UNIVERSITAT POLITÈCNICA DE VALÈNCIA

etsinf

Escola Tècnica Superior d'Enginyeria Informàtica

Escola Tècnica Superior d'Enginyeria Informàtica
Universitat Politècnica de València

Memoria 1 Perimetro

TRABAJO SRE

Grado en Ingeniería Informática

Autor: Cappellaro, Gabriele
Lambaraa Ben Razzouq, Anass
Lorente Núñez, Vicente Rafael
Raga Riera, Pablo
Sanchez Temporal, Sergio
Sopeña Urbano, Enrique

Curso 2024-2025

Resumen

Este proyecto tiene como objetivo diseñar e implementar una red corporativa utilizando dos routers MikroTik para gestionar el tráfico entre varias subredes. La red se estructura para proporcionar conectividad interna eficiente entre distintos departamentos y servidores, garantizando también un acceso controlado a Internet. Las subredes se organizan con fines específicos, como usuarios, auditorías, monitoreo y sistemas, asignándoles rangos de direcciones IP adecuados.

El diseño se centra en dos routers principales: un *router interno*, encargado de la gestión del tráfico interno y de las subredes, y un *router externo*, que maneja el tráfico hacia la WAN y las zonas desmilitarizadas (DMZ), donde se alojan servicios como servidores DNS y web. Este diseño permite separar el tráfico interno del expuesto a Internet, lo que refuerza la seguridad de la red.

Se implementará *Network Address Translation* (NAT) para permitir que los dispositivos internos accedan a Internet a través de una única IP pública, lo cual mejora la seguridad y eficiencia en el uso de direcciones. También se configurarán reglas de *firewall* para proteger la red contra accesos no autorizados, regulando el tráfico de entrada y salida.

Adicionalmente, se integrarán servicios como *DHCP* para la asignación dinámica de direcciones IP, y se establecerá una red WiFi gestionada por el router interno para proporcionar conectividad inalámbrica. Asimismo, se implementará un sistema de monitoreo y auditoría para supervisar el tráfico y detectar posibles anomalías o amenazas, garantizando tanto la seguridad como el rendimiento de la red.

En resumen, el proyecto busca crear una red segura y escalable que ofrezca interconectividad entre dispositivos y servicios, asegurando un acceso controlado a Internet y protegiendo los recursos internos mediante mecanismos de seguridad como la segmentación de red y las reglas de *firewall*.

Palabras clave: DNS, DHCP, Firewall, IDS, IP, NAT, WAN

Abstract

This project aims to design and implement a corporate network using two MikroTik routers to manage traffic between various subnets. The network is structured to provide efficient internal connectivity between different departments and servers, while also ensuring controlled access to the Internet. The subnets are organized for specific purposes, such as users, audits, monitoring, and systems, assigning them appropriate IP address ranges.

The design focuses on two main routers: an internal router responsible for managing internal traffic and subnets, and an external router that handles traffic to the WAN and demilitarized zones (DMZ), where services such as DNS and web servers are hosted. This design allows for the separation of internal traffic from that exposed to the Internet, reinforcing the network's security.

Network Address Translation (NAT) will be implemented to allow internal devices to access the Internet through a single public IP address, enhancing security and efficiency in address usage. Firewall rules will also be configured to protect the network from unauthorized access by regulating incoming and outgoing traffic.

Additionally, services such as DHCP will be integrated for dynamic IP address assignment, and a WiFi network managed by the internal router will be established to provide

wireless connectivity. A monitoring and auditing system will also be implemented to supervise traffic and detect potential anomalies or threats, ensuring both the security and performance of the network.

In summary, the project seeks to create a secure and scalable network that offers interconnectivity between devices and services, ensuring controlled access to the Internet and protecting internal resources through security mechanisms such as network segmentation and firewall rules.

Key words: DNS, DHCP, Firewall, IDS, IP, NAT, WAN

Índice general

Índice de figuras

Índice de tablas

CAPÍTULO 1
Introducción

En un entorno corporativo, la correcta gestión de la red es fundamental para asegurar el funcionamiento eficiente de los servicios, la protección de los datos y la conectividad entre los diferentes usuarios y dispositivos. En este contexto, el presente proyecto se enfoca en la creación e implementación de una red basada en la tecnología de routers MikroTik, que permita tanto la segmentación de la red interna como el acceso controlado a Internet.

El proyecto tiene como base la configuración de dos routers MikroTik que gestionan las comunicaciones internas entre varias subredes y la salida de la red a través de un punto de acceso externo a Internet. Esto no solo implica la creación de una infraestructura de red robusta, sino también la implementación de políticas de seguridad mediante reglas de *firewall* y la configuración de *Network Address Translation* (NAT) para garantizar un acceso seguro y eficiente a la red externa.

Adicionalmente, se integrarán servicios clave, como la asignación de direcciones IP dinámicas mediante *DHCP*, la creación de una red inalámbrica interna y un sistema de monitoreo que permita supervisar el rendimiento de la red, así como detectar y prevenir posibles amenazas.

La correcta segmentación de la red en diferentes subredes permitirá una mejor gestión del tráfico interno y la implementación de políticas de acceso según las necesidades de cada área de la organización. Este enfoque no solo facilita la administración de la red, sino que también asegura una mayor flexibilidad y escalabilidad a medida que las necesidades de la infraestructura evolucionan.

En resumen, el proyecto busca implementar una solución de red eficiente, segura y escalable, adaptada a las necesidades de una organización moderna, garantizando la interconectividad de sus recursos, la protección de sus datos y el acceso controlado a los servicios de Internet.

1.1 Objetivos del Proyecto

El objetivo principal del proyecto es la configuración de una red corporativa eficiente y segura utilizando dos routers MikroTik para gestionar tanto la conectividad interna como el acceso a Internet. A continuación se detallan los objetivos específicos:

- **Configuración de las subredes:** Definir y segmentar la red en varias subredes con fines específicos, asignando rangos de direcciones IP apropiados para cada una, asegurando la interconectividad entre ellas.

