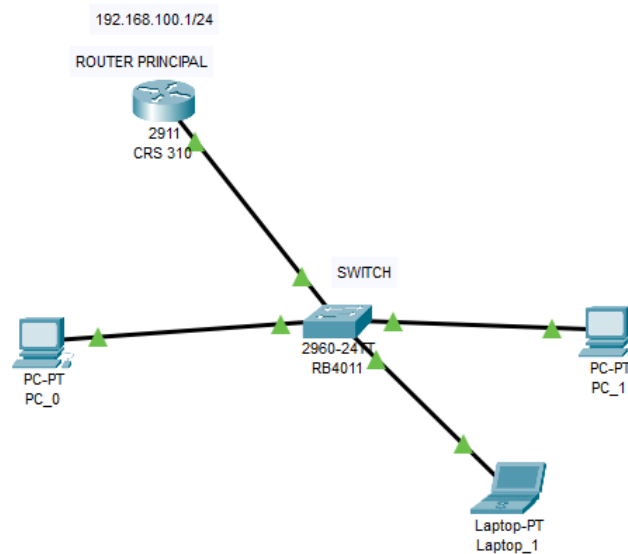
Tema: Acceso a Internet

Objetivo: Configuración de acceso a internet a router MikroTik

Objetivos específicos:

- Diseño de una topología de red que incluya routers, switches MikroTik.
- Ingresar desde winbox y borrar la configuración predeterminada.
- Crear un usuario y contraseña para el acceso al equipo
- Configurar las interfaces LAN Y WAN en nuestro equipo.
- Habilitar un cliente DHCP en la interfaz WAN
- Crear la red local en la interfaz LAN
- Configurar un servidor DHCP en la interfaz LAN
- Crear una regla NAT para acceso a Internet.

Topología implementada



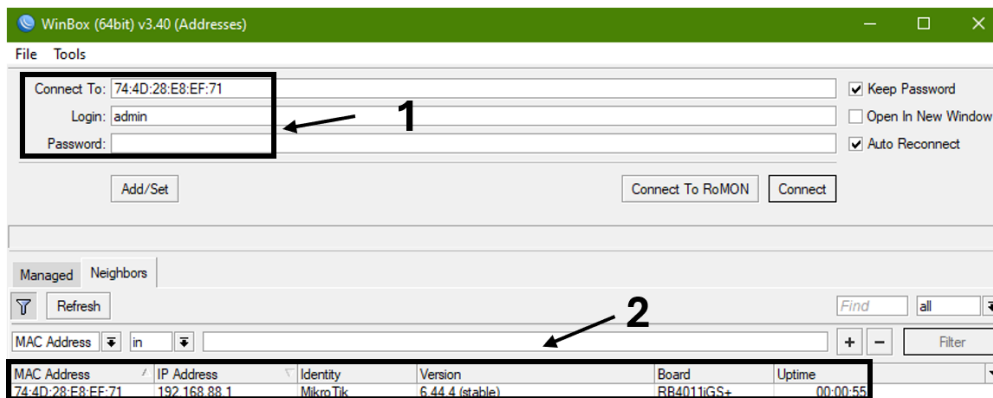
*Figura 84. Topología de Red Acceso a Internet
Imagen elaborada por el autor*

Configuración dentro de la interfaz grafica

Acceder al router

Para comenzar primero debemos tener descargado el software de MikroTik para ello nos dirigimos a la página www.mikrotik.com dentro de la página de MikroTik nos dirigimos a la pestaña de downloads para poder descargar el software seleccionamos el Winbox que tenga el

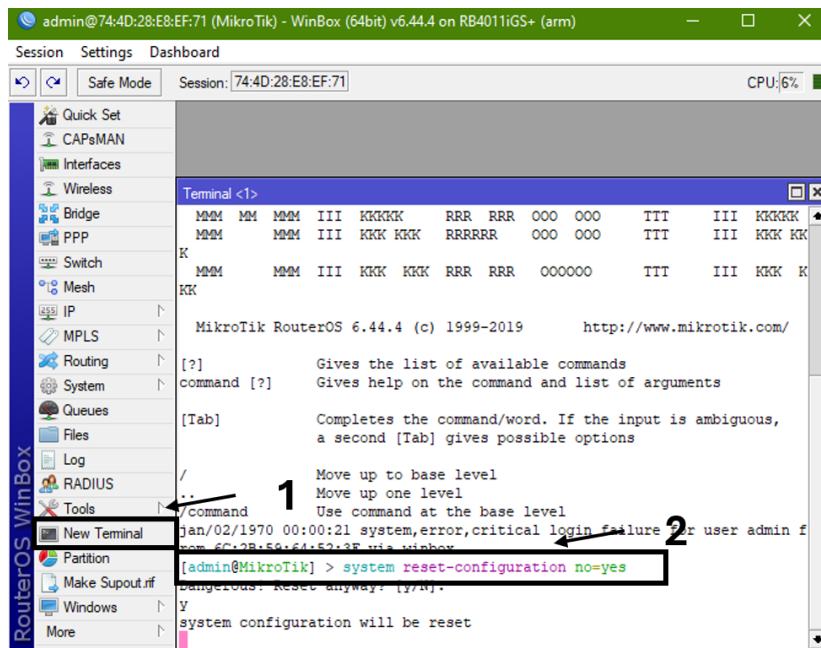
formato 64 bits luego procedemos a descargarlo, una vez descargado ejecutamos el archivo exe y ya tenemos acceso a Windows cómo siguiente seleccionamos el equipo en caso del que el equipo no aparezca damos Clic en el botón refresh para poder ingresar al equipo seleccionamos la dirección MAC y en el apartado de login colocamos **admin** y en el apartado de password lo dejamos vacío por defecto, procedemos a dar clic en el botón connect para acceder al interfaz del equipo.



*Figura 85. Ingreso mediante el winbox
Imagen elaborada por el autor*

Borrar configuración predeterminada

Una vez que ya ingresamos al equipo procedemos a abrir la pestaña new terminal y en la línea de comandos digitamos el siguiente comando **system reset-configuration no=yes** luego nos aparecerá un mensaje en la cual colocamos yes para el equipo se resetee.



*Figura 86. Resetear la configuración
Imagen elaborada por el autor*

Creación de Usuario

Para la creación de un usuario nuevo ingresamos nuevamente al equipo mediante el win box, luego nos dirigimos a la pestaña de System y de ahí damos Clic en el apartado de user list para luego dar clic en (+) se nos desplegará una ventana dónde colocaremos el nombre del usuario el grupo y creamos una contraseña y confirmamos la contraseña para después aplicar los cambios

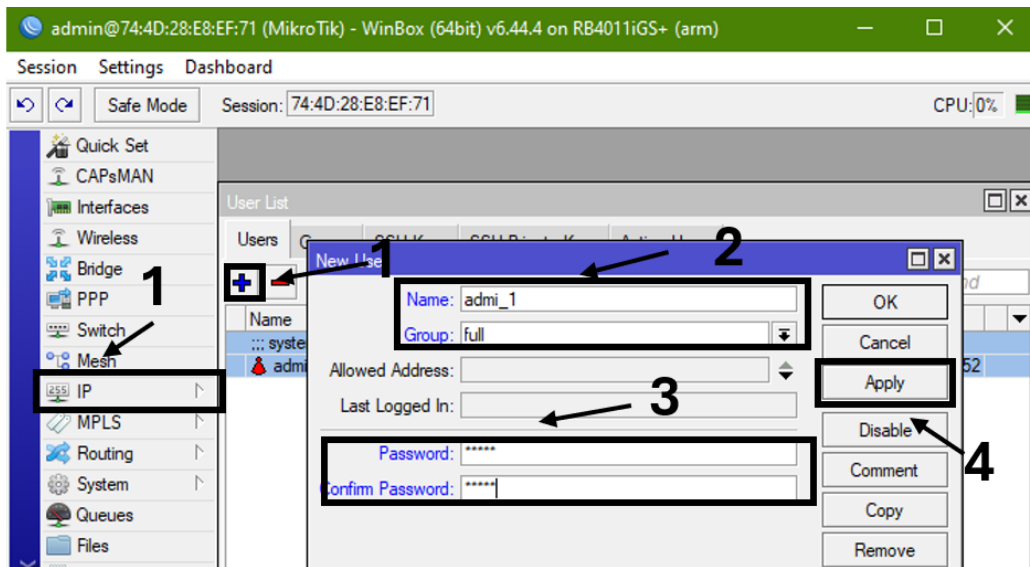


Figura 87. Nuevo usuario y contraseña
Imagen elaborada por el autor

Configurar las interfaces lan y wan

Para configurar la interfaz es LAN igual nos dirigimos a la pestaña de interface se nos desplegará una ventana y podemos observar las interfaces que tenemos en nuestro equipo en este caso vamos a seleccionar la interfaz 3 o cómo se encuentra en el equipo ether 3 al dar doble clic se nos desplegará una ventana dónde le daremos como nombre ether 3_Wan, para no perdemos colocamos un comentario seleccionando la pestaña comment y cómo comentarios dejamos entrada de Internet, luego seleccionamos el ether 4 al dar doble clic se me hace desplegará una ventana y cómo nombre le vamos a colocar ether 4_lan después colocamos un comentario en el que diga salida de Internet por último damos ok.

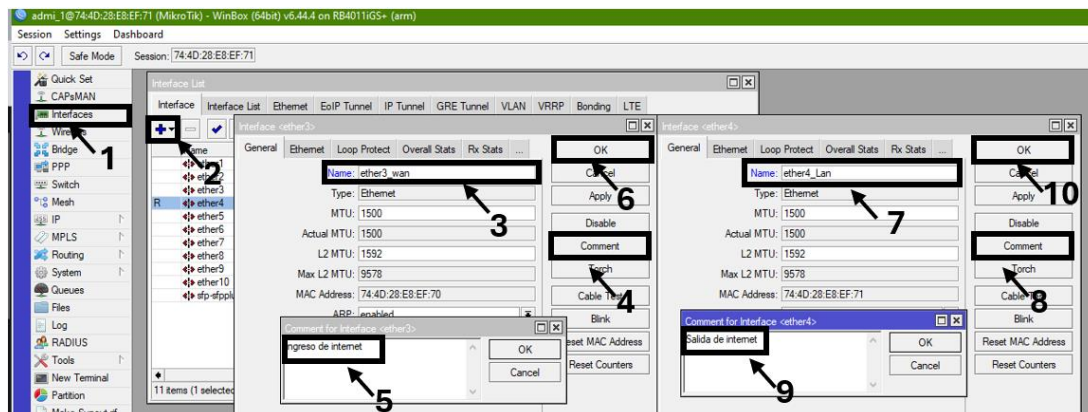


Figura 88. Agregamos la Interfaz lan y wan
Imagen elaborada por el autor

Habilitar un cliente dhcp

Como el siguiente paso habilitamos un cliente DHCP en la interfaz Wan lo activamos para obtener automáticamente la configuración del proveedor de Internet, dentro del winbox nos dirigimos a la pestaña IP luego damos Clic en la pestaña de DHCP client se nos desplegará una ventana damos Clic en más para agregar el nuevo de HCP client en la nueva ventana en la opción interface seleccionamos el R3 ya creado y automáticamente nos designa una dirección IP **192.168.100.5/24**, por último damos Clic en ok para continuar.

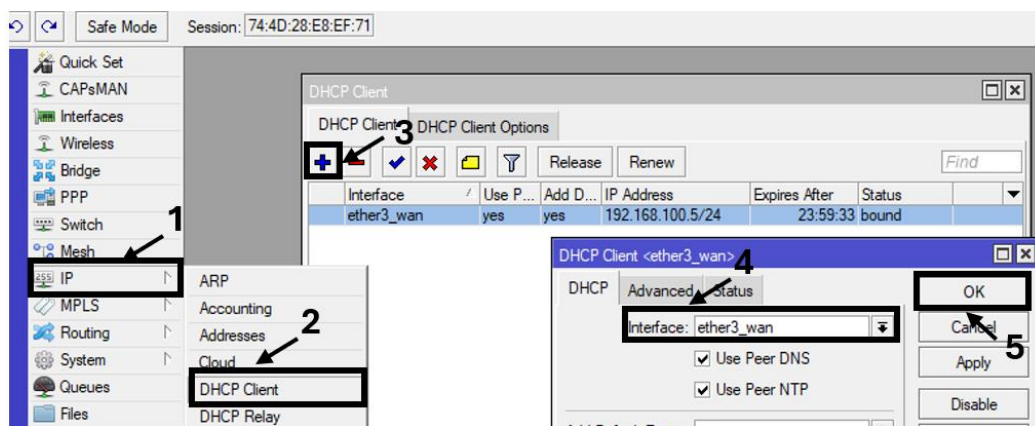


Figura 89. Nuevo cliente DHCP
Imagen elaborada por el autor

Crear la red local en la interfaz lan

Para crear la red local no es dirigimos a la pestaña IP y damos Clic en la opción Address List damos clic en el botón (+), se nos desplegará una ventana dónde cual colocamos una dirección IP distinta a la que nos da nuestro proveedor en este caso colocamos la siguiente dirección **IP 192.168.2.1/24**, en la red local LAN se puede colocar cualquier dirección IP siempre y cuando no sea la misma dirección del proveedor

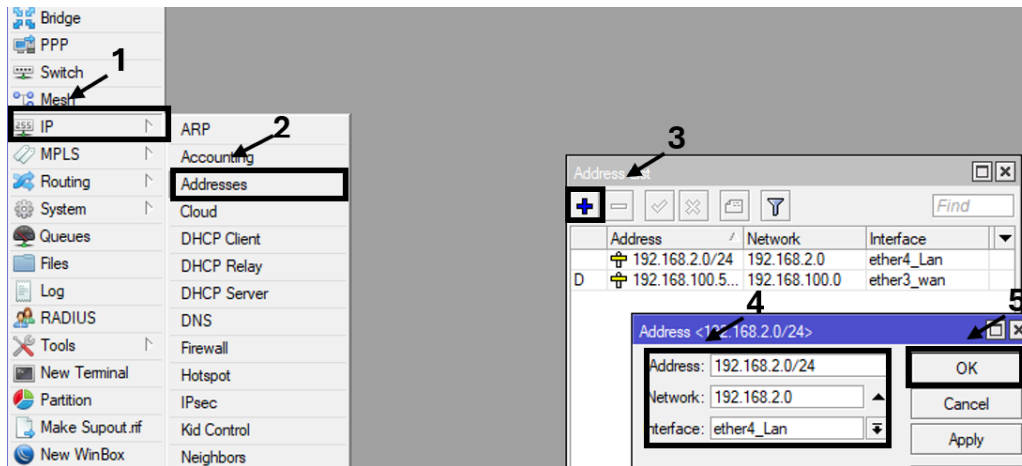


Figura 90. Agregamos las direcciones IP
Imagen elaborada por el autor

Configurar el servidor dhcp

Para configurar el servidor DHCP nuevamente nos dirigimos a la pestaña IP damos clic en DHCP server y nos situamos en DHCP setup en la siguiente ventana seleccionamos la interfaz. Luego de seleccionarla damos clic en el botón next hasta dar clic en el botón o k con esto ya tenemos avanzado un 75% para acceder a Internet, cómo otro paso reiniciamos el equipo para que se actualicen las configuraciones hechas recientemente, para ello nos vamos a la pestaña system y damos clic en Reboot.

