



UNIVERSITAT  
POLITÈCNICA  
DE VALÈNCIA



UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Escuela Técnica Superior de Ingeniería Informática

Interconexión de redes de forma segura mediante  
cortafuegos pfSense

Trabajo Fin de Grado

Grado en Ingeniería Informática

AUTOR/A: Blasco Carmona, Javier

Tutor/a: Pons Terol, Julio

CURSO ACADÉMICO: 2023/2024



# Agradecimientos

---

Me gustaría comenzar agradeciendo a mi tutor Julio Pons por confiar en mí para desarrollar este proyecto y por ayudarme a lo largo del mismo.

También quiero agradecer a todos los profesores que durante estos cuatro años me han transmitido los conocimientos necesarios para llevar a cabo este proyecto y que además me permitirán desarrollar mi futuro profesional.

Además, me gustaría dar las gracias a mi familia y amigos por acompañarme en los buenos y los malos momentos a lo largo de mi etapa universitaria.

Especialmente, agradecer a mis padres por apoyarme, ayudarme y motivarme siempre que lo he necesitado.

Para terminar, quería dedicarle un agradecimiento especial a mi abuelo Carlos que siempre confió en mí.

## Resumen

Se ha desarrollado una solución que permite la interconexión segura de dos redes utilizando el cortafuegos software de código abierto pfSense. Para llevar a cabo la implementación de esta solución, se ha creado un esquema de red virtual en VMware Workstation, simulando un entorno real, en el que se ha conseguido conectar entre sí dos redes privadas mediante la configuración de tres conexiones VPN distintas entre los dos cortafuegos pfSense utilizados. Concretamente, las VPNs que se han configurado son IPsec, OpenVPN y WireGuard. Se ha realizado un estudio comparativo entre estas VPNs, analizando teóricamente los diferentes protocolos y realizando distintas pruebas sobre el entorno virtual creado para medir el rendimiento de cada una de ellas.

**Palabras clave:** pfSense, cortafuegos, firewall, interconexión de redes, túnel, VPN, seguridad

---

## Resum

S'ha desenvolupat una solució que permet la interconnexió segura de dos xarxes utilitzant el tallafocs programari de codi obert pfSense. Per a dur a terme la implementació d'esta solució, s'ha creat un esquema de xarxa virtual en VMware Workstation, simulant un entorn real, en el qual s'ha aconseguit connectar entre sí dos xarxes privades mitjançant la configuració de tres connexions VPN diferents entre els dos tallafocs pfSense utilitzats. Concretament, les VPNs que s'han configurat són IPsec, OpenVPN i WireGuard. S'ha realitzat un estudi comparatiu entre estes VPNs, analitzant teòricament els diferents protocols i realitzant diferents proves sobre l'entorn virtual creat per a mesurar el rendiment de cadascuna d'elles.

**Paraules clau:** pfSense; tallafocs, firewall, interconnexió de xarxes, túnel, VPN, seguretat

---

## Abstract

A solution has been developed that allows the secure interconnection of two networks using the pfSense open source software firewall. To carry out the implementation of this solution, a virtual network scheme has been created in VMware Workstation, simulating a real environment, in which two private networks have been connected by configuring three different VPN connections between the two pfSense firewalls used. Specifically, the VPNs configured were IPsec, OpenVPN and WireGuard. A comparative study has been carried out between these VPNs, theoretically analysing the different protocols and performing different tests on the virtual environment created to measure the performance of each of them.

**Key words:** pfSense, firewall, network interconnection, tunnel, VPN, security

---

# Índice general

---

|                   |  |           |
|-------------------|--|-----------|
| Índice general    | v  |           |
| Índice de figuras | vii  |           |
| Índice de tablas  | x  |           |
| <hr/>             |  |           |
| <b>1</b>          | <b>Introducción</b>  | <b>1</b>  |
| 1.1               | Motivación . . . . .   | 1         |
| 1.2               | Objetivos . . . . .  | 2         |
| 1.3               | Estructura de la memoria . . . . .                                       | 2         |
| <b>2</b>          | <b>Estado del arte</b>   | <b>5</b>  |
| 2.1               | Situación actual de los cortafuegos . . . . .                            | 5         |
| 2.2               | Situación actual de las conexiones seguras de redes . . . . .            | 6         |
| 2.3               | Crítica al estado del arte . . . . .                                     | 6         |
| 2.4               | Propuesta . . . . .  | 7         |
| <b>3</b>          | <b>Fundamentos para la interconexión segura de redes</b>                 | <b>9</b>  |
| 3.1               | Que son los túneles VPN . . . . .  | 9         |
| 3.2               | Tipos de VPN . . . . .   | 10        |
| 3.3               | Protocolos VPN . . . . .   | 10        |
| <b>4</b>          | <b>Análisis del problema</b>   | <b>13</b> |
| 4.1               | Identificación y análisis de soluciones posibles . . . . .               | 13        |
| 4.2               | Solución propuesta . . . . .   | 14        |
| <b>5</b>          | <b>Diseño de la solución</b>   | <b>17</b> |
| 5.1               | Arquitectura del Sistema . . . . .                                       | 17        |
| 5.2               | Diseño Detallado . . . . .   | 18        |
| 5.3               | Tecnología Utilizada . . . . .   | 19        |
| 5.3.1             | Software de virtualización VMware . . . . .                              | 20        |
| 5.3.2             | Firewall virtual pfSense . . . . .                                       | 20        |
| 5.3.3             | Router virtual MikroTik . . . . .  | 21        |
| 5.3.4             | Sistema operativo AlmaLinux . . . . .                                    | 21        |
| <b>6</b>          | <b>Desarrollo de la solución propuesta</b>                               | <b>23</b> |
| 6.1               | Instalación de las máquinas virtuales implicadas . . . . .               | 23        |
| 6.1.1             | Instalación de los cortafuegos pfSense . . . . .                         | 23        |
| 6.1.2             | Instalación del router MikroTik . . . . .                                | 27        |
| 6.1.3             | Instalación de las máquinas AlmaLinux . . . . .                          | 32        |
| 6.2               | Configuraciones iniciales sobre los componentes de la solución . . . . . | 38        |
| 6.2.1             | Configuraciones iniciales en los cortafuegos pfSense . . . . .           | 39        |
| 6.2.2             | Configuraciones iniciales en el router MikroTik . . . . .                | 45        |
| 6.2.3             | Configuraciones iniciales en las máquinas AlmaLinux . . . . .            | 48        |
| 6.3               | Configuración de VPN Site-to-Site con IPsec . . . . .                    | 52        |
| 6.4               | Configuración de VPN Site-to-Site con OpenVPN . . . . .                  | 61        |

---

|          |   |           |
|----------|---|-----------|
| 6.5      | Configuración de VPN Site-to-Site con WireGuard . . . . .             | 66        |
| <b>7</b> | <b>Implantación</b>   | <b>75</b> |
| 7.1      | Puesta en marcha de la VPN con IPsec . . . . .                        | 75        |
| 7.2      | Puesta en marcha de la VPN con OpenVPN . . . . .                      | 76        |
| 7.3      | Puesta en marcha de la VPN con WireGuard . . . . .                    | 77        |
| <b>8</b> | <b>Pruebas</b>  | <b>79</b> |
| 8.1      | Pruebas de conectividad y rendimiento de los túneles VPN . . . . .    | 79        |
| 8.1.1    | Medida de ancho de banda con iperf3 . . . . .                         | 79        |
| 8.1.2    | Transferencia de archivos con scp . . . . .                           | 81        |
| 8.2      | Validación del encapsulado del tráfico en los túneles VPN . . . . .   | 82        |
| <b>9</b> | <b>Conclusiones</b>   | <b>87</b> |
| 9.1      | Relación del trabajo desarrollado con los estudios cursados . . . . . | 88        |
|          | <b>Bibliografía</b>   | <b>89</b> |

---

|           |   |           |
|-----------|---|-----------|
| Apéndices |   |           |
| <b>A</b>  | <b>Configurar un cortafuegos pfSense sin utilizar la interfaz web</b> | <b>93</b> |
| <b>B</b>  | <b>Objetivos De Desarrollo Sostenible</b>                             | <b>97</b> |

# Índice de figuras

---

|      |   |    |
|------|---|----|
| 5.1  | Esquema general de la solución . . . . .  | 17 |
| 5.2  | Esquema de red completo de la solución . . . . .                                  | 19 |
| 6.1  | Crear máquina virtual pfSense . . . . .   | 24 |
| 6.2  | Configuración de hardware VMware del pfsense1 . . . . .                           | 24 |
| 6.3  | Configuración de hardware VMware del pfsense2 . . . . .                           | 25 |
| 6.4  | Primer paso en la instalación de pfSense . . . . .                                | 25 |
| 6.5  | Opciones de instalación de pfSense . . . . .                                      | 26 |
| 6.6  | Opciones de particionado de disco de pfSense . . . . .                            | 26 |
| 6.7  | Opciones de intalación de pfSense . . . . .                                       | 27 |
| 6.8  | Opciones de intalación de pfSense . . . . .                                       | 27 |
| 6.9  | Configuración de hardware VMware del router MikroTik . . . . .                    | 28 |
| 6.10 | Opciones de instalación del router MikroTik . . . . .                             | 29 |
| 6.11 | Software ID y cambio de contraseña del router MikroTik . . . . .                  | 29 |
| 6.12 | Registro en la página de MikroTik . . . . .                                       | 30 |
| 6.13 | Genera una clave de demo en la página de MikroTik . . . . .                       | 30 |
| 6.14 | Clave de demo generada para el router MikroTik instalado . . . . .                | 31 |
| 6.15 | Acceso al router MikroTik desde WinBox . . . . .                                  | 31 |
| 6.16 | Sección de licencia en WinBox . . . . .   | 32 |
| 6.17 | Licencia demo activada en WinBox . . . . .  | 32 |
| 6.18 | Configuración de hardware VMware del PC1 . . . . .                                | 33 |
| 6.19 | Configuración de hardware VMware del PC2 . . . . .                                | 34 |
| 6.20 | Opciones de la instalación de AlmaLinux . . . . .                                 | 34 |
| 6.21 | Proceso de comprobación de archivos de instalación en AlmaLinux . . . . .         | 35 |
| 6.22 | Configuración de la instalación de AlmaLinux . . . . .                            | 36 |
| 6.23 | Configuración del disco para la instalación de AlmaLinux . . . . .                | 36 |
| 6.24 | Configuración de la selección de software para la instalación del PC1 . . . . .   | 37 |
| 6.25 | Configuración de la selección de software para la instalación del PC2 . . . . .   | 37 |
| 6.26 | Instalación completa de AlmaLinux . . . . .                                       | 38 |
| 6.27 | Configuración inicial de AlmaLinux . . . . .                                      | 38 |
| 6.28 | Menú de configuración del pfSense1 . . . . .                                      | 39 |
| 6.29 | Configuración de la interfaz WAN para el pfSense1 . . . . .                       | 40 |
| 6.30 | Configuración de la interfaz LAN para el pfSense1 . . . . .                       | 41 |
| 6.31 | Error de privacidad al acceder al pfSense vía web . . . . .                       | 42 |
| 6.32 | Inicio de sesión en pfSense vía web . . . . .                                     | 42 |
| 6.33 | Wizard de configuración inicial de pfSense . . . . .                              | 43 |
| 6.34 | Configuración de <i>Reserved Networks</i> en la interfaz WAN de pfSense . . . . . | 43 |
| 6.35 | Aplicar los cambios tras una configuración en pfSense . . . . .                   | 44 |
| 6.36 | Añadir nueva regla de firewall para la interfaz WAN en pfSense . . . . .          | 44 |

|  |    |
|--|----|
| 6.37 Configuración de una regla que permite todo el tráfico ICMP en pfSense . . . . .                          | 44 |
| 6.38 Crear un backup de la configuración completa en pfSense . . . . .   | 45 |
| 6.39 Configuración del cliente DHCP en el router MikroTik . . . . .  | 46 |
| 6.40 Configuración de direcciones IP en el router MikroTik . . . . .   | 46 |
| 6.41 Configuración del Bridge en el router MikroTik . . . . .  | 47 |
| 6.42 Configuración de los puertos en el Bridge del router MikroTik . . . . .                                   | 47 |
| 6.43 Comprobación de las rutas creadas dinámicamente en el router MikroTik . . . . .                           | 48 |
| 6.44 Acceso a la ruta y modificación del archivo <i>ifcfg-ens37</i> . . . . .                                  | 48 |
| 6.45 Contenido del archivo <i>ifcfg-ens37</i> para el PC1 . . . . .  | 49 |
| 6.46 Apagado y encendido de la interfaz <i>ens37</i> en el PC1 . . . . .                                       | 49 |
| 6.47 Configuración de red del PC1 . . . . .  | 49 |
| 6.48 Menú de configuración de red cableada en el PC2 . . . . .   | 50 |
| 6.49 Configuración de red cableada en el PC2 . . . . .   | 51 |
| 6.50 Detalles de configuración de red en el PC2 . . . . .  | 51 |
| 6.51 Añadir una fase 1 de IPsec en pfSense1 . . . . .  | 52 |
| 6.52 Información general y configuración de IKE de la fase 1 de IPsec en pfSense1 . . . . .                    | 53 |
| 6.53 Configuración de la fase 1 de IPsec en pfSense1 . . . . .   | 54 |
| 6.54 Opciones avanzadas de la fase 1 de IPsec en pfSense1 . . . . .  | 54 |
| 6.55 Añadir una fase 2 de IPsec en pfSense1 . . . . .  | 55 |
| 6.56 Información general y configuración de redes en la fase 2 de IPsec en pfSense1 . . . . .                  | 55 |
| 6.57 Configuración de la fase 2 de IPsec en pfSense1 . . . . .   | 56 |
| 6.58 Crear una regla para permitir el tráfico por el túnel IPsec en pfSense1 . . . . .                         | 57 |
| 6.59 Configuración de la regla para IPsec en pfSense1 . . . . .  | 57 |
| 6.60 Configuración de fuente, destino y opciones extra en la regla para IPsec en pfSense1 . . . . .            | 58 |
| 6.61 Información general y configuración de IKE de la fase 1 de IPsec en pfSense2 . . . . .                    | 58 |
| 6.62 Tiempo de vida de la fase 1 de IPsec en pfSense2 . . . . .  | 59 |
| 6.63 Opciones avanzadas de la fase 1 de IPsec en pfSense2 . . . . .  | 59 |
| 6.64 Información general y configuración de redes en la fase 2 de IPsec en pfSense2 . . . . .                  | 60 |
| 6.65 Tiempo de vida de la fase 2 de IPsec en pfSense2 . . . . .  | 60 |
| 6.66 Configuración de fuente y destino en la regla para IPsec en pfSense2 . . . . .                            | 61 |
| 6.67 Crear servidor OpenVPN en pfSense1 . . . . .  | 61 |
| 6.68 Información general y modo de configuración del servidor OpenVPN en pfSense1 . . . . .                    | 62 |
| 6.69 Configuración del servidor y ajustes criptográficos de OpenVPN en pfSense1 . . . . .                      | 62 |
| 6.70 Configuración del túnel en el servidor OpenVPN en pfSense1 . . . . .                                      | 63 |
| 6.71 Clave compartida generada automáticamente en el servidor OpenVPN en pfSense1 . . . . .                    | 63 |
| 6.72 Configuración del protocolo y fuente de la regla para el acceso al servidor OpenVPN en pfSense1 . . . . . | 64 |
| 6.73 Configuración del destino de la regla para el acceso al servidor OpenVPN en pfSense1 . . . . .            | 64 |



|      |   |    |
|------|---|----|
| 6.74 | Configuración de la regla para permitir el tráfico por el túnel OpenVPN en pfSense1 . . . . .     | 64 |
| 6.75 | Configuración del servidor en el cliente OpenVPN en pfSense2 . . .                                | 65 |
| 6.76 | Clave compartida copiada en el cliente OpenVPN en pfSense2 . . .                                  | 65 |
| 6.77 | Configuración del túnel en el cliente OpenVPN en pfSense2 . . . .                                 | 66 |
| 6.78 | Búsqueda e instalación del paquete de WireGuard . . . . .   | 67 |
| 6.79 | Intalación completada del paquete de WireGuard . . . . .  | 67 |
| 6.80 | Habilitar WireGuard en los ajustes de la VPN . . . . .  | 68 |
| 6.81 | Configuración del túnel WireGuard en pfSense1 . . . . .   | 69 |
| 6.82 | Editar túnel WireGuard en pfSense1 . . . . .  | 69 |
| 6.83 | Configuración del <i>Peer</i> WireGuard en pfSense1 . . . . .                                     | 69 |
| 6.84 | Clave pública del <i>Peer</i> WireGuard en pfSense1 . . . . .                                     | 69 |
| 6.85 | Redes permitidas del <i>Peer</i> WireGuard en pfSense1 . . . . .                                  | 70 |
| 6.86 | Configuración y clave pública del <i>Peer</i> WireGuard en pfSense2 . . .                         | 70 |
| 6.87 | Redes permitidas del <i>Peer</i> WireGuard en pfSense2 . . . . .                                  | 70 |
| 6.88 | <i>Default gateway</i> en ambos pfSense . . . . .   | 71 |
| 6.89 | Añadir la nueva interfaz para WireGuard en ambos pfSense . . . .                                  | 71 |
| 6.90 | Configuración general de la nueva interfaz WireGuard en pfSense1                                  | 71 |
| 6.91 | Configuración IPv4 de la nueva interfaz WireGuard en pfSense1 . .                                 | 72 |
| 6.92 | Creación del nuevo <i>IPv4 Gateway</i> para la interfaz WireGuard en pfSense1 . . . . .           | 72 |
| 6.93 | Configuración IPv4 de la nueva interfaz WireGuard en pfSense2 . .                                 | 72 |
| 6.94 | Configuración de la regla permitir tráfico al túnel WireGuard desde pfSense2 a pfSense1 . . . . . | 73 |
| 6.95 | Añadir una ruta estática en ambos pfSense . . . . .   | 73 |
| 6.96 | Configuración de la ruta estática en pfSense1 . . . . .   | 73 |
| 6.97 | Configuración de la ruta estática en pfSense2 . . . . .   | 74 |
| 7.1  | Comprobación del estado del túnel IPsec . . . . .   | 75 |
| 7.2  | Conectar el túnel IPsec manualmente . . . . .   | 76 |
| 7.3  | Orden <i>ping</i> desde el PC1 al PC2 antes de crear el túnel IPsec . . . .                       | 76 |
| 7.4  | Orden <i>ping</i> desde el PC1 al PC2 con el túnel IPsec creado y establecido . . . . .           | 76 |
| 7.5  | Comprobación del estado del túnel OpenVPN . . . . .   | 77 |
| 7.6  | Comprobación del estado del túnel WireGuard . . . . .   | 77 |
| 8.1  | Ejecución de <i>iperf</i> como servidor en el PC2 . . . . .                                       | 80 |
| 8.2  | Ejecución de <i>iperf</i> como cliente en el PC1 . . . . .  | 80 |
| 8.3  | Gráfico de anchos de banda máximos de los túneles . . . . .                                       | 81 |
| 8.4  | Ejecución de <i>scp</i> en el PC1 . . . . .   | 82 |
| 8.5  | Gráfico de tiempos de transferencia del archivo en los túneles . . .                              | 82 |
| 8.6  | Orden <i>ping -c 1</i> en el PC1 . . . . .  | 83 |
| 8.7  | Orden <i>ping -c 1</i> en el PC1 . . . . .  | 83 |
| 8.8  | Captura Wireshark en la interfaz <i>ens37</i> del PC2 para IPsec . . . . .                        | 84 |
| 8.9  | Captura Wireshark en la interfaz <i>ether3</i> del MikroTik para IPsec . .                        | 84 |
| 8.10 | Captura Wireshark en la interfaz <i>ens37</i> del PC2 para OpenVPN . .                            | 85 |
| 8.11 | Captura Wireshark en la interfaz <i>ether3</i> del MikroTik para OpenVPN                          | 85 |
| 8.12 | Captura Wireshark en la interfaz <i>ens37</i> del PC2 para WireGuard . .                          | 85 |
| 8.13 | Captura Wireshark en la interfaz <i>ether3</i> del MikroTik para WireGuard                        | 86 |

|     |  |    |
|-----|--|----|
| A.1 | Habilitar <i>SSH</i> en el pfSense1 . . . . .                                | 93 |
| A.2 | Acceder a pfSense1 desde PC1 vía <i>SSH</i> e instalar <i>nano</i> . . . . . | 94 |
| A.3 | Editar el archivo <i>config.xml</i> con <i>nano</i> . . . . .                | 94 |
| A.4 | Desactivar bloqueo de redes reservadas en <i>config.xml</i> . . . . .        | 95 |
| A.5 | Añadir regla para permitir el <i>ping</i> en <i>config.xml</i> . . . . .     | 95 |
| A.6 | Borrar la cache de configuración en pfSense1 . . . . .                       | 95 |

## Índice de tablas

---

|     |  |    |
|-----|--|----|
| 5.1 | Direcciones IP de los componentes de la solución en cada red . . . . . | 18 |
|-----|--|----|

---

---

# CAPÍTULO 1

## Introducción

---

En la actualidad, la interconexión de redes ha tomado un papel fundamental en la forma en la que operan las empresas, facilitando la conexión entre organizaciones o entre diferentes sedes de una misma. Estas interconexiones se pueden realizar con el objetivo de intercambiar información o compartir recursos entre sí, ofreciendo nuevas oportunidades de negocio.

Pero estas interconexiones suponen nuevos desafíos que las empresas deben afrontar. Estas se establecen a través de internet lo que las hace susceptibles a amenazas cibernéticas. Cada una de estas conexiones puede suponer una intrusión maliciosa, un robo de información o una denegación de servicios, entre otros ciberataques. Por tanto, protegerlas es una tarea crucial para mantener la seguridad de las empresas implicadas.

Existen gran cantidad de alternativas para establecer conexiones entre redes de forma segura, con diferencias en cuanto a costes, prestaciones y niveles de seguridad.

### 1.1 Motivación

---

El establecimiento de interconexiones seguras se realiza mediante túneles entre los equipos encargados de conectar la red de la empresa a internet, usualmente un router o un cortafuegos. Estos equipos pueden ser muy costosos para algunas empresas, sin embargo, existen versiones software que pueden ofrecernos las mismas prestaciones y funcionalidades sin necesidad de adquirir un equipo específico para esta función, constituyendo así una alternativa más económica. El cortafuegos *pfSense* es una de estas opciones. Este cortafuegos consiste en un software de código abierto que se puede alojar, tanto en instalaciones propias de la empresa, como en la nube, y que permite la creación de diferentes tipos de conexiones seguras entre redes [1].

*pfSense* supone una alternativa eficiente y flexible como equipo de seguridad y de interconexión de redes. Analizar, estudiar y probar cuales son las configuraciones que permiten extraer el máximo potencial a este cortafuegos en la creación de conexiones seguras es mi principal motivación para la realización de este trabajo.

## 1.2 Objetivos

---

El objetivo principal de este trabajo es interconectar dos redes de forma segura utilizando cortafuegos virtuales *pfSense*.

Para poder llevarlo a cabo, se va necesitar alcanzar los siguientes subobjetivos:

Diseñar y configurar un entorno virtualizado en VMware, para simular un ambiente real en el que se interconectan dos redes estableciendo conexiones entre cortafuegos *pfSense*.

Analizar y comparar las diferentes alternativas de conexiones, tanto de forma teórica, como realizando pruebas prácticas sobre el entorno virtual creado.

Documentar con detalle todo el proceso de configuración, puesta en marcha y pruebas de las distintas alternativas, permitiendo recrear la solución en un entorno real.

## 1.3 Estructura de la memoria

---

El trabajo se dividirá en 8 capítulos:

1. **Introducción:** En este primer capítulo, se describe la problemática actual de las interconexiones seguras entre redes y se comenta el posible uso del cortafuegos *pfSense* para esta tarea, describiendo la motivación y los objetivos de este trabajo.
2. **Estado del arte:** En este apartado, se estudiará el actual estado del arte respecto a la conexión de redes y el porqué se propone la opción del cortafuegos *pfSense* por delante de otras.
3. **Fundamentos para la interconexión segura de redes:** En este capítulo, se abordarán de forma teórica los fundamentos técnicos necesarios para conectar redes entre sí de forma segura, como son los túneles y las VPNs, además de sus diferentes tipos y protocolos existentes.
4. **Análisis del problema:** Este apartado, se centrará en analizar las posibles soluciones para la problemática del trabajo, mostrando las distintas alternativas y indicando en que consiste la solución elegida.
5. **Diseño de la solución:** El objetivo de este capítulo es explicar como se va a desarrollar la solución, cual es el entorno de virtualización escogido y que sistemas se van a utilizar.
6. **Desarrollo de la solución propuesta:** En este apartado, se describirá como se ha desarrollado la propuesta de solución y como se han realizado las diferentes configuración de los equipos implicados.
7. **Implantación:** En este capítulo, se mostrará la puesta en marcha de las diferentes configuraciones desarrolladas.

8. **Pruebas:** En este apartado, se presentarán y analizarán las pruebas realizadas sobre cada configuración para verificar el correcto funcionamiento de la solución, y para poder comparar la eficiencia de las diferentes configuraciones entre si.
9. **Conclusiones:** En esta última sección, se aportarán las conclusiones que se han alcanzado tras la realización y análisis del trabajo junto a la relación que guarda este con los estudios cursados.



---

---

# CAPÍTULO 2

## Estado del arte

---

### 2.1 Situación actual de los cortafuegos

---

Como se ha comentado en la introducción, los dispositivos encargados de establecer conexiones entre dos redes son los enrutadores. En muchos casos, los encargados de realizar este papel son los cortafuegos, ya que funcionan como puerta de enlace de una red a internet. Hoy por hoy, se utilizan los cortafuegos conocidos como firewalls de nueva generación o, en inglés, NGFW (*next generation firewall*). Esta nueva generación busca añadir nuevas funcionalidades a los cortafuegos, como filtrado de paquetes, inspección de estado y prevención de intrusiones [2].

Respecto a las marcas de firewalls más utilizadas, se encuentran Fortinet, Check Point, Palo Alto, Cisco, Sophos y SonicWall según la página *Gartner Peer Insights* [3]. A pesar de que las versiones de cortafuegos más utilizadas son las físicas, algunas de estas marcas como Fortinet y SonicWall disponen de versiones virtuales.

La elección entre un firewall físico o uno virtual se puede tomar en función de ciertos factores: el coste, consumo de recursos, la cantidad de dispositivos que se quieren proteger y la facilidad de uso. En primer lugar, el coste y el consumo de recursos de un cortafuegos virtual es menor que el de uno físico. Además, en muchos casos, son más sencillos de configurar y utilizar, sin embargo, si se quieren proteger un número elevado de dispositivos la opción hardware es la más recomendable [4] [5].

En cuanto a los equipos de seguridad software o virtuales, además de las versiones de algunas de las marcas previamente mencionadas, existen cortafuegos de código abierto. De entre estos, dos de los más utilizados son pfSense y OPNsense. Estas opciones son populares en instalaciones reducidas o en pequeñas empresas [6].