- **Conexión a Internet:** Implementar un enrutamiento adecuado que permita el acceso a Internet desde las subredes internas, utilizando el router externo como punto de salida hacia la WAN.
- **Seguridad de la red:** Establecer políticas de seguridad mediante la configuración de reglas de *firewall* para proteger la red de accesos no autorizados, controlando el tráfico entre las subredes internas y el tráfico hacia y desde Internet.
- **Implementación de NAT:** Configurar *Network Address Translation* (NAT) para permitir que las máquinas dentro de la red interna accedan a Internet utilizando una única dirección IP pública, mejorando la gestión de direcciones IP y la seguridad.
- **WiFi:** Configurar una red inalámbrica gestionada por el router interno, que permita la conexión de dispositivos móviles y portátiles a la red corporativa de forma segura.
- **Monitoreo y auditoría:** Implementar un sistema de monitoreo para supervisar el tráfico de la red y un sistema de auditoría que permita la detección de anomalías o posibles amenazas, garantizando la seguridad y el rendimiento de la red.
- **Optimización y escalabilidad:** Asegurar que la red esté optimizada para un funcionamiento eficiente, con una arquitectura que permita la escalabilidad para adaptarse a futuras expansiones de la infraestructura.

1.2 Tareas del proyecto

El éxito de un proyecto de red depende en gran medida de la planificación y ejecución meticulosa de diversas tareas. A continuación, se describen las principales tareas involucradas en el desarrollo de este proyecto, cada una de las cuales desempeña un papel crucial en la creación de una infraestructura de red eficiente y segura. Estas tareas abarcan desde el diseño inicial de la red hasta la implementación de medidas de seguridad y la documentación del proceso. A continuación, se presentan las tareas de manera más detallada:

1. **Diseño de la red:** Esta fase implica la planificación de la arquitectura de la red, teniendo en cuenta factores como la topología, la capacidad de los dispositivos y la distribución geográfica de los equipos. El diseño debe garantizar que la red sea escalable, eficiente y capaz de satisfacer las necesidades de los usuarios.
2. **Asignación de las IPs a las distintas subredes:** En esta etapa, se llevará a cabo la segmentación de la red en subredes adecuadas y la asignación de direcciones IP. Esto incluye la definición de rangos de IP, la creación de subredes y la planificación de la asignación de direcciones para dispositivos específicos, lo que facilita una gestión más eficiente del tráfico de red.
3. **NAT:** La implementación de la traducción de direcciones de red (NAT) es esencial para permitir la comunicación entre dispositivos en una red privada y el acceso a Internet. Esta tarea incluye la configuración de NAT para que las direcciones IP internas se traduzcan correctamente a direcciones públicas.
4. **Router:** La configuración adecuada de los routers es fundamental para el funcionamiento óptimo de la red. Esto incluye:

a. **Router Interno:**
   I. **Configuración Inicial:** Se establece la configuración básica del router, incluyendo parámetros como la dirección IP, las credenciales de acceso y la configuración de las interfaces.
   II. **Servidor DHCP:** Esta tarea implica configurar un servidor DHCP en el router interno para asignar direcciones IP dinámicas a los dispositivos de la red, facilitando la gestión de direcciones.
   III. **Configuración Wireless:** Se configurará la red inalámbrica, incluyendo la seguridad y el nombre de la red (SSID), para proporcionar conectividad a dispositivos móviles y portátiles.

b. **Router Externo:**
   I. **Configuración Inicial:** Al igual que el router interno, se establece la configuración básica del router externo, asegurando que esté correctamente conectado a Internet y configurado para manejar el tráfico de entrada y salida.
   II. **Desactivar opción wireless:** Dado que el router externo no necesita ofrecer conectividad inalámbrica, se desactivará esta opción para mejorar la seguridad y reducir la superficie de ataque.

5. **Seguridad:** La implementación de medidas de seguridad es vital para proteger la red contra amenazas externas e internas. Esto incluye:

   a. **Firewall del router interno:** Se configurará un firewall en el router interno para filtrar el tráfico no deseado y proteger la red local de posibles ataques.
   b. **Firewall del router externo:** Del mismo modo, se establecerán reglas de firewall en el router externo para proteger la red de amenazas provenientes de Internet.

6. **Documentación del proyecto:** La última tarea consiste en documentar todo el proceso, incluyendo el diseño de la red, la configuración de los dispositivos y la seguridad implementada. Esta documentación será esencial para futuras referencias y para la gestión del mantenimiento de la red.

CAPÍTULO 2
Desarrollo del proyecto (Actualmente)

2.1 Fase de documentación

Antes de iniciar la configuración de los routers y la implementación de la red, se llevó a cabo una fase de documentación exhaustiva. Esta fase fue crucial para comprender las mejores prácticas y procedimientos necesarios para configurar de manera efectiva los routers MikroTik, especialmente en lo que respecta a la asignación de direcciones IP, la configuración del *DHCP* y la correcta gestión de las interfaces de red. Durante esta etapa, se consultaron varias fuentes de información confiables, que nos permitieron adquirir un conocimiento detallado sobre las características y funcionalidades de los equipos MikroTik.

Una de las fuentes principales utilizadas fue la página web oficial de MikroTik, específicamente en su guía titulada *"Cómo configurar un router"*[2]. Este recurso proporcionó una visión clara y estructurada sobre los pasos iniciales para la configuración básica del router. Desde la asignación de una dirección IP estática en la interfaz principal hasta la creación de rutas predeterminadas para la salida a Internet, la guía sirvió como base para entender cómo establecer correctamente el enrutamiento en una red local. Además, permitió definir el esquema de direccionamiento para las interfaces, asegurando que cada una estuviera correctamente asignada según su función dentro de la topología de red diseñada.

Otro aspecto clave que se documentó fue la configuración del servidor *DHCP*. Para ello, también se utilizó una segunda guía de MikroTik titulada *"Cómo hacer un servidor DHCP"*[1]. Esta documentación resultó esencial para configurar de forma precisa el servicio de *DHCP* en los routers. Gracias a esta guía, aprendimos a crear *pools* de direcciones IP dinámicas, definir *leases* estáticos para dispositivos críticos de la red y, en general, cómo garantizar que el servidor *DHCP* distribuyera las direcciones IP correctamente a todos los dispositivos conectados a la red. La documentación también cubrió aspectos avanzados, como la configuración de múltiples *DHCP pools* para distintas subredes, lo que fue necesario dado el diseño segmentado de la red.