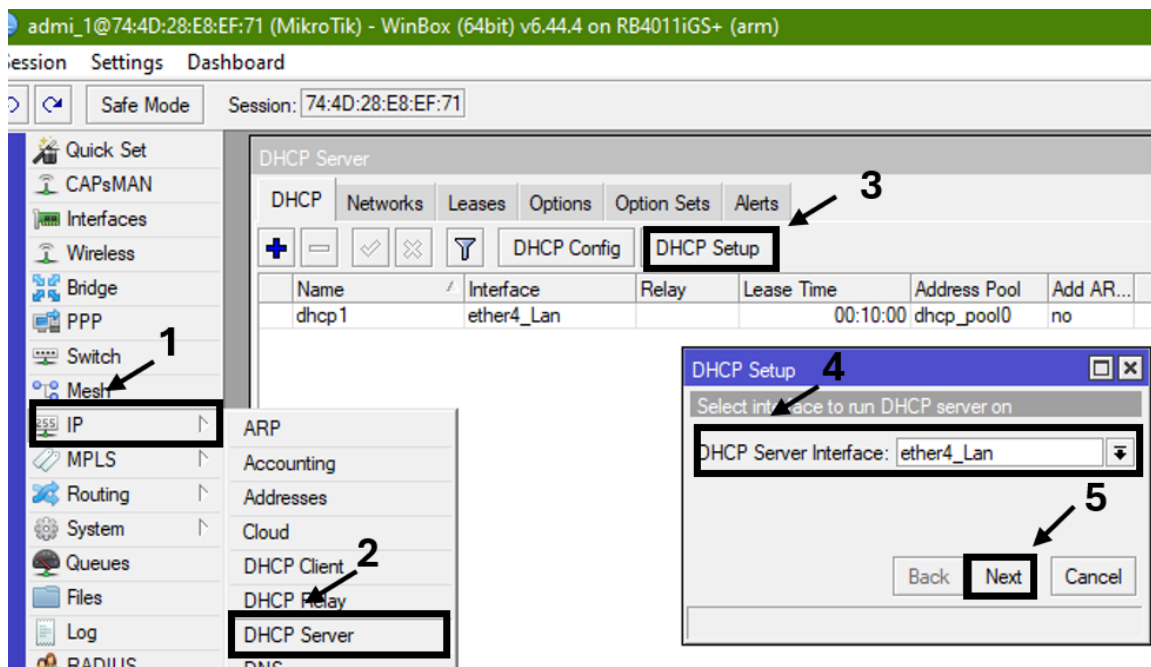
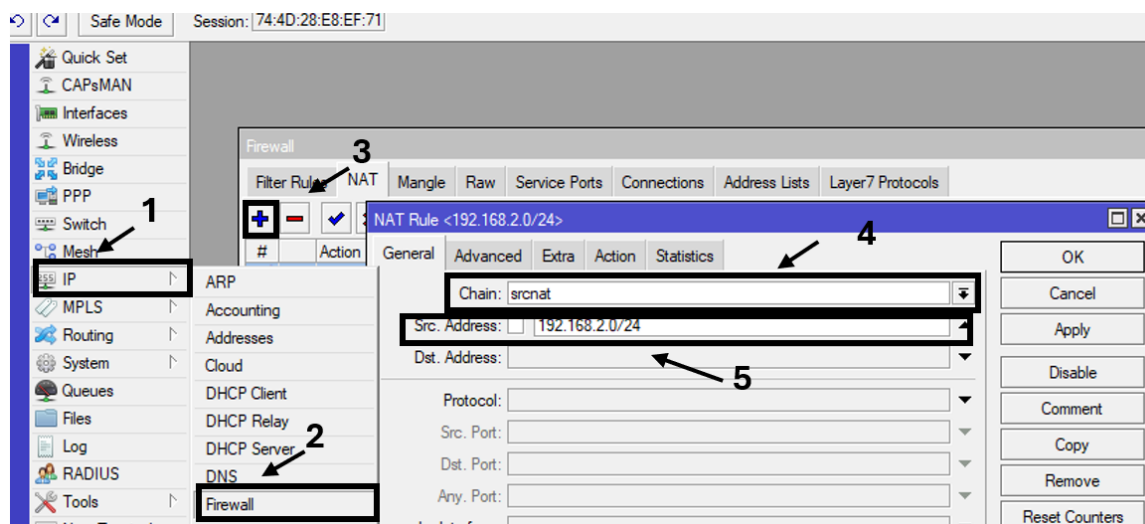


Figura 91. Configuración de DCHP Server
Imagen elaborada por el autor

Creación de la regla nat

Como último paso nos dirigimos nuevamente a la pestaña **hype** y nos situamos en **firewall** damos clic en (+) para luego dirigirnos a la opción **chain** y seleccionamos **Sr nat** y en la opción **Sr Address** colocamos la dirección IP del área local que es la dirección **192.168.2.0/24**, después nos dirigimos a la pestaña **Action** luego seleccionamos la opción **masquerade** por último damos **ok** y con este último paso ya tenemos acceso a Internet correctamente.



*Figura 92. Agregamos la dirección ip para la salida del internet
Imagen elaborada por el autor*

Como resultado

Como resultado de qué estamos conectados a Internet podemos verificar mediante el panel de control de nuestro PC dirigiéndonos a **redes e Internet** luego seleccionamos la red en la ventana general damos clic en **detalles** y podemos observar que tenemos la siguiente dirección IP **192.168.2.9/24** colocada en el área local previamente del equipo, como otra prueba realicemos **pin** a la dirección IP **192.168.100.1** de nuestro proveedor y realizamos una prueba de testeo para ver la calidad de Internet.

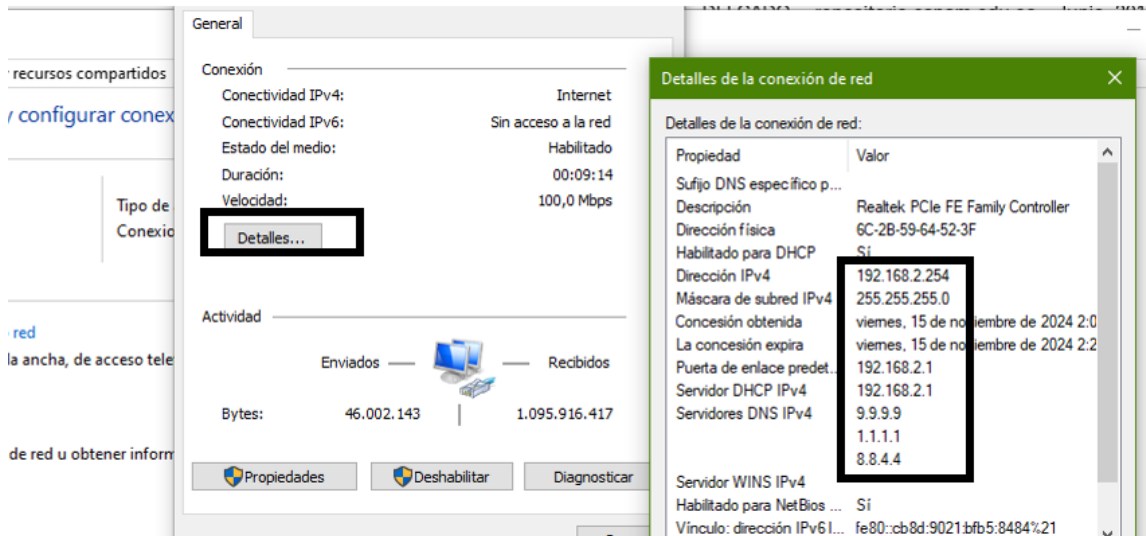


Figura 93. Detalles de la conexión de red
 Imagen elaborada por el autor

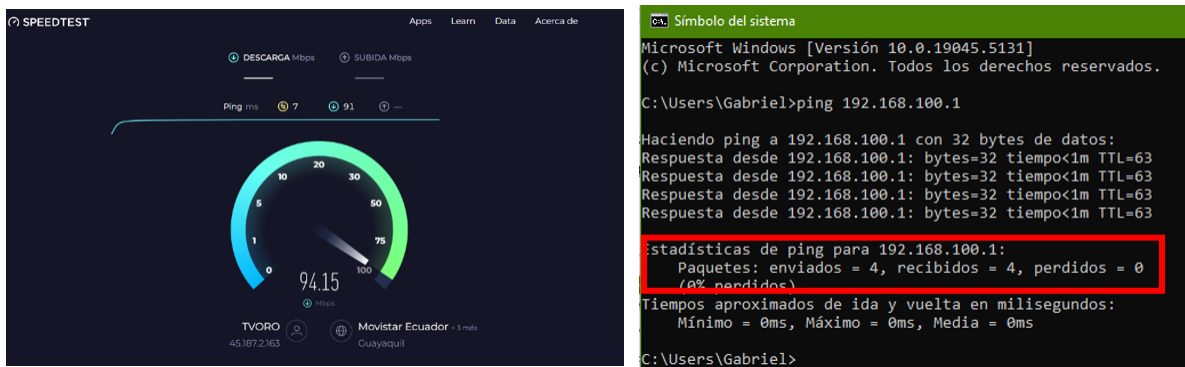


Figura 94. Acceso a internet y ping exitoso
 Imagen elaborada por el autor

Practica N°2

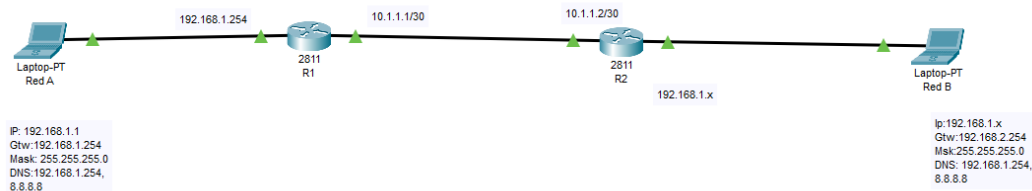
Tema: Túneles Eo IP

Objetivo: Configuración de túneles eoip en equipos mikrotik

Objetivos específicos:

- Configuración los Routers R1 y R2
- Configurar un Túnel Ethernet/IP
- Configuración de Bridge
- Realizar un DHCP Server para R1 y R2
- hacer ping entre la red a y red b

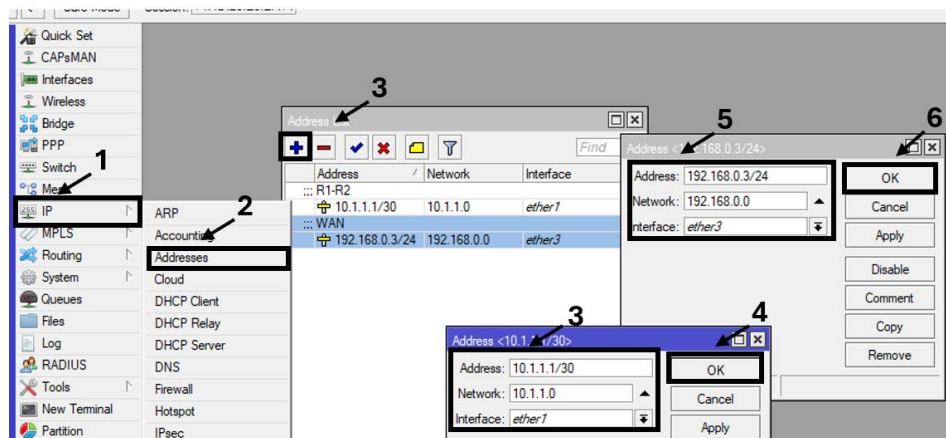
Topología de Red



*Figura 95. Topología de red túnel eoip
Imagen elaborada por el autor*

Configuración del router R1

Primero comenzamos a gestionar la comunicación en el router R1, cuando nos dirigimos al Winbox nos vamos a la pestaña IP luego a la pestaña address ti configuramos las direcciones IP que van a llevar tanto el router 1 cómo el router dos y también colocamos las interfaces por dónde van a salir



*Figura 96. Agregar las direcciones IP a R1
Imagen elaborada por el autor*

Túnel eoip en R1

Comenzamos realizando las configuraciones de El túnel ethernet sobre IP en el router 1, luego nos dirigimos a la pestaña interface damos clic en (+), luego en la opción EoIP tunnel, se nos desplegará una ventana dónde como nombre cuando lo dejamos por defecto luego nos dirigimos a la sección local Address para colocar la siguiente dirección IP **10.1.1.1**, luego en la sección de más abajo remote Address colocamos la siguiente dirección IP **10.1.1.2**, y por último en tunnel ID colocamos el valor de 10 con este parámetro sabemos hacia dónde gestionamos y quién gestiona la comunicación al momento de realizar la conexión entre dispositivos.

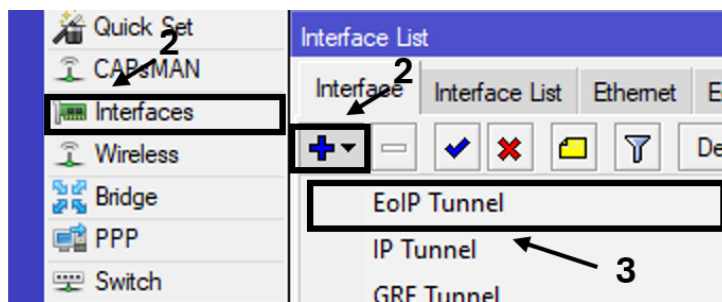


Figura 97. Agregamos una configuración nueva eoip tunnel
Imagen elaborada por el autor

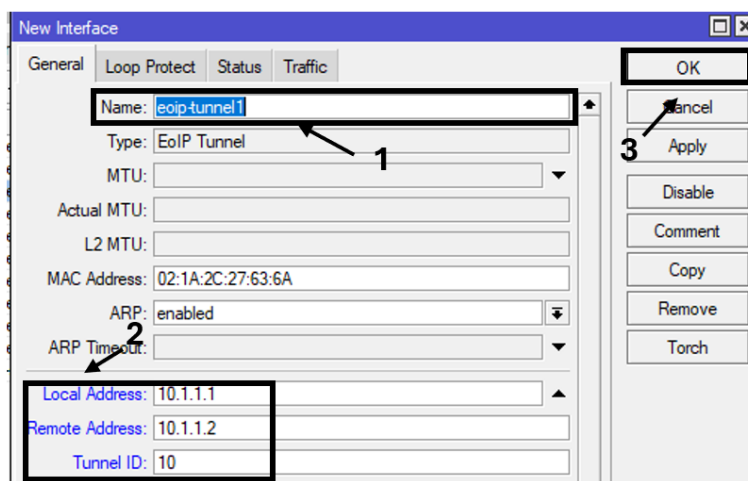


Figura 98. Agregamos la nueva interface con sus direcciones ip
Imagen elaborada por el autor

Configuración del router R2

Pasamos al siguiente router en ese caso al router dos nos dirigimos a la pestaña IP y damos clic en la opción Address para colocar la dirección IP que va a llevar este router **10.1.1.2/30** también colocamos su interfaz de salida esta es ether 1 por último etiquetamos el Address List como comentario R2-R1 finalmente damos ok.

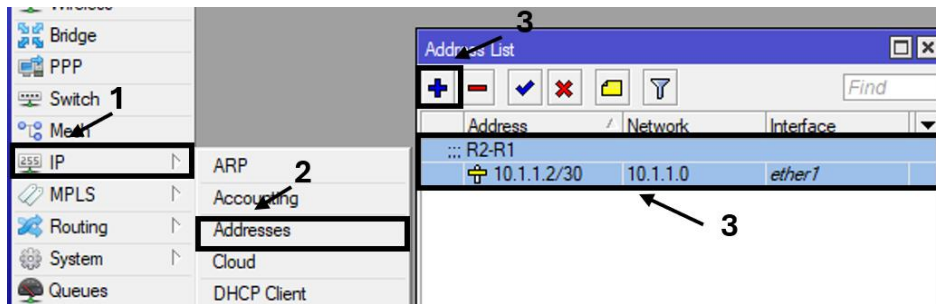


Figura 99. Comunicación entre R2 Y R1
Imagen elaborada por el autor

Túnel eoip en R2

Comenzamos a gestionar la comunicación del ethernet sobre IP dentro del R2, no dirigimos a interfaces, se desplegará una ventana luego damos clic en (+), seleccionamos EoIP tunnel, el nombre lo dejamos por defecto y nos centramos en la opción local address y colocamos la siguiente dirección IP **10.1.1.2**, continuando en la opción remote address colocamos la IP remota que es la siguiente IP **10.1.1.1**, seguido en el tunnel ID colocamos el número 10, aplicamos los datos y damos clic en el botón ok.