---

## 2.2 Situación actual de las conexiones seguras de redes

---

Existen diferentes protocolos que permiten establecer VPNs o conexiones seguras entre redes, actualmente los principales y más utilizados son OpenVPN, IPSec (IKEv2 y L2P2), WireGuard y SSTP. La elección de cual utilizar puede basarse en las necesidades de la conexión y en los equipos que se utilicen para establecerla [7].

---

## 2.3 Crítica al estado del arte

---

Realizando una búsqueda en la plataforma **RiuNet** no se ha encontrado ningún trabajo académico que trate en profundidad la problemática de la interconexión segura de redes mediante cortafuegos de código abierto en entornos virtualizados. Sin embargo, se han encontrado algunos trabajos que abordan diferentes aspectos sobre el uso de conexiones VPN.

Entre ellos, encontramos el trabajo *Creación de un nodo multi-VPN en la nube para el ámbito empresarial* del compañero Álvaro Marín García [8], en el que ha utilizado y comparado distintas VPNs configuradas en un servidor en la nube de Oracle Cloud. Este servidor fue utilizado como intermediario para permitir acceder a una red empresarial de forma segura desde un dispositivo cualquiera. No obstante, este trabajo está orientado al uso de las VPN como medio para acceder remotamente a una red, mientras que no aborda la posibilidad de unir entre sí distintas redes privadas. Además, la solución propuesta utiliza el cortafuegos propio de Oracle, lo cual no cubre el uso de otros cortafuegos o de servicios de virtualización diferentes. La posibilidad de utilizar un cortafuegos de código abierto, como pfSense, en su lugar, aumentaría en gran medida la adaptabilidad de la solución.

También, el compañero José Alapont Casañ en su trabajo *Cortafuegos y VPN para pymes con Raspberry* [9] expone una solución en la que configura un cortafuegos y una VPN en una Raspberry Pi, que permite proteger una red empresarial y acceder a ella remotamente de forma segura. Sin embargo, al igual que el trabajo comentado anteriormente, esta solución se centra en el uso de una VPN para acceder remotamente a una red y no para la interconexión de redes. Adicionalmente, destacar que la VPN se configura de forma automática utilizando un script. Este método es realmente ágil y óptimo a la hora de realizar la configuración pero puede dificultar el entendimiento de la conexión que se está desarrollando. En su lugar, realizar esta configuración paso a paso de forma manual podría ayudar a la hora de replicar la solución propuesta con unos requisitos distintos.

Con respecto al análisis y aplicación de los cortafuegos virtuales, solo se han encontrado algunos trabajos que utilizan de manera superficial el firewall pfSense desde el punto de vista únicamente de protección de redes virtualizadas o seguridad de viviendas inteligentes, como es el caso del trabajo *Introducción de aspectos de seguridad en una vivienda inteligente* del compañero Jesús Melo Solanes



[10]. Estos trabajos dejan sin abordar el uso de este cortafuegos para la conexión entre diferentes redes y la transferencia segura de datos.

Cabe destacar que cada uno de los trabajos mencionados a lo largo de este apartado abordan aspectos diferentes sobre las conexiones VPN y los cortafuegos virtuales. No obstante, las críticas realizadas buscan únicamente recalcar los posibles puntos de mejora y aspectos no cubiertos, con la finalidad de facilitar la búsqueda de los espacios de conocimiento a rellenar con este trabajo.

## 2.4 Propuesta

---

Este trabajo propone profundizar en la utilización de cortafuegos virtuales de código abierto como extremos para conseguir conectar redes de forma segura. Concretamente el cortafuegos utilizado será pfSense, uno de los más populares y utilizados de su categoría, como indica la página *TrustRadius* en su artículo *Best Virtualized Next-Generation Firewalls* [11]. Además, según la información de la página web de reviews tecnológicas *G2 Marketing Solutions* [12], pfSense ocupa un 69 % del mercado de pequeños negocios y el 25 % de negocios medianos en el campo de la tecnologías de la información y la seguridad de redes y sistemas.

Se abordará la creación de un entorno virtual en el que dos redes independientes se conectarán utilizando las diferentes alternativas en cuando a protocolos para la conexión de redes que ofrece pfSense. Todo esto se instalará sobre máquinas virtuales VMware, lo que permitirá realizar diferentes pruebas para comparar las prestaciones de las distintas configuraciones. Este esquema podría extrapolarse a un entorno empresarial real, tanto en una instalación propia, como en la nube.



---

## CAPÍTULO 3

# Fundamentos para la interconexión segura de redes

---

El establecimiento de una conexión segura entre dos redes a través de internet requiere de una serie de medidas que protejan los datos que se transmiten y las propias redes que establecen la conexión. Entre estas medidas se encuentran: el uso de cortafuegos como barrera que separa una red privada de internet y el establecimiento de túneles cifrados entre las redes implicadas. Las conexiones que se establecen a través de estos túneles son conocidas como **Redes Privadas Virtuales** o **VPN** del inglés *Virtual Private Network*.

### 3.1 Que son los túneles VPN

---

Al igual que un túnel físico ayuda a atravesar un espacio que sin él no se podría atravesar, los túneles en las redes ofrecen la posibilidad de transferir datos a través de una red, utilizando protocolos que no son compatibles con dicha red [13].

Los paquetes de datos que se envían a través de la red están compuestos fundamentalmente por dos partes, el encabezado y los datos o carga útil. El encabezado contiene información que ayuda a los enrutadores a dirigir el paquete a su destino, como las direcciones origen y destino. Además, incluye el protocolo de red utilizado para la comunicación, entre otra información relativa al paquete. Estos paquetes pueden encapsularse en otros paquetes para modificar el protocolo de red con el que se transmiten y así poder llegar y ser recibidos por redes no compatibles con dicho protocolo. Este proceso consiste en que se introduce el paquete original con su encabezado y datos en la carga útil de un nuevo paquete, que tendrá un encabezado con la información de origen y destino del paquete original pero un protocolo de red distinto.

Las **VPN** o **túneles VPN** son conexiones seguras y cifradas que se realizan a través de un túnel basado en el encapsulado de paquetes cifrados. En este proceso, se cifra el paquete original utilizando una clave secreta que solo es conocida por los extremos que establecen la conexión. Este paquete se introduce en la carga útil de un nuevo paquete que será transmitido por internet hasta llegar a su des-

tino, donde se desencapsulará y descifrará, este destino suele ser otra red privada [13].

## 3.2 Tipos de VPN

---

En la actualidad, destacan dos tipos de conexiones VPN, las **VPN de acceso remoto** y las **VPN sitio a sitio**. Ambos tipos cuentan con ventajas y desventajas, sin embargo, se utilizan habitualmente para propósitos diferentes.

Las **VPN de acceso remoto** (*Remote Access VPN*) permiten que usuarios puedan conectarse a una red privada independientemente de la localización en la que se encuentren. Estas conexiones utilizan un sistema de autenticación y cifrado de datos, creando así, un túnel privado y seguro entre el dispositivo remoto y la red a la que se conecta. Son comúnmente utilizadas para que empleados puedan acceder de forma remota a la red corporativa de una empresa, pudiendo hacer uso de los recursos de esta, sin poner en riesgo la información transmitida o la propia red de la organización [14].

Por otra parte, las **VPN de sitio a sitio** (*Site-to-Site VPN*) también conocidas como VPN router-to-router, son conexiones que se establecen entre enrutadores, permitiendo una comunicación segura entre dos redes privadas que se encuentran en distintas ubicaciones geográficas. De esta forma, las redes quedan unificadas entre si mediante un puente virtual que funciona como enlace seguro, asegurando la confidencialidad e integridad de la información que se trasmite y los recursos que se comparten. Este tipo de conexión se utiliza cotidianamente para interconectar diferentes sedes de una empresa, facilitando la colaboración segura entre ellas [15].

Esencialmente, las VPN de acceso remoto están orientadas a las conexiones de equipos individuales a una red, mientras que, las VPN sitio a sitio están encaminadas a la interconexión de distintas redes entre sí [16]. Este segundo tipo de conexión se ajusta perfectamente con el propósito de este trabajo, es por eso por lo que, las diferentes conexiones que se realizarán entre los cortafuegos en la solución propuesta, serán del tipo **Site-to-Site**.

## 3.3 Protocolos VPN

---

Los protocolos más utilizados para establecer conexiones VPN actualmente son IPSec, L2TP, IKEv2, OpenVPN, SSTP y WireGuard. Estos protocolos se diferencian en distintos factores, como el nivel de seguridad que ofrecen, la velocidad que soportan y la compatibilidad con los diferentes elementos de una red [17].

- **IPSec:** *Internet Protocol Security* o **IPSec** es un protocolo que se utiliza para asegurar y proteger las comunicaciones que se establecen a través del Protocolo de Internet (IP). Para conseguir esto, el protocolo realiza una autenticación de la sesión y el cifrado de los paquetes transmitidos en la conexión. **IPSec** es un protocolo ampliamente utilizado, tanto para conexiones de tipo

acceso remoto, como de tipo sitio a sitio, debido a sus altos niveles de seguridad, alta versatilidad y gran cantidad de opciones en cuanto a algoritmos de cifrado. Sin embargo, puede ser complejo de configurar y gestionar. Este protocolo puede funcionar en dos modos: modo transporte, en el que se cifra únicamente los datos y modo túnel, cifrando el paquete completo [17].

- **L2TP:** *Layer 2 Tunneling Protocol* o **L2TP** es un protocolo que no proporciona cifrado por sí mismo, por lo que suele utilizarse únicamente de establecer un túnel entre dos puntos de conexión. Habitualmente, se combina con otros protocolos como **IPSec** para establecer una VPN con un elevado nivel de seguridad. Mientras que **L2TP** se encarga de encapsular el tráfico que se comunica entre los dos extremos para establecer la conexión, **IPSec** cifra los paquetes que se transmiten por el túnel proporcionando seguridad. Esta combinación de protocolos se conoce como **L2TP/IPSec**. A pesar de los beneficios de compatibilidad que puede aportar este protocolo, cuenta con una gran desventaja, la ralentización de las comunicaciones debido a posibles cuellos de botella creados por la doble encapsulación (**L2TP** y **IPSec**). Además, este protocolo puede tener dificultades para pasar a través de algunos cortafuegos, a diferencia de otros protocolos [17].
- **IKEv2:** El protocolo de intercambio de claves de Internet versión 2 (*Internet key exchange*) o **IKEv2** fue desarrollado en colaboración entre Microsoft y Cisco Systems. Se trata de un protocolo, que al igual que L2TP, no proporciona cifrado, si no que se encarga de establecer y mantener una conexión segura entre dos extremos. Es por esto que, también se suele combinar con IPSec para que este realice el cifrado de la información, que se transmite por el túnel. Este protocolo no es compatible con todos los sistemas operativos y proveedores de VPN, a pesar de esto, es bastante utilizado porque proporciona conexiones con altas velocidades de internet [18]. Además, cuenta con la capacidad de restablecer conexiones de forma rápida tras una interrupción eventual, convirtiéndolo en una opción adecuada para conexiones móviles a través de redes Wi-Fi [19].
- **OpenVPN:** Es un protocolo de código abierto, basado en el uso de la biblioteca OpenSSL y que utiliza el protocolo *TLS* para cifrar y proteger las comunicaciones. Las conexiones se establecen entre un cliente **openvpn** y un servidor **openvpn** [20]. Este protocolo es considerado uno de los más seguros en la actualidad, destaca por ser altamente configurable y estar soportado por gran cantidad de plataformas de conexión VPN, lo que le permite atravesar algunos cortafuegos con facilidad. Además, ofrece un balance adecuado entre seguridad y velocidad. Sin embargo, este protocolo es complejo de configurar si no se dispone de conocimientos suficientes sobre conexiones VPN. Existen dos tipos de **OpenVPN**, uno que funciona con el protocolo TCP (*Transmission Control Protocol*) y otro que utiliza UDP (*User Datagram Protocol*) [19].
- **SSTP:** *Secure socket tunneling protocol* o **SSTP** es un protocolo VPN desarrollado por Microsoft, que utiliza *SSL/TLS* para el cifrado de las comunicaciones, concretamente en su versión *SSL 3.0*. Este protocolo emplea por general el puerto TCP 443, lo que permite que las conexiones puedan atravesar cortafuegos y otros filtros o restricciones de red. Esto lo convierte en

una buena opción en casos en los que otros protocolos VPN quedarían bloqueados o filtrados, como puede ser el uso de una conexión VPN desde redes Wi-Fi públicas [17]. **SSTP** cuenta con ventajas seguridad semejantes a **OpenVPN**, además, al ser un protocolo propiedad de Microsoft es muy estable en sistemas operativos Windows. Sin embargo, su uso puede ser más restrictivo en otros de sistemas operativos [20].

- **WireGuard:** Este innovador protocolo de código abierto, lanzado en 2015, propone una solución diseñada para ser eficiente y ligera, convirtiéndolo en uno de los protocolos más rápidos actualmente [19]. Su funcionamiento está basado en un mecanismo propio llamado *cryptokey routing*, este sistema asigna una dirección IP estática a cada cliente VPN y gestiona el tráfico usando claves criptográficas. Este proceso simplifica el establecimiento de las conexiones y reduce la latencia, mejorando así la eficiencia en comparación con otros protocolos VPN. Debido a su naturaleza ligera y ágil, este protocolo es utilizado para múltiples tipos de conexiones, destacando su uso en dispositivos varios como sistemas embebidos, y en servicios en la nube. No obstante, la asignación de direcciones IP estáticas podría suponer, a su vez, un riesgo para la privacidad de los usuarios conectados, permitiendo que se registre su actividad [17].

---

## CAPÍTULO 4

# Análisis del problema

---

La problemática de la interconexión segura de redes es una cuestión de gran importancia para las empresas debido al modelo de negocio actual. El intercambio de datos y compartición de recursos son algunas de las acciones realizadas a través de internet, que son necesarias para el correcto funcionamiento de muchas organizaciones. Las posibles amenazas cibernéticas que acarrearán estos procesos, han forzado a las entidades a elevar los niveles de seguridad en sus comunicaciones. Actualmente, los protocolos más confiables respecto al intercambio de claves para establecer las conexiones son **ECDH** y **RSA-2048**. Asimismo, en lo que respecta al algoritmo de cifrado y al tamaño de la clave, la combinación más segura consiste en utilizar **AES-256** que trabaja con claves de 256 bits [21].

Con el auge de los servidores virtuales, muchos de los componentes de la infraestructura informática de una empresa se están migrando a entornos virtuales, bien sobre servidores físicos en instalaciones propias, o bien en servidores alojados en la nube. Incluyendo la transición de algunos componentes de la infraestructura de red, como pueden ser switches, routers y cortafuegos, a sus versiones virtuales.

Esta necesidad de seguridad junto al avance a la virtualización de cortafuegos, dan pie a distintas soluciones que pueden proporcionar distintos niveles de seguridad, prestaciones y costes. El establecimiento de conexiones VPN, que sigan los estándares de seguridad actuales, entre cortafuegos de código abierto es una solución que presenta equilibrio entre altos niveles de seguridad y rendimiento. Además, esta solución constituye una reducción de los costes de la misma. De entre los cortafuegos virtuales de código abierto, los principales candidatos para resolver esta problemática son **pfSense** y **OPNsense** [6].

### 4.1 Identificación y análisis de soluciones posibles

---

Como se ha comentado anteriormente, las soluciones a valorar consisten en utilizar dos cortafuegos virtuales, que pueden ser **pfSense** o **OPNsense**, para establecer conexiones VPN entre ellos. Para poder seleccionar cual es la mejor alternativa en este caso, se va a realizar un análisis sobre algunas ventajas y desventajas de cada uno de ellos.

Por una parte, **pfSense** es un cortafuegos software de la compañía *Netgate*. Dispone de gran cantidad de documentación sobre su configuración y uso, a través de manuales oficiales [22] y foros impulsados por su gran comunidad, formada a lo largo de su extensa trayectoria desde el año 2004 [1]. En lo que respecta a la usabilidad e interfaz de usuario, este firewall opta por una estética tradicional y que, en ocasiones, puede no resultar muy intuitiva, sin embargo, puede ser más cómoda para usuarios experimentados. En cuanto a las funcionalidades, **pfSense** dispone de todas las que se podrían encontrar en un cortafuegos de nueva generación, además soporta la instalación de paquetes que permiten añadir algunas funcionalidades extra para propósitos específicos [23].

Por otra parte, **OPNsense** es una bifurcación del proyecto **pfSense**, que se creó en 2015. Es por esto que, a pesar de que existe un manual soportado por su comunidad [24], este cortafuegos no dispone de tanta documentación como **pfSense**. Su interfaz de usuario es actual y está organizada de forma lógica y ágil, lo que la hace apropiada para usuarios menos experimentados. Al igual que su homónimo, este cortafuegos cuenta con todas las funcionalidades de las que dispone cualquier otro cortafuegos actual y con la posibilidad de extenderlas añadiendo distintos paquetes [23].

En lo que respecta a las conexiones VPN, las dos opciones se encuentran en igualdad de condiciones, ya que ambos soportan los protocolos IPSec, OpenVPN y WireGuard, tanto para configuraciones de tipo *Site-to-Site*, como de tipo *Remote Access* [23]. Estos tres protocolos proporcionan un elevado nivel de seguridad, que se ajusta con el modelo actual. Por un lado, **IPSec** y **OpenVPN** permiten funcionar con el algoritmo de cifrado *AES-256*, considerado el cifrado más seguro, como se comentó anteriormente. Por otro lado, **WireGuard** utiliza *ChaCha20*, que, a pesar de que trabaja con claves más cortas que *AES*, también ofrece altos niveles de seguridad permitiendo un cifrado y descifrado más rápido [25].

Por último, con lo que respecta al nivel de reconocimiento e implantación, **pfSense** cuenta con la mayor parte del mercado. Este cortafuegos destaca en popularidad con números mucho mayores que **OPNsense**, como se documenta en el artículo *pfSense vs. OPNsense: Complete Firewall Comparison* [23] de *WunderTech*. En este artículo se utiliza la herramienta *Google Charts* para comparar las búsquedas realizadas en *Google* sobre ambos cortafuegos.

## 4.2 Solución propuesta

---

Aunque ambos cortafuegos son equivalentes en muchos de los aspectos analizados, la elección final será **pfSense** debido a diversos motivos. Por un lado, se dispone de una documentación más detallada sobre la configuración y establecimiento de túneles VPN entre distintos de estos cortafuegos. Además, el software tiene un mayor recorrido y cantidad de parches, por lo que dispone de versiones más estables que **OPNsense**. Por último, en cuanto a su nivel de implantación, es un cortafuegos que ya se ha utilizado para distintos tipos de instalaciones y en gran cantidad de empresas, lo que facilita su aprovechamiento para la implementación de la solución propuesta.



En cuanto las conexiones que se establecerán entre estos dispositivos virtuales, se realizarán un total de tres configuraciones diferentes. En todas ellas, se utilizarán conexiones VPN del tipo Sitio-a-Sitio, ya que serán conexiones establecidas entre dos enrutadores, en este caso los cortafuegos, creando un túnel seguro entre las redes privadas que se encontrarán detrás de ellos. Se ha decidido realizar una configuración por cada uno de los tres protocolos VPN soportados en **pfSense**, con el objetivo de abordar las diferentes opciones posibles para esta solución y poder comparar su funcionamiento práctico. Estos protocolos son IPSec, OpenVPN y WireGuard. Se configurará el algoritmo de cifrado *AES-256* para las conexiones IPSec y OpenVPN, mientras que WireGuard trabajará con *ChaCha20*, ya que no funciona con AES. De esta manera, se busca lograr el mayor nivel de seguridad en cada una de las configuraciones, de acuerdo con los requisitos actuales de seguridad.

Para llevar a cabo esta solución, se comenzará por instalar en el software de virtualización **VMware**, las máquinas virtuales necesarias para simular un entorno real con dos redes privadas virtuales aisladas. Después, se realizarán cada una de las tres configuraciones, acompañadas de una serie de pruebas que permitan comparar su funcionamiento a nivel práctico en el contexto propuesto. De esta forma, podrán extrapolarse a un escenario empresarial real.



---

# CAPÍTULO 5

## Diseño de la solución

---

La solución, como se ha comentado anteriormente, consistirá en un conjunto de máquinas y redes virtuales **VMware** desplegadas sobre un PC, que se nombrará como *PC Anfitrión* para los próximos apartados. Todas las comunicaciones se realizarán de forma local, internamente en esta máquina. Sin embargo, las redes podrían distribuirse y ser desplegadas en distintas ubicaciones, estableciendo las mismas comunicaciones a través de Internet, únicamente realizando algunas modificaciones sobre la configuración de los equipos enrutadores **pfSense**.

El diseño de la solución se abordará primero desde un punto de vista más amplio para examinar la idea general. Después, se realizará un análisis más detallado sobre el esquema final y los componentes que lo forman.

### 5.1 Arquitectura del Sistema

---

El esquema de la solución se dividirá en dos redes privadas que se comunicarán entre sí a través de una simulación de internet. Entre estas redes se establecerán las distintas conexiones VPN, tal y como se muestra en la figura 5.1, que permitirán proteger las comunicaciones y enlazar las redes.

La dirección IP de la *Red 1* será *10.24.1.0/24* y la *Red 2* tendrá la *10.24.2.0/24*.

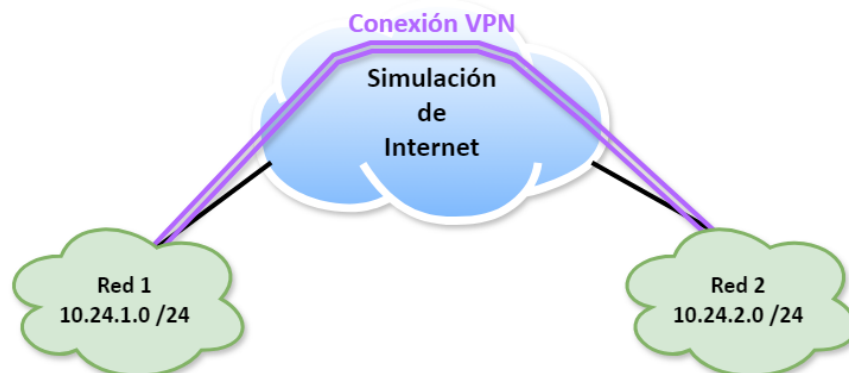


Figura 5.1: Esquema general de la solución

## 5.2 Diseño Detallado

Cada una de las redes contendrá dos componentes, un cortafuegos virtual **pfSense** y, conectada directamente a este, un máquina de usuario Linux (figura 5.2). Por una parte, el cortafuegos funcionará como puerta de enlace de la red, conectándola a Internet. Por otra parte, las máquinas de usuario permitirán realizar configuraciones sobre los cortafuegos y resultarán útiles para efectuar validaciones y pruebas, sobre las conexiones establecidas entre estos.

Habitualmente, las conexiones VPN de tipo *site-to-site* se establecen a través de Internet entre los routers o cortafuegos de dos redes, que realizan la función de enrutadores. Con la finalidad de simular este entorno, se ha optado por utilizar un router virtual del fabricante **MikroTik**, este dispositivo se introducirá entre las dos redes de forma que enrutará el tráfico entre ellas, funcionando como un nodo de un proveedor de servicios de Internet (ver figura 5.2). Podría utilizarse otro router software para realizar esta función, sin embargo, **MikroTik** ofrece una solución relativamente sencilla y cómoda.

El esquema final de la solución está compuesto por cuatro redes virtuales VMnet, como se puede observar en la figura 5.2: las redes VMnet5 y VMnet6 son las encargadas de simular Internet junto al router **MikroTik**, a pesar de que las direcciones de estas redes son privadas, representan las direcciones públicas que asignaría el proveedor de Internet, en un entorno real, a los equipos enrutadores de cada una de las redes; las redes VMnet2 y VMnet4, representan respectivamente las redes 1 y 2, formadas por un cortafuegos y una máquina de usuario cada una. Además de estas redes virtuales, una de las interfaces del router **MikroTik** estará conectada a la red local real utilizando un *Bridge*, a través del *PC anfitrión* (enlace verde en la figura 5.2), de esta manera el router formará parte de la red LAN física de igual manera que cualquier otro equipo conectado a esta. Las direcciones IP de los componentes de la solución en cada una de estas redes se presentan en la tabla 5.1.

|                | PC anfitrión                 | MikroTik                     | pfSense1   | pfSense2      | PC1                        | PC2                        |
|----------------|------------------------------|------------------------------|------------|---------------|----------------------------|----------------------------|
| VMnet5         | -                            | 172.16.0.1                   | 172.16.0.2 | -             | -                          | -                          |
| VMnet6         | -                            | 192.168.254.1                | -          | 192.168.254.2 | -                          | -                          |
| VMnet2         | 10.24.1.3                    | -                            | 10.24.1.1  | -             | <a href="#">10.24.1.52</a> | -                          |
| VMnet4         | -                            | -                            | -          | 10.24.2.1     | -                          | <a href="#">10.24.2.51</a> |
| Red local real | <a href="#">192.168.1.48</a> | <a href="#">192.168.1.68</a> | -          | -             | -                          | -                          |

**Tabla 5.1:** Direcciones IP de los componentes de la solución en cada red

Aclarar que las direcciones que aparecen en [azul](#) en la tabla 5.1 y en la figura 5.2 están asignadas dinámicamente utilizando el protocolo *DHCP* (*Dynamic Host Configuration Protocol*), mientras que el resto están configuradas de forma estática en cada uno de los componentes. Concretamente, las direcciones IP de la interfaz *ether5* del router **MikroTik** y de la interfaz física del *PC anfitrión* están asignadas por el router NAT real; en cambio, la dirección de la interfaz *ens37* de cada uno de los *PCs* es asignada por el **pfSense** al que se encuentra conectado cada equipo.

Las máquinas *PC1* y *PC2* utilizan sistemas operativos **AlmaLinux**, una distribución de Linux. Los equipos son idénticos en cuanto a configuración, excep-

tuando lo que respecta a la interfaz gráfica. El *PC1* no cuenta con interfaz gráfica, mientras que el *PC2* sí. Esto permitirá estudiar las distintas formas de configuración que ofrecen los cortafuegos **pfSense**, realizando algunas configuraciones sencillas sobre el *pfSense1* mediante consola desde el *PC1*. El análisis de esta alternativa de configuración se realizará en el apéndice A.

Además, cabe destacar que la red *VMnet2* se encuentra en modo *Host Only*, permitiendo que la máquina anfitriona tenga una interfaz virtual en dicha red. De esta forma, se podrá utilizar para realizar las principales configuraciones sobre el cortafuegos de la *Red 1*, ya que el *PC1* no cuenta con interfaz gráfica debido lo propuesto anteriormente. De esta forma, tanto el *pfSense1* como el *pfSense2* podrán ser configurados, con mayor facilidad, utilizando la interfaz web.