La fase de documentación no solo nos proporcionó las instrucciones necesarias para la configuración básica de los routers, sino que también nos permitió prever posibles problemas relacionados con la seguridad y la gestión del tráfico. Por ejemplo, se incluyeron recomendaciones sobre cómo limitar el acceso a ciertas interfaces de administración del router, asegurando que solo el tráfico autorizado pudiera interactuar con estas. Además,

la documentación facilitó la comprensión sobre cómo manejar la asignación eficiente de los recursos de red mediante el uso adecuado del *DHCP*.

En conclusión, la fase de documentación fue un paso fundamental en el proyecto. Las guías consultadas no solo proporcionaron el conocimiento técnico necesario para la configuración de los routers MikroTik, sino que también nos permitieron planificar y estructurar la red de manera más eficiente y segura. Gracias a esta etapa, se logró una base sólida sobre la cual construir la red que responde a los requisitos de la organización, asegurando conectividad y fiabilidad en la asignación de direcciones IP y el enrutamiento de la red.

2.2 Análisis de requisitos

El análisis de requisitos es una etapa fundamental en el desarrollo de cualquier proyecto de red, ya que proporciona una comprensión clara de las necesidades y expectativas de los usuarios finales. En esta fase, se identifican los requisitos técnicos y funcionales que guiarán el diseño y la implementación de la infraestructura de red. A continuación, se detallan los principales requisitos identificados para este proyecto.

2.2.1. Requisitos Funcionales

Los requisitos funcionales definen las funcionalidades específicas que la red debe proporcionar. Para este proyecto, se han identificado los siguientes:

- **Conectividad de Red:** La red debe permitir la conexión de al menos 100 dispositivos simultáneamente, asegurando que todos los usuarios puedan acceder a los recursos compartidos sin interrupciones.
- **Acceso a Internet:** La red debe proporcionar acceso a Internet de alta velocidad, permitiendo a los usuarios realizar tareas en línea, como navegación web, videoconferencias y transferencias de datos.
- **Seguridad de la Red:** Se deben implementar medidas de seguridad efectivas, incluyendo firewalls, autenticación de usuarios y cifrado de datos, para proteger la red contra accesos no autorizados y amenazas externas.
- **Gestión de Direcciones IP:** La red debe incluir un sistema de asignación de direcciones IP que permita una gestión eficiente y escalable de las direcciones, facilitando la conexión de nuevos dispositivos sin conflictos.
- **Soporte para Dispositivos Inalámbricos:** La infraestructura de red debe ofrecer conectividad inalámbrica para dispositivos móviles, permitiendo el acceso a la red desde cualquier lugar dentro del área de cobertura.

2.2.2. Requisitos No Funcionales

Los requisitos no funcionales se refieren a las características de rendimiento y calidad de la red. Para este proyecto, se han establecido los siguientes requisitos:

- **Disponibilidad:** La red debe garantizar un tiempo de actividad del 99.9 %, minimizando el tiempo de inactividad para asegurar que los usuarios puedan acceder a los recursos en todo momento.

- **Escalabilidad:** La infraestructura debe ser escalable, permitiendo la incorporación de nuevos dispositivos y la expansión de la red sin necesidad de una reconfiguración completa.
- **Facilidad de Mantenimiento:** La red debe ser fácil de mantener, con documentación clara que permita a los administradores gestionar y resolver problemas de manera eficiente.
- **Rendimiento:** Se espera que la red ofrezca un rendimiento adecuado, con tiempos de respuesta rápidos y capacidad para manejar un alto volumen de tráfico sin degradar la experiencia del usuario.
- **Compatibilidad:** Todos los componentes de la red deben ser compatibles entre sí y con los sistemas existentes, evitando problemas de integración y asegurando una implementación fluida.

2.2.3. Requisitos de Seguridad

La seguridad es una de las principales preocupaciones en la configuración de redes modernas. Este proyecto incluirá varios requisitos de seguridad específicos:

- **Autenticación y Autorización:** Se implementarán mecanismos de autenticación robustos para garantizar que solo los usuarios autorizados puedan acceder a la red y sus recursos.
- **Firewall:** Se instalarán firewalls en los routers interno y externo para filtrar el tráfico no deseado y proteger la red de amenazas externas.
- **Monitoreo de Seguridad:** Se establecerán sistemas de monitoreo para detectar y responder a posibles ataques o vulnerabilidades en tiempo real.
- **Cifrado de Datos:** Todos los datos sensibles que circulen por la red serán cifrados para proteger la información de accesos no autorizados.

2.3 Diseño de la Red y Asignación de IPs

Para lograr una infraestructura de red eficiente y funcional, es crucial prestar atención tanto al diseño de la red como a la asignación de direcciones IP. En esta sección, se abordará la planificación y estructura de la red, considerando la topología adecuada que se adapte a las necesidades del usuario y los dispositivos conectados. Además, se presentará un esquema de asignación de direcciones IP que garantice una gestión eficiente de los recursos, minimizando conflictos y facilitando la expansión futura de la red. A través de un diseño cuidadoso y una adecuada planificación de la asignación de IPs, se busca asegurar no solo la conectividad, sino también la escalabilidad y la seguridad de la red.

La división de la red se lleva a cabo mediante la implementación de dos routers, cada uno con funciones específicas que optimizan el rendimiento y la seguridad de la infraestructura. El router externo actúa como la puerta de enlace hacia Internet y es responsable de gestionar el tráfico entrante y saliente. Este router alberga una conexión a una subred donde se aloja el servidor DNS que resuelve las peticiones de nombres de dominio y otra conexión a otra subred donde está el servidor web, que proporciona acceso a los recursos on-line de la organización.

Por otro lado, el router interno se encarga de la gestión de las distintas subredes que dan servicio a los usuarios finales, tiene una conexión a una subred donde esta el servidor

IDS e internamente, contiene también un servidor DHCP que asignará las IPs a todos los dispositivos de la red.