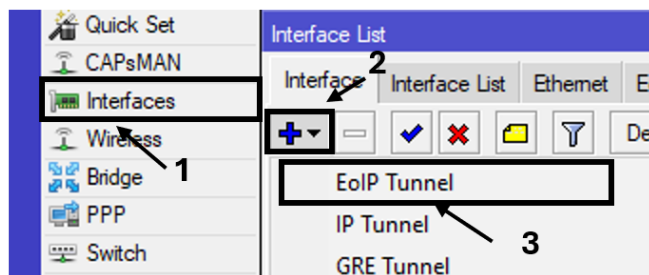


Figura 100. Agregamos de nuevo el eoip tunnel
Imagen elaborada por el autor

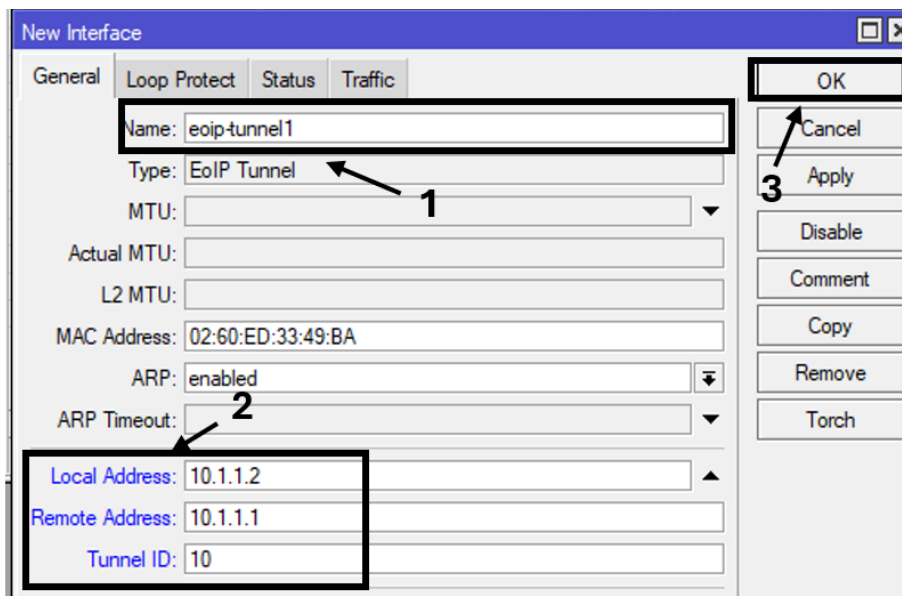


Figura 101. Se agregan las siguientes IP
Imagen elaborada por el autor

Configuración de bridge en R1

El bridge nos dará la oportunidad de unificar dos puertos ya que el bridge al genera puertos esclavos que se encuentran dentro de él, dentro del R1 nos dirigimos a la pestaña bridge se desplegará una ventana y daremos clic en (+), aparecerá otra ventana dejamos por defecto las opciones que aparecen damos clic en aplicar y ok.

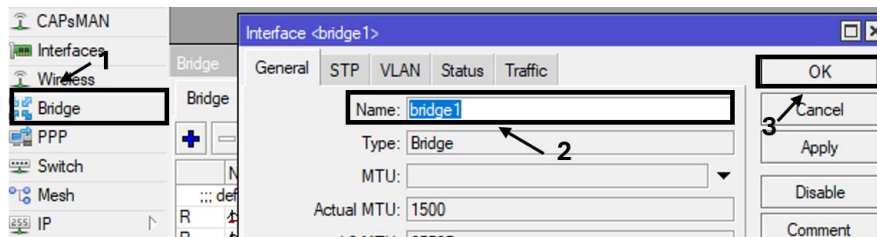


Figura 102. Creamos un bridge nuevo
Imagen elaborada por el autor

En la pestaña interface damos clic en (+), dónde seleccionamos la interfaz creada para el túnel y en la casilla bridge seleccionamos el bridge 1, en el mismo bridge creamos otra con ether 2y en la opción bridge dejamos la que colocamos anteriormente en este caso bridge 1 aplicamos y damos OK.

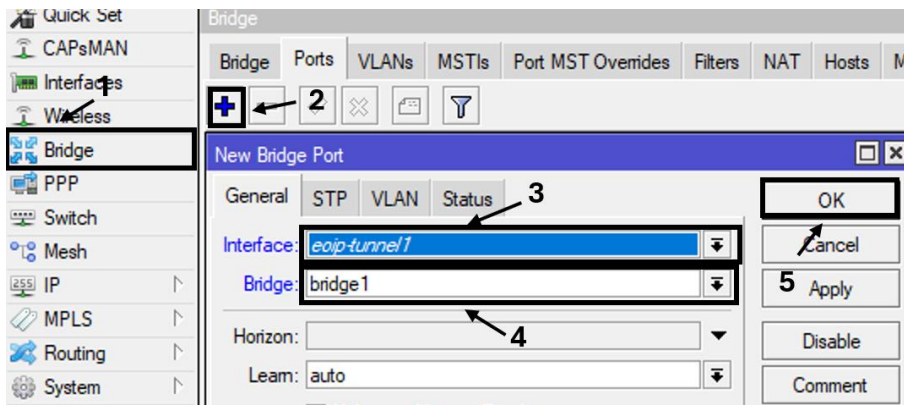
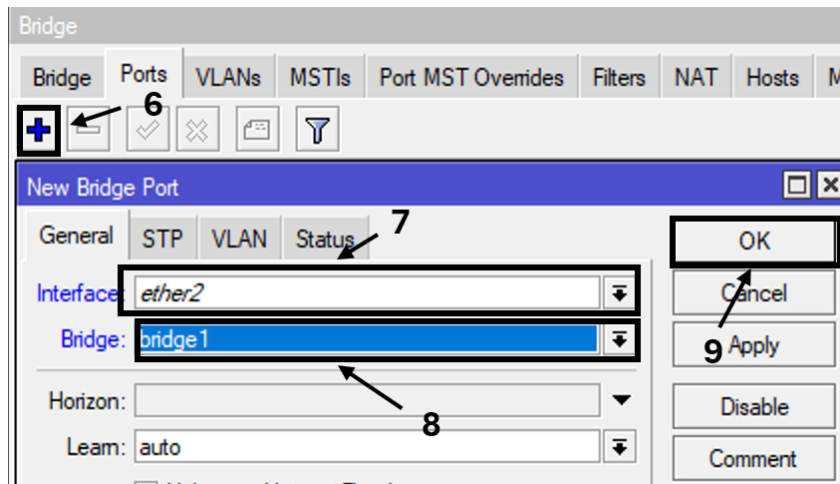
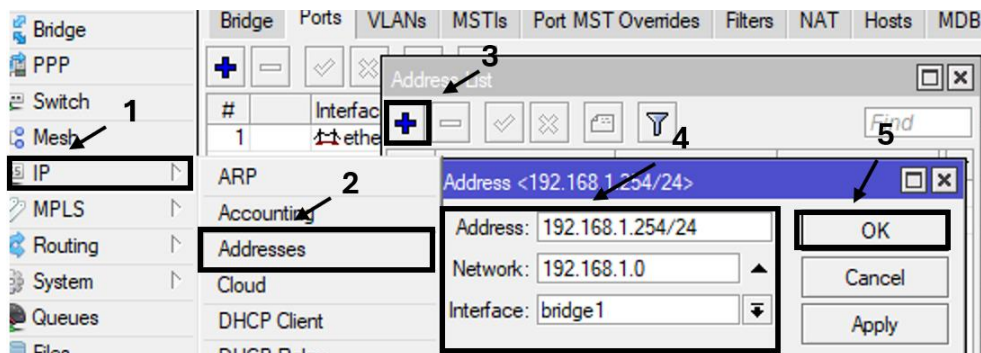


Figura 103. Nuevo puerto del bridge
Imagen elaborada por el autor



*Figura 104. Se añade nuevo puerto con la interfaz ether2
Imagen elaborada por el autor*

Cuando creamos un bridge el bridge genera que los puertos que estén dentro de él sean puertos esclavos, Es por ello que una vez que estos puertos sean esclavos cualquier tipo de direccionamiento deberá ser no agregado a estos puertos esclavos si no el puerto máster que en este caso será la bridge, ya que tenemos en cuenta cuando creamos la bridge ahora nos dirigimos a la pestaña IP y seleccionamos la opción address dónde generaremos un direccionamiento IP para el ingreso **192.168.1.254/24**, abre el bridge va a contener este direccionamiento IP con esto decimos que el direccionamiento IP puede fluir a través de las interfaces que se encuentren dentro de él.



*Figura 105. añadimos la siguiente ip en address list
Imagen elaborada por el autor*

Seguido realizaremos es un DHCP Server nos dirigimos a la pestaña nuevamente IP y seleccionamos la casilla de DHCP Server se desplegará una ventana y daremos clic en (+), para luego dar clic en el botón De HP Setup dónde daremos clic en next hasta llegar a DNS servers dónde vamos a colocar el siguiente DNS 8.8.8.8

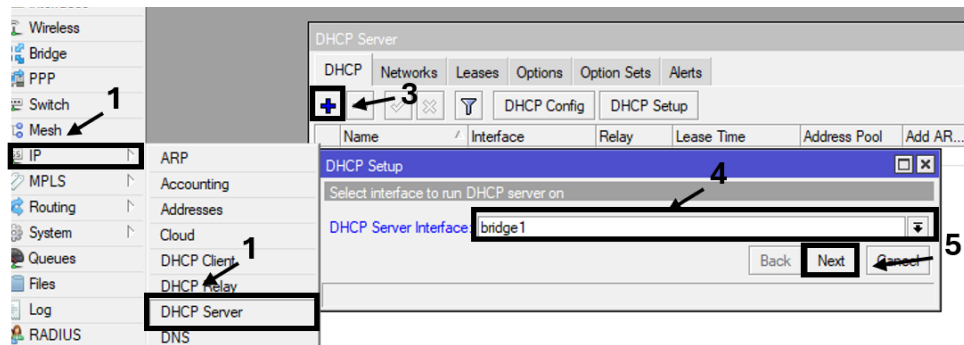


Figura 106. Configuración de dhcp server
 Imagen elaborada por el autor

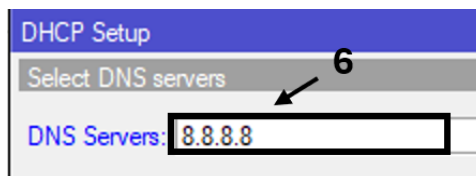


Figura 107. Colocamos las direcciones DNS
 Imagen elaborada por el autor

Ahora nos dirigimos a nuestro router R2, lo que vamos a generar es un DHCP Client para ello nos dirigimos a la pestaña IP seleccionamos la casilla de DHCP Client luego damos clic en (+), seguido colocamos la interfaz EoIP tunnel aplicamos y damos ok.

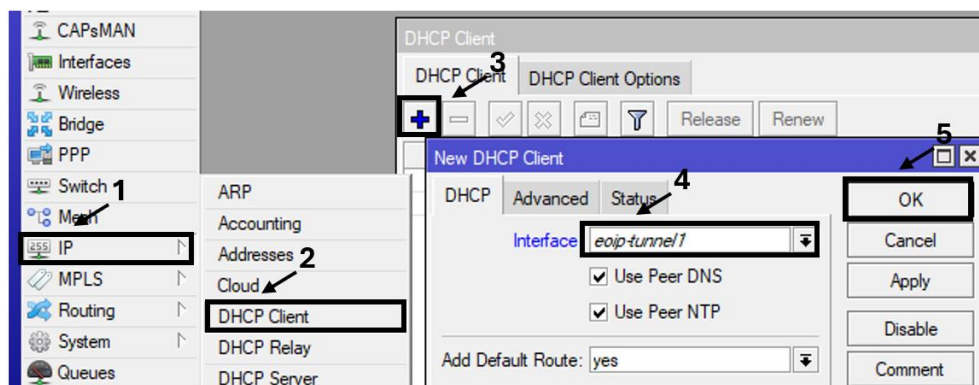


Figura 108. Configuración de dhcp client
 Imagen elaborada por el autor

Para poder hacer que el DHCP Server pase a la red LAN para que se pueda conectar con los dispositivos que se encuentran detrás del router R2, para ello nos dirigimos la opción bridge en bridge damos clic en (+), se nos desplegará una ventana y en el nombre le colocamos la bridge 1, luego damos clic en la ventana puerto dentro de bridge para crear un nuevo puerto en las bridge, se desplegará una ventana dónde seleccionamos el nombre de EoIP túnel y en la opción bridge colocamos la bridge 1, y por medio de este túnel se genera la comunicación hacia R1, como último procedimiento agregamos otro nuevo bridge port con la interfaz ether2

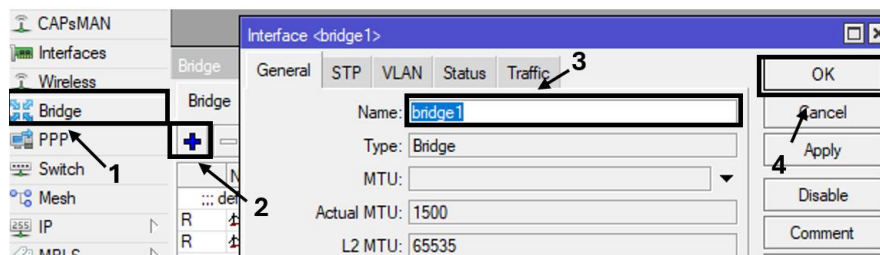


Figura 109. Se agrega una nueva bridge1
Imagen elaborada por el autor

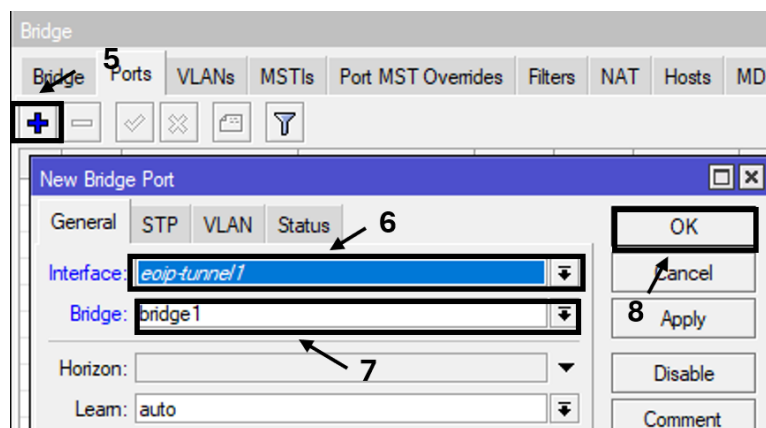


Figura 110. Agregamos un nuevo ports con la bridge1
Imagen elaborada por el autor

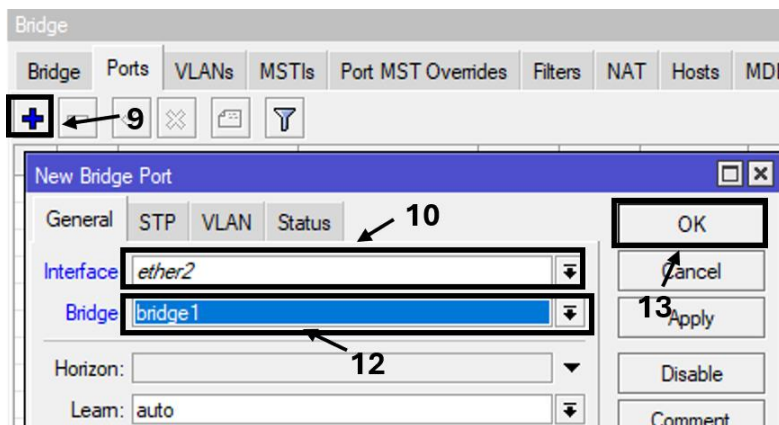


Figura 111. Agregar otra configuración en ports
Imagen elaborada por el autor

Realizar ping entre redes A y B

Por último, revisamos que todas las configuraciones ya hechas están incorrectamente ingresadas procedemos a realizar ping en ambas computadoras en este caso la red a lleva como dirección IP para realizar el ping **192.168.1.252**, y como podemos observar contamos con comunicación entre la otra máquina de la misma manera realizamos un ping desde la otra red en este caso la red b hacia la red a con la siguiente dirección IP **192.168.1.251**, con esto podemos decir que ambos

dispositivos se sitúan en el mismo dominio del broadcast, esta estructura nos permite sobre el ethernet IP que se gestione una comunicación completamente transparente, y por esto se conoce que el tunnel EoIP es un túnel que trabaja en capa 2, teniendo esto en cuenta podemos observar qué haciendo ping entre ambas computadoras tenemos una conexión exitosa.

```
Símbolo del sistema
Microsoft Windows [Versión 10.0.19045.5131]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\Gabriel>ping 192.168.1.251

Haciendo ping a 192.168.1.251 con 32 bytes de datos:
Respuesta desde 192.168.1.251: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.251: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.251: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.251: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.1.251:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\Gabriel>
```