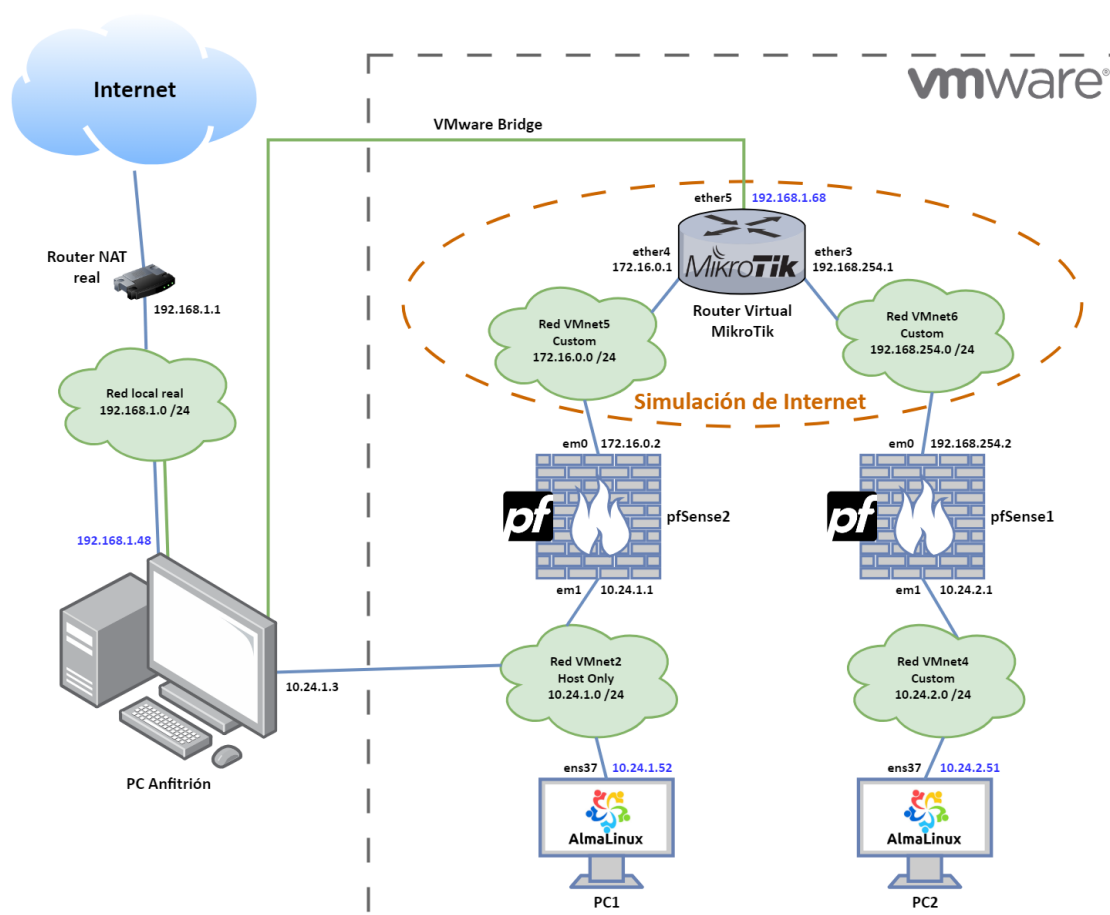


Figura 5.2: Esquema de red completo de la solución

## 5.3 Tecnología Utilizada

Para la implantación de la solución se van a utilizar distintas tecnologías que ya han sido mencionadas a lo largo del trabajo. En esta sección se pretende tratar de una forma más detallada cada una de ellas y justificar su elección.

### 5.3.1. Software de virtualización VMware

El software de virtualización, también conocido como *hipervisor*, es el encargado de virtualizar el hardware de un equipo físico para poder alojar distintos sistemas operativos sobre él. Existen dos tipos de hipervisores en función de su forma de ejecutarse [26].

Por un lado, los hipervisores de tipo 1 o bare-metal, se ejecutan directamente sobre el hardware de la máquina como un sistema operativo y se utilizan concretamente para la gestión las máquinas virtuales. Se suelen utilizar en servidores físicos para conseguir un uso más eficiente de estos. Por otro lado, los hipervisores de tipo 2 o alojados, se ejecutan como una aplicación sobre un sistema operativo anfitrión, como Windows o Linux, y se utilizan en ordenadores personales [27].

El hipervisor que se utilizará para implementar la solución será de tipo 2, ya que permitirá probar las distintas configuraciones sobre una máquina con un sistema operativo anfitrión, esta solución resulta más cómoda para el análisis planteado en este trabajo. Sin embargo, realizando unos cambios leves sobre la configuración de algunos componentes, la solución podría migrarse a servidores que utilicen hipervisores de tipo 1.

Existen distintas opciones en cuanto a hipervisores alojados, actualmente los principales son **VirtualBox**, un software de código abierto que pertenece a *Oracle* y **VMware Workstation**, la opción de la empresa *Broadcom Inc*, que ofrece versiones de pago y gratuitas. Ambas alternativas son muy similares pero presentan algunas diferencias en aspectos concretos, que convierten a **VMware** en la mejor elección para implementar la solución propuesta. En primer lugar, ofrece un mayor rendimiento y dispone de versiones más estables que su homónimo [28]. A su vez, en lo que respecta a la creación de redes virtuales, **VMware** se coloca por delante de **VirtualBox**, ya que ofrece una mayor flexibilidad y más opciones de configuración [29]. Además, **VMware** dispone también de un hipervisor de tipo 1, lo que podría facilitar la migración de la solución a servidores, en un entorno real. Por último, cabe señalar que **VMware** está más orientado a un uso empresarial mientras que **VirtualBox** destaca en el uso doméstico [28].

Concretamente se utilizará **VMware Workstation Player**, la versión gratuita que ofrece **VMware**.

### 5.3.2. Firewall virtual pfSense

A modo de enrutador de cada una de las redes podría utilizarse un router virtual, pero como se busca un solución más segura, la mejor opción es un software que realice, a su vez, las funciones de enrutador y cortafuegos. Como ya se ha comentado en el análisis del problema a tratar, se busca una solución que ofrezca un balance en cuanto a rendimiento, niveles de seguridad y costes. Los cortafuegos virtuales de código abierto, como los ya analizados **OPNsense** y **pfSense**, satisfacen adecuadamente estas necesidades.

Ambos sistemas son muy similares en muchos aspectos y pertenecen a la categoría de los cortafuegos de nueva generación o, en inglés, *next generation firewall*, disponiendo así de todas la funcionalidades de un firewall actual. Por una par-

te, cuentan con funciones de seguridad entre las que se encuentran las reglas de seguridad, sistema de autenticación de usuarios, proxy y filtrado de contenido, sistema de prevención de intrusiones, bloqueo GeoIP y capacidad para establecer conexiones VPN. Por otra parte, disponen de funciones de enrutador, como la creación de redes, servidor DHCP y DNS, enrutamiento estático, traducciones NAT de entrada y salida y soporte de VLAN. Adicionalmente, tienen herramientas que permiten monitorizar las redes y el hardware del sistema [23].

Tras la comparación de ambas alternativas, ya realizada en el análisis de las posibles soluciones, **pfSense** es la opción escogida para implementar la solución. Debido a su extensa documentación, la estabilidad de sus versiones y la amplia implantación en el ámbito de las pequeñas empresas, este cortafuegos supone una elección ligeramente mejor que **OPNsense**.

### 5.3.3. Router virtual MikroTik

Como se ha mencionado previamente, se utilizará un router virtual **MikroTik** para imitar un router de proveedor de servicios de Internet, simulando así una conexión entre los cortafuegos a través de Internet.

Cualquier router virtual podría funcionar para conseguir el efecto que se busca, no obstante, **MikroTik** ofrece su alternativa para sistemas X86. Esta solución consiste en un router virtual relativamente sencillo de configurar y que cuenta con una licencia gratuita. Esta licencia tiene algunas limitaciones en la cantidad de funciones que permite configurar [30], sin embargo, es suficiente para conseguir el objetivo expuesto. **MikroTik** dispone de abundante documentación acerca de cómo utilizar sus principales funciones [31]. Además, este router cuenta con la funcionalidad *Bridge*, que permite la comunicación entre distintas redes de forma sencilla, sin necesidad de crear rutas, simplemente añadiendo las distintas interfaces a un mismo *puente* [32]. Esta función es ideal para cumplir con su propósito en la solución planteada.

### 5.3.4. Sistema operativo AlmaLinux

El sistema operativo utilizado en las máquinas virtuales *PC1* y *PC2* será Linux, ya que es gratuito, a diferencia de Windows y permite configurar completamente las interfaces de red. Además, permitirá mostrar como realizar algunas configuraciones sobre uno de los cortafuegos a través de consola de comandos, sin utilizar interfaz gráfica, algo que solo es posible utilizando este sistema operativo. Este método de configuración se abordará de forma independiente en el apéndice A

Aunque existen gran cantidad de distribuciones de Linux, para estas máquinas se utilizará **AlmaLinux** [33], una de las distribuciones más utilizadas y descendiente directa de **CentOS**, tras su discontinuidad en 2021 [34]. Sin embargo, cabe mencionar que se podría utilizar otra distribución, como **Ubuntu**, para realizar las configuraciones y pruebas que se proponen a fin de llevar a cabo la solución.





---

# CAPÍTULO 6

## Desarrollo de la solución propuesta

---

El desarrollo de la solución comienza con la instalación y la realización de configuraciones iniciales de las máquinas virtuales, correspondientes a cada uno de los elementos del esquema. Posteriormente, se configurarán las tres conexiones VPN, cada una de ellas utilizando un protocolo distinto. Tras cada configuración, se realizarán las pruebas correspondientes, que se analizarán en un capítulo dedicado a esto y se desharán los cambios aplicados, devolviendo los equipos al estado posterior a las configuraciones iniciales. De esta manera, se descartan posibles conflictos entre las diferentes conexiones, permitiendo hacer pruebas de forma independiente sobre cada una de las configuraciones.

### 6.1 Instalación de las máquinas virtuales implicadas

---

Para llevar a cabo la instalación de cada una de las máquinas virtuales, primero se descargará la imagen de sistema operativo correspondiente (*ISO*), se creará la máquina en VMware y se seguirá el proceso de instalación.

#### 6.1.1. Instalación de los cortafuegos pfSense

Las instalaciones de las dos máquinas virtuales que alojan los cortafuegos pfSense son idénticas, por lo que se abordará la instalación de una de ellas únicamente.

Primero, descargaremos la imagen ISO desde la página oficial de pfSense [35]. Después, crearemos una nueva máquina virtual y seleccionaremos la opción *Installer disc image file (iso)* añadiendo la imagen descargada previamente (ver figura 6.1). Continuando con el wizard de instalación, elegiremos el nombre de la máquina, en este caso *pfSense1* o *pfSense2*. Avanzando hasta el último paso de este proceso de creación, presionamos la opción *Customize Hardware...* y configuramos 3 GB de memoria, 2 procesadores y 20 GB de disco duro virtual. Aunque se recomienda 4 GB memoria para este software, por motivos de rendimiento del equipo anfitrión se decidió reducir ligeramente este parámetro. En cuanto a los adaptadores de red, añadiremos uno además del que aparece por defecto, presionando sobre la opción *add* de la parte inferior seleccionando *network adapter* y configuraremos, para el *pfSense1*, la VMnet5 en el primero, con la que se conectará

al router MikroTik y la VMnet2 a la que conectaremos el *PC1*. La configuración de hardware completa de *pfSense1* se muestra en la figura 6.2. Para el *pfSense2*, configuraremos la VMnet6 en el primero, para conectarlo al router MikroTik y la VMnet4 a la que conectaremos el *PC2*, tal y como se puede observar en la figura 6.3. Una vez terminada la configuración haremos clic en finalizar y, si hemos dejado marcada la opción de arrancar la máquina tras la creación, se nos abrirá automáticamente.

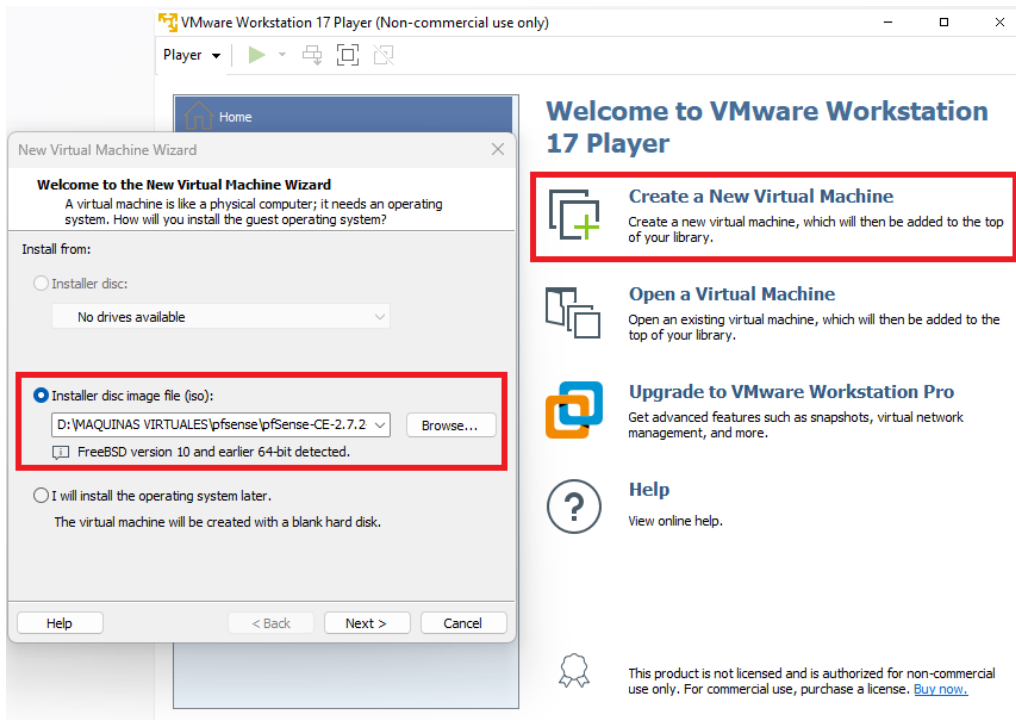


Figura 6.1: Crear máquina virtual pfSense

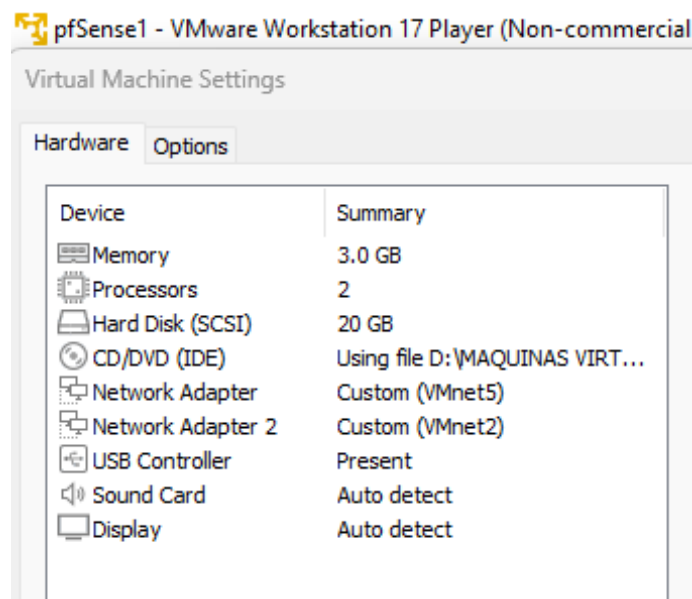


Figura 6.2: Configuración de hardware VMware del pfsense1

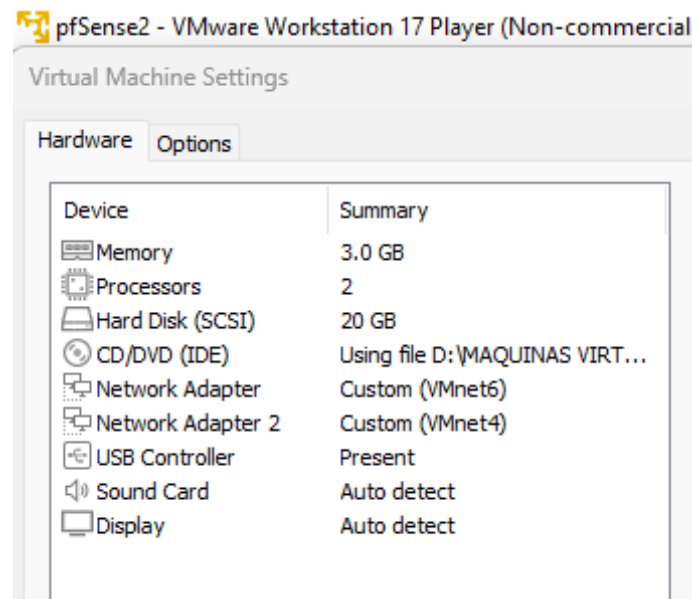


Figura 6.3: Configuración de hardware VMware del pfsense2

Para la instalación de pfSense podemos seguir la guía que se encuentra en el manual oficial [36], en nuestro caso, la instalación que se va a realizar es lo más sencilla posible ya que estamos creando un entorno de pruebas, sin embargo, en esta guía podemos encontrar una explicación de forma detallada cada una de las distintas opciones que aparecen este proceso.

Lo primero que observamos es la información de *Copyright* (figura 6.4), pulsaremos *enter* y obtendremos un menú para elegir la opción a realizar, seleccionaremos *Install* (figura 6.5).

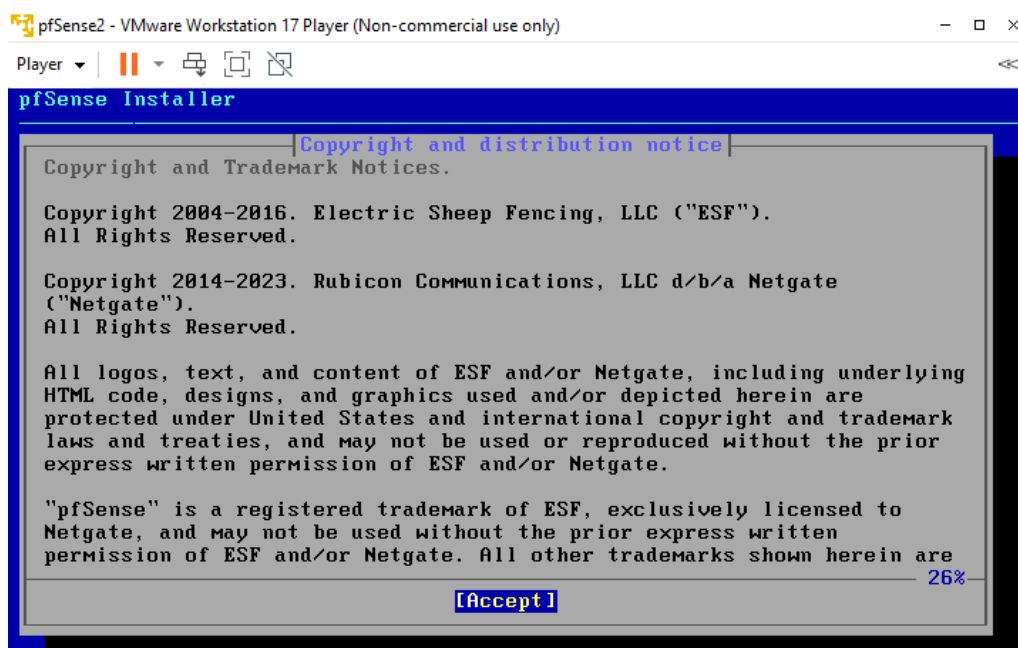


Figura 6.4: Primer paso en la instalación de pfSense

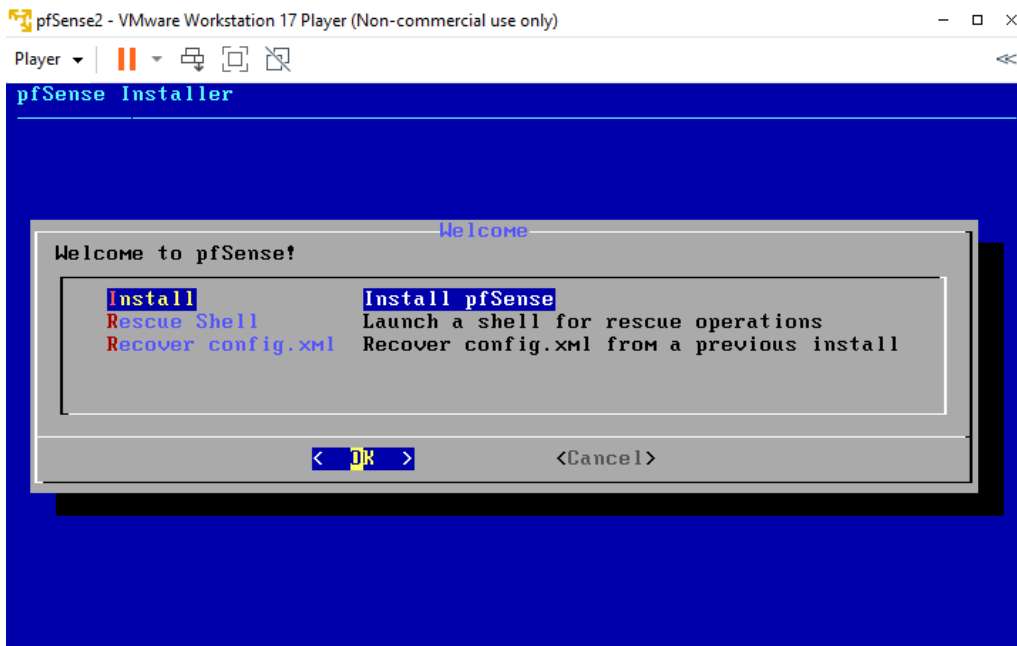


Figura 6.5: Opciones de instalación de pfSense

En cuanto al sistema de particiones, seleccionaremos *Auto (UFS)*, como se muestra en la figura 6.6, luego *Entire Disk*, a continuación, escogeremos *MBR DOS Partitions*. Para terminar el proceso de instalaciones, tras obtener el resumen de la configuración de del disco (figura 6.7) presionaremos *enter* sobre la opción *finish* y, si todo ha salido correctamente, podremos observar el progreso del proceso de instalación (figura 6.8). Cuando este proceso termine seleccionaremos *Reboot* y, después de un reinicio, la instalación estará completa.

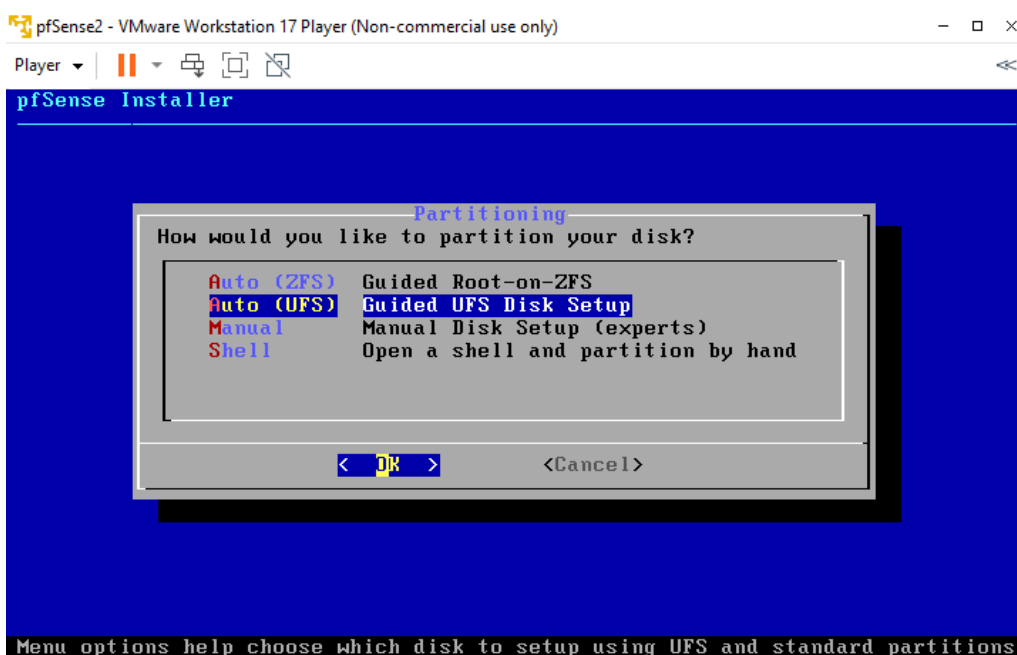


Figura 6.6: Opciones de particionado de disco de pfSense

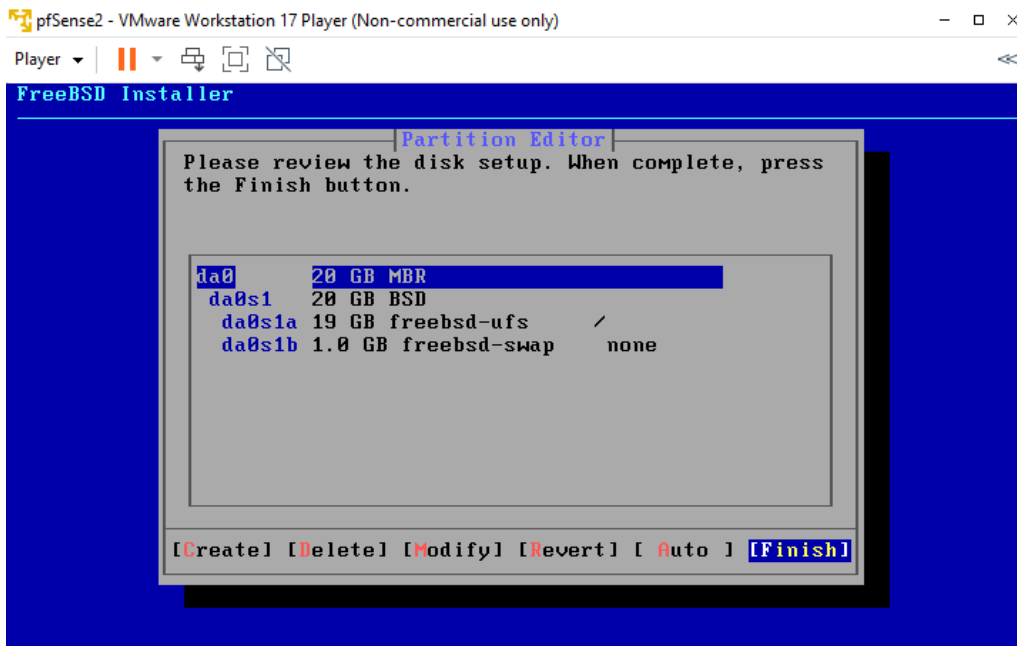


Figura 6.7: Opciones de intalación de pfSense

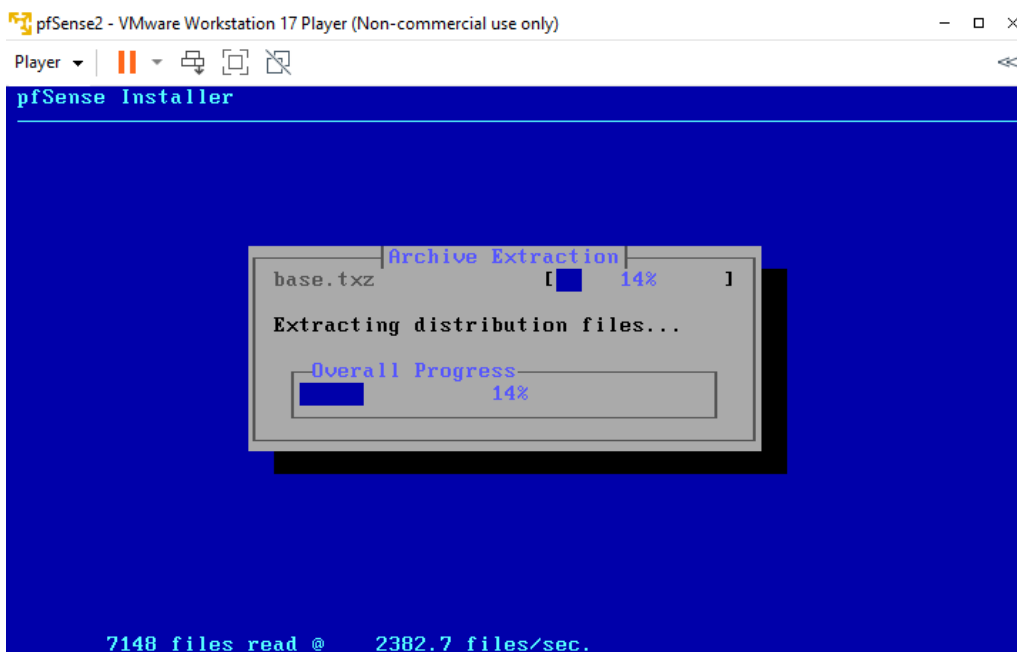


Figura 6.8: Opciones de intalación de pfSense

### 6.1.2. Instalación del router MikroTik

El primer paso, al igual que para el resto de máquinas, será descargar la imagen ISO de la pagina oficial de MikroTik [37]. En este caso, podemos elegir una versión en concreto, sin embargo, para el objetivo que se busca en esta solución, cualquier versión de la de la rama 7.X funcionará correctamente. Seleccionamos la versión escogida y descargamos la opción que aparece como X86 y .iso.