Cada subred está diseñada para agrupar dispositivos con características similares, facilitando la administración y mejorando la eficiencia en la asignación de recursos. Esta estructura de red no solo mejora el rendimiento general, sino que también refuerza la seguridad al segmentar el tráfico y limitar el acceso a diferentes áreas de la red. El esquema resultante de la red se muestra en la figura 2.1. Se ha añadido al esquema el servidor DHCP para representar la existencia de uno en la red, pero realmente está interno en el propio router.

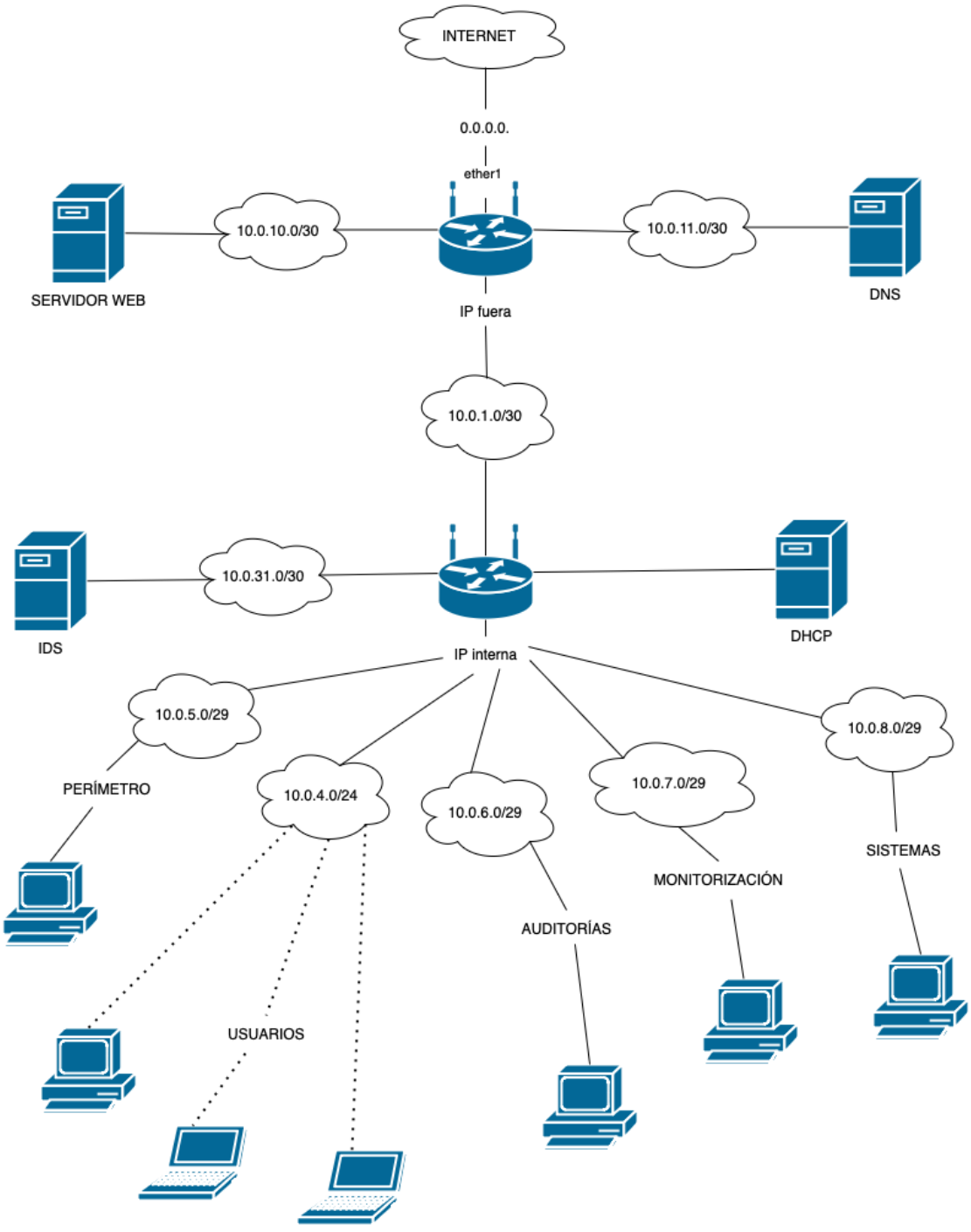

Figura 2.1: Diseño de la red, con las asignaciones IP

2.4 Router Interno

Para la gestión de las subredes de los usuarios, se ha seleccionado el router MikroTik MKT4011A, un dispositivo robusto y versátil que ofrece un rendimiento confiable. Este router no solo albergará las distintas subredes, sino que también actuará como servidor DHCP, facilitando la asignación automática de direcciones IP a los dispositivos conectados. Además, estará conectado a la subred del servidor de Intrusion Detection System (IDS), lo que permitirá monitorizar y proteger la red contra posibles amenazas. Por último, otra de sus interfaces se conectará al router externo, asegurando una comunicación fluida y eficiente entre la red interna y el acceso a Internet.

2.4.1. Configuración Inicial

En esta etapa de la configuración principal del router Mikrotik, se han definido y configurado las distintas subredes que estarán conectadas a él, asegurando un flujo de datos eficiente y seguro entre las diferentes redes que forman parte de la infraestructura. Para lograrlo, se han asignado las direcciones IP correspondientes a cada una de las interfaces del router, asegurando que cada interfaz pertenezca correctamente a su respectiva subred.

La configuración de las direcciones IP en cada interfaz es crucial para garantizar que el tráfico de red se enrute adecuadamente. Estas IPs actúan como puntos de acceso y salida para el tráfico dentro de las subredes, facilitando la comunicación fluida entre los dispositivos conectados y el router, que funcionará como el nodo principal de enrutamiento.