*Figura 112. Ping desde la computadora red A
Imagen elaborada por el autor*

```
C:\Windows\system32\cmd.e: X + v
Microsoft Windows [Versión 10.0.22621.4317]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\Usuario>ping 192.168.1.252

Haciendo ping a 192.168.1.252 con 32 bytes de datos:
Respuesta desde 192.168.1.252: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.252: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.252: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.1.252: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.1.252:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 1ms, Media = 0ms

C:\Users\Usuario>
```

*Figura 113. Ping desde otra computadora conectada
Imagen elaborada por el autor*

Practica N°3

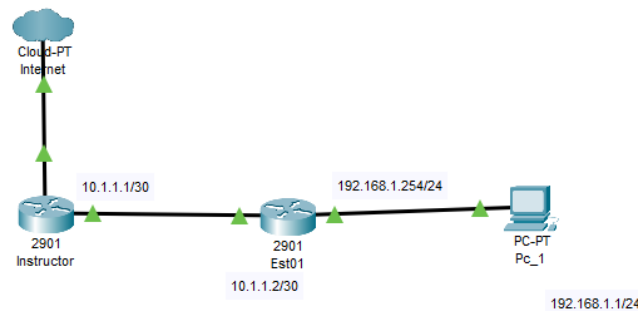
Tema: Firewall NAT

Objetivo: Familiarizarse con el firewall nat

Objetivo específicos:

- Diseñar una topología de red
- Configurar la NAT en el Router Instructor
- Investigar como acceder con una ip pública a un Equipo MikroTik
- Configuración de ip pública
- Acceder al equipo Est01 mediante la NAT configurada
- Realizar un ping para demostrar el acceso al Router Est01

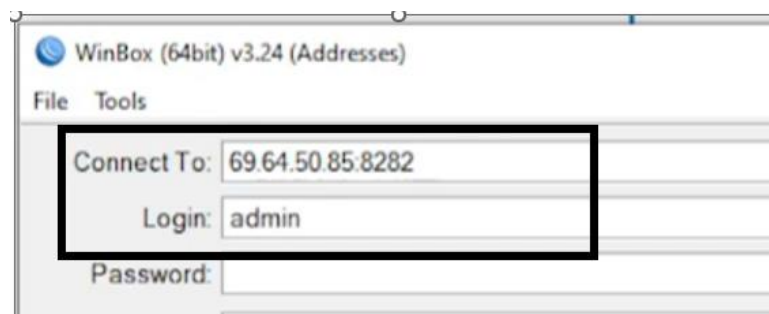
Topología de red



*Figura 114. Topología de red
Imagen elaborada por el autor*

Configuración de la nat router instructor

Comenzamos Ingresando al router instructor, para poder ingresar colocamos una IP pública **69.64.50.85** con el puerto **8282**, luego colocamos el usuario y contraseña, continuando se nos desplegará la ventana cuna del Winbox del router instructor para saber que hemos ingresado al router instructor en la parte de arriba de la ventana del Winbox podemos observar el nombre del Equipo.



*Figura 115. Ingreso al Equipo mediante winbox
Imagen elaborada por el autor*

Configuración de la nat

Comenzamos dirigiéndonos a la pestaña IP luego a firewall y daremos clic en la ventana NAT para crear una nueva NAT damos clic en (+) se desplegará una ventana dónde en la opción chain damos clic y seleccionamos **dstnat**, luego especificamos hacia dónde hacia afuera se va a ir preguntando al dispositivo final para qué esta forma el dispositivo final pueda generar el forward guardado de la petición, luego utilizamos la siguiente dirección Ip **192.168.0.3** estará haciendo una nateada por el equipo que tiene el IP pública, y de esta manera puedo acceder mediante la IP pública y es por eso que puedo acceder por la IP pública ya antes mencionada **69.64.50.85**, es el mismo proceso que vamos a realizar en nuestro dispositivo para que aquel dispositivo que se encuentra detrás del instructor pueda ser accesible también cada vez que llega una petición a este router que venga con la ip del destino **192.168.0.3** con el protocolo TCP y que vaya relacionado a puerto en este caso el puerto 8260 cada vez que coincidan en un “match” en ese instante el dispositivo enviará esta petición hacia el destino **10.1.1.2** esta IP es la que se encuentra entre el dispositivo de Est01, la red que podemos ver que comunican a los dispositivos es la red **10.1.1.0/30**, es por eso que especificamos la siguiente dirección IP **10.1.1.2** que en realidad es la IP con la que se alcanza el router Est01 como parte final especificamos el puerto del servicio al cual quisiéramos acceder en este caso el puerto **8291** las reglas NAT la colocamos al principio

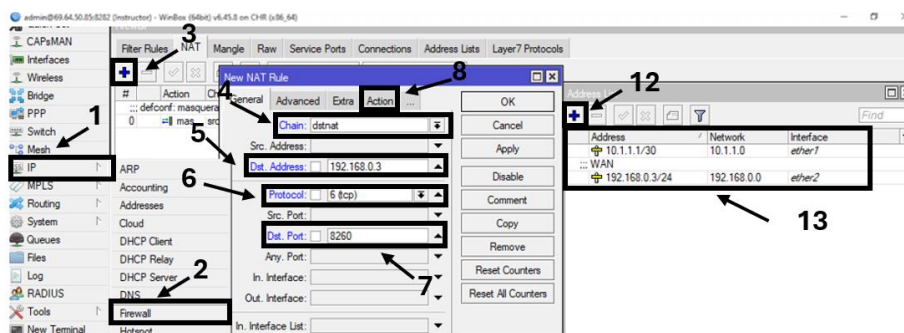


Figura 116. Configuración de nueva nat
Imagen elaborada por el autor

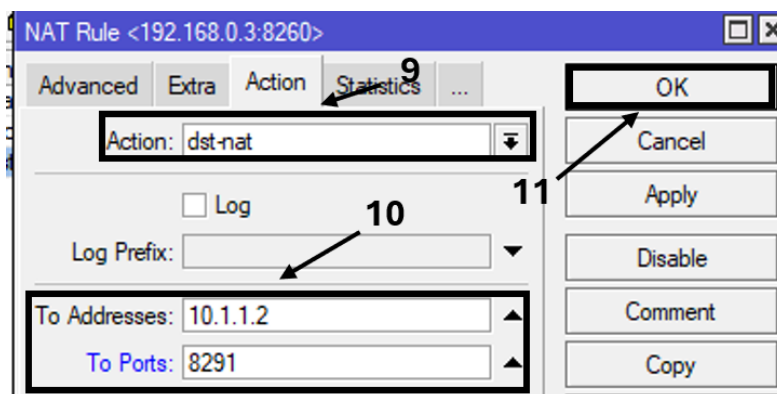


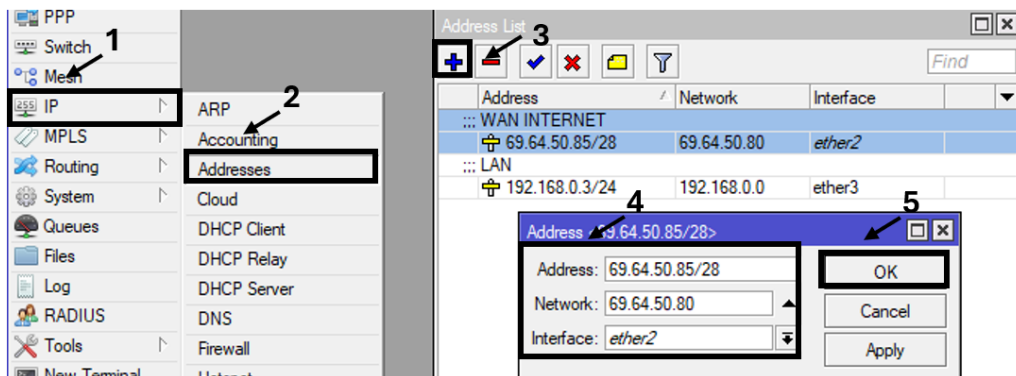
Figura 117. Configuración de la pestaña action
Imagen elaborada por el autor

#	Action	Chain	Src. Address	Dest. Address	Proto	Src. Port	Dest. Port	In. Inter	Out. Int	In. Bytes	Out. Bytes	Packets
0	dstnat	dstnat	192.168.0.3	6 (tcp)			8260				0 B	0
1	srcnat	srcnat							WAN		0 B	0

*Figura 118, Visualizamos los paquetes que ingresan
Imagen elaborada por el autor*

Insertar una ip Pública

Para insertar una ip publica nos dirigimos dentro del Winbox, damos clic en la sección IP luego clic en la pestaña Addresses, dentro del Adres List damos clic en el recuadro (+) y colocamos la dirección IP que nos da nuestro proveedor de la siguiente manera en este caso es la **69.64.50.85/28**, seleccionamos la interfaz por la cual se conecta el cable del proveedor, seguido damos aplicar y dejamos un comentario, al final damos OK, también creamos una LAN con la siguiente dirección IP **192.168.0.3** con la interfaz ether3, cometamos y damos en aplicar y OK



*Figura 119. Ingreso de la dirección Ip en el address list
Imagen elaborada por el autor*

Continuamos, no dirigimos a la opción ip y seleccionamos la pestaña DNS, se desplegará una ventana donde en el apartado de servers damos clic y colocamos el siguiente valor **8.8.8.8**, ya que son los DNS de Google el resto de los valores demos por defecto y damos aplicar y OK.

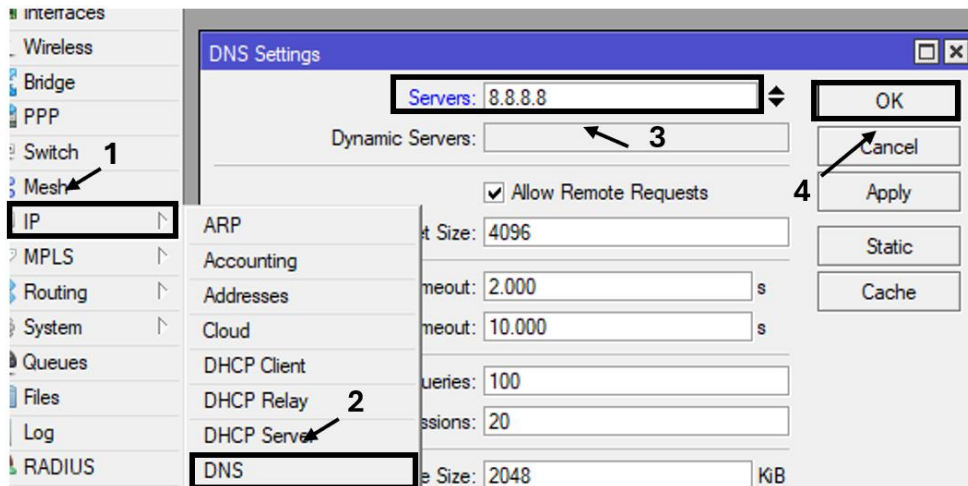


Figura 120. Se configuran las dns
Imagen elaborada por el autor

Luego creamos un DHCP Server para ellos nos dirigimos a la pestaña IP y damos clic en DHCP Server, luego damos clic en DHCP Setup, seleccionamos la interfaz de la LAN en este caso es la ether3, luego damos clic en next y dejamos por defecto la dirección ip hasta llegar a los servidores DNS don vemos que automáticamente se colocaron **8.8.8.8** por último damos en ok y ya estaría configurado el servidor DHCP.

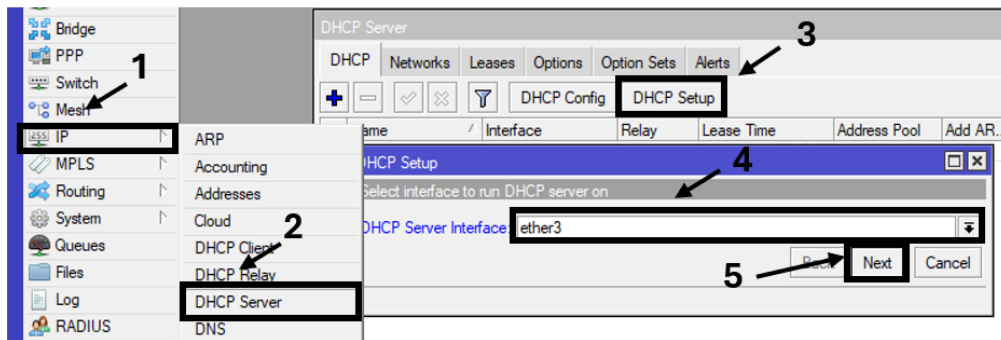


Figura 121. Realizamos otro dhcp server con otra interfaz ether 3
Imagen elaborada por el autor

Ahora nos situamos en la opción IP y damos clic en firewall, empezamos dando clic en NAT luego en el recuadro (+) en la opción Chain colocamos snat, en el apartado de Out. Interface seleccionamos la ether2, luego damos clic en la ventana Action y clic en la opción Action seleccionamos **masquerade**, por último, colocamos aplicar y OK.