Tras la descarga, procedemos a crear la máquina en el software VMware, de igual manera que en las máquinas pfSense (ver figura 6.1), creamos una nueva máquina y seleccionando la opción *Installer disc image file (iso)* pero añadimos, en este caso, la ISO descargada de MikroTik. Seleccionamos como sistema operativo *Other x64* y ponemos el correspondiente nombre a la máquina, en nuestro caso, *MikroTik*, y avanzamos las distintas partes del wizard hasta llegar a la última ventana. Seleccionamos la opción *Customize Hardware...* para realizar las configuraciones de hardware de la máquina. En este caso, el sistema operativo no requiere de mucha memoria, configuraremos 512 MB y un procesador y dos discos virtuales de 60 y 512 MB respectivamente. Para la configuración de red necesitaremos 3 adaptadores, por lo que añadiremos dos más. En el primer adaptador configuraremos la VMnet6, con la que establecerá conexión con el *pfSense2*; en el segundo la VMnet5, para conectarlo con el *pfSense1* y en el tercer adaptador se configurará en modo *Bridge (Automatic)*, para que salga a internet a través del PC anfitrión utilizando una dirección IP independiente dentro de la red local física. Toda esta configuración se muestra en la figura 6.9. Una vez terminada la configuración del hardware, presionamos *finalizar* y la máquina arrancará.

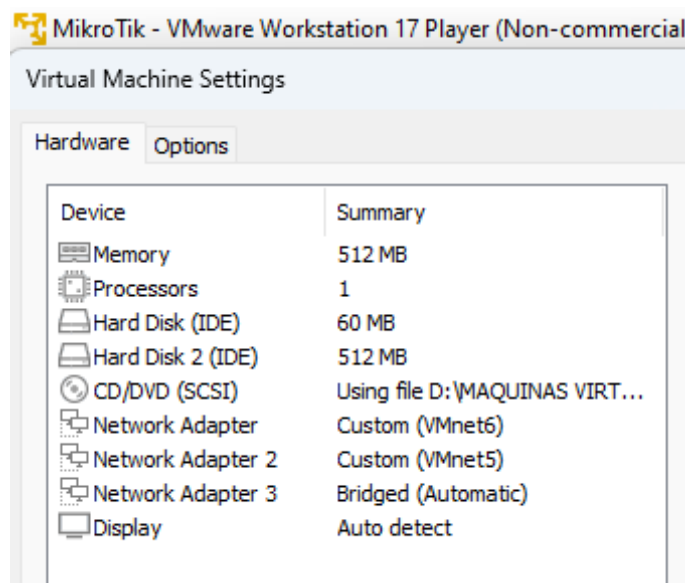


Figura 6.9: Configuración de hardware VMware del router MikroTik

Al comenzar la instalación, observamos un menú con diversas opciones como el de la figura 6.10, para comenzar el proceso presionamos la tecla 'i'. Tras terminar el proceso nos solicitará reiniciar la máquina y tras el reinicio podremos iniciar sesión, el usuario por defecto es *admin* y sin contraseña. Una vez introducidas las credenciales. El sistema nos ofrecerá mostrarnos la licencia actual, podemos omitirlo escribiendo una 'n', y aparecerá el *software ID*, que será necesario para solicitar la licencia (marcado en rojo en la figura 6.11). También, nos solicitará que introduzcamos una nueva contraseña.

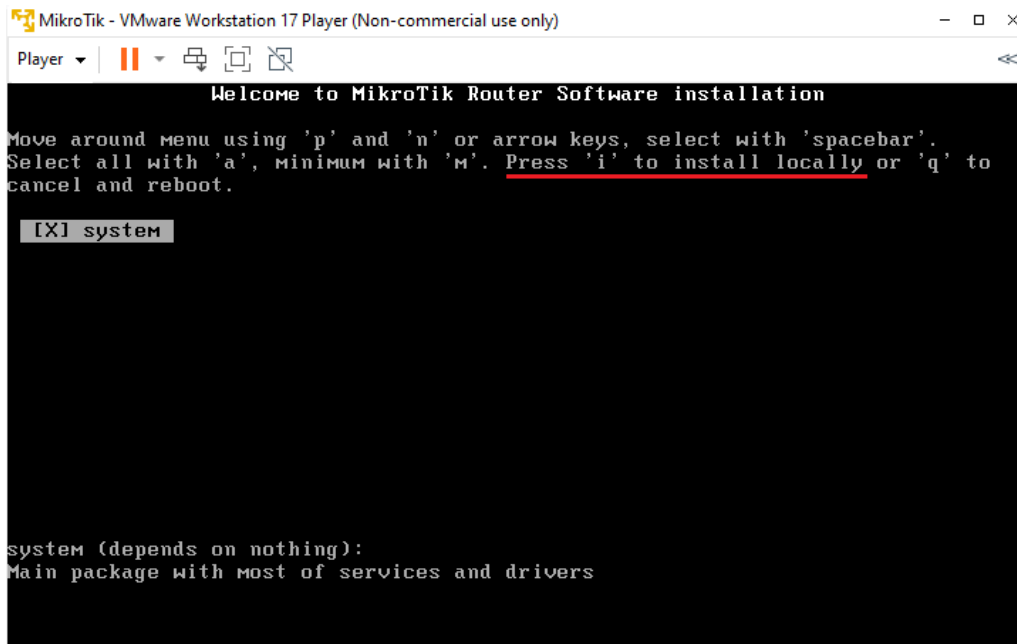


Figura 6.10: Opciones de instalación del router MikroTik

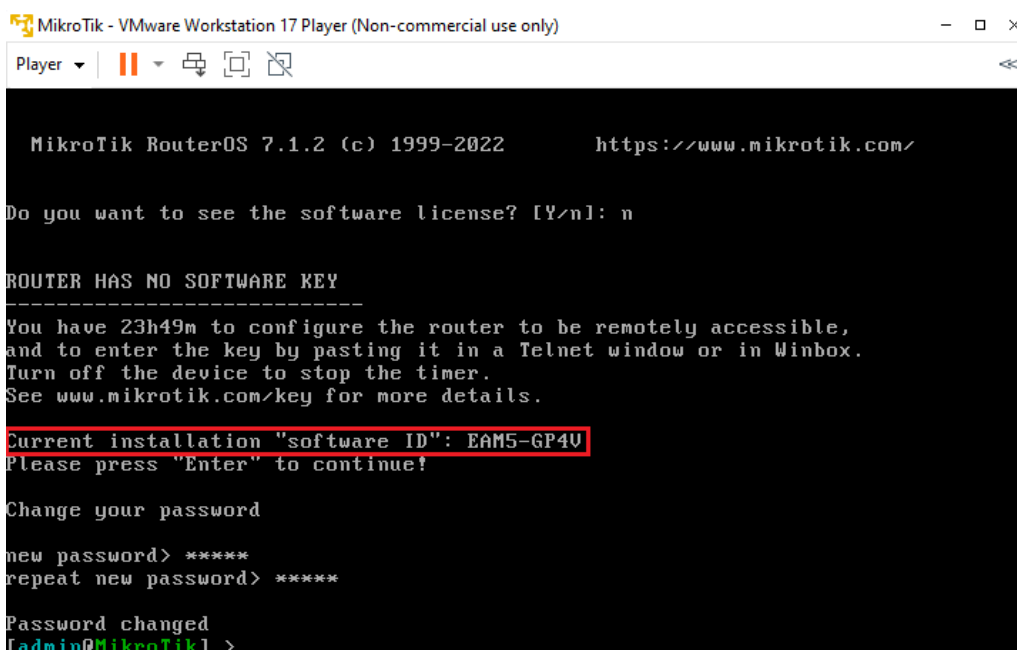


Figura 6.11: Software ID y cambio de contraseña del router MikroTik

Después de la instalación, pasaremos a activar la licencia demo gratuita que se comentó anteriormente. Para ello es necesario registrarse en la página de MikroTik (ver figura 6.12). Una vez cumplimentados todos los campos y creada la cuenta, recibiremos un correo con las credenciales de acceso. A continuación, iniciamos sesión y en la sección de cuenta, seleccionamos *Make a demo key* y rellenamos el apartado de *Software ID* con el ID de la máquina previamente instalada (figura 6.13). Después, presionamos en *Generate* y obtenemos una clave de licencia que usaremos a continuación (figura 6.14).

mikrotik.com/client/register

**MIKROTIK** Home About Buy Jobs Hardware Software Support Training Account

Register User

## REGISTER

LOG IN

Registration type  Natural person  Legal person

First name  Required

Last name  Required

E-mail  Required

Residential address

Country  Select country

Province/state or region  Required

City  Required

Postcode  Required

Address line  Required

Phone Number

Website URL

Figura 6.12: Registro en la página de MikroTik

mikrotik.com/client/keyDemo

**MIKROTIK** Home About Buy Jobs Hardware Software Support Training Account

My account Log out

Toggle menu

ACCOUNT INFORMATION  
Home  
Balance  
Edit account details  
Edit email settings  
Manage employees  
Events

WEB ORDERS  
My web orders and invoices  
Purchase a RouterOS license key

ROUTEROS KEYS  
Search and view all keys  
Request RouterBOARD license key  
Transfer prepaid keys (none)  
Make a demo key

CHR LICENCES  
All CHR keys  
Transfer CHR prepaid keys (none)

TRAINING  
My training sessions  
My certificates

SUPPORT  
My support tickets  
Support.rtf viewer

OTHER  
Lockpack creator

## Make a demo key

Free Demo (Trial) License Key for RouterOS 2.9 and up

- demo (trial) license key is level 1 key
- has limits of maximum connections each for PPTP, PPPoE, Queues, NAT, EoIP, and DHCP
- does not have wireless interface support
- does not include version upgrades
- does not expire (no time limit)
- does not include support
- not for resale

After you install the router it will report a Software ID.

Place in folder:  Demo keys

Software ID  EAMS-GP4V

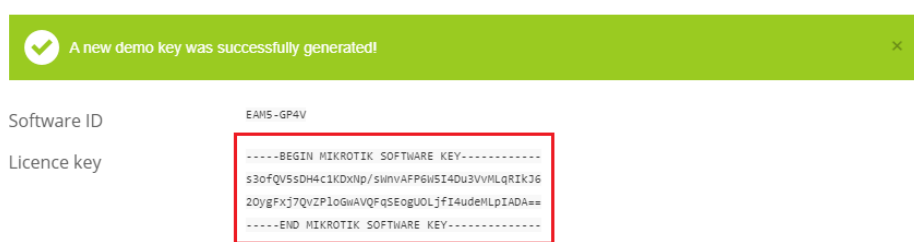
Send key to my email (jblasocarmona@gmail.com).

Note: This key works with any installation method. Only for 2.9 and up.

Figura 6.13: Genera una clave de demo en la página de MikroTik

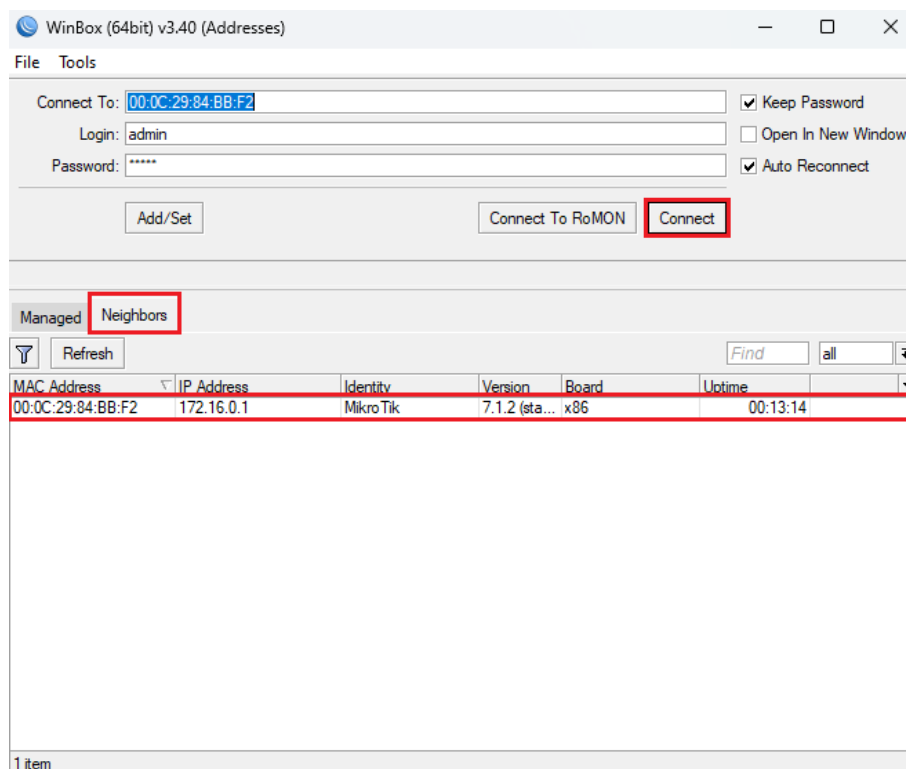


## Make a demo key



**Figura 6.14:** Clave de demo generada para el router MikroTik instalado

El router MikroTik dispone de una herramienta propia para su configuración, esta software se denomina *WinBox* y puede descargarse en su página oficial [37]. Una vez, descargamos la herramienta y la abrimos desde el PC anfitrión, accedemos al apartado de *Neighbors* y, si la máquina virtual está inicia, nos aparecerá listado, lo seleccionamos, introducimos la nueva contraseña que hemos configurado y pulsamos *Connect* (ver figura 6.15).



**Figura 6.15:** Acceso al router MikroTik desde WinBox

Una vez dentro del menú de configuración, copiamos desde la página web de *MikroTik*, la clave de licencia y dentro del *WinBox*, en *System* accedemos a *License* y seleccionamos *Paste Key*, tal y como se muestra en la figura 6.16 [30]. El sistema solicitará un reinicio y tras él, podemos volver a consultar la licencia y comprobar que el nivel ha cambiado a 1, por lo que se ha activado la licencia correctamente (ver figura 6.17). Con esto hemos concluido la instalación de esta máquina virtual.

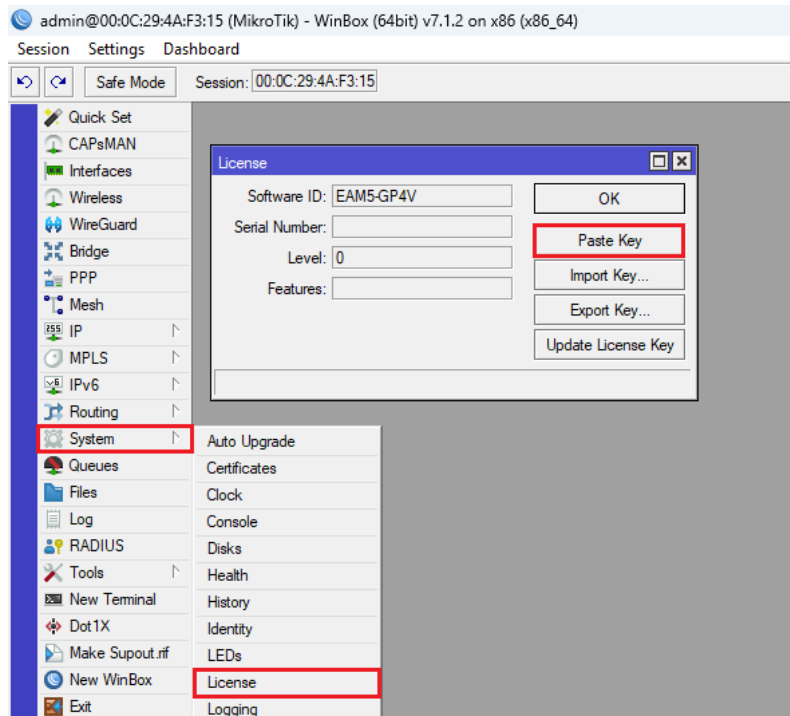


Figura 6.16: Sección de licencia en WinBox

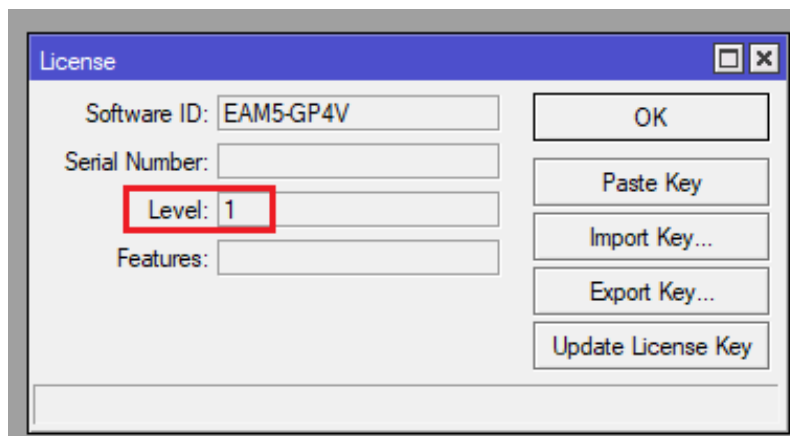


Figura 6.17: Licencia demo activada en WinBox

### 6.1.3. Instalación de las máquinas AlmaLinux

Comenzamos descargando la imagen del sistema operativa desde la página oficial de AlmaLinux OS [38]. De igual manera que con el router MikroTik, cualquiera de las versiones es suficiente para el uso básico que se le dará a esta máquinas en la solución planteada. Independientemente de elegir la versión 8 o 9 de este sistema operativo, tendremos que acceder al apartado *Intel/AMD(x86\_64)*, ya que esta es la versión compatible con máquinas VMware y en la sección de *ISO Images*, descargaremos la imagen *DVD ISO*. Este tipo de imágenes incluyen todos los paquetes necesarios para la instalación de la máquina y suponen la instalación más sencilla [38].

A continuación, crearemos las dos máquinas virtuales, una para el *PC1* y otra para el *PC2*. Al igual que en la creación del resto de máquinas virtuales (ver figura 6.1), iniciamos el proceso de creación y seleccionamos, en la opción *Installer disc image file (iso)*, la imagen que hemos descargado. Después, elegimos un nombre para la máquina, en este caso, *PC1* y *PC2* y avanzamos al último paso donde, al igual que en los casos anteriores, configuraremos el hardware de la máquina presionando en *Customize Hardware....* En este caso, las configuraciones de ambas máquinas diferirán en la memoria ya que sobre una de ellas se instalará el sistema operativo sin interfaz gráfica y, por tanto, no necesitará de muchos recursos, sin embargo, la otra si se instalara con interfaz gráfica y necesitará un hardware mayor.

En el caso del *PC1*, tal y como se muestra en la figura 6.18, configuraremos 2 GB de memoria, 2 procesadores y un disco duro virtual de 20 GB. En lo que respecta a los adaptadores de red, solo necesitaremos uno, que configuraremos en la *VMnet2* para establecer conexión con el cortafuegos *pfSense1*.

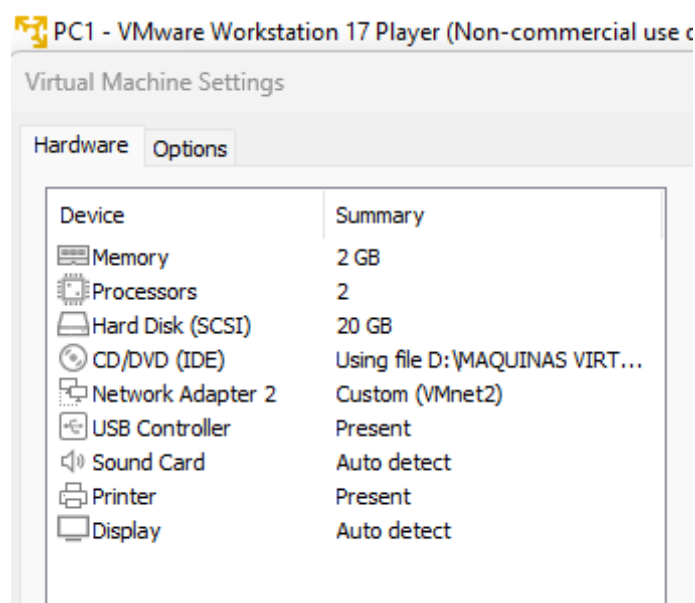


Figura 6.18: Configuración de hardware VMware del PC1

Para el *PC2*, aumentaremos la memoria a 4 GB para conseguir un mejor rendimiento en el uso de la interfaz gráfica y, al igual que en *PC1*, seleccionaremos 2 procesadores y un disco duro 20 GB. Esta máquina también contará únicamente con un adaptador de red que configuraremos en la *VMnet4*, para poder establecer conexión con el cortafuegos *pfSense2*. Podemos observar esta configuración al completo en la figura 6.19.

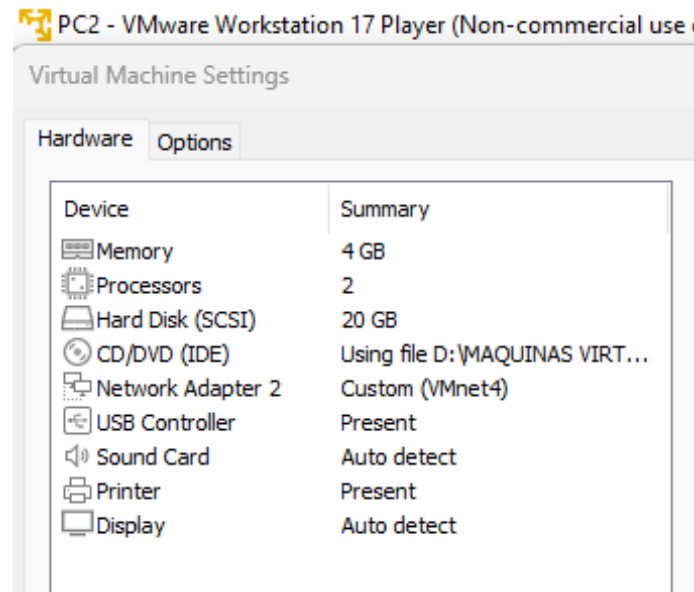


Figura 6.19: Configuración de hardware VMware del PC2

A fin de realizar la instalación se ha utilizado la guía de instalación de la página oficial de AlmaLinux [39]. El proceso comienza con un menú en el que seleccionaremos la opción de *Install AlmaLinux* pulsando *enter* (figura 6.20). Esto comenzará un proceso de chequeo de los archivos de la imagen (ver figura 6.21), que al terminar nos dirigirá a un proceso para configurar la instalación.

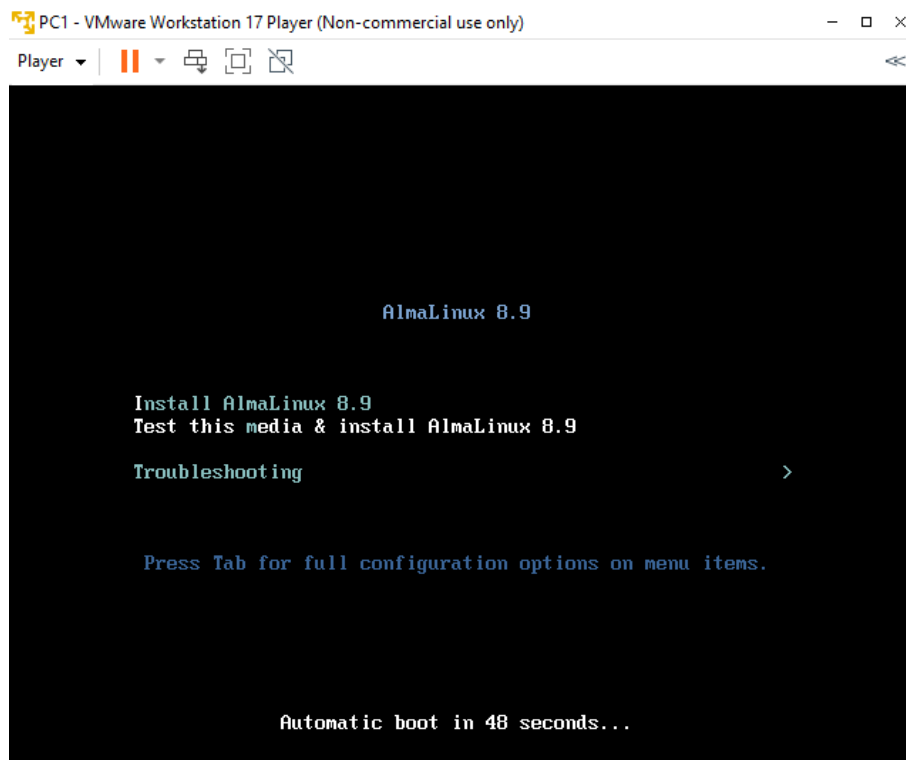


Figura 6.20: Opciones de la instalación de AlmaLinux

```

PC1 - VMware Workstation 17 Player (Non-commercial use only)
Player
[ 6.895674] dracut-pre-udev[551]: anaconda-modprobe: Module floppy not found
[ 7.354664] dracut-pre-udev[551]: anaconda-modprobe: Module cbc not found
[ OK ] Started Show Plymouth Boot Screen.
[ OK ] Started Forward Password Requests to Plymouth Directory Watch.
[ OK ] Reached target Paths.
[ OK ] Reached target Local Encrypted Volumes.
[ OK ] Started cancel waiting for multipath siblings of nme0n1.
[ OK ] Started udev Wait for Complete Device Initialization.
Starting Device-Mapper Multipath Device Controller...
[ OK ] Started Device-Mapper Multipath Device Controller.
Starting Open-iSCSI...
[ OK ] Reached target Local File Systems (Pre).
[ OK ] Reached target Local File Systems.
Starting Create Volatile Files and Directories...
[ OK ] Started Open-iSCSI.
Starting dracut initqueue hook...
[ OK ] Started Create Volatile Files and Directories.
[ OK ] Reached target System Initialization.
[ OK ] Reached target Basic System.
[ OK ] Started Hardware RNG Entropy Gatherer Daemon.
[ OK ] Started Show Plymouth Boot Screen.
[ OK ] Started Forward Password Requests to Plymouth Directory Watch.
[ OK ] Reached target Paths.
[ OK ] Reached target Local Encrypted Volumes.
[ OK ] Started cancel waiting for multipath siblings of nme0n1.
[ OK ] Started udev Wait for Complete Device Initialization.
Starting Device-Mapper Multipath Device Controller...
[ OK ] Started Device-Mapper Multipath Device Controller.
Starting Open-iSCSI...
[ OK ] Reached target Local File Systems (Pre).
[ OK ] Reached target Local File Systems.
Starting Create Volatile Files and Directories...
[ OK ] Started Open-iSCSI.
Starting dracut initqueue hook...
[ OK ] Started Create Volatile Files and Directories.
[ OK ] Reached target System Initialization.
[ OK ] Reached target Basic System.
[ OK ] Started Hardware RNG Entropy Gatherer Daemon.
/dev/sr0: bf6f37c6b5f575b52b1ead5c1c99a345
Fragment sums: a2288c81a963a865f5f115ff969a694d7422743a66e132caeab1d7ebe636
Fragment count: 20
Supported ISO: yes
Press [Esc] to abort check.
Checking: 056.2%

```

Figura 6.21: Proceso de comprobación de archivos de instalación en AlmaLinux

Primero seleccionamos el idioma, en este caso español, y obtenemos un menú con los diferentes apartados a configurar. En este menú configuraremos, tal como se muestra en la figura 6.22, la *Fecha y hora* actual, en este caso seleccionamos *Europa/Madrid*; el *Destino de la instalación*, en nuestro caso lo dejamos por defecto y presiona *Hecho* (figura 6.23); una *Contraseña de root*, también podemos crear algún usuario, aunque para nuestra solución trabajaremos como root; la *Red y nombre de equipo*, aunque únicamente modificaremos el nombre del equipo a *pc1* o *pc2* en cada una de las máquinas respectivamente, ya que la configuración de red se realizará posteriormente en el apartado de configuraciones iniciales.