A continuación, se presenta el esquema de asignación de direcciones IP para las interfaces del router interno:

Interfaz	IP	Nombre de red
`eth1`	10.0.1.1	Red de routers
`eth2`	10.0.31.1	Red IDS
`eth3`	10.0.5.1	Subred Perímetro
`eth4`	10.0.4.1	Subred Usuarios
`eth5`	10.0.6.1	Subred Auditorías
`eth6`	10.0.7.1	Subred Monitorización
`eth7`	10.0.8.1	Subred Sistemas

Tabla 2.1: Conexiones de interfaces, direcciones IP y nombres de red

Además de la asignación de IPs, se han implementado tablas de redirección, conocidas como *routing tables*, que permiten gestionar el tránsito de los paquetes entre las subredes de manera eficiente. Estas tablas son esenciales para garantizar que los datos lleguen correctamente a su destino, ya que permiten que el router sepa exactamente cómo dirigir los paquetes de una subred a otra. Esto es particularmente importante en redes complejas, donde existen múltiples subredes y rutas posibles.

Por otro lado, se han configurado las reglas de NAT (*Network Address Translation*) con el fin de realizar el enmascaramiento del tráfico externo. El NAT permite que las direcciones IP privadas de la red interna permanezcan ocultas frente al tráfico que viaja hacia

y desde una red externa (en este caso la del router externo), proporcionando un nivel adicional de seguridad y facilitando que múltiples dispositivos en la red interna compartan una única dirección IP pública para el acceso externo. Esta técnica es indispensable para redes con un gran número de dispositivos, ya que minimiza el uso de direcciones IP públicas y mejora la gestión del tráfico hacia el exterior, además de agregar una capa de seguridad adicional.

En resumen, la configuración inicial incluye la asignación de direcciones IP en las interfaces del router, la creación de tablas de redirección para gestionar el tráfico entre subredes y la implementación de reglas de NAT para el enmascaramiento del tráfico externo, todo ello con el fin de garantizar una conectividad óptima y segura entre los distintos componentes de la red.

2.4.2. DHCP

La configuración de un servidor DHCP (Dynamic Host Configuration Protocol) es un proceso esencial para la gestión eficiente de direcciones IP en una red. Aunque el servidor DHCP se representa como un componente separado en el esquema de red, en realidad está integrado dentro del router MikroTik, lo que permite una administración centralizada de la asignación de direcciones IP a los dispositivos que se conectan a la red.

El servidor DHCP del MikroTik permite la asignación automática de direcciones IP a los dispositivos conectados, eliminando la necesidad de configurar manualmente cada uno de ellos. Para una correcta operación, es fundamental definir un rango de direcciones IP que el servidor utilizará para la asignación dinámica. Este rango debe diseñarse de forma que no interfiera con las direcciones IP estáticas asignadas a dispositivos críticos, como servidores o impresoras.

Una vez establecido el rango de direcciones IP, se procede a crear pools de direcciones para cada subred a través de la interfaz gráfica de Winbox. Cada pool representa un conjunto de direcciones que el servidor puede asignar automáticamente a los dispositivos conectados. Para evitar conflictos de direcciones IP, es esencial configurar estos pools correctamente. Para ello, se deben seguir los siguientes pasos:

1. Acceder a **IP** en el menú lateral.
2. Seleccionar **DHCP Server**.
3. Hacer clic en la pestaña **Pools**.
4. Hacer clic en el botón **Add** (+) para crear un nuevo pool.
5. Introducir un nombre para el pool y definir el rango de direcciones IP.

Esto asegurará que el servidor DHCP pueda asignar direcciones IP dinámicas a los dispositivos sin generar conflictos.

Después de definir los pools, es crucial añadir las redes correspondientes en el servidor DHCP para garantizar que las direcciones IP asignadas estén dentro del rango establecido. Este paso permite que el servidor reconozca qué subredes están disponibles para la asignación de direcciones IP, asegurando así una gestión eficiente de las conexiones de red. Los pasos a seguir son:

1. Desde el menú principal, seleccionar **IP** y luego **DHCP Server**.
2. Acceder a la pestaña **Networks**.

3. Hacer clic en el botón **Add** (+) para agregar una nueva red.
4. Introducir la dirección de la subred, la dirección del gateway y, si es necesario, el servidor DNS.

Esto garantiza que el servidor DHCP gestione correctamente las asignaciones de direcciones IP en función de la red configurada.

La implementación del servidor DHCP en un router MikroTik automatiza la asignación de direcciones IP, simplificando notablemente la administración de la red. Cada vez que un dispositivo se conecta, el servidor DHCP le asigna automáticamente una dirección IP válida dentro del rango dinámico disponible. Este proceso no solo reduce el riesgo de errores humanos en la asignación manual de direcciones IP, sino que también permite a los administradores de red concentrarse en otras tareas críticas.

2.4.3. Configuración de la Red Wi-Fi en el Router MikroTik

La configuración de la red Wi-Fi en el router MikroTik para que esté operativa exclusivamente en la subred de usuarios, con su propio pool de direcciones IP, es fundamental para garantizar una correcta segmentación y gestión de la red. Este proceso implica configurar la interfaz Wi-Fi, el servidor DHCP y asegurarse de que la red esté aislada de otras subredes. A continuación, se detallan los pasos para lograrlo, siguiendo los principios de segmentación de red y configuración del pool de IPs para la subred Wi-Fi (10.0.4.0/24).

Configuración de la Interfaz Wi-Fi

El primer paso para configurar la red Wi-Fi es habilitar la interfaz Wi-Fi en el router MikroTik. Para ello, se accede a la interfaz gráfica de Winbox y se configuran los parámetros básicos de la red inalámbrica.

1. **Acceder a la sección Wireless:** En el menú lateral, seleccionar `Wireless`.
2. **Configurar el modo de la interfaz:** Seleccionar el `Mode` como `ap bridge`, para establecer el router como punto de acceso.
3. **Asignar un nombre a la red Wi-Fi (SSID):** Establecer un nombre para la red Wi-Fi, por ejemplo, `Red_Usuarios`.
4. **Seleccionar el canal:** Elegir un canal adecuado para evitar interferencias con otras redes cercanas.
5. **Configurar seguridad:** Definir un perfil de seguridad con encriptación WPA2 o WPA3, y establecer una contraseña robusta para la red.

Configuración del Pool de Direcciones IP para la Subred Wi-Fi

Una vez configurado el punto de acceso Wi-Fi, se debe crear un pool de direcciones IP para la subred de usuarios. El pool es un rango de direcciones que el servidor DHCP puede asignar automáticamente a los dispositivos que se conecten a la red Wi-Fi.