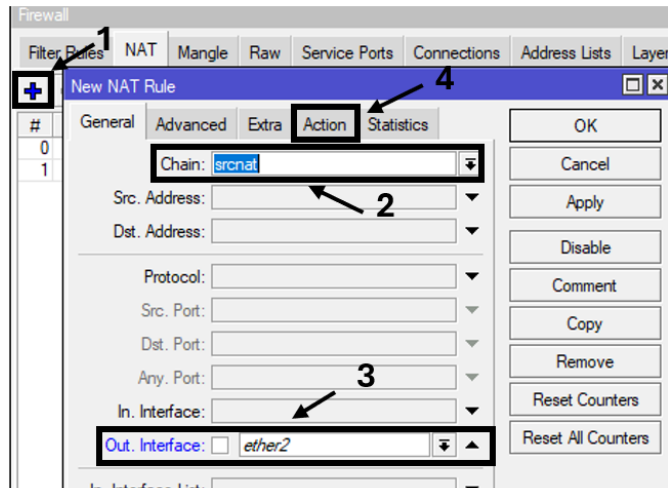


Figura 122. Configuración de nat
Imagen elaborada por el autor

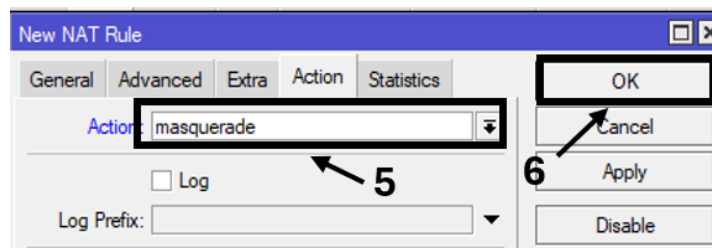


Figura 123. Configuración de la ventana acción
Imagen elaborada por el autor

Como parte Final nos dirigimos crear nuestra ruta empezando con la opción IP y damos clic en la pestaña Routes, se desplegará una ventana llamada Route List damos clic en el recuadro (+), en la nueva ventana dejamos en 0.0.0.0/0 por defecto y en Gateway colocamos la dirección IP del Proveedor en este caso la **69.64.50.85/28** el resto de las casillas las dejamos por defecto con estos pasos ya tendremos nuestra ip pública correctamente,

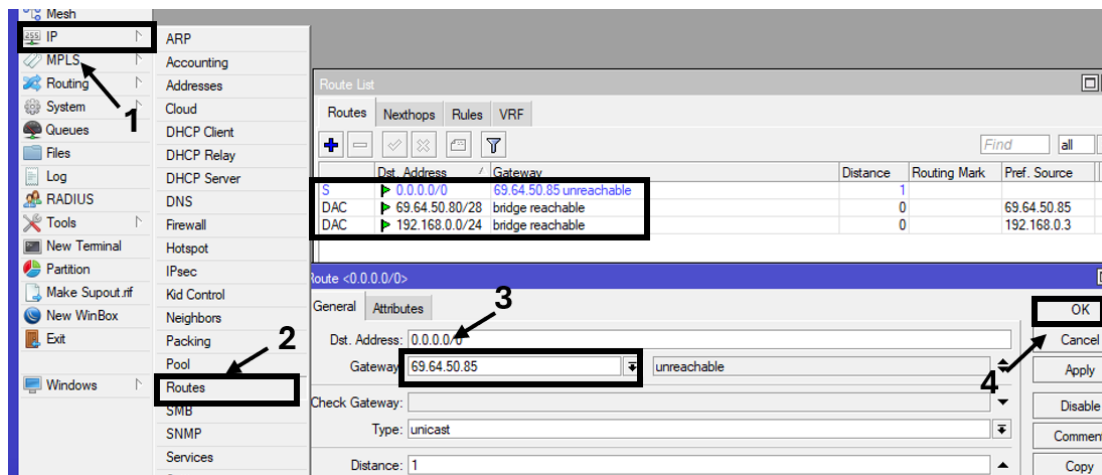
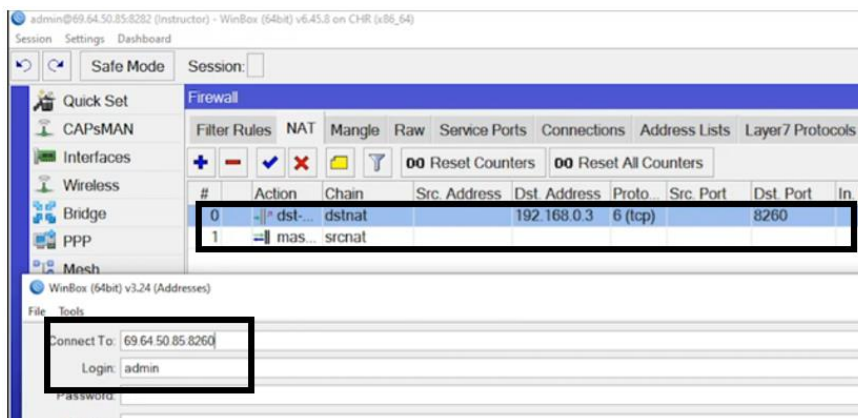


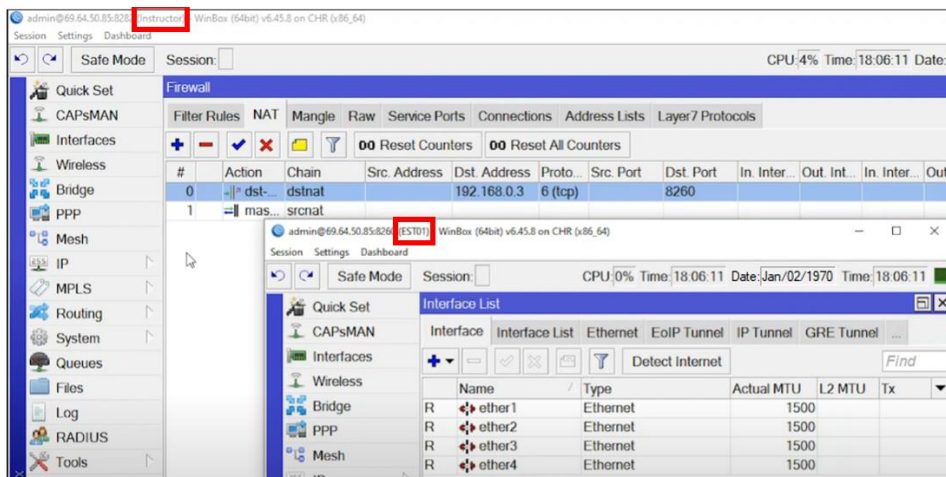
Figura 124. Añadimos la dirección Ip Publica al Gateway
Imagen elaborada por el autor

Acceso al equipo est01

Ya que hemos definido la regla del firewall NAT abrimos otra pestaña nueva de Winbox e ingresamos al equipo Est01 con la siguiente dirección IP **69.64. 50.85: 8260** siguiente en el apartado del login colocamos el usuario y en password la contraseña y como se puede observar en la imagen tenemos acceso total al router Est01, de esa forma el destination NAT nos permite a nosotros poder llegar desde la red externa hacia algún dispositivo que se encuentre dentro de la red interna.



*Figura 125. Ingre hacia el secundario equipo est01
Imagen elaborada por el autor*