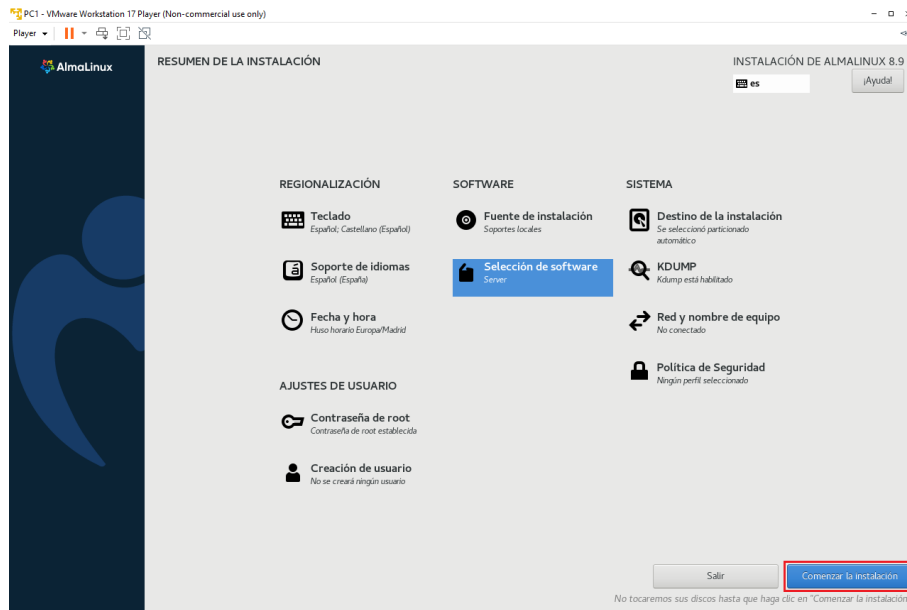


Figura 6.22: Configuración de la instalación de AlmaLinux



Figura 6.23: Configuración del disco para la instalación de AlmaLinux

Por último, en el apartado *Selección de software* escogeremos la opción *Server* en el caso del *PC1*, de esta forma conseguiremos una instalación sin interfaz gráfica tal y como se buscaba (figura 6.24). Mientras que en el caso del *PC2* seleccionare-

mos la opción *Servidor con GUI*, para obtener una instalación con interfaz gráfica (figura 6.25).

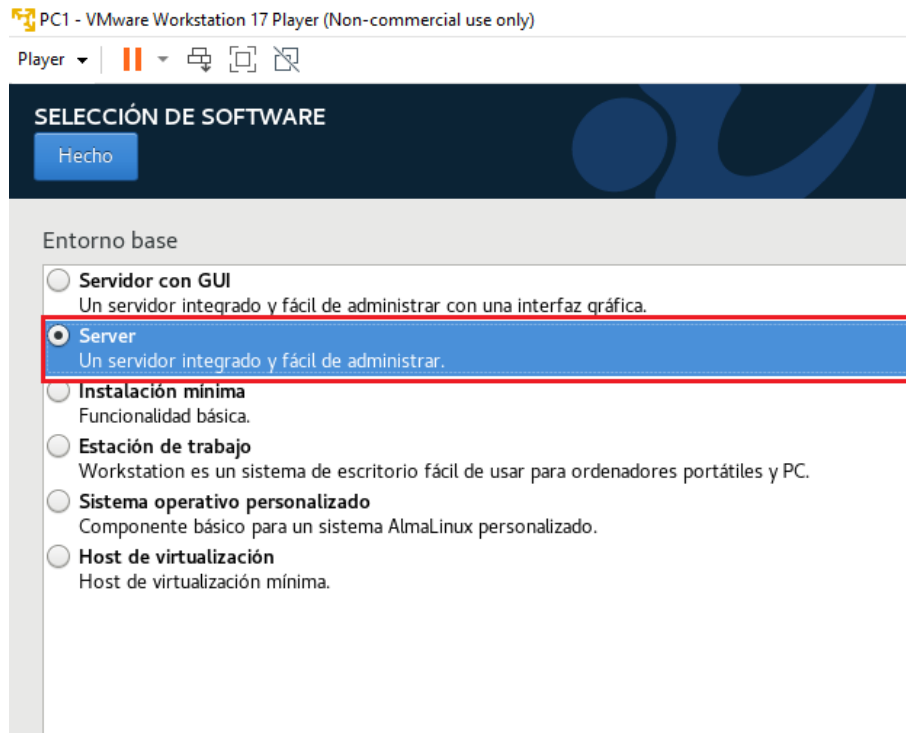


Figura 6.24: Configuración de la selección de software para la instalación del PC1

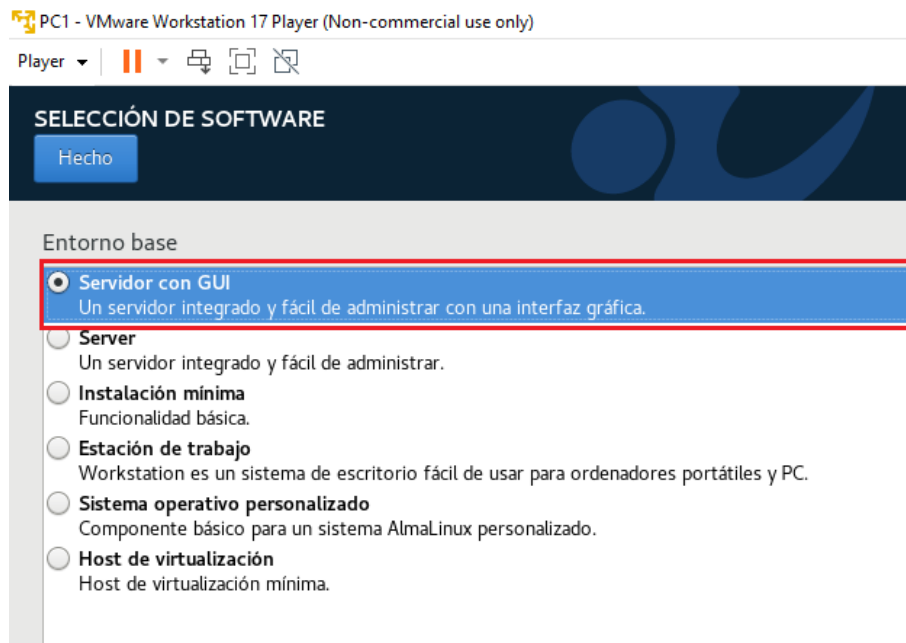


Figura 6.25: Configuración de la selección de software para la instalación del PC2

Dejando el resto de secciones por defecto, presionamos sobre comenzar la instalación y esperamos a que el proceso termine. Una vez nos aparezca completado, podemos aplicar un reinicio del sistema (figura 6.26). Tras el arranque, nos solicitará que aceptemos la licencia y podremos presionar *Finalizar configuración*, con

lo que completaremos la instalación (ver figura 6.27). En el primer inicio, el sistema nos solicitará la creación de un usuario; sin embargo, este no es relevante, ya que, como se ha mencionado anteriormente, se trabajará como root a lo largo de la solución.



Figura 6.26: Instalación completa de AlmaLinux

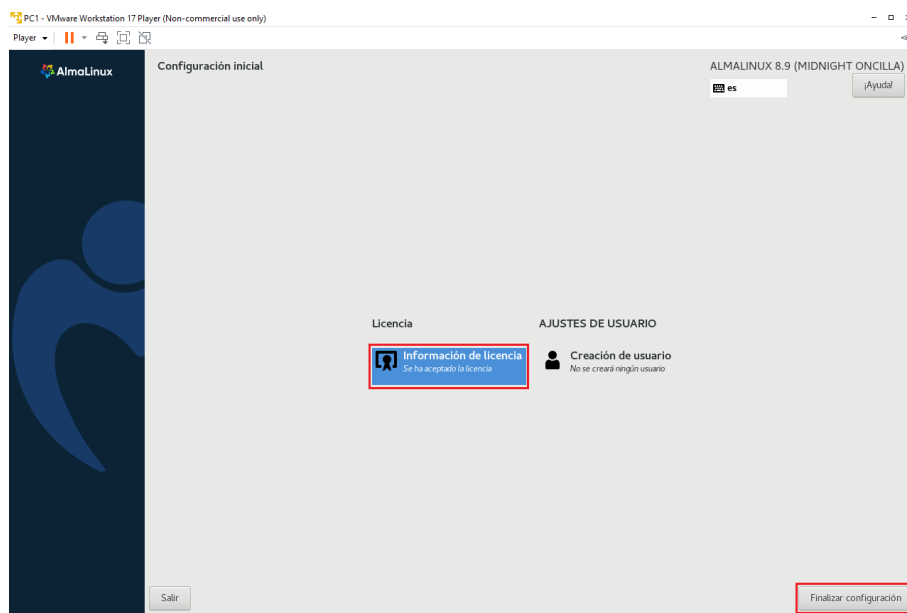


Figura 6.27: Configuración inicial de AlmaLinux

## 6.2 Configuraciones iniciales sobre los componentes de la solución

Antes de configurar las distintas conexiones VPN entre los cortafuegos, se realizarán las configuraciones de red básicas sobre cada uno de los componentes. En

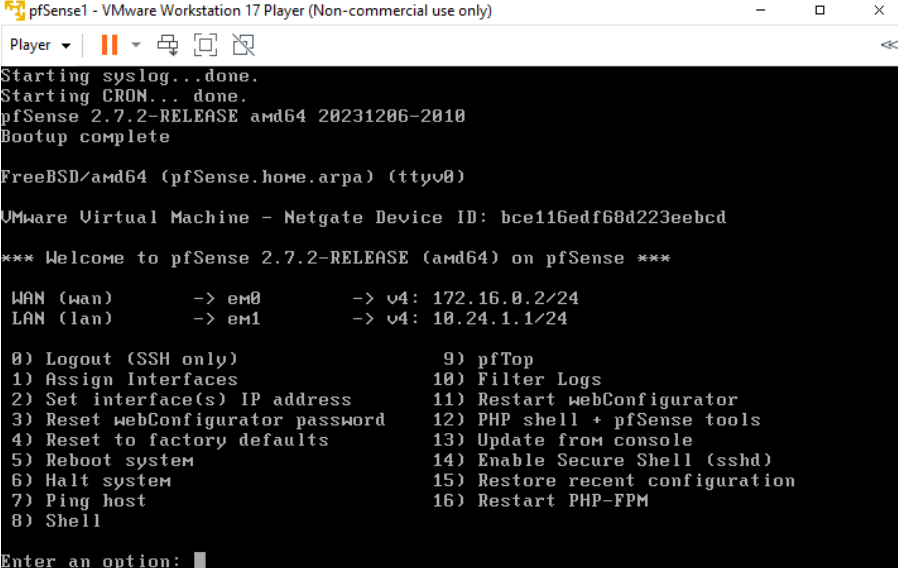


el caso del router MikroTik y las máquinas de usuario, estos ajustes completarán la configuración que se mantendrá a lo largo del desarrollo de la solución.

### 6.2.1. Configuraciones iniciales en los cortafuegos pfSense

Para que cada uno de los cortafuegos pueda establecer correctamente las conexiones con el resto de componentes de la solución, tendremos que configurar las distintas interfaces de los . Por una parte, la interfaz WAN (*em0*), se utiliza para conectar el dispositivo al Internet, en nuestro caso, conecta el cortafuegos con el router MikroTik, encargado de simular Internet. Por otra parte, la interfaz LAN (*em1*), se encarga de establecer la conexión con la red privada, en el caso de la solución propuesta conectará equipo con el correspondiente PC.

Ambas interfaces pueden configurarse, o bien utilizando la interfaz web que proporciona , o bien directamente desde el menú de configuración en la propia máquina virtual (ver figura 6.28). En este caso se ha escogido esta segunda opción, ya que estas primeras configuraciones son sencillas y permiten ilustrar esta alternativa. Esta opción facilita realizar algunas configuraciones básicas en caso de no poder disponer de ningún otro equipo conectado.



```
pfSense1 - VMware Workstation 17 Player (Non-commercial use only)
Player | [Pause] [Full Screen] [Close]
Starting syslog...done.
Starting CRON...done.
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)
VMware Virtual Machine - Netgate Device ID: bce116edf68d223eebcd

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4: 172.16.0.2/24
LAN (lan)      -> em1      -> v4: 10.24.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults    13) Update from console
5) Reboot system              14) Enable Secure Shell (ssh)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: |
```

Figura 6.28: Menú de configuración del pfSense1

Concretamente para configurar las interfaces, seleccionaremos la opción 2) *Set Interface(s) IP address* introduciendo el número 2 y presionando *enter*. Tras la seleccionar la opción, el sistema nos solicitará diferentes parámetros para configurar cada una de las interfaces, introduciremos cada uno de ellos y pulsaremos *enter* para avanzar al siguiente.

Respecto al cortafuegos *pfSense1*, comenzamos configurando su interfaz WAN, por lo que seleccionamos la opción 1, y configuramos de forma estática, es decir sin DHCP, la IPv4 como *172.16.0.2/24*, indicamos que el *default gateway* será *172.16.0.1* y no configuramos IPv6, ya que no será utilizada para las pruebas. En el caso de esta interfaz no activaremos el *DHCP server* y dejaremos *HTTPS* como protocolo para configuración vía web. La configuración paso por paso de la

interfaz se muestra en la figura 6.29. Después configuraremos la interfaz LAN, escogiendo la opción 2, configuraremos estáticamente la IPv4 como *10.24.1.1/24*, pero dejando en blanco el *gateway* y, al igual que en la interfaz WAN, no configuraremos IPv6. Para esta interfaz si que activaremos el *DHCP server* con el rango *10.24.1.50 - 10.24.1.254*, de manera que el cortafuegos se encargue de asignar las direcciones IP a los dispositivos de nuestra red privada. Del mismo modo que en la interfaz WAN dejaremos *HTTPS* como protocolo para el acceso vía web. En la figura 6.30 se puede observar, al completo, la configuración de esta interfaz.

```
Available interfaces:
1 - WAN (em0)
2 - LAN (em1)

Enter the number of the interface you wish to configure: 1
Configure IPv4 address WAN interface via DHCP? (y/n) n
Enter the new WAN IPv4 address. Press <ENTER> for none:
> 172.16.0.2

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new WAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 172.16.0.1

Should this gateway be set as the default gateway? (y/n) y
Configure IPv6 address WAN interface via DHCP6? (y/n) n
Enter the new WAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on WAN? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

Please wait while the changes are saved to WAN...
Reloading filter...
Reloading routing configuration...
DHCPD...

The IPv4 WAN address has been set to 172.16.0.2/24
Press <ENTER> to continue.█
```

Figura 6.29: Configuración de la interfaz WAN para el pfSense1

```
Available interfaces:
1 - WAN (em0 - static)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2

Configure IPv4 address LAN interface via DHCP? (y/n) n

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 10.24.1.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0    = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address LAN interface via DHCP6? (y/n) n

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 10.24.1.50
Enter the end address of the IPv4 client address range: 10.24.1.254
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

Please wait while the changes are saved to LAN...
Reloading filter...
Reloading routing configuration...
DHCPD...

The IPv4 LAN address has been set to 10.24.1.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
      https://10.24.1.1/

Press <ENTER> to continue.█
```

Figura 6.30: Configuración de la interfaz LAN para el pfSense1

Con lo que respecta a la configuración de las interfaces en el cortafuegos *pfSense2* el proceso es idéntico al realizado en su homónimo, por lo se comentarán solamente las diferencias. En cuanto a la interfaz WAN, únicamente difieren la dirección IPv4, que en este caso configuraremos como *192.168.254.2/24* y el *default gateway*, que modificaremos a *192.168.254.1*. Respecto a la interfaz LAN, las únicas diferencias son la dirección IPv4 que será *10.24.2.1/24* y el rango del servidor DHCP, que cambiaremos por *10.24.2.50 - 10.24.2.254*.

Una vez configuradas las interfaces en ambos cortafuegos se realizarán algunas configuraciones utilizando las interfaz web. Como se ha mencionado previamente, el *pfSense1* se configurará desde el PC anfitrión ya que la red VMnet2 se encuentra en modo *Host-Only*, mientras que el *pfSense2* se configurará desde el PC2.

En ambos casos, abrimos un navegador e introducimos la dirección IP de LAN de cada uno de los cortafuegos respectivamente. El buscador nos alertará de que la conexión no es privada, seleccionamos las opciones avanzadas y pulsamos en continuar (ver figura 6.31). Lo primero que encontramos es la página de inicio de sesión de , introducimos las credenciales por defecto, usuario *Admin* y contraseña *pfSense* (figura 6.32).

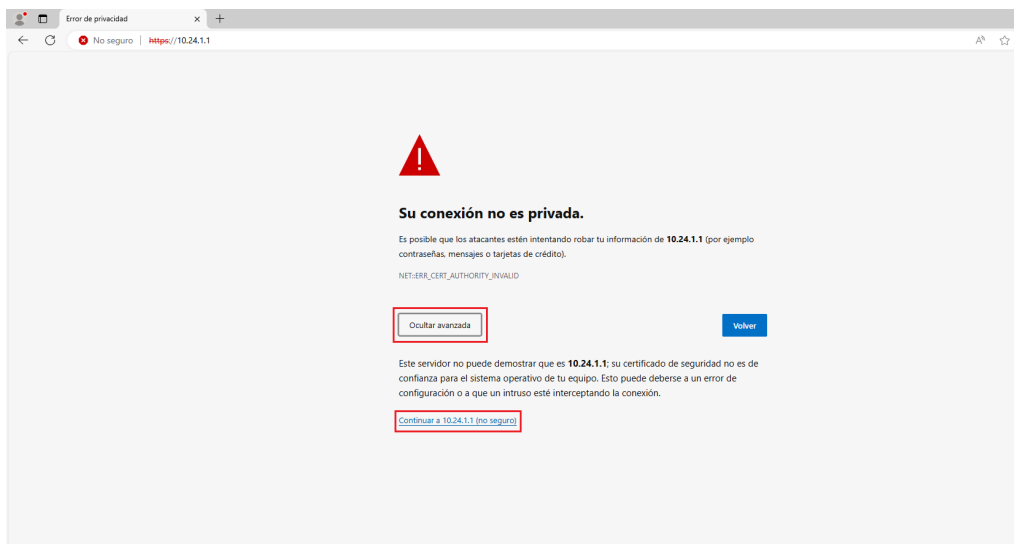


Figura 6.31: Error de privacidad al acceder al pfSense vía web

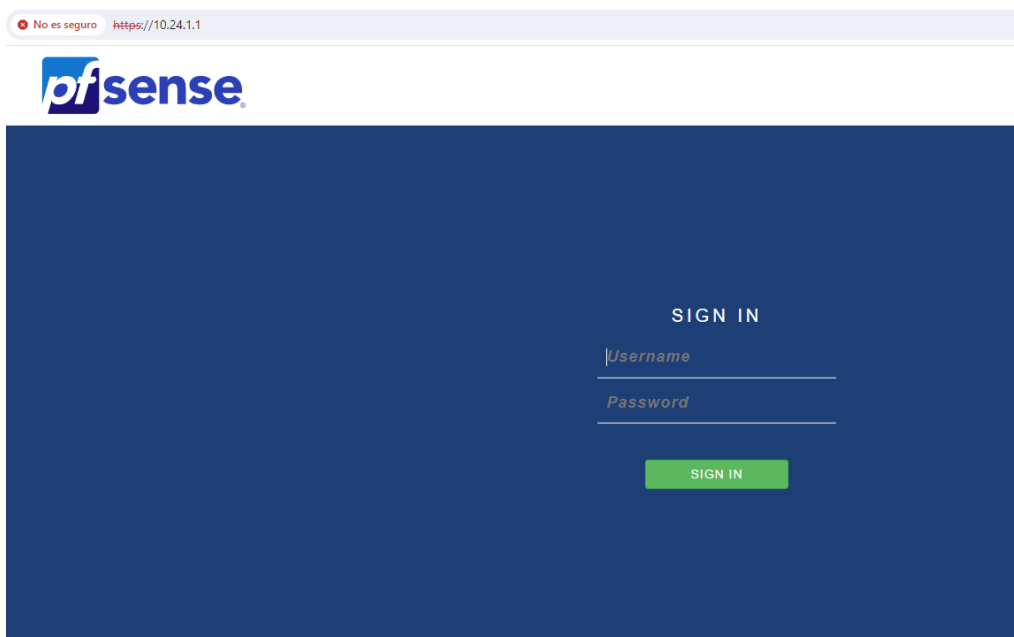
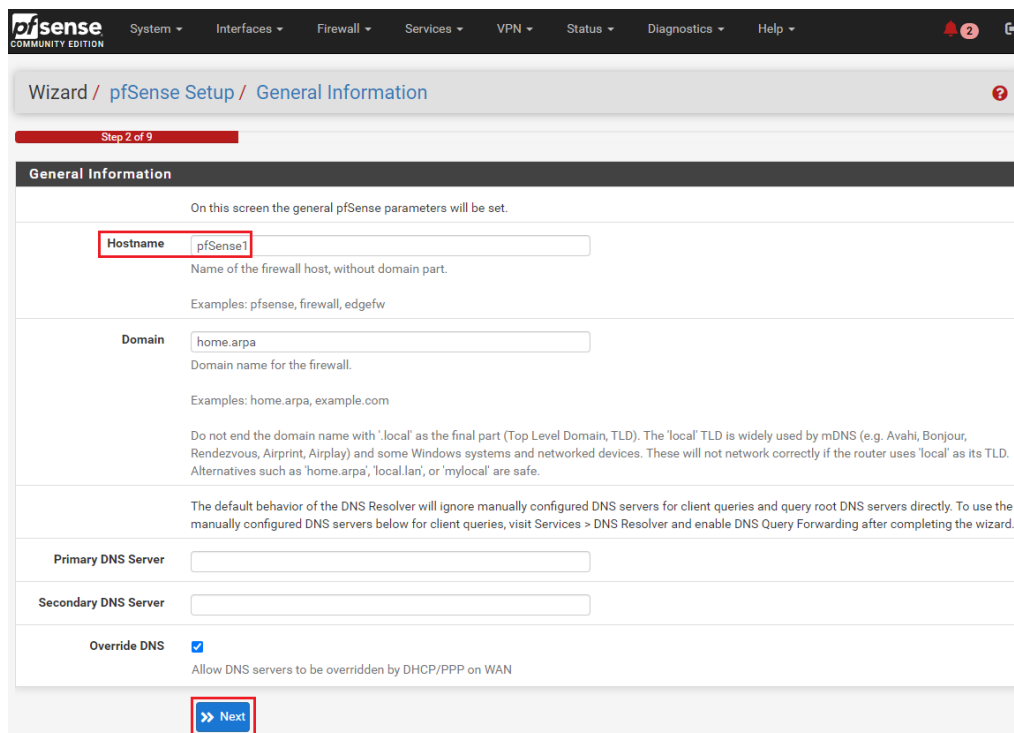


Figura 6.32: Inicio de sesión en pfSense vía web

Una vez nos conectamos, al ser la primera conexión, encontramos un *wizard* que nos guiará para configurar los parámetros esenciales del cortafuegos. En nuestro caso, modificaremos, en el paso dos, el nombre del equipo a *pfSense1* o *pfSense2*, respectivamente (figura 6.33). En el siguiente paso, modificamos la zona horaria, en nuestro caso, a *Europe/Madrid*. Los siguientes dos pasos podemos saltarlos sin realizar ningún cambio, ya que se trata de las configuraciones de las interfaces de red, que ya hemos realizado previamente en la configuración inicial de la máquina. En el sexto paso escogemos una nueva contraseña para el usuario *Admin* y en el séptimo y último paso, presionamos *Reload* para reiniciar el cortafuegos y aplicar los cambios.



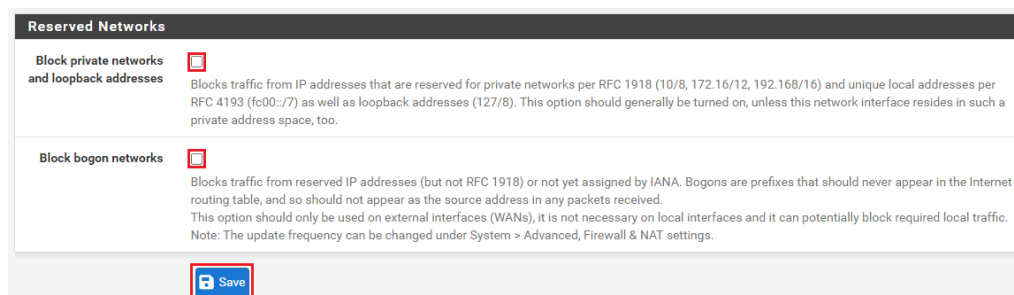
The screenshot shows the pfSense Setup Wizard, Step 2 of 9, titled "General Information". The interface includes a navigation menu at the top with options like System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main content area contains the following fields and options:

- Hostname:** A text input field containing "pfSense1".
- Domain:** A text input field containing "home.arpa".
- Primary DNS Server:** An empty text input field.
- Secondary DNS Server:** An empty text input field.
- Override DNS:** A checked checkbox with the label "Allow DNS servers to be overridden by DHCP/PPP on WAN".