1. **Acceder a la sección IP en Winbox:** En el menú lateral, seleccionar `IP` y luego `Pools`.
2. **Crear un nuevo pool de direcciones IP:** Hacer clic en el botón `Add (+)` para crear un nuevo pool.

3. **Nombre del pool:** Introducir el nombre `Usuarios-wifi-pool`.
4. **Rango de direcciones IP:** Definir el rango de direcciones IP como `10.0.4.2 - 10.0.4.100`, que será el rango de direcciones IP que el servidor DHCP asignará a los dispositivos conectados por Wi-Fi.

Este pool asegura que los dispositivos conectados de manera inalámbrica reciban direcciones IP dentro de la subred `10.0.4.0/24`.

Configuración del Servidor DHCP para la Subred Wi-Fi

A continuación, se configura el servidor DHCP para que asigne direcciones IP de la subred Wi-Fi a los dispositivos que se conecten a la red inalámbrica.

1. **Acceder a la sección DHCP Server:** Desde el menú principal, seleccionar `IP` y luego `DHCP Server`.
2. **Crear un nuevo servidor DHCP:** Hacer clic en el botón `Add (+)` para crear un nuevo servidor DHCP.
3. **Interface:** Seleccionar la interfaz Wi-Fi configurada previamente.
4. **Address Pool:** Seleccionar el pool de direcciones IP `Usuarios-wifi-pool`.
5. **Gateway:** Definir la dirección IP del gateway de la subred Wi-Fi, que en este caso es `10.0.4.1` (la IP del router en la subred Wi-Fi).
6. **DNS Servers:** Configurar servidores DNS como `1.1.1.1` (CloudFlare DNS) aunque posteriormente será el servidor DNS creado por el departamento de Sistemas.

Configuración de la Red en el Servidor DHCP

Para que el servidor DHCP gestione correctamente las direcciones IP en la subred Wi-Fi, es necesario añadir la red correspondiente.

1. **Acceder a la pestaña Networks:** En `IP >DHCP Server`, seleccionar la pestaña `Networks`.
2. **Añadir una nueva red:** Hacer clic en el botón `Add (+)` para agregar la red.
3. **Network:** Introducir la dirección de la subred Wi-Fi, `10.0.4.0/24`.
4. **Gateway:** Definir la dirección del gateway `10.0.4.1`.
5. **DNS Servers:** Introducir los servidores DNS si es necesario.

Verificación de la Configuración

Una vez completada la configuración, es importante verificar que tanto la red Wi-Fi como el servidor DHCP estén funcionando correctamente.

1. **Verificar la conexión Wi-Fi:** Conectar un dispositivo a la red Wi-Fi y verificar que reciba una dirección IP dentro del rango `10.0.4.2 - 10.0.4.100` desde el servidor DHCP.
2. **Verificar la conexión Ethernet:** Conectar un dispositivo por Ethernet y asegurarse de que reciba una dirección IP dentro del rango de la subred LAN (por ejemplo, `10.0.0.2 - 10.0.0.100`).

2.5 Router Externo

La correcta configuración de un router externo es un aspecto fundamental para asegurar el funcionamiento óptimo de la infraestructura de red. En este caso, se ha optado por el router MikroTik MKT3011A, que destaca por su robustez y versatilidad. Este modelo es capaz de gestionar eficientemente múltiples conexiones, lo que favorece una distribución adecuada del tráfico y permite implementar políticas de seguridad efectivas.

En esta sección se describen los pasos seguidos para llevar a cabo la configuración del dispositivo, desde la preparación inicial hasta la asignación de interfaces y la gestión del tráfico de red. Cada uno de estos pasos fue cuidadosamente planificado con el fin de optimizar el rendimiento y garantizar la seguridad de la red.

2.5.1. Configuración de la interfaz de red del ordenador

El primer paso consistió en ajustar la interfaz de red del ordenador utilizado para acceder al router. Esta acción es fundamental para garantizar la comunicación directa entre ambos dispositivos, lo que permite la gestión y configuración del router a través de su panel de administración.

Para ello, se asignó una dirección IP al ordenador dentro de la misma subred que la del router, asegurando que ambos dispositivos se encuentren en el mismo rango de direcciones IP y, por lo tanto, puedan intercambiar datos sin problemas. Esta asignación es crítica para el acceso a las funciones de gestión del router mediante herramientas como Winbox.

Acceso al router mediante Winbox

Una vez configurada la interfaz de red del ordenador, se procedió a acceder al router mediante la aplicación *Winbox*, una herramienta gráfica que facilita la administración de dispositivos de red basados en MikroTik.

Winbox proporciona una interfaz intuitiva para la configuración y monitorización de parámetros clave del router, lo que agiliza la gestión de las interfaces, la asignación de direcciones IP y la configuración de servicios adicionales. A través de esta herramienta, se estableció una conexión con el router para iniciar el proceso de configuración detallada de sus diferentes parámetros.

Asignación de una interfaz dedicada para la configuración

Para una gestión eficaz del router, se decidió dedicar una interfaz específica para la administración y configuración. En este caso, se seleccionó la interfaz número 6 del dispositivo.

Razonamiento técnico La asignación de una interfaz dedicada para la administración del router es una práctica común que permite gestionar de forma aislada las configuraciones sin interferir en el funcionamiento de las otras interfaces. Esto minimiza el riesgo de interrumpir el tráfico de red o generar conflictos durante el proceso de configuración.

Acción ejecutada Se configuró la interfaz de red del ordenador (`eno1`) con una dirección IP dentro de la misma subred que la interfaz 6 del router, garantizando así una comuni-

cación directa. Esta IP se asignó de forma estática, con el fin de asegurar que la conexión se mantuviera estable durante todo el proceso de configuración.

Desconexión del DNS Server

Con el fin de optimizar los recursos del router y reducir su carga de procesamiento, se decidió deshabilitar el *DNS Server* en el dispositivo.

Motivo de la acción En redes donde existen servidores DNS dedicados o donde la resolución de nombres es gestionada por el proveedor de servicios de internet, no es necesario que el router actúe como servidor DNS. Deshabilitar esta funcionalidad permite que el dispositivo se concentre en sus tareas principales de enrutamiento y gestión de paquetes de red.