*Figura 126. Conexión establecida
Imagen elaborada por el autor*

Por último, realizamos un ping hacia la siguiente dirección IP **10.1.1.2** con esto verificamos que tenemos comunicación entre el router Est01 y también tenemos conexión en el router instructor de esta forma mediante IP p pública podemos acceder a esta red externamente siempre y cuando utilicemos esta regla de NAT

```
C:\ Símbolo del sistema
Paquetes: enviados = 4, recibidos = 0, perdidos = 4
(100% perdidos),

C:\Users\Gabriel>ping 10.1.1.2

Haciendo ping a 10.1.1.2 con 32 bytes de datos:
Respuesta desde 10.1.1.2: bytes=32 tiempo<1m TTL=64
Respuesta desde 10.1.1.2: bytes=32 tiempo<1m TTL=64
Respuesta desde 10.1.1.2: bytes=32 tiempo<1m TTL=64
Respuesta desde 10.1.1.2: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 10.1.1.2:
Paquetes: enviados = 4, recibidos = 4, perdidos = 0
(0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

*Figura 127. Conexión Exitosa
Imagen elaborada por el autor*

Practica N°4

Tema: Implementación de protocolo bgp.

Objetivo: Familiarizarse con la configuración del protocolo bgp.

Objetivos específicos:

- Diseño de la topología de red.
- Realizar la configuración de las interfaces LAN y WAN.
- Configuración del Protocolo BGP.
- Realizar Configuración DHCP en las interfaces LAN.
- Realizar un ping para comprobar la conectividad.

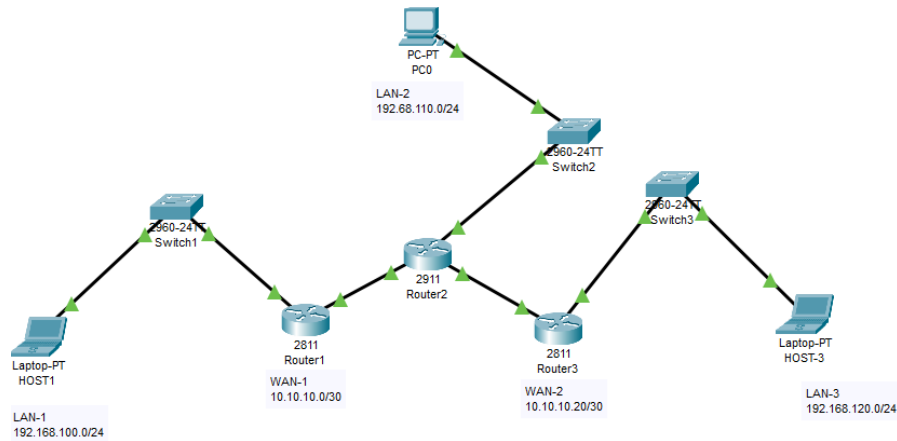


Figura 128. Topología de red bgp
Imagen elaborada por el autor

Tabla de direcciones ip

Nombre de Red	Red	Mask	INT	Dirección Ip	Mask
Wan1	10.10.10.0	/30	R1(Eth1)	10.10.10.1	/30
			R2(Eth1)	10.10.10.2	
Wan2	10.10.20.0	/30	R2(Eth2)	10.10.20.1	/30
			R3(Eth1)	10.10.20.2	
Lan1	192.168.100.0	/24	R1(Eth1)	192.168.100.1	/24
Lan2	192.168.110.0	/24	R2(Eth1)	192.168.110.1	/24
Lan3	192.168.120.0	/24	R3(Eth1)	192.168.120.1	/24

Tabla 2. Direccionamiento ip

Configuración de las interfaces lan y wan

Empezamos dirigiéndonos al Router R1 ingresamos mediante winbox, dentro del equipo nos dirigimos a la pestaña ip y seleccionamos la opción addresses, se desplegará una ventana donde daremos clic en el recuadro (+), en la nueva ventana agregamos las interfaces WAN damos clic en Address y con la siguiente dirección IP 10.10.10.1/30 en la interface colocamos ether 1, LAN con la dirección IP 192.168.100.1/24 y la interfaz ether 2, para ordenarlas agregamos un comentario de WAN-1 y LAN-1.

Ahora nos dirigimos al Router (R2) donde también colocamos las direcciones IP de la WAN y LAN, siguiendo los pasos del Router R1 colocamos la siguiente dirección IP 10.10.10.2/30 y de comentario dejamos el siguiente WAN-1, con la interfaz ether 1, a continuación, Agregamos otra dirección IP 10.10.20.1/30 con la interfaz ether 2 y de comentario insertamos WAN-2, ingresamos otra dirección IP 192.168.110.1/24 con la interfaz ether 3 y por último comentamos LAN-2.

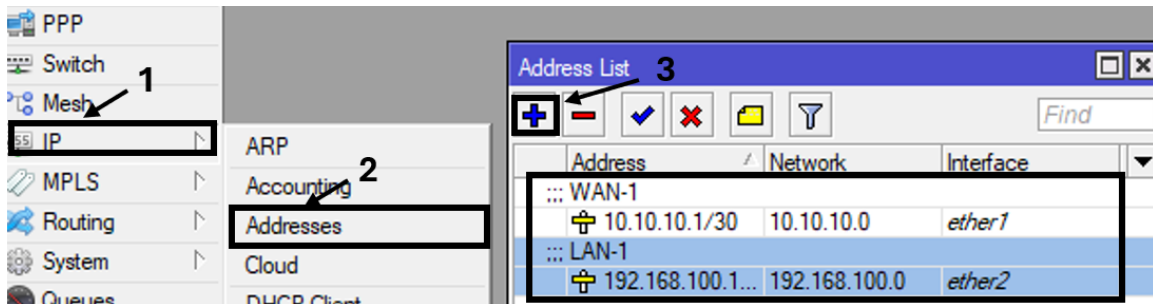


Figura 129. Configuración de ip's R1
Imagen elaborada por el autor

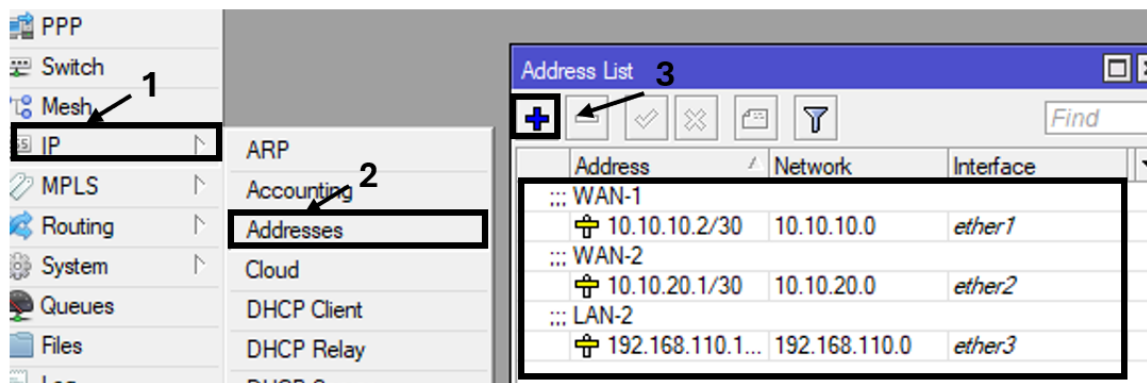


Figura 130. Configuración de ip's R2
Imagen elaborada por el autor

Continuando con los pasos de R1 y R2 agregamos las siguientes direcciones al router 3 (R3) dentro de la ventana Address List damos clic en (+), se desplegará una ventana donde en el apartado de Address colocamos la siguiente dirección IP 10.10.20.2/30 y en interface seleccionamos la ether1 luego agregamos un comentario WAN-2, continuando agregamos otra

dirección IP 192.168.120.1/24 y seleccionamos la interfaz ether 2, como comentario le colocamos LAN-3.

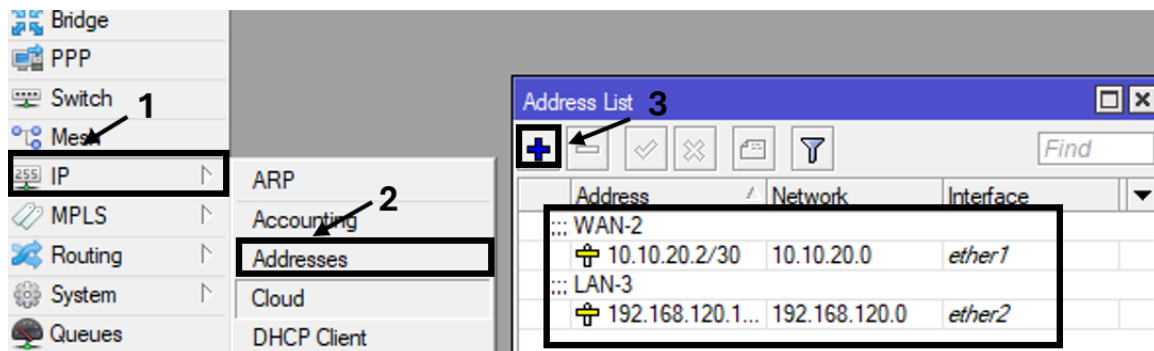


Figura 131. Configuración de ip's R3
Imagen elaborada por el autor

Configuración del protocolo bgp

Para entender mejor el Protocolo BGP es el encargado de intercambiar la información del enrutado entre sistemas que son autónomos, teniendo esto en cuenta comenzamos dentro del Winbox del Router R1 nos dirigimos a la pestaña **Routing** y seleccionamos la casilla BGP, se desplegará una ventana donde nos situamos en la ventana **Interfaces** damos clic el recuadro de (+) en la nueva ventana colocamos el siguiente Nombre este nombre es una variable cualquiera para este caso lo designamos como R1 100 como nombre del sistema autónomo, en el apartado de AS colocamos un valor del sistema para distinguirlo en este caso el 100, y en la sección Router ID insertamos la siguiente dirección IP **10.10.10.1**, por último seleccionamos la casilla **Redistribute Other BGP**, damos clic en Ok para que se guarde la configuración.

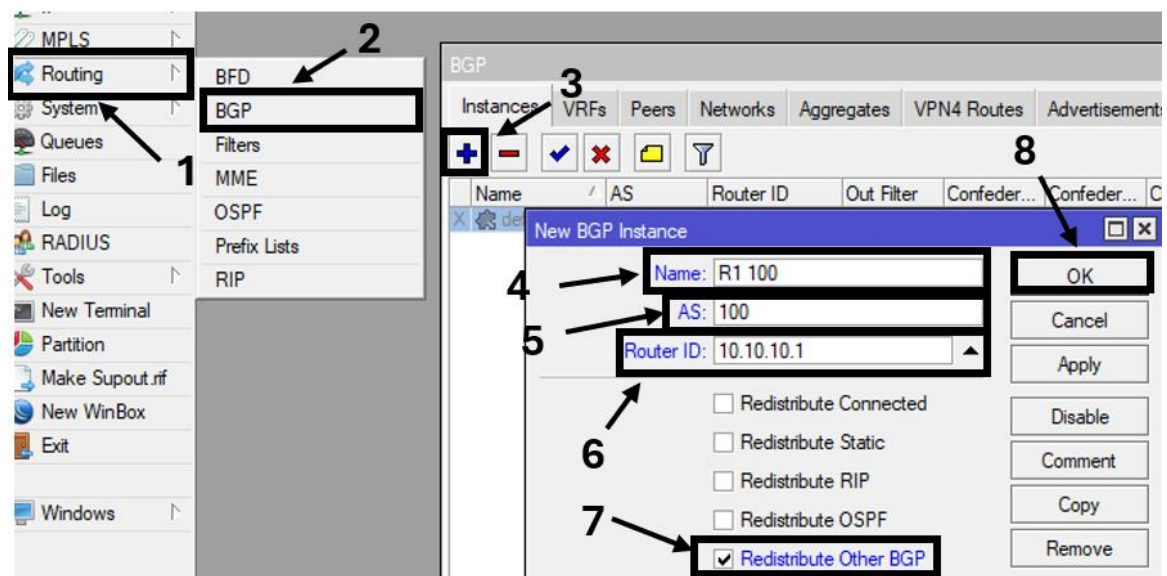


Figura 132. Configuración Protocolo bgp
Imagen elaborada por el autor

Continuando con el protocolo BGP nos dirigimos al Router R2 y hacemos el mismo paso del Router R1 damos clic en el recuadro de (+) en la ventana desplegada como nombre insertamos R1 en la sección de AS colocamos 200 y en Router ID insertamos la siguiente dirección IP 10.10.10.2, como parte final seleccionamos la casilla **Redistribute Other BGP**, por últimos damos aplicar y Ok, dentro del mismo Router 2 agregamos otro protocolo BGP con el siguiente Nombre R3 en la casilla AS insertamos el valor de 200 en Router ID la siguiente dirección IP 10.10.20.1y también seleccionamos la opción de **Redistribute Other BGP**, aplicamos y damos ok.

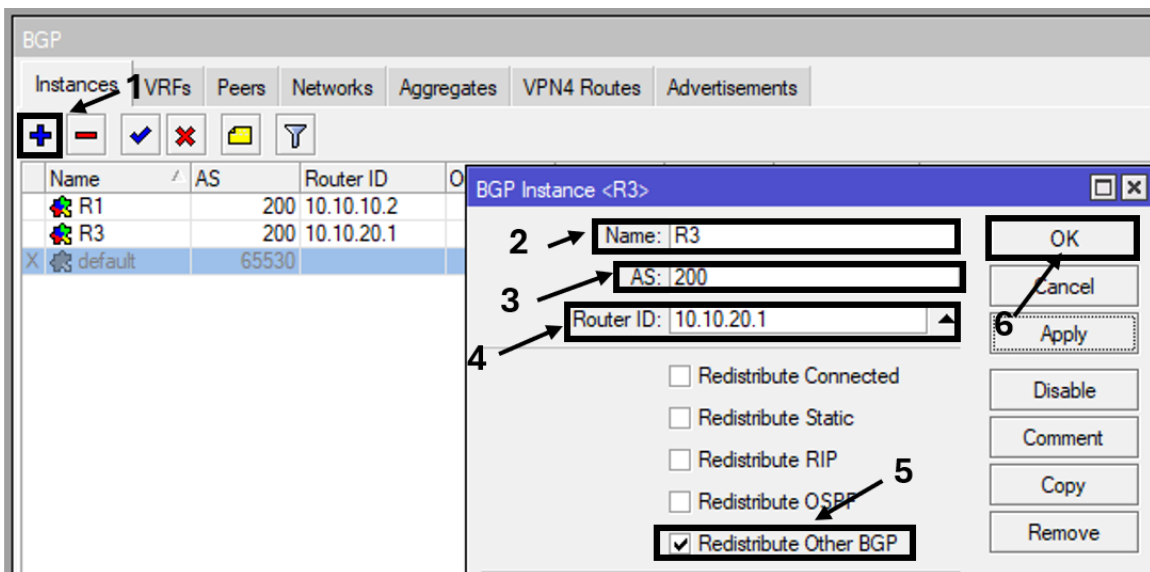


Figura 133. Configuración de protocolo bgp del router R2
Imagen elaborada por el autor

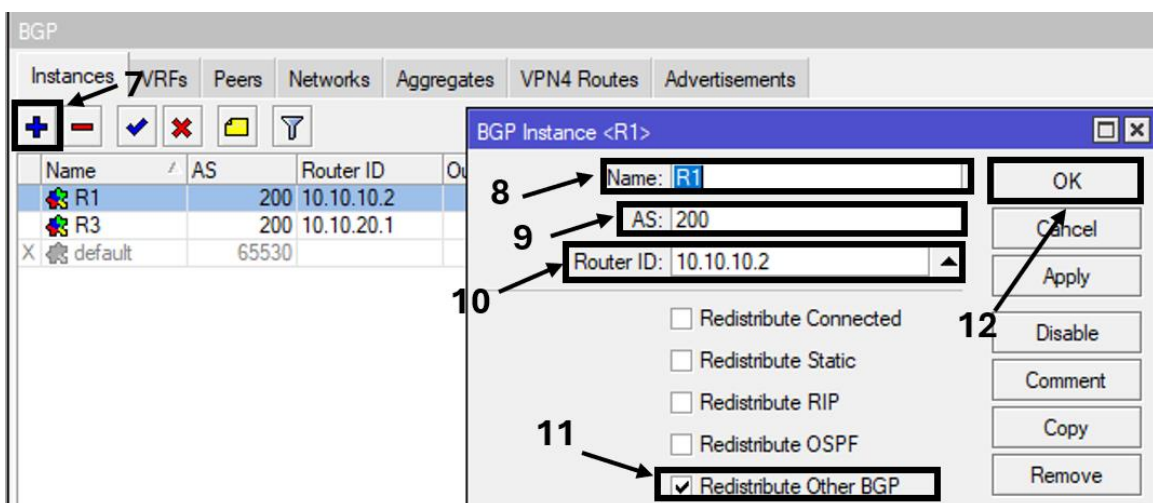


Figura 134 Configuración del BGP
Imagen elaborada por el autor

Nos dirigimos al Router R3 y procedemos hacer la misma configuración del Router R1 y Router R2, nos dirigimos a la pestaña de Routing y seleccionamos BGP damos clic en la ventana interfaces y clic en el recuadro (+) en la casilla de Name insertamos el siguiente nombre R3300, en la sección de AS insertamos 300 y en Router ID la siguiente dirección IP 10.10.20.2 por último seleccionamos la casilla **Redistribute Other BGP**, aplicamos y damos OK.

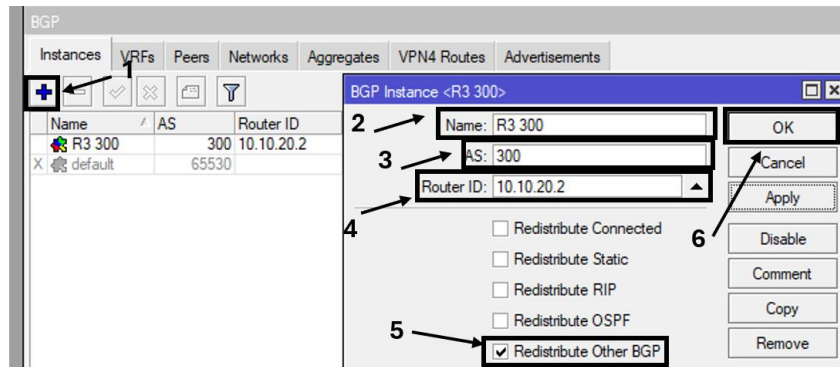


Figura 135. Configuración del protocolo bgp en router 3 R3
Imagen elaborada por el autor

Continuamos con el protocolo BGP dentro de BGP seleccionamos la pestaña **PEERS**, en esta pestaña configuramos la comunicación entre los sistemas autónomos, damos clic en (+) se desplegará una ventana donde nos situamos en la pestaña **General**, en la sección de Name insertamos un nombre relacionado entre equipos R1-R2, seguido en la casilla **Instance** y seleccionamos la R1 100, en **Remote Address**, colocamos la siguiente dirección IP **10.10.10.2** esta es la ip vecina, continuando en la sección de Remote AS le damos un valor de sistema autónomo del router vecino con su relación par de 200, por ultimo damos aplicar y OK,

Ahora nos situamos en el Router R2 en la pestaña **Routing** y sección **BGP** en el pestaña **PEERS**, damos clic en (+) para comenzar en el apartado de Nombre digitamos el siguiente R2-R1, en **Instance** seleccionamos la R1 con la siguiente dirección IP **10.10.10.1**, damos clic en Remote AS e insertamos el valor de 100, dentro del mismo equipo agregamos otra relación damos clic en (+) en Name de la ventana general colocamos en este caso la relación R2-R3 en **Instance** seleccionamos la R3, en Remote Address digitamos la siguiente dirección IP **10.10.20.2**, y en Remote AS le damos el valor de 300 por últimos damos clic en aplicar y OK.

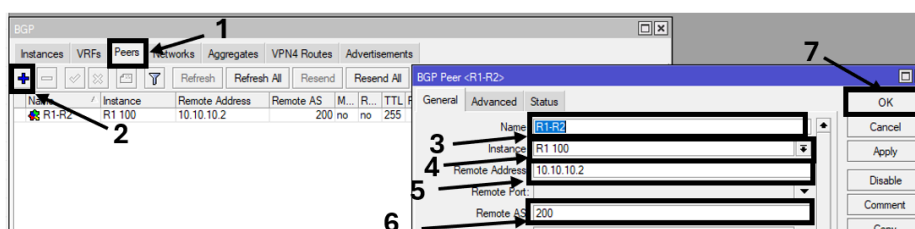


Figura 136. Añadir sistema autónomo a R1
Imagen elaborada por el autor