At the bottom of the form, there is a blue button labeled "Next" with a right-pointing arrow.

Figura 6.33: Wizard de configuración inicial de pfSense

Adicionalmente, vamos a realizar unas configuraciones que nos permitan realizar *ping* entre los cortafuegos pfSense a través de nuestra simulación de Internet. Esta no es una práctica recomendada en un contexto real, sin embargo, nos ayudará a comprobar que los se están pudiendo comunicar correctamente a través del router MikroTik. Para permitir esto en cada uno de los cortafuegos, accedemos a la sección de interfaces y seleccionamos la WAN, bajamos al final de la configuración y en el apartado *Reserved Networks*, desactivamos ambas opciones y presionamos en *Save* como se muestra en la figura 6.34. Esto es necesario ya que en nuestra simulación las interfaces WAN, en vez de tener direcciones IP públicas, tiene direcciones privadas, el tráfico de las cuales está bloqueado por defecto para dicha interfaz. Tras guardar, el cortafuegos nos avisará de que para que los cambios sean efectivos tenemos que aplicar los cambios, para esto presionamos en *Apply Changes* (ver figura 6.35). Esto será necesario tras cada una de las configuraciones que realicemos sobre .

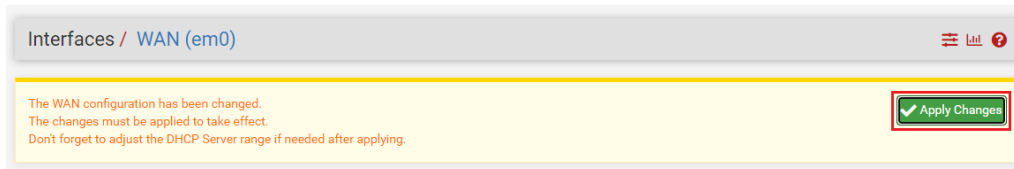


The screenshot shows the "Reserved Networks" configuration page in pfSense. It contains two sections, each with a checkbox and a description:

- Block private networks and loopback addresses:** The checkbox is checked. The description states: "Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too."
- Block bogon networks:** The checkbox is checked. The description states: "Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received. This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic. Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings."

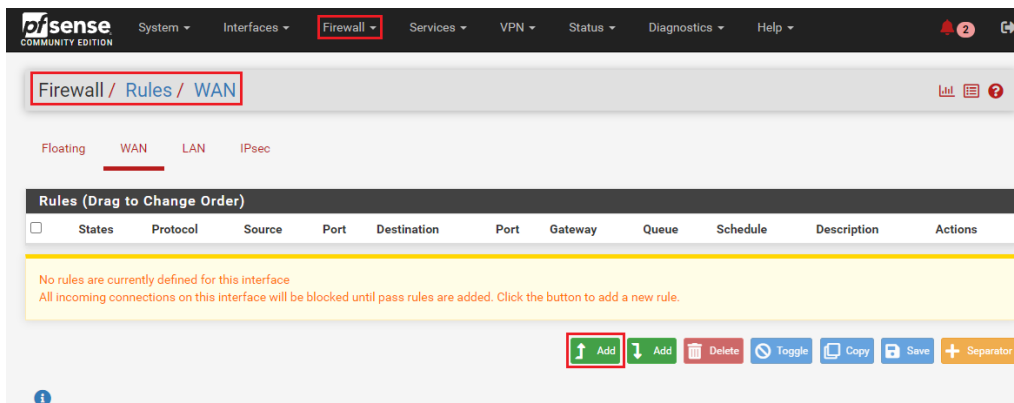
At the bottom of the page, there is a blue button labeled "Save" with a floppy disk icon.

Figura 6.34: Configuración de *Reserved Networks* en la interfaz WAN de pfSense

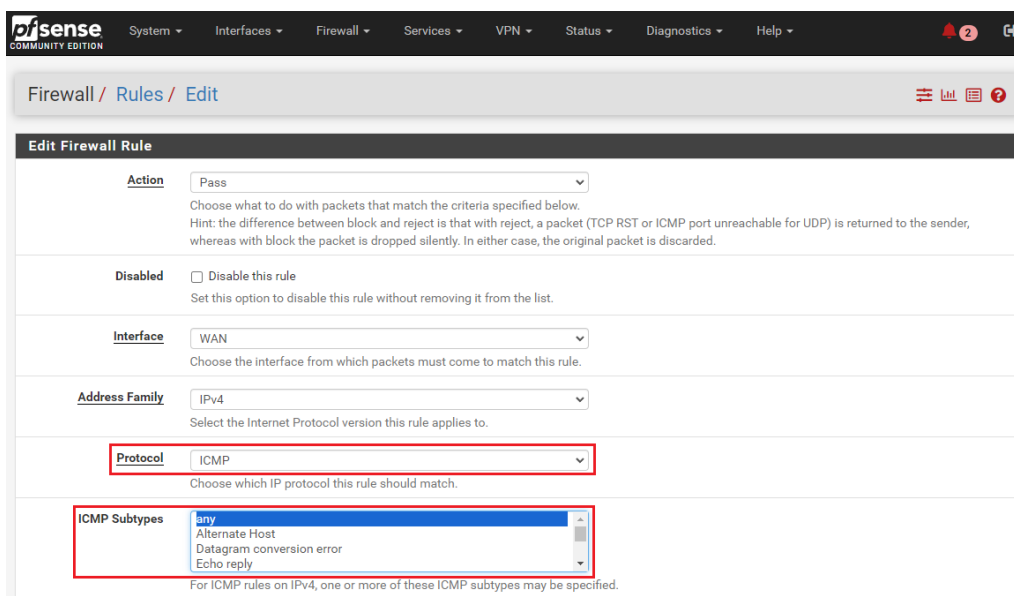


**Figura 6.35:** Aplicar los cambios tras una configuración en pfSense

Además, necesitamos añadir una regla que permita los *ping* en la interfaz, ya que por defecto están bloqueados. Para esto nos dirigimos a la sección *Firewall*, seleccionamos *Rules* y en el apartado WAN presionamos el botón *Add* para crear la regla, tal y como se muestra en la figura 6.36. Respecto a la configuración de la regla, modificamos el protocolo a *ICMP*, seleccionamos *any* en el apartado *ICMP Subtypes* y, dejando todo el resto de apartados por defecto, pulsamos en *Save* y aplicamos los cambios, tal y como se ha mencionado previamente 6.37.



**Figura 6.36:** Añadir nueva regla de firewall para la interfaz WAN en pfSense



**Figura 6.37:** Configuración de una regla que permite todo el tráfico ICMP en pfSense

Por último, se realizará un *backup* o copia de seguridad de la configuración realizada hasta el momento de cada uno de los cortafuegos. Como ya se ha men-

cionado, esto nos permitirá volver a este estado inicial de los cortafuegos tras la configuración y pruebas de cada uno de los túneles VPN, pudiendo configurar el siguiente túnel desde el mismo punto de partida. Para realizar el *backup*, en cada uno de los cortafuegos, accedemos a *Diagnostics* y concretamente a *Backup & restore*. En el apartado de *Backup Configuration*, seleccionamos *all* como *Backup area*, para que nos guarde la configuración al completo y, dejando el resto de opciones por defecto, presionamos en *Download configuration as XML* (ver figura 6.38). Esto nos descargará un archivo que guardaremos para usarlo posteriormente.

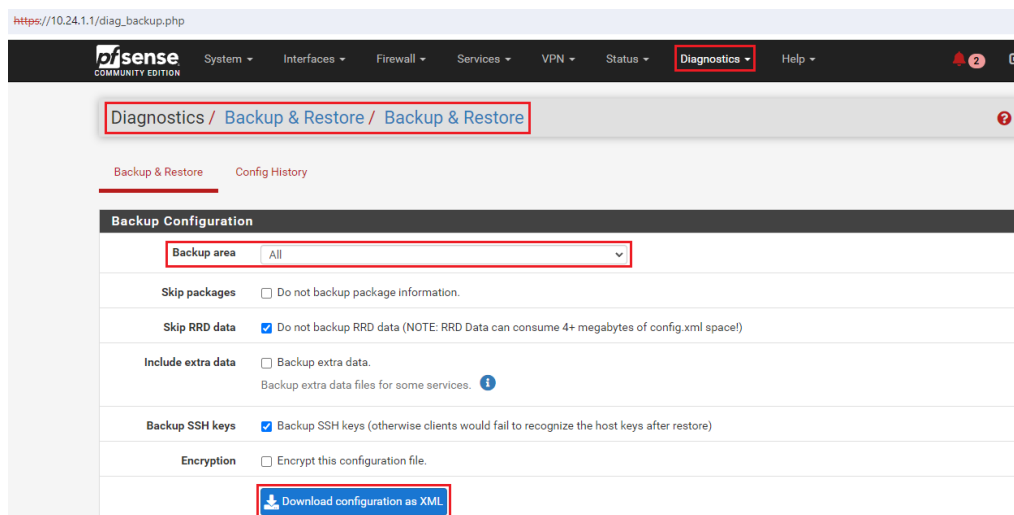


Figura 6.38: Crear un backup de la configuración completa en pfSense

### 6.2.2. Configuraciones iniciales en el router MikroTik

Se realizarán las configuraciones necesarias para conseguir que el router MikroTik sea capaz de enrutar el tráfico entre cada una de las redes a las que está conectado. Para conseguirlo se utilizará la funcionalidad *Bridge*, como ya se mencionó anteriormente. Esta función de MikroTik, tal como explica en su guía oficial [32], se utiliza para crear puentes MAC entre las interfaces que pertenezcan a un *bridge*, es decir, que establece uniones a nivel dos entre las interfaces. Estos puentes permiten la interconexión de distintas redes LAN como si estuvieran conectadas a una única LAN. Esto se realiza de forma transparente utilizando el protocolo de túnel *EoIP* (*Ethernet over IP*).

Para acceder al router MikroTik, utilizaremos la herramienta *WinBox*, tal y como se realizó previamente para activar la licencia (ver figura 6.15). Una vez dentro, comenzamos accediendo a la ventana de *DHCP Client* dentro de la sección *IP*, pulsamos el botón + y creamos un nuevo cliente DHCP seleccionando la interfaz *ether5*, correspondiente al adaptador configurado en modo *Bridge* (ver figura 6.39). De esta forma, la interfaz obtendrá una dirección IP asignada por el router NAT real y se crearán dinámicamente las rutas necesarias para salir a Internet a través de esta interfaz (figura 6.43).

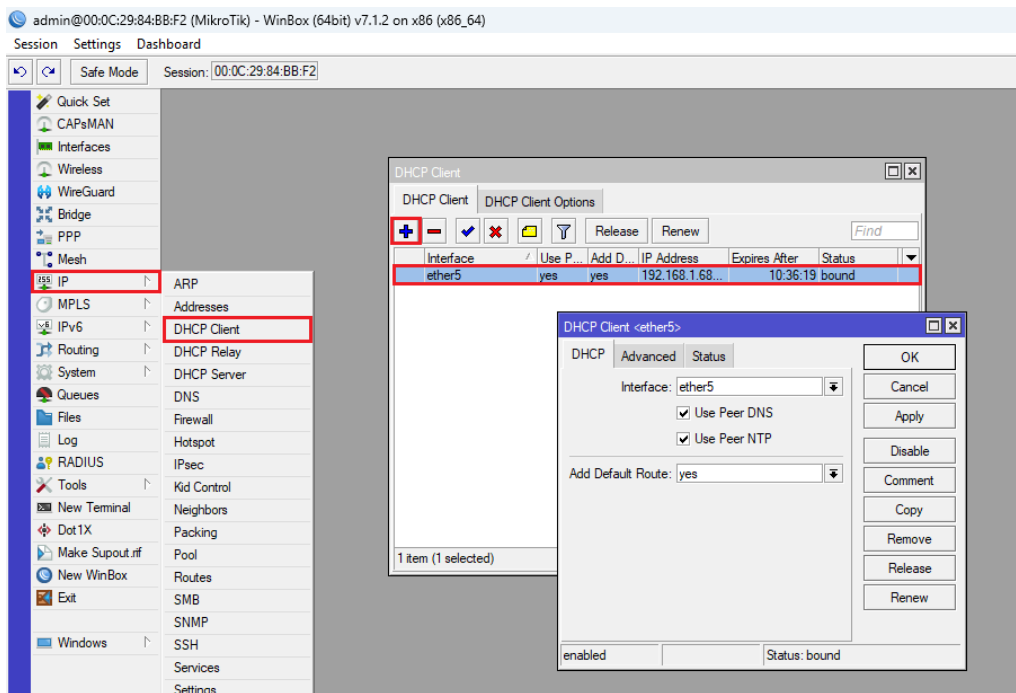


Figura 6.39: Configuración del cliente DHCP en el router MikroTik

A continuación, asignamos direcciones IP a las otras dos interfaces correspondientes a las conexiones con los cortafuegos. Para ello, también dentro de la sección *IP*, seleccionamos *Addresses*, y utilizando el botón +, creamos dos nuevas direcciones, una con la dirección *172.16.0.1/24* y la red *172.16.0.0* que asignaremos a la interfaz *ether4*, y otra, con la dirección *192.168.254.1/24* y la red *192.168.254.0* que asignaremos a la interfaz *ether3* (ver figura 6.40).

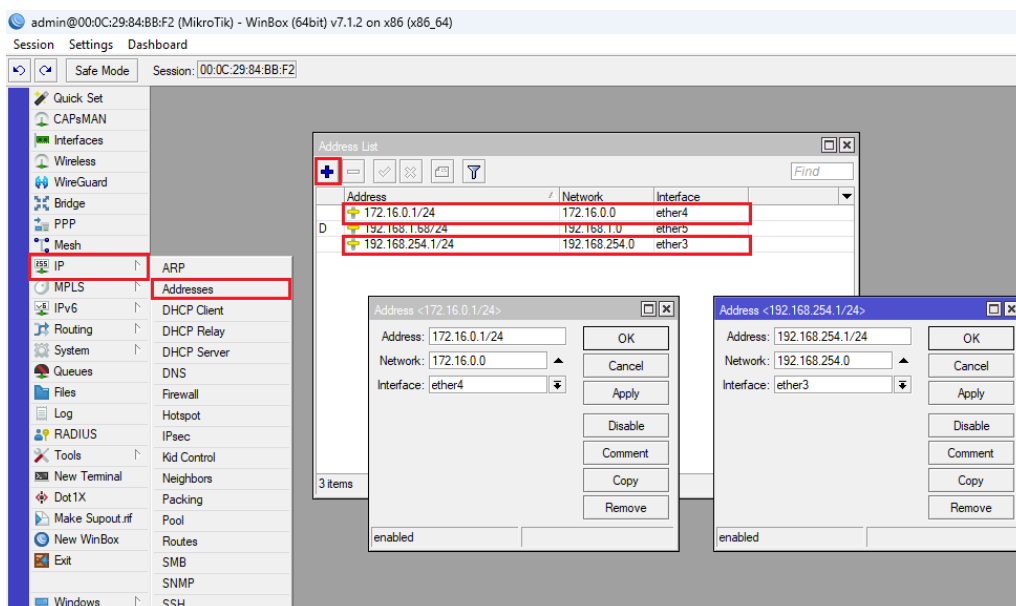


Figura 6.40: Configuración de direcciones IP en el router MikroTik

Por último, crearemos el *Bridge* que se ha mencionado previamente, para conectar las redes de los cortafuegos. Nos dirigimos a la sección *Bridge*, creamos



un nuevo puente utilizando el botón +, únicamente configurándole un nombre y dejando el resto por defecto (figura 6.41). Una vez hemos creado el *Bridge*, accedemos a la pestaña *Ports* dentro de la misma ventana *Bridge* y utilizando de nuevo el + añadimos ambas interfaces al puente que hemos creado (figura 6.42).

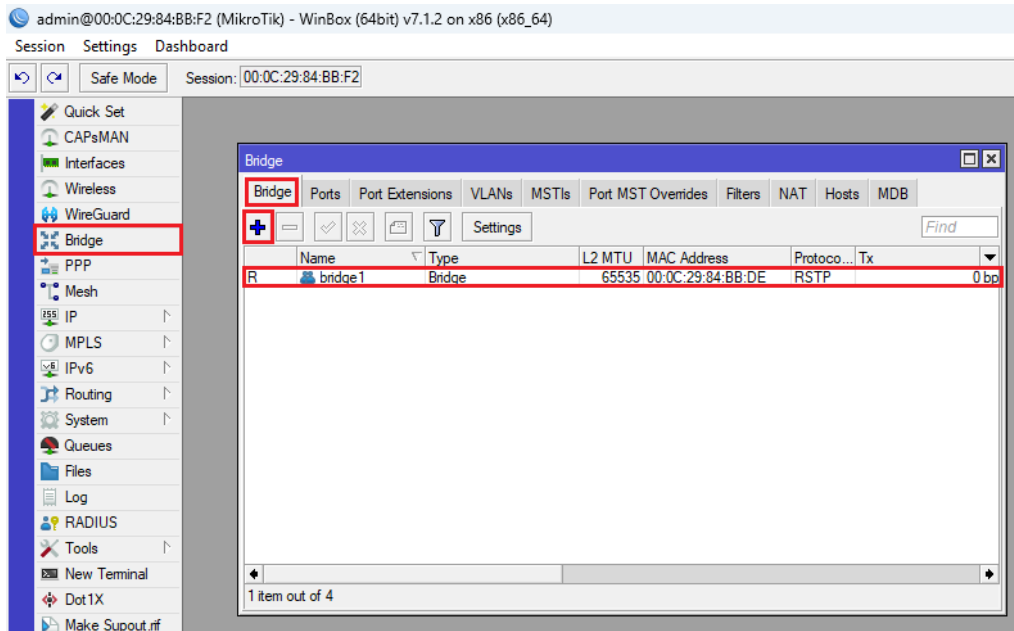


Figura 6.41: Configuración del Bridge en el router MikroTik

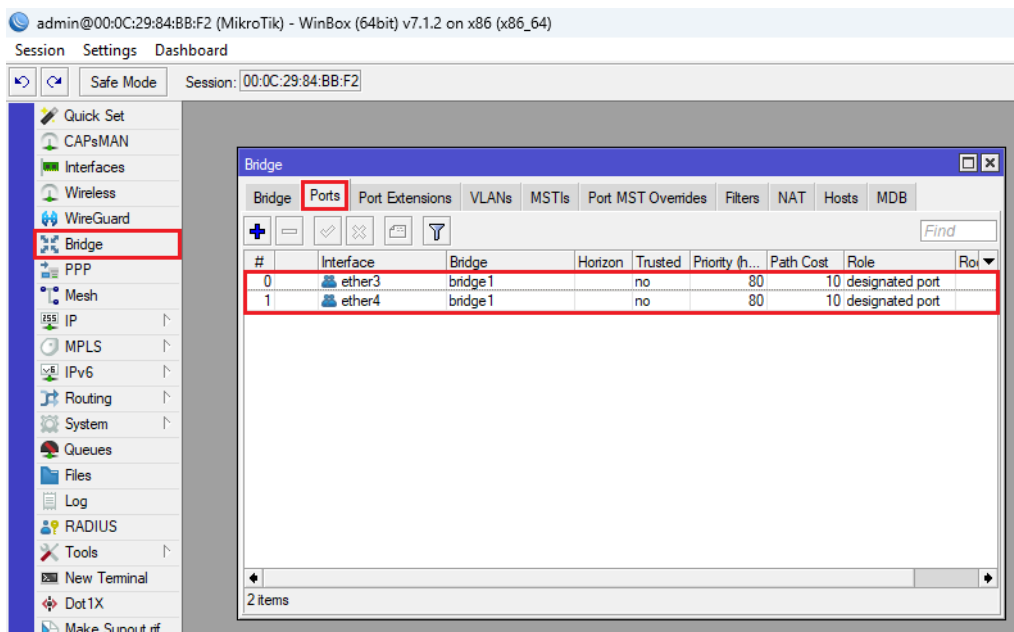


Figura 6.42: Configuración de los puertos en el Bridge del router MikroTik

Al igual que previamente con la interfaz *ether5*, se crearán de forma dinámica las rutas necesarias para dirigir el tráfico a las redes de cada uno de los pfSense a través del *Bridge*. Esto se puede comprobar en el apartado *Routes* dentro de la sección *IP*, como se muestra en la figura 6.43.

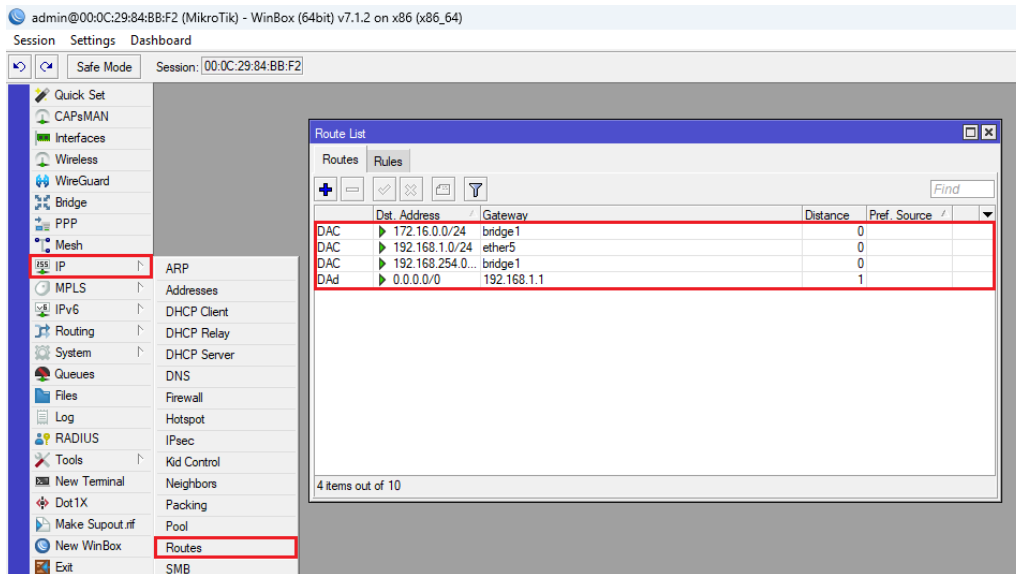


Figura 6.43: Comprobación de las rutas creadas dinámicamente en el router MikroTik

### 6.2.3. Configuraciones iniciales en las máquinas AlmaLinux

En el caso de los PCs, se realizarán únicamente configuraciones a nivel de red. Ambas máquinas cuentan con una sola interfaz, en este caso, *ens37*. Esta se configurará en ambos casos como DHCP, es decir, que su dirección IP será asignada de forma dinámica por el cortafuegos al se encuentran conectadas cada una de las máquinas.

Para el *PC1*, accedemos a la ruta */etc/sysconfig/network-scripts/* y editamos utilizando *vi* el archivo *ifcfg-ens37*, correspondiente a la configuración de la interfaz *ens37* (ver figura 6.44).

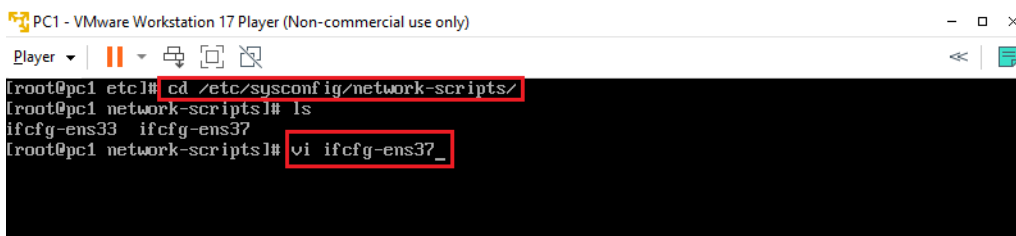
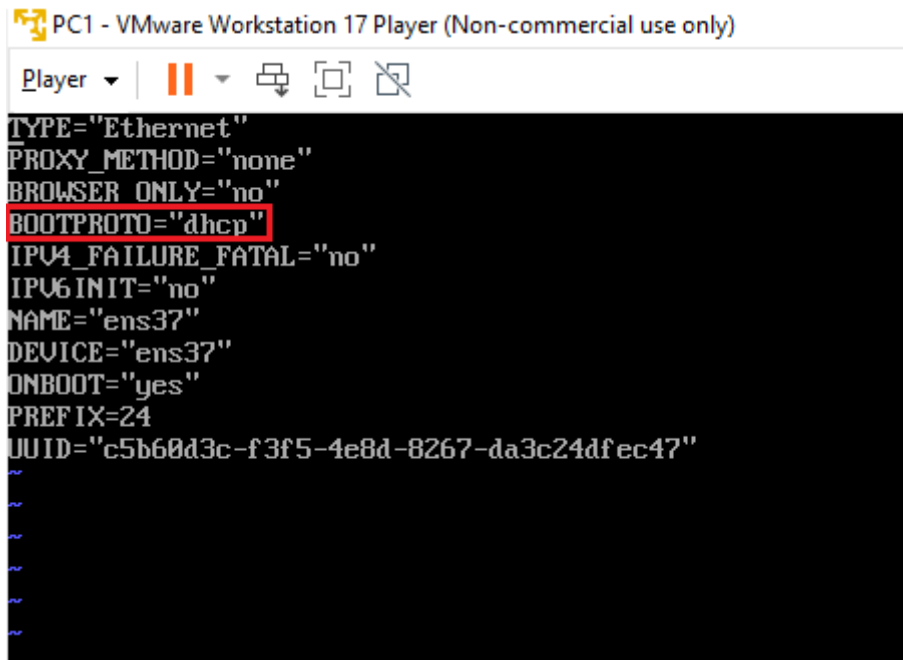


Figura 6.44: Acceso a la ruta y modificación del archivo *ifcfg-ens37*

Dentro de este archivo, modificamos el parámetro *BOOTPROTO* a *"dhcp"*, de forma que el archivo quedará como se muestra en la figura 6.45. Después, guardamos los cambios.



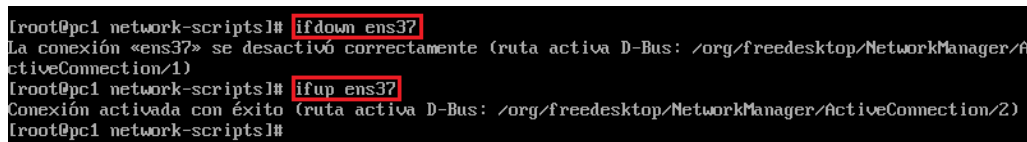
```

PC1 - VMware Workstation 17 Player (Non-commercial use only)
Player | || | |
TYPE="Ethernet"
PROXY_METHOD="none"
BROWSER_ONLY="no"
BOOTPROTO="dhcp"
IPV4_FAILURE_FATAL="no"
IPV6INIT="no"
NAME="ens37"
DEVICE="ens37"
ONBOOT="yes"
PREFIX=24
UUID="c5b60d3c-f3f5-4e8d-8267-da3c24dfec47"

```

Figura 6.45: Contenido del archivo *ifcfg-ens37* para el PC1

Por último, reiniciamos la interfaz para que se apliquen los cambios, para esto apagamos la interfaz con el comando *ifdown ens37* y la volvemos a encender con *ifup ens37* (figura 6.46).