Resultado Al desactivar el servidor DNS, se previenen posibles conflictos relacionados con la resolución de nombres de dominio y se mejora el rendimiento global del router, ya que no está asumiendo una carga de trabajo adicional que puede ser innecesaria en este entorno.

Configuración de las interfaces del *bridge* y restricción de acceso al router

El último paso en la configuración fue la gestión de las interfaces del router, organizándolas en un *bridge* y estableciendo políticas de acceso para las distintas subredes.

Configuración del *bridge* Se creó una estructura de *bridge* para agrupar varias interfaces físicas del router bajo una interfaz lógica. Esta técnica facilita la administración de los dispositivos conectados, permitiendo que varias interfaces físicas se comporten como si pertenecieran a la misma red local. Además, simplifica la gestión de las conexiones y la asignación de recursos de red.

Restricción de acceso al router desde las subredes Se configuraron las interfaces correspondientes a las subredes para evitar que estas tuvieran acceso directo al router. Esta medida es crucial para garantizar la seguridad de la red, ya que impide que dispositivos de las subredes puedan acceder o modificar los parámetros de configuración del router.

Beneficio de esta configuración Al restringir el acceso al router desde las subredes, se asegura que solo los dispositivos y usuarios autorizados tengan la capacidad de gestionar el router, reduciendo así los riesgos de ataques internos o configuraciones no deseadas.

La tabla 2.2 presenta la configuración de las interfaces del router externo, indicando las máquinas conectadas y sus direcciones IP. Cada interfaz está asignada a un dispositivo específico, con algunas direcciones IP que son entregadas de manera dinámica.

Interfaz	Máquina	IP
ether3	DNS	10.0.11.2
ether2	Servidor Web	10.0.10.2
ether1	Conexión router interno/externo	158.42.180.50
ether6	Perímetro 1 (para configurar router)	Dinámica
ether6	Monitorización 1	-
ether9	Perímetro 2 (configuración router)	Dinámica

Tabla 2.2: Resumen de configuraciones del router externo

2.5.2. Deshabilitar la Interfaz Wi-Fi en el Router Externo

En el caso del router MikroTik externo, la interfaz Wi-Fi está habilitada por defecto. Sin embargo, como en este proyecto no interesa el uso de Wi-Fi en el router externo, es necesario deshabilitar esta interfaz para evitar posibles conexiones no deseadas a la red externa y mantener la seguridad de la infraestructura.

El proceso de deshabilitación de la interfaz Wi-Fi en el router externo se realiza a través de la interfaz gráfica de Winbox. A continuación, se describen los pasos para realizar esta configuración:

Deshabilitar la Interfaz Wi-Fi

Para deshabilitar la interfaz Wi-Fi en el router MikroTik externo, se deben seguir los siguientes pasos:

1. **Acceder a la interfaz de Winbox:** Conéctese al router externo utilizando Winbox.
2. **Abrir la sección de Wireless:** En el menú lateral de Winbox, seleccione `Wireless` para acceder a la configuración de las interfaces inalámbricas.
3. **Seleccionar la interfaz Wi-Fi:** En la lista de interfaces inalámbricas, localice la interfaz Wi-Fi habilitada (generalmente llamada `wlan1` o similar).
4. **Deshabilitar la interfaz:** Haga clic en la interfaz Wi-Fi y luego en el botón `Disable` ubicado en la parte superior de la ventana de configuración.

Una vez realizada esta acción, la interfaz Wi-Fi quedará deshabilitada y no podrá ser utilizada para realizar conexiones inalámbricas a la red externa.

Verificación de la Configuración

Para asegurarse de que la interfaz Wi-Fi se ha deshabilitado correctamente, se pueden seguir los siguientes pasos de verificación:

1. Acceder nuevamente a la sección `Wireless` desde el menú lateral de Winbox.

2. Verificar que la interfaz Wi-Fi aparece con el estado `Disabled`, lo que indica que la interfaz ha sido deshabilitada correctamente.

2.6 Configuración del Servidor VPN

A raíz de la catástrofe natural ocurrida en Valencia, se procedió a implementar la configuración del servidor OpenVPN de manera remota. Este proceso incluyó la generación de certificados, configuración de direcciones IP, reglas de firewall, perfiles secretos y la instalación final del servidor. A continuación, se describen los pasos realizados con detalle técnico.

2.6.1. Generación de Certificados

Se generaron tres certificados fundamentales para el correcto funcionamiento del servidor OpenVPN:

- **Certificado de Autoridad de Certificación (CA Certificate):** Este certificado actúa como la entidad emisora, utilizada para firmar y validar los demás certificados.
- **Certificado del Servidor (SERVER Certificate):** Específico para el servidor OpenVPN, permite autenticar el servidor ante los clientes.
- **Certificado del Cliente (CLIENT Certificate):** Proporcionado a los clientes para autenticar su conexión al servidor. Este incluye la clave privada del cliente, que debe ser manejada con estricta confidencialidad.

A los clientes se les entrega tanto el *CA Certificate* como su *CLIENT Certificate*, asegurando que puedan establecer conexiones seguras al servidor.

2.6.2. Configuración de las Pools de Direcciones IP

Se definió una *pool* de direcciones IP que será utilizada por el servidor OpenVPN para asignar direcciones a los clientes conectados. El rango definido para esta *pool* es:

10.0.20.2 - 10.0.20.254

Esto asegura un direccionamiento ordenado y evita conflictos de IP en la red interna.

2.6.3. Configuración de las Reglas de Firewall

Para garantizar el flujo de tráfico entre los dispositivos internos y externos, se configuraron las siguientes reglas de firewall:

- **Router Externo:** Se añadió una regla de *forwarding* que redirige el tráfico destinado al servidor OpenVPN hacia el router interno.
- **Router Interno:** Se creó una regla de NAT (*Network Address Translation*) para enmascarar el tráfico saliente desde la VPN hacia la red externa también se añadió una regla input Accept a los paquetes procedentes de Open VPN para permitir la configuración del router.

Estas configuraciones aseguran la correcta comunicación de la VPN con las redes internas y externas.