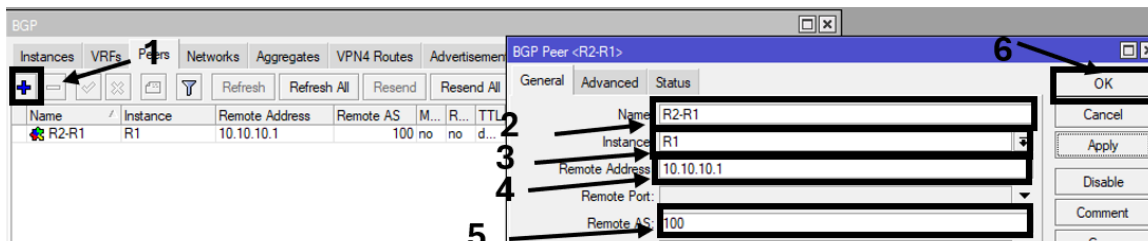


Figura 137. Añadir sistema autónomo a R2
Imagen elaborada por el autor

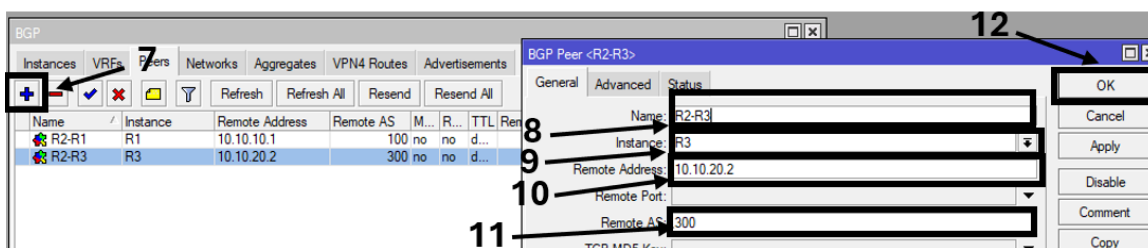


Figura 138. Añadir sistema autónomo a R2
Imagen elaborada por el autor

Dentro del Router R3, seguimos los mismos pasos del de Router R1 y R2 dentro del Winbox del Router R3 nos dirigimos a la pestaña Routing la sección BGP luego nos centramos en la ventana **PEERS**, damos clic en (+), en la sección Name digitamos R3-R2 en **Intance** seleccionamos la opción R3 300, en Remote Address digitamos la dirección IP 10.10.20.1, y en Remote AS digitamos el siguiente valor de 200 por último aplicamos y damos OK.

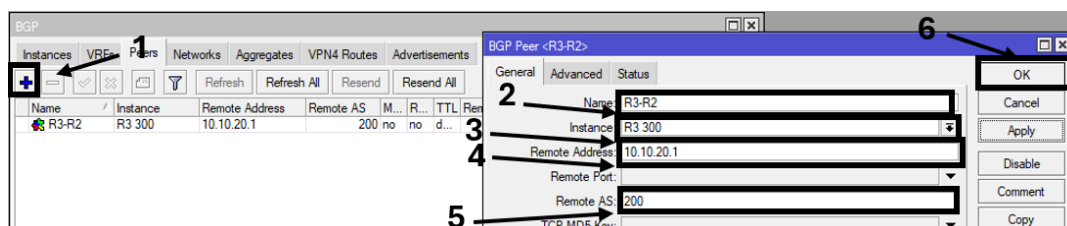


Figura 139. Añadir sistema autónomo a R3
Imagen elaborada por el autor

Como siguiente nos dirigimos a la ventada de Networks para configurar la publicación de las LAN en cada router se procede hacer la siguiente configuración dentro de la ventana Networks damos clic en (+) , se desplegara una nueva ventada y colocamos la siguiente dirección IP **192.168.100.0/24**, damos clic en comment luego digitamos el nombre en este caso LAN-1, por ultimo damos aplicar y OK, realizamos el mismo paso para el Router R2 y el Router R3, para router R2 ingresamos la siguiente dirección IP **192.168.110.0/24**, y dejamos un comentario LAN-

2, para el ultimo equipo R3 digitamos la siguiente dirección IP **192.168.120.0/24** y de comentario colocamos LAN-3 como ultimo daos en aplicar y OK.

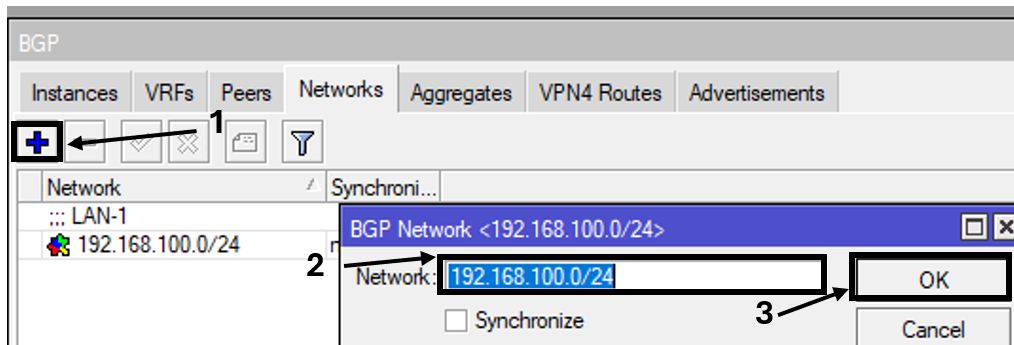


Figura 140. Configuración de la ventana networks en router1
Imagen elaborada por el autor

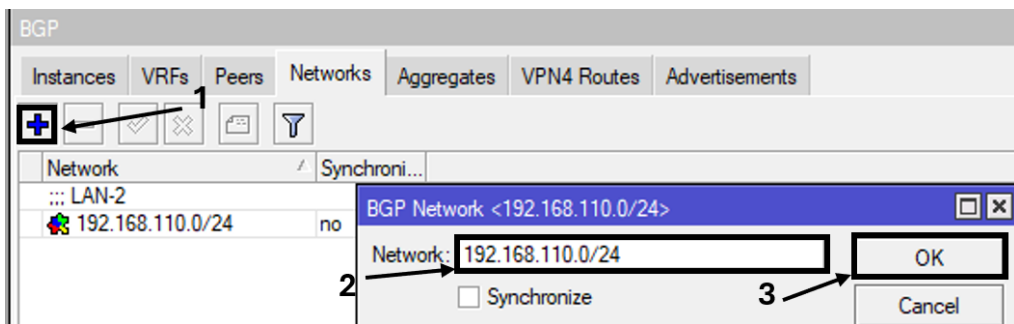


Figura 141. Configuración de la ventana networks en router2
Imagen elaborada por el autor

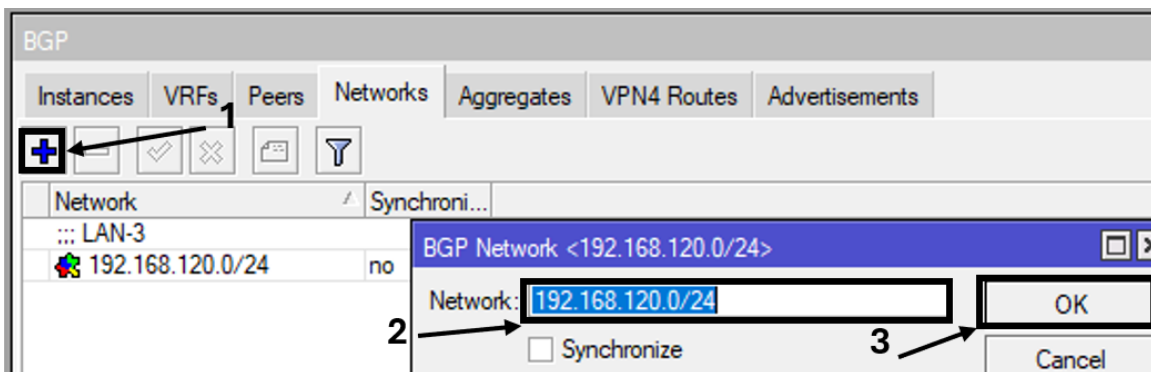
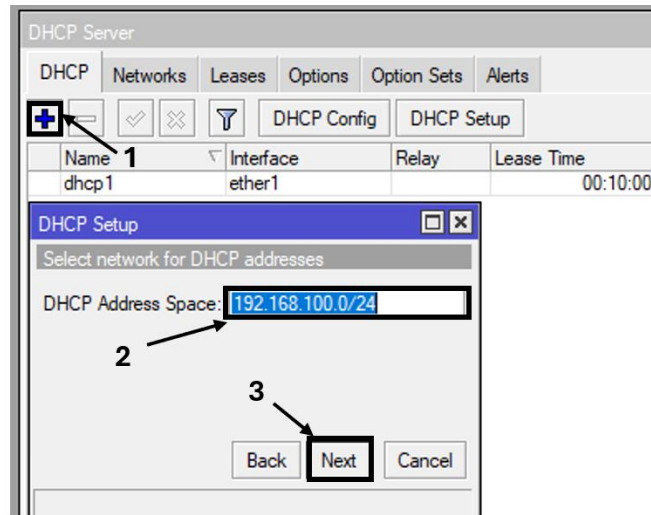


Figura 142. Configuración de networks en R3
Imagen elaborada por el autor

Configuración dhcp en las interfaces lan.

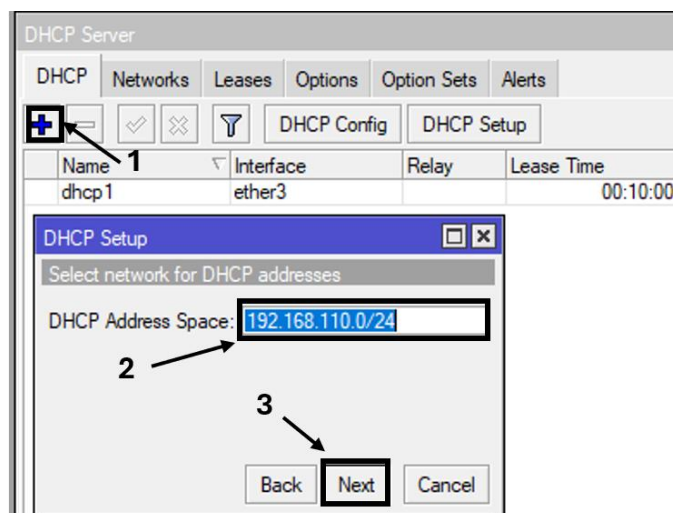
Para siguiente configuración DHCP nos situamos dentro del Winbox del Router R1, dentro de la pestaña IP seleccionamos la opción de DHCP Server, una vez dentro damos clic en (+) se nos desplegara una ventana donde seleccionamos DHCP Setup damos clic en la interfaz ether 2, luego ingresamos la red LAN-1, continuando damos clic en next y en DHCP Address Space digitamos

siguiente dirección IP **192-168.100.1** del Gateway, después se ingresa el rango de direcciones IP **192-168.100.2 - 192-168.100.254** y el tiempo le dejamos por defecto 10 minutos, damos ok y podemos observar el DHCP server ya creado.



*Figura 143. Configurar dhcp setup R1
Imagen elaborada por el autor*

El mismo paso del Router R1 lo realizamos para el Router R2 dentro del Winbox, nos dirigimos a la pestaña IP seleccionamos la opción DHCP Server, damos clic en DHCP Setup, se desplegará una ventana dónde colocamos primero la interfaz en este caso seleccionamos la interfaz ether 3, luego damos clic en next y colocamos la siguiente dirección IP **192.168.110.0/24**, continuando colocamos el rango de direcciones IP **192-168.110.2 - 192-168.110.254**, por último dejamos los 10 minutos por defecto, ya realizado podemos observar la interfaz ya creada.



*Figura 144. Configurar dhcp setup R2
Imagen elaborada por el autor*

Realizamos el mismo paso en el router 3 nos dirigimos al Winbox dentro seleccionamos la casilla IP y damos clic en DHCP Server, se desplegará una ventana donde primero seleccionamos la interfaz ether 2 luego insertamos en la casilla DHCP Address Space la siguiente dirección Ip **192.168.120.0/24**, damos clic en next y colocamos el rango de direcciones IP **192-168.120.2 - 192-168.120.254**, damos clic en next y nos pedirá que ingresemos un tiempo este le dejamos por defecto 10 mins por ultimo damos ok y podemos observar la interfaz ya creada.

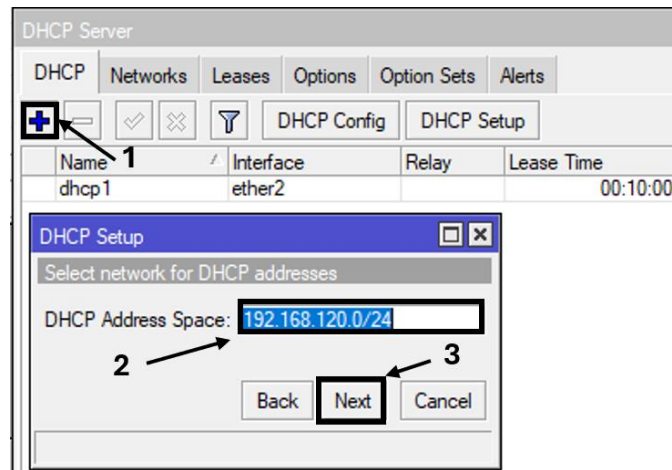


Figura 145. Configurar dhcp setup R3
Imagen elaborada por el autor

Dentro de Router R1 nos dirigimos a la pestaña de IP y seleccionamos la opción Routes, donde se nos desplegará una ventana donde podemos observar las rutas de los equipos mediante el Protocolo BGP de la misma manera revisamos el Route List en los demos Routers R2 y R3

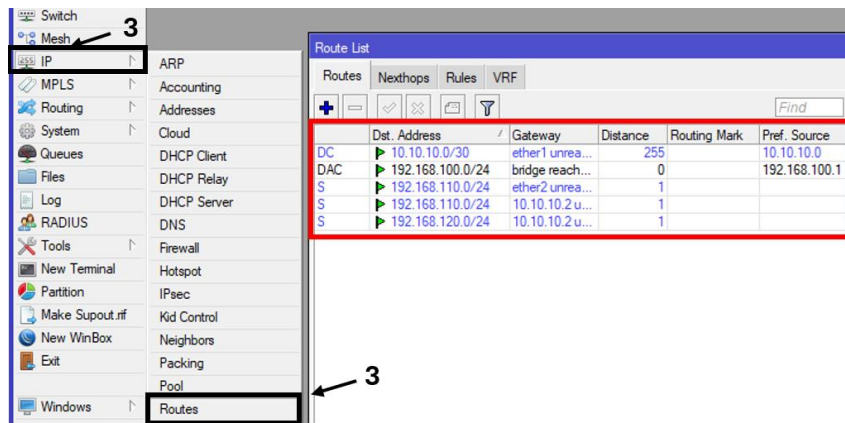


Figura 146. Tabla de direcciones ip enlazadas R1
Imagen elaborada por el autor

Route List del Router 2 Tabla de Enrutamiento por parte del protocolo BGP

	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
S	10.10.10.0/30	10.10.10.2 unre...	1		10.10.10.2
S	10.10.20.0/30	ether2 unreacha...	1		10.10.20.1
DAC	192.168.2.0/24	bridge reachable	0		192.168.2.3
S	192.168.110.0/24	ether3 unreacha...	1		192.168.110.1
S	192.168.120.0/24	ether2 unreacha...	1		

*Figura 147. Tabla de direcciones ip enlazadas R2
Imagen elaborada por el autor*

Route List del Router 3 Tabla de Enrutamiento por parte del protocolo BGP

	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
S	192.168.120.0/24	ether2 unreachable	1		192.168.120.1
S	10.10.20.0/30	ether1 unreachable	1		10.10.20.2
DAC	192.168.5.0/24	bridge reachable	0		192.168.5.6
S	192.168.100.0/24	10.10.20.1 unreach...	1		
S	192.168.110.0/24	10.10.20.1 unreach...	1		

*Figura 148. Tabla de direcciones ip enlazadas R3
Imagen elaborada por el autor*

Comprobar la conectividad

Para comprobar la conectividad entre LAN-1 Y LAN-2 se procede a realizar un ping mediante el terminal de Windows de la PC(HOST1) hacia la LAN-2, como se puede observar en el Router R1, dentro del Winbox en la opción DHCP Server damos clic en la ventana Leases, observamos que existe una conectividad, ingresando al Router R2 con el mismo paso del R1 en DHCP Server -Lease podemos ver que recibe la conectividad.

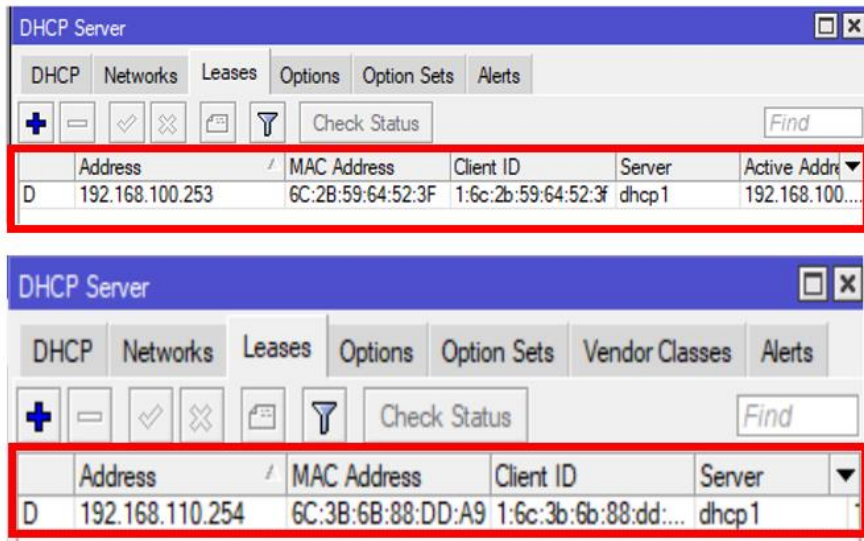


Figura 149. dhcp de lan-1 y lan-2
Imagen elaborada por el autor

Dentro del terminal (CMD) realizamos un **ipconfig** para ver la dirección ip del ordenador, observamos que es la siguiente **192.168.100.253**, continuando realizamos un ping hacia la siguiente dirección **192.168.110.254** y como resultado vemos que existe una conectividad.

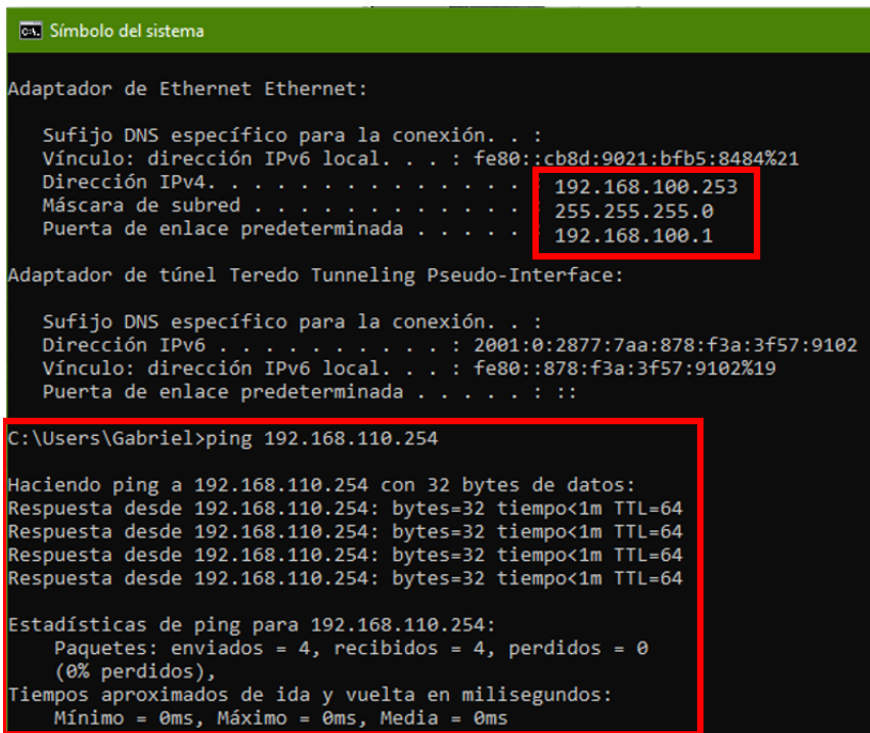
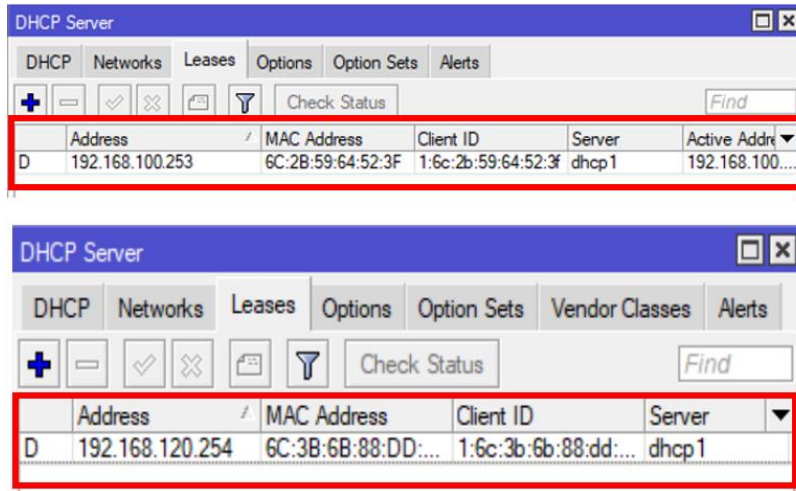


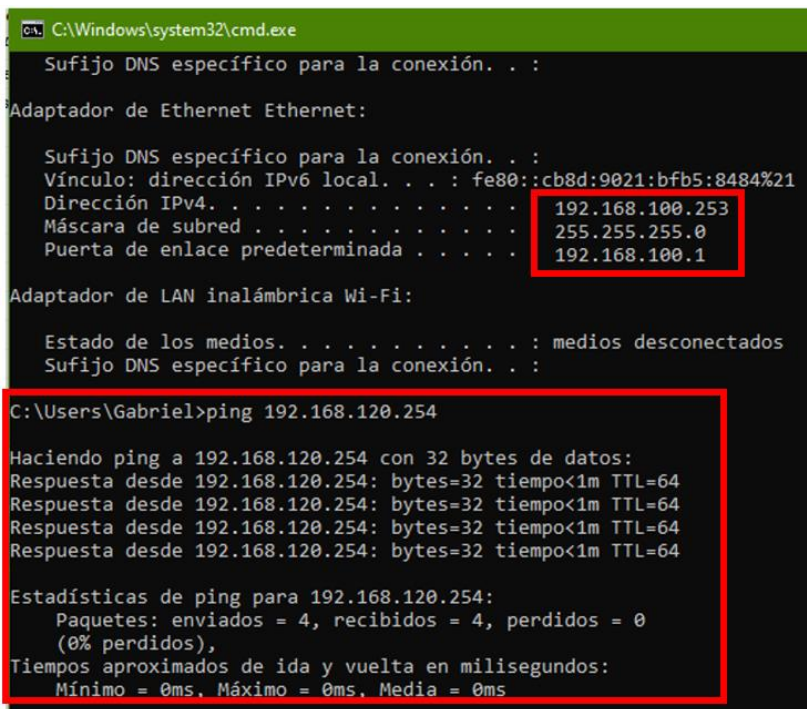
Figura 150. Conexión establecida entre lans
Imagen elaborada por el autor

De la misma manera como segunda prueba, realizaremos un ping desde la LAN-1 hacia la LAN-3 comprobamos dentro del router R1 y el router R3 que exista conectividad como se puede observar dentro de los equipos podemos ver las direcciones IP de las LANS.



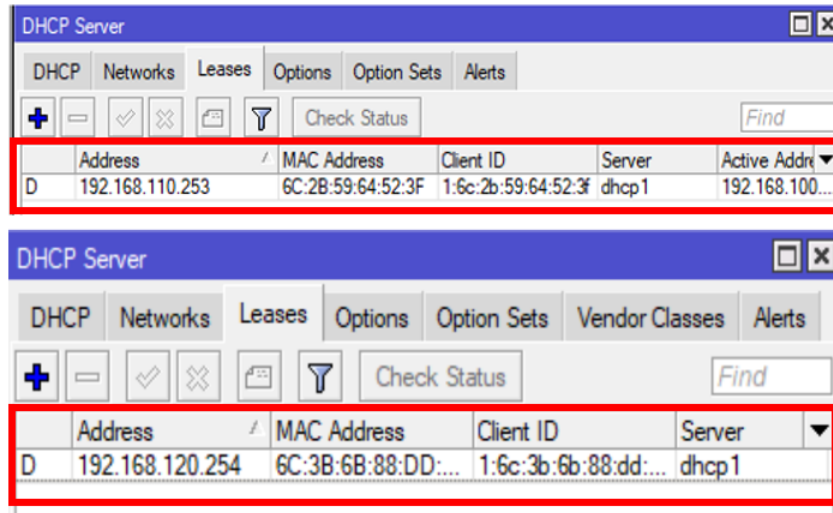
*Figura 151. dhcp de lan-1 y lan-3
Imagen elaborada por el autor*

Desde la terminal de Windows CMD desde el Host1 hacemos ping al Host3 de la LAN-3 como podemos ver contamos con la misma dirección IP de la PC1 que es la **192.168.100.253**, realizamos ping hacia la siguiente dirección IP **192.168.120.254**, y como respuesta podemos ver que existe una conectividad.

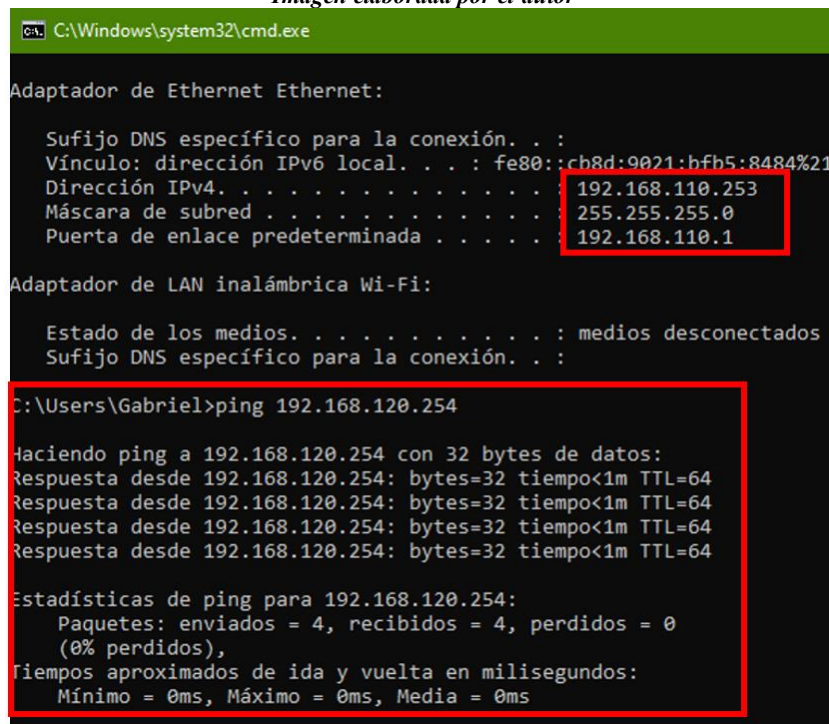


*Figura 152. Conectividad exitosa
Imagen elaborada por el autor*

Como tercera prueba se realizará un ping desde la LAN-2 hacia la LAN-3, se realiza el mismo procedimiento del router R1 y R2 ingresando al Winbox donde podemos ver que existe una conectividad, dentro del Host2 realizaremos un ping hacia el Host3 mediante el CMD del Host2 realizamos un ping con la siguiente dirección IP **192.168.120.254**, podemos ver que exitosamente existe conectividad.