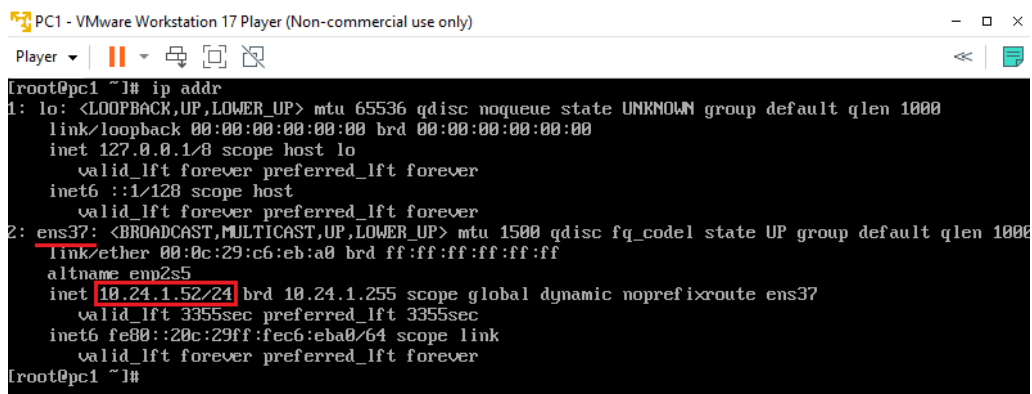
```

[root@pc1 network-scripts]# ifdown ens37
La conexión «ens37» se desactivó correctamente (ruta activa D-Bus: /org/freedesktop/NetworkManager/ActiveConnection/1)
[root@pc1 network-scripts]# ifup ens37
Conexión activada con éxito (ruta activa D-Bus: /org/freedesktop/NetworkManager/ActiveConnection/2)
[root@pc1 network-scripts]#

```

Figura 6.46: Apagado y encendido de la interfaz *ens37* en el PC1

Podemos comprobar que la interfaz está configurada correctamente ejecutando la orden *ip addr* y consultado que el cortafuegos ha asignado correctamente una dirección IP a la interfaz, perteneciente al rango configurado anteriormente (ver figura 6.47).



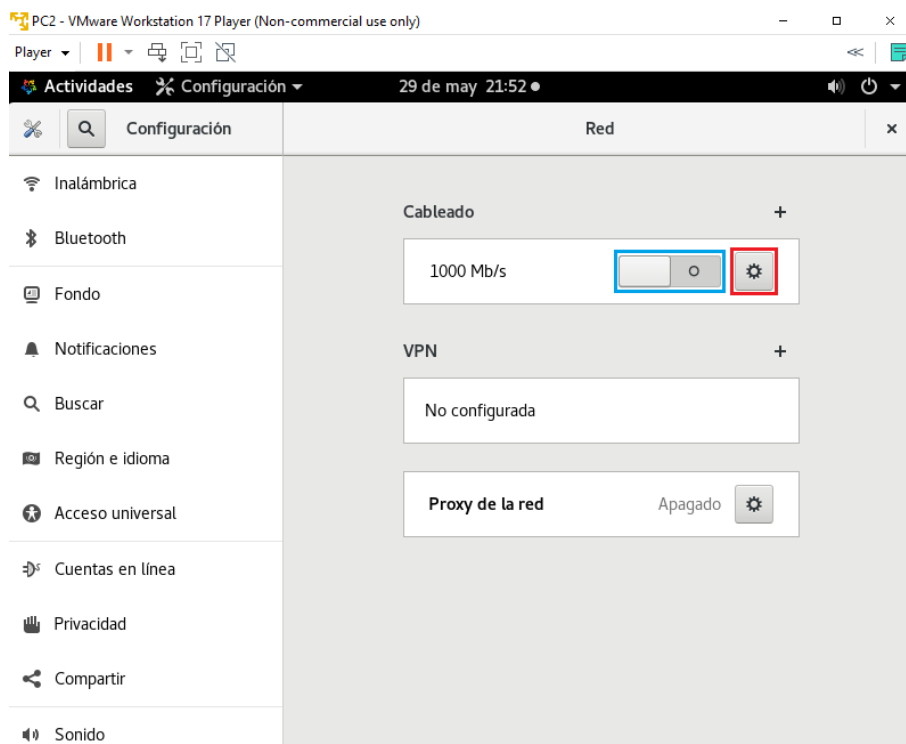
```

PC1 - VMware Workstation 17 Player (Non-commercial use only)
Player | || | |
[root@pc1 ~]# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens37: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:c6:eb:a0 brd ff:ff:ff:ff:ff:ff
    altname emp2s5
    inet 10.24.1.52/24 brd 10.24.1.255 scope global dynamic noprefixroute ens37
        valid_lft 3355sec preferred_lft 3355sec
    inet6 fe80::20c:29ff:fec6:eba0/64 scope link
        valid_lft forever preferred_lft forever
[root@pc1 ~]#

```

Figura 6.47: Configuración de red del PC1

La configuración de la interfaz en el caso del *PC2*, se puede realizar de una forma más sencilla, ya que disponemos de interfaz gráfica. En la esquina superior derecha de la pantalla encontramos un icono desplegable al lado del botón de apagado, presionando se despliegan diversas opciones, seleccionamos *Cableado apagada* y accedemos a *Configuración de red cableada*. En el menú seleccionamos el símbolo de configuración (marcado en rojo en la figura 6.48) en el apartado de cableado, nos desplazamos a la sección *IPv4*, marcamos *Automático (DHCP)* y presionamos *Aplicar* (ver figura 6.49).



**Figura 6.48:** Menú de configuración de red cableada en el PC2

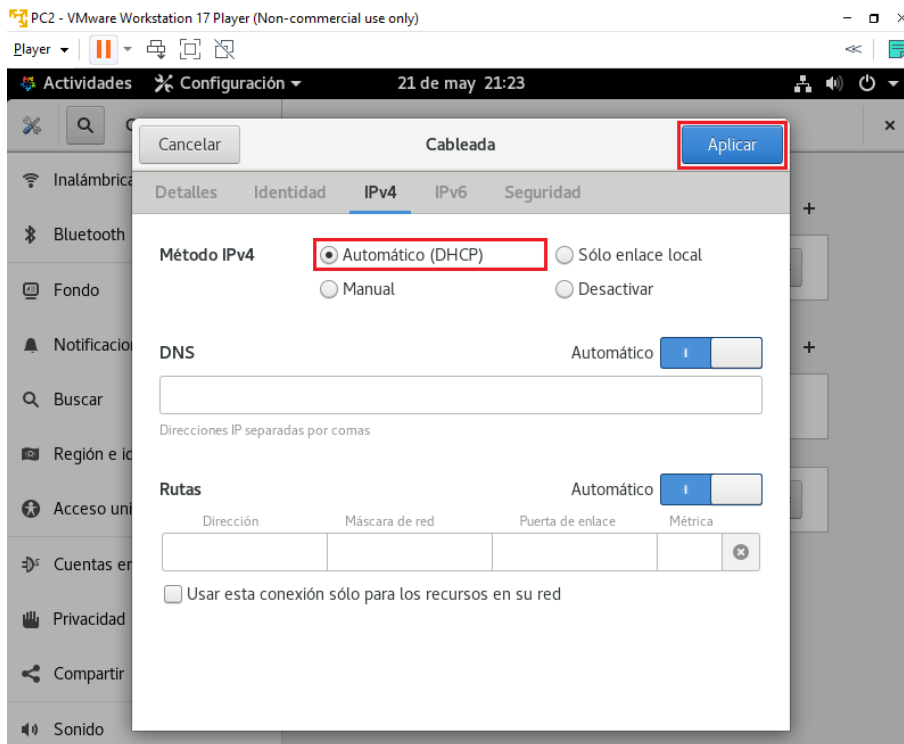


Figura 6.49: Configuración de red cableada en el PC2

Tras realizar el cambio, podemos apagar y encender la interfaz utilizando el interruptor (marcado en azul en la figura 6.48). Para comprobar que la configuración se ha aplicado adecuadamente, podemos acceder de nuevo a la configuración de la interfaz y en la sección *Detalles*, verificamos que la *Dirección IPv4* pertenezca al rango DHCP configurado en el *pfSense2* (figura 6.50).

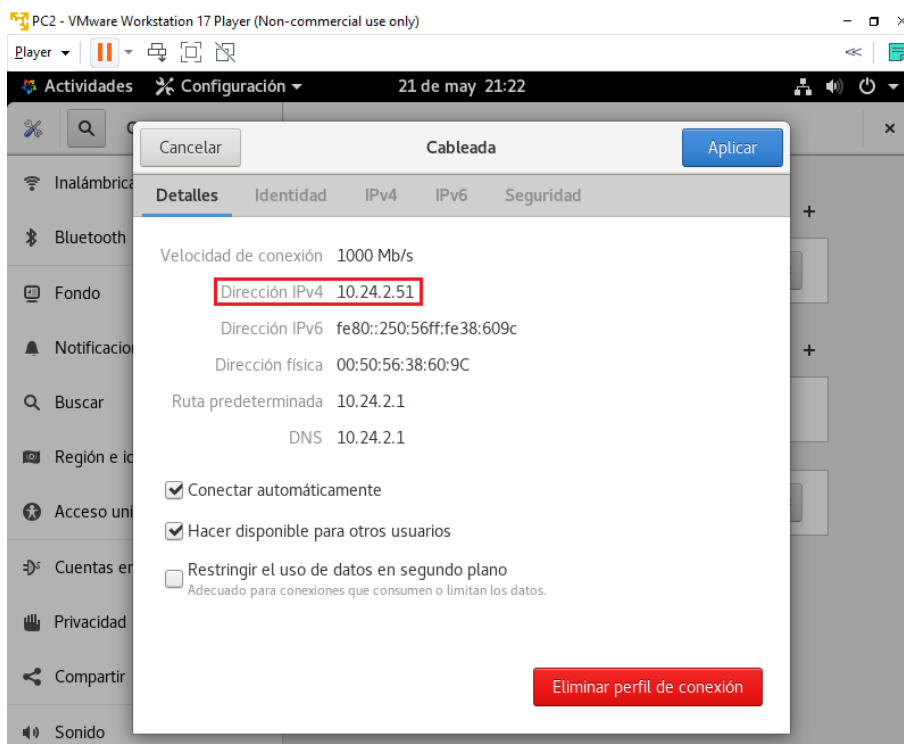


Figura 6.50: Detalles de configuración de red en el PC2

## 6.3 Configuración de VPN Site-to-Site con IPsec

La configuración de los distintos túneles VPN se realizará utilizando la interfaz web de ambos cortafuegos, de igual forma que se realizaron las últimas configuraciones iniciales anteriormente. Para llevar a cabo la creación del túnel IPsec se seguirá el artículo de la guía oficial de sobre la creación de una VPN de tipo site-to-site IPsec con clave precompartida [40].

Para crear el túnel tendremos que configurar cada uno de los dos extremos, comenzaremos configurando el *pfSense1*. Primero, accedemos a la sección VPN y seleccionamos *IPsec*, creamos una nueva fase 1 de túnel en el apartado de *Tunnels* presionando en *Add P1* (ver figura 6.51).

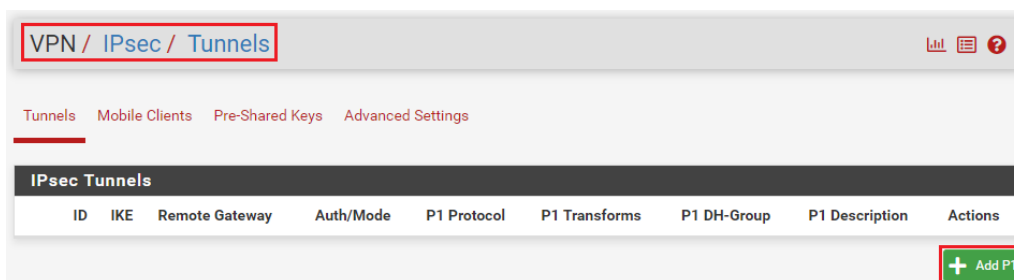


Figura 6.51: Añadir una fase 1 de IPsec en pfSense1

A continuación, vamos a rellenar los campos necesarios. En cuanto a la descripción, introduciremos un nombre para el túnel, en nuestro caso *Túnel a pfSense2*. Respecto a la configuración del protocolo IKE utilizaremos *IKEv2* ya que es recomendable siempre que sea compatible con ambos extremos, debido a su mayor nivel de seguridad. Dejamos el protocolo de Internet y la interfaz por defecto, e introducimos como *Remote Gateway* la dirección IP de WAN del otro extremo, en nuestro caso es *192.168.254.2* que se trata de una IP privada ya que es una simulación, sin embargo, en un caso real esta dirección será pública (ver figura 6.52).

VPN / IPsec / Tunnels / Edit Phase 1

Tunnels Mobile Clients Pre-Shared Keys Advanced Settings

### General Information

**Description** Túnel a pfSense2  
A description may be entered here for administrative reference (not parsed).

**Disabled**  Set this option to disable this phase1 without removing it from the list.

**IKE ID** 1

### IKE Endpoint Configuration

**Key Exchange version** IKEv2  
Select the Internet Key Exchange protocol version to be used. Auto uses IKEv2 when initiator, and accepts either IKEv1 or IKEv2 as responder.

**Internet Protocol** IPv4  
Select the Internet Protocol family.

**Interface** WAN  
Select the interface for the local endpoint of this phase1 entry.

**Remote Gateway** 192.168.254.2  
Enter the public IP address or host name of the remote gateway. ⓘ

Figura 6.52: Información general y configuración de IKE de la fase 1 de IPsec en pfSense1

Después, avanzamos a la configuración de la fase 1 y dejamos las opciones seleccionadas por defecto debido a que utilizaremos una clave precompartida. En cuanto a la elección de dicha clave, es recomendable utilizar la función *Generate new Pre-Shared Key* que nos ofrece el propio cortafuegos para generarla. Es muy importante que nos guardemos esta clave para configurarla de igual manera en el otro extremo. Para los algoritmos de cifrado utilizaremos la combinación más segura, que como se ha comentado en apartados anteriores de este trabajo, es *AES* con una clave de 256 bits, *SHA256* para el hash y el grupo de *DH 14* (figura 6.53). En lo que respecta al apartado *Expiration and Replacement* dejaremos todos los tiempos configurados por defecto.

The screenshot shows two sections of the pfSense configuration interface:

- Phase 1 Proposal (Authentication):**
  - Authentication Method:** A dropdown menu set to "Mutual PSK", which is highlighted with a red box.
  - My identifier:** A dropdown menu set to "My IP address".
  - Peer identifier:** A dropdown menu set to "Peer IP address".
  - Pre-Shared Key:** A text input field containing a long alphanumeric string. Below it is a red button labeled "Generate new Pre-Shared Key".
- Phase 1 Proposal (Encryption Algorithm):**
  - Encryption Algorithm:** A dropdown menu set to "AES", highlighted with a red box.
  - Key length:** A dropdown menu set to "256 bits".
  - Hash:** A dropdown menu set to "SHA256".
  - DH Group:** A dropdown menu set to "14 (2048)".
  - A red box highlights the "Encryption Algorithm", "Key length", "Hash", and "DH Group" dropdowns.
  - A "Delete" button is visible to the right.
  - A note below states: "Note: SHA1 and DH groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided."
  - An "Add Algorithm" button with a plus sign is at the bottom.

Figura 6.53: Configuración de la fase 1 de IPsec en pfSense1

Por último, respecto a las opciones avanzadas únicamente modificamos la *Child SA Close Action* a *Restart/Reconnect* para que en caso de que el túnel se desconectase, volviese automáticamente a conectarse (figura 6.54). Dejando el resto de opciones por defecto, guardamos y aplicamos los cambios.

The screenshot shows the "Advanced Options" section of the pfSense configuration interface:

- Child SA Start Action:** A dropdown menu set to "Default".
- Child SA Close Action:** A dropdown menu set to "Restart/Reconnect", which is highlighted with a red box.

Figura 6.54: Opciones avanzadas de la fase 1 de IPsec en pfSense1

Una vez configurada la fase 1, pasaremos a configurar la fase 2, para ello volvemos a la sección *Tunnels*, seleccionamos *Show Phase 2 Entries (0)* y creamos una nueva fase 2 presionando en *Add P2* (ver figura 6.55).



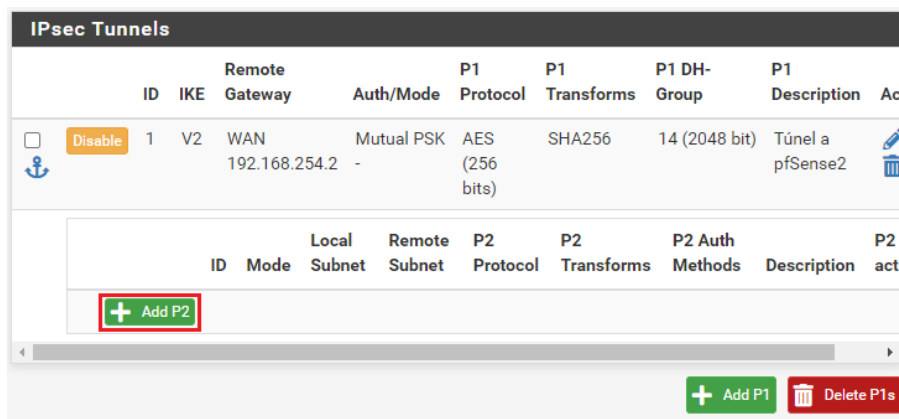


Figura 6.55: Añadir una fase 2 de IPsec en pfSense1

Primero introducimos una descripción, en nuestro caso *Túnel a pfSense2*, la misma que para la fase 1 y dejamos el modo en *Tunnel IPv4*. Respecto a la configuración de las redes, la red local es la red de este extremo que vamos a pasar por el túnel y la red remota es la red del otro extremo a la que accederemos por el túnel. En este caso, la red local podemos dejarla en *LAN subnet* que incluye nuestra red LAN o introducir manualmente la red *10.24.1.0/24*, en la red remota introducimos la red local del otro extremo, es decir, *10.24.2.0/24* y en el *NAT/BINAT translation* seleccionamos *None* (ver figura 6.56).

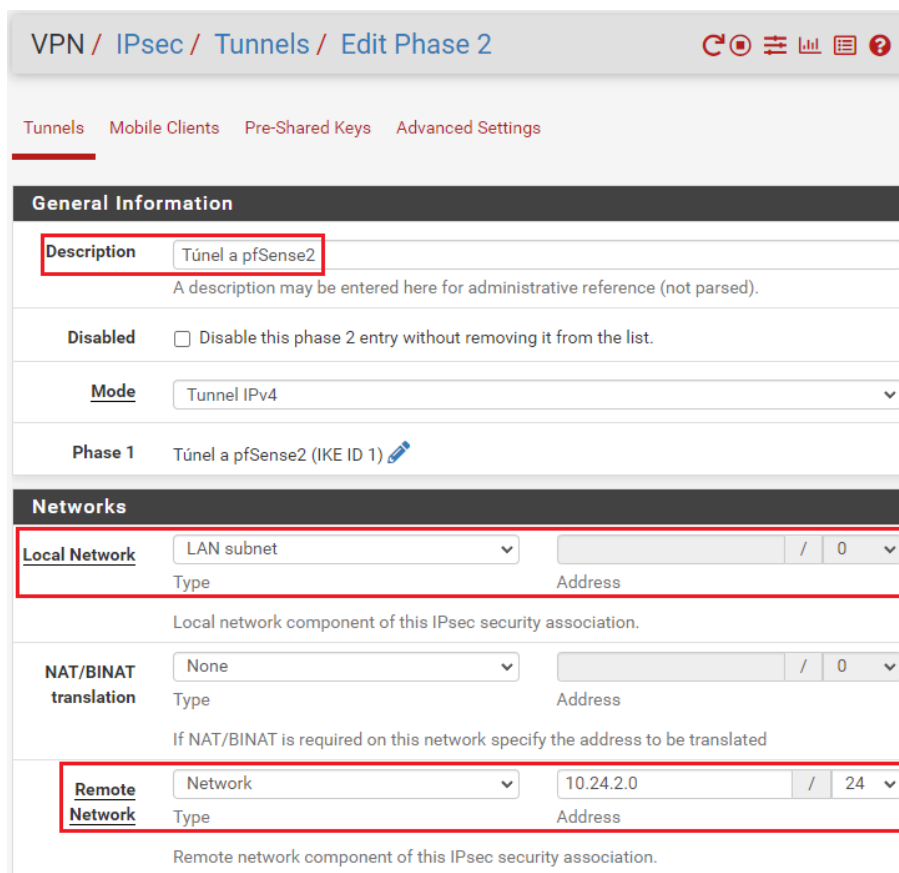


Figura 6.56: Información general y configuración de redes en la fase 2 de IPsec en pfSense1

Como configuración para la fase 2, siguiendo con buenas prácticas utilizaremos de nuevo la combinación más segura. Por lo que configuramos el protocolo *ESP*, *AES256-GCM* como algoritmo de cifrado, *SHA256* como algoritmo de hash y como grupo de *PFS* (*Perfect Forward Secrecy*) utilizaremos el 14 (figura 6.57). Dejamos el resto de apartados con los tiempos que vienen configurados por defecto y, para terminar la configuración de la fase 2, guardamos y aplicamos nuevamente los cambios.

**Phase 2 Proposal (SA/Key Exchange)**

**Protocol**    
 Encapsulating Security Payload (ESP) performs encryption and authentication, Authentication Header (AH) is authentication only.

**Encryption Algorithms**

- AES 128 bits
- AES128-GCM 128 bits
- AES192-GCM Auto
- AES256-GCM 128 bits
- CHACHA20-POLY1305

**Hash Algorithms**

- SHA1
- SHA256
- SHA384
- SHA512
- AES-XCBC

Note: Hash is ignored with GCM algorithms. SHA1 provides weak security and should be avoided.

**PFS key group**    
 Note: Groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.

Figura 6.57: Configuración de la fase 2 de IPsec en pfSense1

Para terminar la configuración del túnel en este primer extremo, necesitamos crear una regla que permita el tráfico entre las redes conectadas por el túnel. Para ello, en la sección *Firewall*, accedemos a *Rules* y seleccionamos el apartado *IPsec*. Tal y como se muestra en la figura 6.58, utilizamos el botón *Add* para crear una nueva regla en la cual modificaremos el protocolo a *any*, de forma que nos permita realizar distintos tipo de pruebas con tráfico de distintos protocolos, como ICMP, TCP, etc (ver figura 6.59).

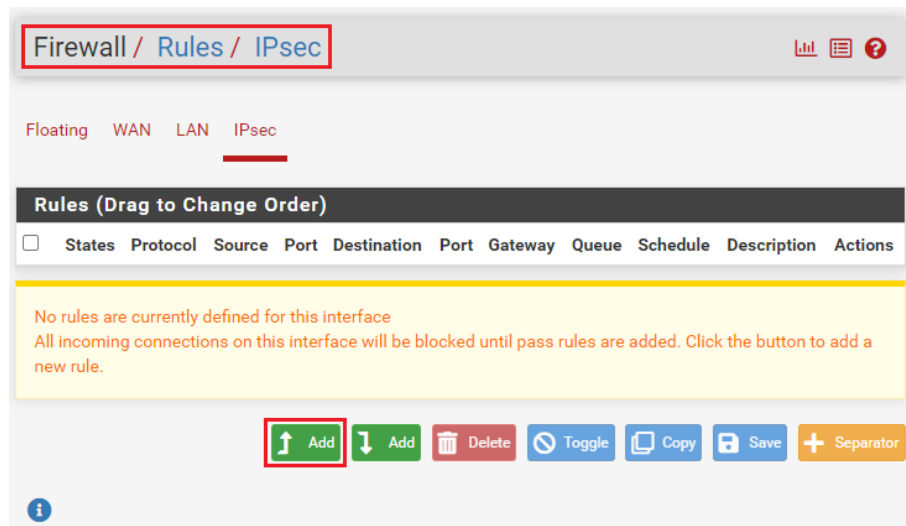


Figura 6.58: Crear una regla para permitir el tráfico por el túnel IPsec en pfSense1

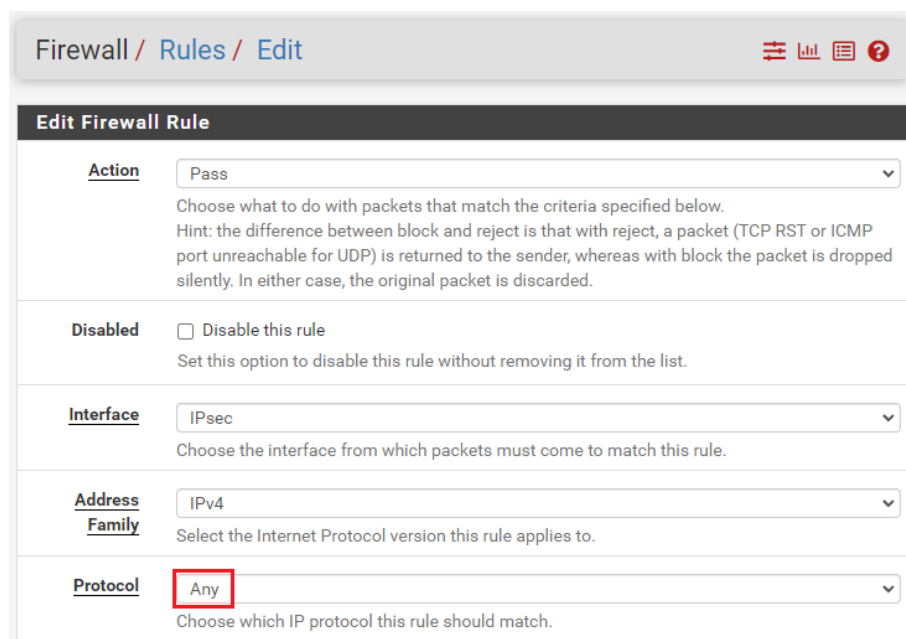


Figura 6.59: Configuración de la regla para IPsec en pfSense1

Después, configuramos como fuente la red local del otro extremo, es decir,  $10.24.2.0/24$  y como destino la red local del cortafuegos que estamos configurando, es decir,  $10.24.1.0/24$  (figura 6.60). De esta forma permitimos la entrada del tráfico que viene a través del túnel desde el otro extremo. Para terminar, marcamos la opción *Log* por si fuese necesario analizar posteriormente el tráfico permitido por esta regla (figura 6.60), guardamos y aplicamos los cambios. Cabe destacar que es posible crear esta regla de una forma más restrictiva o incluso crear distintas reglas con objetivos más concretos, sin embargo, se ha considerado realizar la regla de la forma más permisiva para facilitar las pruebas posteriores.