2.6.4. Definición de Perfiles PPP y Configuración de Secretos

Se definió un perfil PPP (*Point-to-Point Protocol*) específico para la conexión OpenVPN. En el apartado de *Secrets*, se añadieron las credenciales de los clientes, incluyendo:

- Nombre de usuario y contraseña.
- Certificados asignados a cada cliente, vinculados con sus claves privadas.

Esto permite gestionar de manera segura las conexiones de los usuarios al servidor.

2.6.5. Configuración del Servidor OpenVPN

Finalmente, se creó y configuró el servidor OpenVPN en el router MikroTik. Posteriormente, se exportaron los archivos necesarios para que los clientes pudieran establecer la conexión, incluyendo:

- Certificados (*CA* y *CLIENT*).
- Archivo de configuración del cliente (`.ovpn`).

Esta configuración completa permite a los clientes establecer conexiones seguras y fiables con el servidor OpenVPN. [**?**]

CAPÍTULO 3
Próximas tareas

3.1 Implementación de un Firewall en el Router Externo

En esta fase del proyecto, se procederá a la implementación de un *firewall* en el router externo. El objetivo principal de esta medida es proteger la red de amenazas externas, controlando y filtrando el tráfico entrante y saliente desde y hacia la red.

El *firewall* en el router externo permitirá:

- Filtrar el tráfico no deseado proveniente de Internet, permitiendo únicamente el acceso a los servicios autorizados.
- Proteger los recursos internos de la red frente a intentos de intrusión y ataques.
- Aplicar políticas de seguridad, tales como el bloqueo de ciertos puertos o la limitación de conexiones desde direcciones IP no confiables.

Esta configuración será vital para garantizar la seguridad de la red frente a amenazas externas, manteniendo el flujo de datos dentro de los parámetros establecidos por las políticas de seguridad. Para ello, se establecerán reglas específicas para el filtrado de paquetes, basadas en criterios como la dirección IP, los protocolos utilizados y el puerto de destino.

3.2 Implementación de un Firewall en el Router Interno

Además del *firewall* en el router externo, se implementará un *firewall* en el router interno. Este firewall se enfocará en proteger y controlar el tráfico dentro de la red local, garantizando que los dispositivos conectados sigan las políticas de seguridad establecidas.

El *firewall* en el router interno permitirá:

- Filtrar el tráfico entre diferentes subredes de la red interna, asegurando que sólo los dispositivos autorizados puedan comunicarse entre sí.
- Aplicar restricciones adicionales para el tráfico saliente de la red local hacia el exterior.
- Detectar y bloquear comportamientos anómalos o no deseados dentro de la red interna, como intentos de acceso no autorizados entre dispositivos.

Este firewall permitirá una mayor granularidad en las políticas de seguridad dentro de la red, optimizando el control del flujo de datos entre dispositivos conectados y previniendo accesos no autorizados dentro del entorno local.

3.3 Instalación de Sistemas de Detección de Intrusos (IDS)

Como parte de las tareas planificadas, se procederá a la instalación de sistemas de detección de intrusos (IDS) para analizar el tráfico de red en busca de actividades sospechosas o maliciosas. Un IDS permitirá monitorizar la red en tiempo real, alertando ante cualquier comportamiento inusual que pueda indicar un ataque o una brecha de seguridad.

Los sistemas IDS se encargarán de:

- Analizar el tráfico de la red en busca de patrones de ataque conocidos, como intentos de explotación de vulnerabilidades o escaneos de puertos.
- Proporcionar alertas automáticas cuando se detecte un posible incidente de seguridad, lo que permitirá una respuesta rápida y eficaz.
- Registrar el tráfico de red y los eventos sospechosos para su posterior análisis y toma de decisiones.

Con la instalación de los IDS, se busca no solo prevenir intrusiones, sino también mejorar la capacidad de detección de posibles amenazas antes de que estas comprometan la red. El análisis proactivo del tráfico será una herramienta clave para garantizar la seguridad y el buen funcionamiento de la infraestructura de red.

CAPÍTULO 4
Conclusiones

Hasta el momento, el proyecto ha logrado establecer las bases para una red corporativa robusta y eficiente mediante la configuración inicial de dos routers MikroTik. Esta fase inicial ha permitido no solo habilitar la conectividad a Internet, sino también sentar las bases para una gestión adecuada del tráfico interno y la segmentación de la red.

La implementación del router externo ha sido clave, ya que actúa como la puerta de enlace hacia Internet, permitiendo un acceso controlado que protege los recursos internos de la organización. Por su parte, el router interno facilita la gestión del tráfico entre las distintas subredes, preparando el terreno para una estructura de red organizada que permitirá un rendimiento óptimo y una administración más sencilla.

La conexión a Internet ya establecida marca un avance significativo, ya que permite a los dispositivos internos comunicarse con el exterior, lo que es fundamental para el funcionamiento diario de la empresa. Este paso inicial refuerza la seguridad de la red al permitir la planificación de futuras implementaciones de medidas de seguridad, como reglas de firewall y NAT, así como la integración de servicios adicionales como DHCP y WiFi.

A medida que avanzamos hacia la siguiente fase del proyecto, el enfoque se centrará en la implementación de medidas de seguridad más complejas y en la optimización de la infraestructura de red. Se buscará asegurar un entorno de red escalable y seguro, que no solo responda a las necesidades actuales de la organización, sino que también esté preparado para adaptarse a futuros requerimientos.

En conclusión, los logros hasta la fecha son prometedores y sentarán las bases para las próximas etapas del proyecto, donde se implementarán servicios adicionales y se fortalecerán las medidas de seguridad, garantizando así una red corporativa integral y eficiente.

Bibliografía

[1] MikroTikHowTo. (s.f.). *Cómo configurar un servidor DHCP en MikroTik*. Recuperado de https://mikrotikhowto.net/posts/como-configurar-un-servidor-dhcp-en-mikrotik/

[2] MikroTikLabs. (2019). *Los 5 pasos para configurar una red en MikroTik*. Recuperado de https://www.mikrotiklabs.com/2019/07/18/los-5-pasos-para-configurar-una-red-en-mikrotik/