*Figura 153. dhcp de lan-2 y lan-3
Imagen elaborada por el autor*



*Figura 154. Conexión establecida
Imagen elaborada por el autor*


Bibliografía

- [1] J. J. Santos Chavez, «eltaprotect,» 21 Mayo 2024. [En línea]. Available: <https://www.deltaprotect.com/blog/seguridad-de-la-red>. [Último acceso: 10 Octubre 2024].
- [2] G. Verdejo, «cs.upc.edu,» 2020. [En línea]. Available: <https://www.cs.upc.edu/~gabriel/files/pretesis-es-3ObjetivosdelatesissobreDDOS.pdf>.
- [3] F. D. Cuyo, «dspace.udla.edu.ec,» 2019. [En línea]. Available: <https://dspace.udla.edu.ec/bitstream/33000/11567/1/UDLA-EC-TIRT-2019-29.pdf>.
- [4] Marco, «Youtube,» [En línea]. Available: <https://www.youtube.com/watch?v=KvhmCBcyFV8>.
- [5] P. Ricardo Delgado, «repositorio.espam.edu.ec,» Junio 2019. [En línea]. Available: <https://repositorio.espam.edu.ec/bitstream/42000/477/1/TC107.pdf>.
- [6] D. O. Espin, Agosto 2022. [En línea]. Available: <https://dspace.ups.edu.ec/bitstream/123456789/23007/1/UPS%20-%20TTS857.pdf>.
- [7] «redfibra,» 28 Septiembre 2020. [En línea]. Available: <https://redfibra.mx/que-es-un-firewall-y-como-funciona-tipos-de-firewall/>.
- [8] Z. Alvarez Torres, «dspace.udla.edu.ec,» 2019. [En línea]. Available: <https://dspace.udla.edu.ec/jspui/bitstream/33000/10898/1/UDLA-EC-TIERI-2019-08.pdf>.
- [9] J. L. Valenzuela, «tesis.pucp.edu.pe,» Junio 2012. [En línea]. Available: https://tesis.pucp.edu.pe/repositorio/bitstream/handle/20.500.12404/1448/VALENZUELA_GONZALES_JORGE_ARQUITECTURA_SEGURIDAD_PERIMETRAL.pdf;jsessionid=29C326E50271B401F6C5034989C1B360?sequence=1.
- [10] B. V. Georges y H. L. Vera, «dspace.espol.edu.ec,» 2011. [En línea]. Available: <https://dspace.espol.edu.ec/bitstream/123456789/41168/1/T-83280%20FLAMENT-VERA.pdf>.
- [11] H. C. Manchenoy I. L. Robles, «repositorio.ucsg.edu.ec,» 2013. [En línea]. Available: <http://repositorio.ucsg.edu.ec/bitstream/3317/1399/1/T-UCSG-PRE-TEC-ITEL-13.pdf>.
- [12] «UNAD,» [En línea]. Available: https://kevin-florez3382.github.io/OVI_SEGURIDA_INFORMATICA/Firewalls.html.

- [13] J. Urbano Plaza, «dspace.utb.edu.ec,» 2022. [En línea]. Available: <https://dspace.utb.edu.ec/bitstream/handle/49000/11648/E-UTB-FAFI-SIST-000314.pdf?sequence=1&isAllowed=y>.
- [14] Mackie, «RICLabs,» 16 Abril 2016. [En línea]. Available: <https://packetmasters.wordpress.com/2016/04/16/mikrotik-firewall/>.
- [15] M. Camí, «mscdroidlabs,» 22 Enero 2021. [En línea]. Available: <https://mscdroidlabs.es/modo-de-red-restringido-la-nueva-funcion-implementada-en-android-12/>.
- [16] J. Delgado, «dspace.ups.edu.ec,» 2018. [En línea]. Available: <https://dspace.ups.edu.ec/bitstream/123456789/15961/1/UPS-GT002232.pdf>.
- [17] P. I. U. T. I. L. Quinte Sinche, «bibdigital.epn.edu.ec,» 13 Enero 2020. [En línea]. Available: <https://bibdigital.epn.edu.ec/handle/15000/20647>.
- [18] Instituto Tecnológico ADA, «MTCNA,» 2023. [En línea]. Available: <https://adaits.es/certificaciones/mtcna/>.
- [19] B. Mauricio Palate y D. Alvia Pesantez, «Mitigación de vulnerabilidades en la red central de un ISP: Un caso de estudio,» GDEON, 2021.
- [20] S. Tech, «Sinip,» 14 Noviembre 2020. [En línea]. Available: <https://sinip.tech/2020/11/14/como-configurar-un-mikrotik-para-prevenir-intrusos/>.
- [21] J. E. Báez Cheza, «Metodología de detección y mitigación de ataques DDOS en entornos SDN basado en la norma ISO/IEC 27001 para mejorar la seguridad en el plano de control,» repositorio.utn.edu.ec, Ibarra, 2021.
- [22] S. D. Medina Joven y D. A. Losada Ninco, «Conocimiento de un ataque DDoS,» repository.ucc.edu.co, 2017.
- [23] D. X. Bonifaz Herrera y M. M. Miranda Martínez, «<http://dspace.unach.edu.ec/>,» 2018. [En línea]. Available: <http://dspace.unach.edu.ec/bitstream/51000/5489/1/UNACH-EC-ING-SIT-COMP-2019-0003.pdf>.
- [24] J. O. Tamayo Portero, «Detección de ataques de denegación de servicio activados mediante botnets en redes definidas por software,» bibdigital.epn.edu.ec, 2023.
- [25] R. X. Amaguaya Ramos, «bibdigital.epn.edu.ec,» 2020. [En línea]. Available: <https://bibdigital.epn.edu.ec/bitstream/15000/21374/1/CD%2010446.pdf>.
- [26] J. A. Abril Useche y A. K. Sánchez Rodríguez, «Detección y alarma de ataques DDoS en servicio DNS,» repository.javeriana.edu.co, Bogotá, 2023.
- [27] J. J. Toaquiza Morocho, «<http://dspace.unach.edu.ec/>,» 2019. [En línea]. Available: <http://dspace.unach.edu.ec/bitstream/51000/6178/1/An%c3%a1lisis%20del%20m>

- ecanismo%20de%20detecci%3%b3n%20y%20defensa%20h%3%adbrido%20fre
nte%20a%20los%20ataques%20IP%20Spoofting.pdf.
- [28] D. A. Cazar Jácome, «Análisis de IP Spoofing en redes IPv6,» bibdigital.epn.edu.ec, Quito, 2015.
- [29] F. J. Aguilar Feijóo, «repositorio.uta.edu.ec,» 2019. [En línea]. Available: <https://repositorio.uta.edu.ec/server/api/core/bitstreams/6f10dfa8-17a7-451f-8f6f-6725d6124394/content>.
- [30] H. L. Herrera Figueroa, «dspace.ucuenca.edu.ec,» 2015. [En línea]. Available: <https://dspace.ucuenca.edu.ec/bitstream/123456789/22353/3/Tesis.pdf>.
- [31] G. A. Rodríguez Paladines, «Implementación de un prototipo de laboratorio para el estudio de ataques de seguridad en redes,» bibdigital.epn.edu.ec, Quito, 2016.
- [32] «kaspersky,» [En línea]. Available: <https://latam.kaspersky.com/resource-center/threats/ip-spoofing>.
- [33] E. F. Ruiz Andino, Junio 2022. [En línea]. Available: <http://dspace.esepoch.edu.ec/bitstream/123456789/17176/1/20T01575.pdf>.
- [34] R. Bustamante Sánchez, 2005. [En línea]. Available: <https://www.uaeh.edu.mx/docencia/Tesis/icbi/licenciatura/documentos/Seguridad%20en%20redes.pdf>.
- [35] A. D. V. Gualotuña, «bibdigital.epn.edu.ec,» Febrero 2021. [En línea]. Available: <https://bibdigital.epn.edu.ec/bitstream/15000/21434/1/CD%2010926.pdf>.
- [36] M. E. N. PORTILLO, «dspace.ups.edu.ec,» Mayo 2015. [En línea]. Available: <https://dspace.ups.edu.ec/bitstream/123456789/10179/6/UPS%20-%20ST001825.pdf>.
- [37] «arroba system,» 2021 Febrero 2021. [En línea]. Available: ¿Qué son las amenazas informáticas y cómo protegerte de ellas?.
- [38] «inttelec,» [En línea]. Available: <https://www.inttelec.com/shop/swl6-swl6-licencia-mikrotik-routeros-nivel-6-29133>.

ANEXO

 **CERTIFICADO DE ANÁLISIS**
magister

Tesina_FINAL

7%
Textos sospechosos

< 1% Similitudes
< 1% similitudes entre comillas
0% entre las fuentes mencionadas

1% Idiomas no reconocidos

5% Textos potencialmente generados por la IA

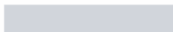
Nombre del documento: Tesina_FINAL.pdf
ID del documento: 5c407ab8014de8f3e32502b4349902981c4e0a7c
Tamaño del documento original: 12,38 MB
Autores: []

Depositante: FERNANDO VINICIO CHAMBA MACAS
Fecha de depósito: 26/11/2024
Tipo de carga: interface
fecha de fin de análisis: 26/11/2024






Número de palabras: 22.228
Número de caracteres: 154.395

Ubicación de las similitudes en el documento:

Fuente con similitudes fortuitas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	 bibdigital.epn.edu.ec Repositorio Digital - EPN: Maestría en Software (FIS) https://bibdigital.epn.edu.ec/handle/15000/19618	< 1%		 Palabras idénticas: < 1% (11 palabras)

Fuentes mencionadas (sin similitudes detectadas) Estas fuentes han sido citadas en el documento sin encontrar similitudes.

-  <http://www.mikrotik.com/>
-  <https://www.deltaprotect.com/blog/seguridad-de-la-red>
-  <https://www.cs.upc.edu/~gabriel/files/pretesis-es>
-  <https://dspace.udla.edu.ec/bitstream/33000/11567/1/UDLA-EC-TIRT-2019>
-  <https://www.youtube.com/watch?v=KvhmCBcyFV8>