The screenshot shows the configuration for a rule in pfSense. It is divided into three sections: Source, Destination, and Extra Options. In the Source section, the 'Source' dropdown is set to 'Network', and the IP address and netmask are '10.24.2.0' and '24' respectively. In the Destination section, the 'Destination' dropdown is set to 'Network', and the IP address and netmask are '10.24.1.0' and '24' respectively. In the Extra Options section, the 'Log' checkbox is checked, with the text 'Log packets that are handled by this rule'. A hint below states: 'Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).'

Figura 6.60: Configuración de fuente, destino y opciones extra en la regla para IPsec en pfSense1

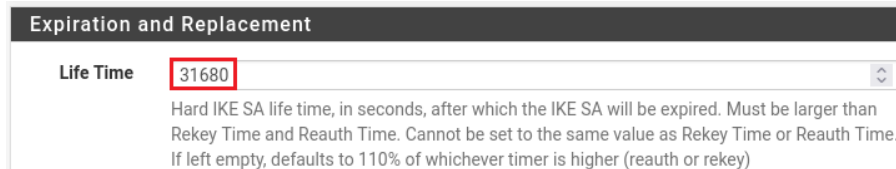
Tras completar la configuración del primer lado del túnel, pasamos a configurar el otro extremo, en este caso, el cortafuegos *pfSense2*. Este proceso de configuración es igual que en el *pfSense1* pero cambiando algunos parámetros, por lo que nos centraremos en las diferencias.

Comenzamos, creando la fase 1 del túnel, de igual manera que en el extremo del *pfSense1* pero, en este caso, introducimos como descripción *Túnel a pfSense 1* y como *Remote Gateway*, la dirección IP de la WAN del otro extremo, es decir, 172.16.0.2 (figura 6.61).

The screenshot shows the pfSense web interface for configuring Phase 1 of an IPsec tunnel. The URL in the browser is 'https://10.24.2.1/vpn\_ipsec\_phase1.php?ikeid=1'. The page title is 'VPN / IPsec / Tunnels / Edit Phase 1'. The 'General Information' section includes: 'Description' set to 'Túnel a pfSense1', 'Disabled' checkbox unchecked, and 'IKE ID' set to '1'. The 'IKE Endpoint Configuration' section includes: 'Key Exchange version' set to 'IKEv2', 'Internet Protocol' set to 'IPv4', 'Interface' set to 'WAN', and 'Remote Gateway' set to '172.16.0.2'.

Figura 6.61: Información general y configuración de IKE de la fase 1 de IPsec en pfSense2

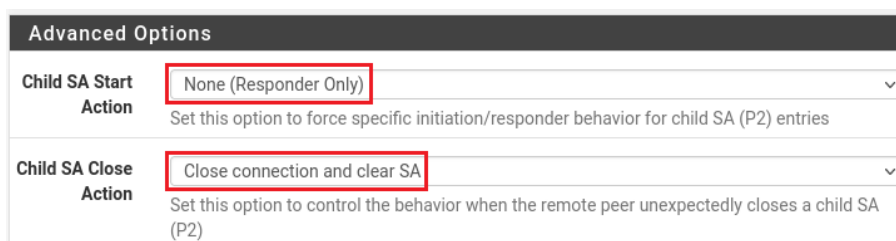
En cuanto a la configuración de fase 1 dejamos todo por defecto e introducimos la clave precompartida que hemos generado anteriormente. A continuación, configuramos el algoritmo de cifrado de forma idéntico al configurado en el *pfSense1*. En este caso, modificamos el *Life Time* a 31680, ya que para evitar conflictos en la renegociaciones de la fase 1, se recomienda configurar un tiempo al menos un 10 % mayor al configurado en el otro extremo (ver figura 6.62).



| Expiration and Replacement  |       |
|---|-------|
| Life Time   | 31680 |
| Hard IKE SA life time, in seconds, after which the IKE SA will be expired. Must be larger than Rekey Time and Reauth Time. Cannot be set to the same value as Rekey Time or Reauth Time. If left empty, defaults to 110% of whichever timer is higher (reauth or rekey) |       |

Figura 6.62: Tiempo de vida de la fase 1 de IPsec en pfSense2

Por último, en las opciones avanzadas, configuramos la *Child SA Start Action* a *None (Responder Only)*, y la *Child SA Close Action* a *Close connection and clear SA* (figura 6.63). De esta forma conseguimos que en caso de una caída del túnel, el extremo del *pfSense1* sea el encargado de volver a levantar el túnel. Terminamos guardando y aplicando los cambios, al igual que en los pasos anteriores.



| Advanced Options   |                               |
|--|-------------------------------|
| Child SA Start Action  | None (Responder Only)         |
| Set this option to force specific initiation/responder behavior for child SA (P2) entries        |                               |
| Child SA Close Action  | Close connection and clear SA |
| Set this option to control the behavior when the remote peer unexpectedly closes a child SA (P2) |                               |

Figura 6.63: Opciones avanzadas de la fase 1 de IPsec en pfSense2

Después de configurar la fase 1, pasamos a crear la fase 2, de igual manera que realizamos en el otro extremo. En este caso la configuración será idéntica a la del *pfSense1* exceptuando tres parámetros. La descripción, que en este caso será *Túnel a pfSense1*, la *Remote Network* que corresponde a la red local del extremo al que nos vamos a conectar, es decir, *10.24.1.0/24* (figura 6.64) y el *Life Time*, que configuraremos como 3600 (figura 6.65). De la misma forma que en la fase 1, establecemos un tiempo al menos un 10 % mayor al configurado en el otro extremo. De nuevo, acabamos la configuración de la fase 2 guardando y aplicando los cambios.

**General Information**

**Description** Túnel a pfSense1  
A description may be entered here for administrative reference (not parsed).

**Disabled**  Disable this phase 2 entry without removing it from the list.

**Mode** Tunnel IPv4

**Phase 1** Túnel a pfSense1 (IKE ID 1)

**Networks**

**Local Network** LAN subnet / 0  
Type Address  
Local network component of this IPsec security association.

**NAT/BINAT translation** None / 0  
Type Address  
If NAT/BINAT is required on this network specify the address to be translated

**Remote Network** Network 10.24.1.0 / 24  
Type Address  
Remote network component of this IPsec security association.

Figura 6.64: Información general y configuración de redes en la fase 2 de IPsec en pfSense2

**Expiration and Replacement**

**Life Time** 3600  
Hard Child SA life time, in seconds, after which the Child SA will be expired. Must be larger than Rekey Time. Cannot be set to the same value as Rekey Time. If left empty, defaults to 110% of Rekey Time. If both Life Time and Rekey Time are empty, defaults to 3960.

**Rekey Time** 3240  
Time, in seconds, before a Child SA establishes new keys. This works without interruption. Cannot be set to the same value as Life Time. Leave blank to use a default value of 90% Life Time. If both Life Time and Rekey Time are empty, defaults to 3600. Enter a value of 0 to disable, but be aware that when rekey is disabled, connections can be interrupted while new Child SA entries are negotiated.

**Rand Time** 360  
A random value up to this amount will be subtracted from Rekey Time to avoid simultaneous renegotiation. If left empty, defaults to 10% of Life Time. Enter 0 to disable randomness, but be aware that simultaneous renegotiation can lead to duplicate security associations.

Figura 6.65: Tiempo de vida de la fase 2 de IPsec en pfSense2

Para finalizar, necesitamos crear la regla inversa a la creada anteriormente en el *pfSense1*. Esta nueva regla se creará de la misma manera que la anterior, permitiendo cualquier protocolo, pero invirtiendo la fuente y el destino del tráfico. En este caso, como fuente configuramos la red local del *pfSense1*, es decir, la *10.24.1.0/24* y como destino la red local del extremo que estamos configurando, esta es la *10.24.2.0/24* (figura 6.66). Tras crear la regla, guardamos y aplicamos los cambios. Con esto ya hemos terminado con la configuración del túnel IPsec en ambos extremos de la conexión.

The screenshot shows the configuration for an IPsec rule in pfSense2. It is divided into two main sections: 'Source' and 'Destination'.  
 In the 'Source' section, there is a 'Source' label, an unchecked 'Invert match' checkbox, a dropdown menu set to 'Network', an input field containing '10.24.1.0', a slash separator, and another dropdown menu set to '24'.  
 In the 'Destination' section, there is a 'Destination' label, an unchecked 'Invert match' checkbox, a dropdown menu set to 'Network', an input field containing '10.24.2.0', a slash separator, and another dropdown menu set to '24'.  
 Red boxes highlight the dropdown menus and input fields in both sections.

Figura 6.66: Configuración de fuente y destino en la regla para IPsec en pfSense2

## 6.4 Configuración de VPN Site-to-Site con OpenVPN

La configuración de la conexión VPN utilizando el protocolo OpenVPN se realizará utilizando como apoyo el artículo de la guía oficial de sobre la configuración de un túnel OpenVPN en modo site-to-site con clave precompartida [41]. A pesar de que la versión más segura de OpenVPN es la que utiliza el protocolo SSL/TLS en vez de clave precompartida, se ha decidido utilizar esta última ya que la versión SSL/TLS requiere la creación de certificados para los equipos y de un tercer cortafuegos que funcione como servidor de la VPN, esto aumenta significativamente la complejidad de la configuración del túnel. Se ha descartado esta alternativa porque se considera que excede el objetivo de este trabajo. Además, a pesar de tener un menor nivel de seguridad, la opción con clave precompartida es suficiente para ilustrar la configuración y el comportamiento de esta VPN.

En las conexiones establecidas con OpenVPN, se necesita configurar un servidor en uno de los extremos del túnel y un cliente el otro, en nuestro caso, el servidor se creará en el *pfSense1* y el cliente se configurará en el *pfSense2*.

Comenzamos configurado el extremo del pfSense1, por lo que nos dirigimos a la sección VPN, seleccionamos OpenVPN y, en el apartado *Servers*, creamos un nuevo servidor presionando sobre *Add* (figura 6.67).

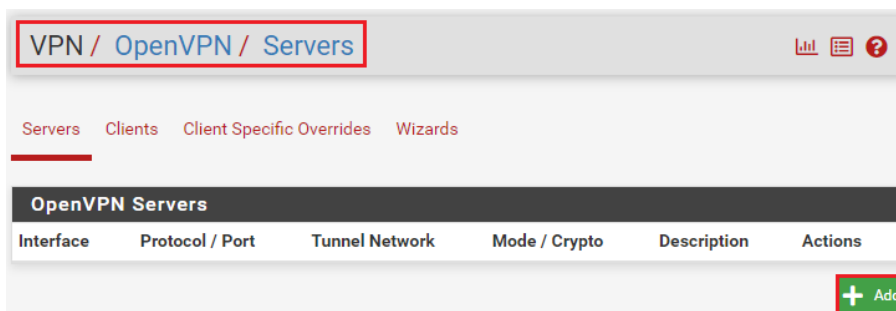


Figura 6.67: Crear servidor OpenVPN en pfSense1

Para este servidor configuramos primero una descripción, en nuestro caso, *Túnel OpenVPN a pfSense2*, seleccionamos como modo de servidor *Peer to Peer (Shared Key)* y como modo de dispositivo *tun - Layer 3 Tunnel Mode*, ya que el túnel funcionará a nivel de IPv4 (ver figura 6.68). El dispositivo nos notificará con un *Warning* sobre los bajos niveles de seguridad de este modo de configuración, sin embargo, lo seleccionamos igualmente debido a lo que ya se ha comentado previamente.

VPN / OpenVPN / Servers / Edit

Servers Clients Client Specific Overrides Wizards

### General Information

**Description** Túnel OpenVPN a pfSense2  
A description of this VPN for administrative reference.

**Disabled**  Disable this server  
Set this option to disable this server without removing it from the list.

### Mode Configuration

**Server mode** Peer to Peer ( Shared Key )

**WARNING:** OpenVPN has deprecated shared key mode as it does not meet current security standards. Shared key mode will be removed from future versions. Convert any existing shared key VPNs to TLS and do not configure any new shared key OpenVPN instances.

**Device mode** tun - Layer 3 Tunnel Mode  
"tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms.  
"tap" mode is capable of carrying 802.3 (OSI Layer 2.)

**Figura 6.68:** Información general y modo de configuración del servidor OpenVPN en pfSense1

En cuanto a la *Endpoint Configuration*, dejamos todos los valores por defecto, es decir, que utilizaremos el protocolo UDP únicamente sobre IPv4 por la interfaz WAN y utilizando el protocolo 1194 (figura 6.69). Con lo que respecta al los ajustes criptográficos dejamos marcada la opción *Automatically generate a shared key*, para que nos genere una clave automáticamente y no modificamos ninguno del resto de parámetros ya que están configurados con las opciones más seguras por defecto (ver figura 6.69).

### Endpoint Configuration

**Protocol** UDP on IPv4 only

**Interface** WAN  
The interface or Virtual IP address where OpenVPN will receive client connections.

**Local port** 1194  
The port used by OpenVPN to receive client connections.

### Cryptographic Settings

**Shared key**  Automatically generate a shared key

**Figura 6.69:** Configuración del servidor y ajustes criptográficos de OpenVPN en pfSense1

Para las configuraciones del túnel tenemos que añadir una nueva red, esta red únicamente se utiliza para las comunicaciones internas entre el servidor y el cliente de la VPN. En este caso, hemos seleccionado la red *10.24.3.0/30*, que incluye direcciones IP fuera de los rangos de las redes privadas de ambos cortafuegos, esta



red se configurará en ambos extremos y cada uno tomará una dirección dentro de ella, que utilizará para realizar las comunicaciones a través del túnel. Además de esta red, introducimos como red remota IPv4 la red local del otro extremo, es decir, *10.24.2.0/24* (figura 6.70). El resto de configuraciones las mantenemos como están por defecto y guardamos los cambios.

**Tunnel Settings**

**IPv4 Tunnel Network**

This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.

A tunnel network of /30 or smaller puts OpenVPN into a special peer-to-peer mode which cannot push settings to clients. This mode is not compatible with several options, including Exit Notify, and Inactive.

**IPv6 Tunnel Network**

This is the IPv6 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the network will be assigned to the server virtual interface. The remaining addresses will be assigned to connecting clients.

**IPv4 Remote network(s)**

IPv4 networks that will be routed through the tunnel, so that a site-to-site VPN can be established without manually changing the routing tables. Expressed as a comma-separated list of one or more CIDR ranges or host/network type aliases. If this is a site-to-site VPN, enter the remote LAN/s here. May be left blank for non site-to-site VPN.

**Figura 6.70:** Configuración del túnel en el servidor OpenVPN en pfSense1

Antes de avanzar al siguiente paso, editamos de nuevo el servidor que acabamos de crear, nos dirigimos al apartado de ajustes criptográficos y copiamos la *Shared Key* en un bloc de notas (ver figura 6.71). Esta clave será necesaria para introducirla posteriormente en el lado del cliente.

**Cryptographic Settings**

**Shared Key**

Paste the shared key here

**Figura 6.71:** Clave compartida generada automáticamente en el servidor OpenVPN en pfSense1

A continuación, tendremos que crear dos reglas de firewall. Una primera regla que permita el acceso al servidor OpenVPN que hemos creado. Para crear esta regla, accedemos a la sección *Firewall*, escogemos *Rules* y en el apartado WAN añadimos una nueva regla presionando en *Add*. En la configuración de esta regla seleccionamos como protocolo UDP, ya que es el protocolo que hemos configurado para que el cliente establezca conexión con el servidor e introducimos como fuente la dirección IP de la interfaz WAN del extremo del cliente, es decir, la *192.168.254.2* (ver figura 6.72).

The screenshot shows the configuration for a firewall rule. The 'Protocol' dropdown is set to 'UDP'. Under the 'Source' section, the 'Source' dropdown is set to 'Address or Alias' and the text input field contains '192.168.254.2'. There is a 'Display Advanced' button and a note about source port ranges.

**Figura 6.72:** Configuración del protocolo y fuente de la regla para el acceso al servidor OpenVPN en pfSense1

Además, configuramos como destino la dirección IP de la WAN del extremo que estamos configurando, o simplemente seleccionamos *WAN Address*. Determinamos el puerto destino con el que hemos configurado en el servidor, que es nuestro caso es el por defecto de OpenVPN, es decir, el 1194 (figura 6.73).

The screenshot shows the configuration for the destination of a firewall rule. The 'Destination' dropdown is set to 'WAN address'. Under the 'Destination Port Range' section, both the 'From' and 'To' dropdowns are set to 'OpenVPN (1194)'. There are 'Custom' buttons for both fields and a note about specifying the destination port or port range.

**Figura 6.73:** Configuración del destino de la regla para el acceso al servidor OpenVPN en pfSense1

Por último, marcamos la opción de *Log* y añadimos una descripción a la regla, por ejemplo, *Acceso a OpenVPN desde pfsense2*. Terminamos guardando y aplicando los cambios.

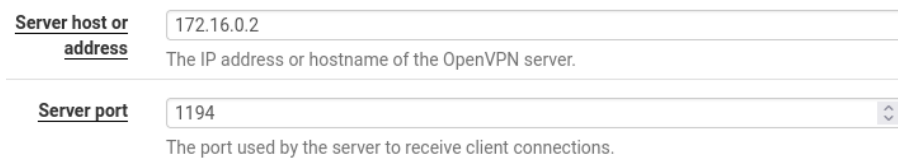
Para terminar la configuración del extremo del servidor, creamos una regla que permita todo el tráfico a través del túnel. Al igual que en el caso del túnel IPsec, esta regla podría configurarse de una forma más restrictiva, permitiendo tráfico únicamente de algún protocolo en concreto o desde un equipo específico, sin embargo, para facilitar las pruebas crearemos la regla de la forma más permisiva. Para ello, nos dirigimos de nuevo a la sección *Firewall*, concretamente a *Rules* y en el apartado de OpenVPN creamos una nueva regla con *Add*. Configuramos el protocolo, la fuente y el destino como *any*, tal y como se muestra en la figura 6.74, para que permita el tráfico que pase por el túnel utilizando cualquier protocolo e independientemente del origen y el destino. Al igual que en la regla anterior, activamos la opción *Log* y podemos añadir una descripción como *Permitir tráfico en el túnel OpenVPN*. Por último, guardamos y aplicamos los cambios.

The screenshot shows the configuration for a firewall rule where the 'Protocol', 'Source', and 'Destination' dropdowns are all set to 'Any'. There are 'Invert match' checkboxes for both source and destination, and 'Source Address' and 'Destination Address' input fields.

**Figura 6.74:** Configuración de la regla para permitir el tráfico por el túnel OpenVPN en pfSense1

Una vez tenemos terminado el extremo del *pfSense1*, comenzamos con la configuración del *pfSense2* creando un cliente OpenVPN. Primero accedemos a la sec-

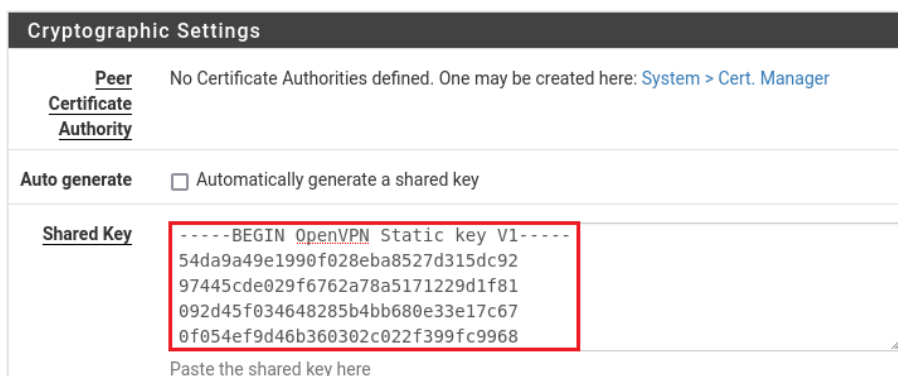
ción VPN, seleccionamos OpenVPN y añadimos un nuevo cliente en el apartado *Clients*. En este caso, introducimos como descripción *Túnel OpenVPN a pfSense1* y configuramos los distintos parámetros de acuerdo como el servidor creado anteriormente. Por tanto, seleccionamos el modo de servidor *Peer to Peer (Shared Key)*, el modo de dispositivo *tun*, el protocolo *UDP on IPv4 only* y la interfaz WAN. Introducimos la dirección y el puerto del extremo del servidor, es decir, *172.16.0.2* y *1194* (figura 6.75).



The image shows a configuration form for an OpenVPN client. It has two main sections. The first section is labeled 'Server host or address' and contains a text input field with the value '172.16.0.2'. Below this field is a small text description: 'The IP address or hostname of the OpenVPN server.' The second section is labeled 'Server port' and contains a dropdown menu with the value '1194'. Below this dropdown is another small text description: 'The port used by the server to receive client connections.'

Figura 6.75: Configuración del servidor en el cliente OpenVPN en pfSense2

En cuanto a la clave compartida, en este caso, desactivamos la opción de auto generarla y introducimos la que hemos copiado previamente desde el servidor (ver figura 6.76). Por último, configuramos como red del túnel la misma red que escogimos en el servidor para este propósito, es decir, la red *10.24.3.0/24* y como red remota, configuramos la red *10.24.1.0/24* que representa la red privada del extremo del *pfSense1* (ver figura 6.77). Dejamos todo el resto de opciones por defecto y guardamos los cambios.



The image shows the 'Cryptographic Settings' page in pfSense2. It has a dark header with the title 'Cryptographic Settings'. Below the header, there are three main sections. The first section is labeled 'Peer Certificate Authority' and contains the text 'No Certificate Authorities defined. One may be created here: [System > Cert. Manager](#)'. The second section is labeled 'Auto generate' and contains a checkbox with the label 'Automatically generate a shared key', which is currently unchecked. The third section is labeled 'Shared Key' and contains a text input field with a long alphanumeric string: '-----BEGIN OpenVPN Static key V1-----  
54da9a49e1990f028eba8527d315dc92  
97445cde029f6762a78a5171229d1f81  
092d45f034648285b4bb680e33e17c67  
0f054ef9d46b360302c022f399fc9968'. This string is highlighted with a red rectangular box. Below the input field is the text 'Paste the shared key here'.

Figura 6.76: Clave compartida copiada en el cliente OpenVPN en pfSense2

**Tunnel Settings**

**IPv4 Tunnel Network**

This is the IPv4 virtual network or network type alias with a single entry used for private communications between this client and the server expressed using CIDR notation (e.g. 10.0.8.0/24).

This should be left blank in most cases as servers typically provide addresses to clients dynamically.

The second usable address in this network will be assigned to the client virtual interface. Ensure the Topology setting matches the server when using SSL/TLS and TUN modes or the interface address may not be configured properly. A tunnel network of /30 or smaller puts OpenVPN into a special peer-to-peer mode which cannot receive settings from the server dynamically. This mode is not compatible with several options, including Exit Notify, and Inactive.

**IPv6 Tunnel Network**

This is the IPv6 virtual network or network alias with a single entry used for private communications between this client and the server expressed using CIDR notation (e.g. fe80::/64). When set static using this field, the ::2 address in the network will be assigned to the client virtual interface. Leave blank if the server is capable of providing addresses to clients.

**IPv4 Remote network(s)**

IPv4 networks that will be routed through the tunnel, so that a site-to-site VPN can be established without manually changing the routing tables. Expressed as a comma-separated list of one or more CIDR ranges or host/network type aliases. If this is a site-to-site VPN, enter the remote LAN/s here. May be left blank for non site-to-site VPN.

Figura 6.77: Configuración del túnel en el cliente OpenVPN en pfSense2

El último paso, es crear en el extremo del cliente, la regla que permita el tráfico por el túnel OpenVPN, tal y como se creó en extremo del servidor. Al igual que en el *pfSense1*, creamos la regla con el protocolo, fuente y destino como *any*, permitiendo el paso de todo el tráfico que atraviese el túnel. Activamos la opción *Log*, añadimos una descripción a la regla, es este caso podemos mantener la misma que en el otro extremo, guardamos y aplicamos los cambios. Tras esto, hemos terminado la configuración del túnel OpenVPN.

## 6.5 Configuración de VPN Site-to-Site con WireGuard

En el caso de la VPN con WireGuard, a diferencia de los dos protocolos anteriores, tenemos que instalar un paquete adicional en cada uno de los cortafuegos. Como ambos se encuentran conectados a Internet, nos dirigimos a la sección *System* y seleccionamos la opción *Package Manager*. En el apartado de paquetes disponibles, buscamos WireGuard, presionamos en *Install* y confirmamos la instalación (figura 6.78). Esperamos a que termine el proceso y cuando obtenemos lo que se muestra en la figura 6.79, ya podemos pasar a la configuración del túnel.

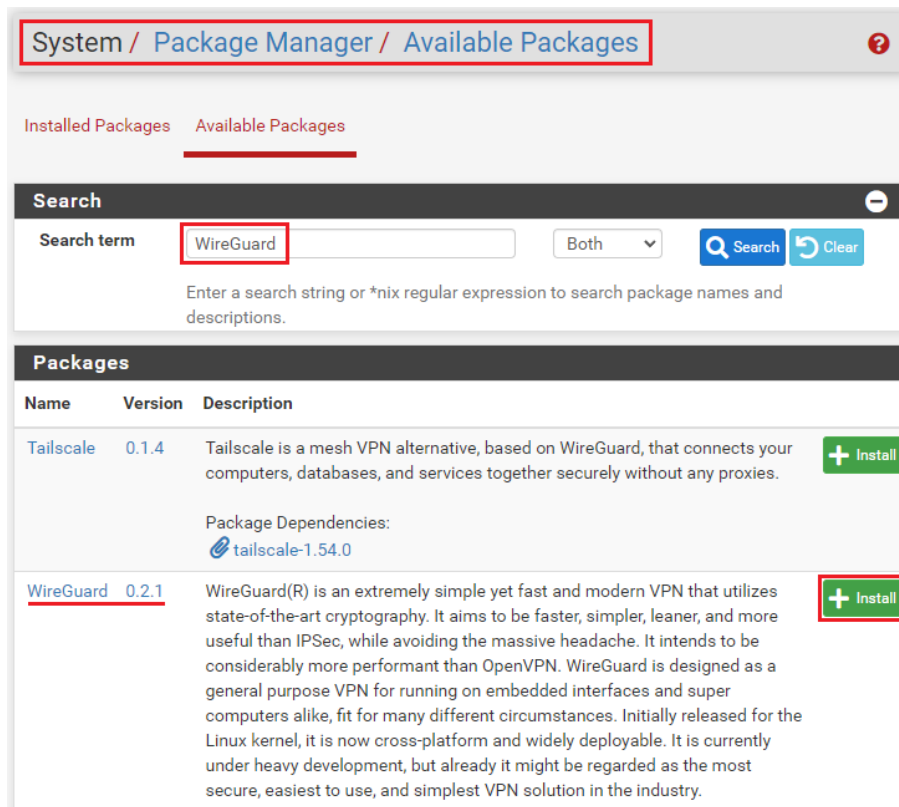


Figura 6.78: Búsqueda e instalación del paquete de WireGuard

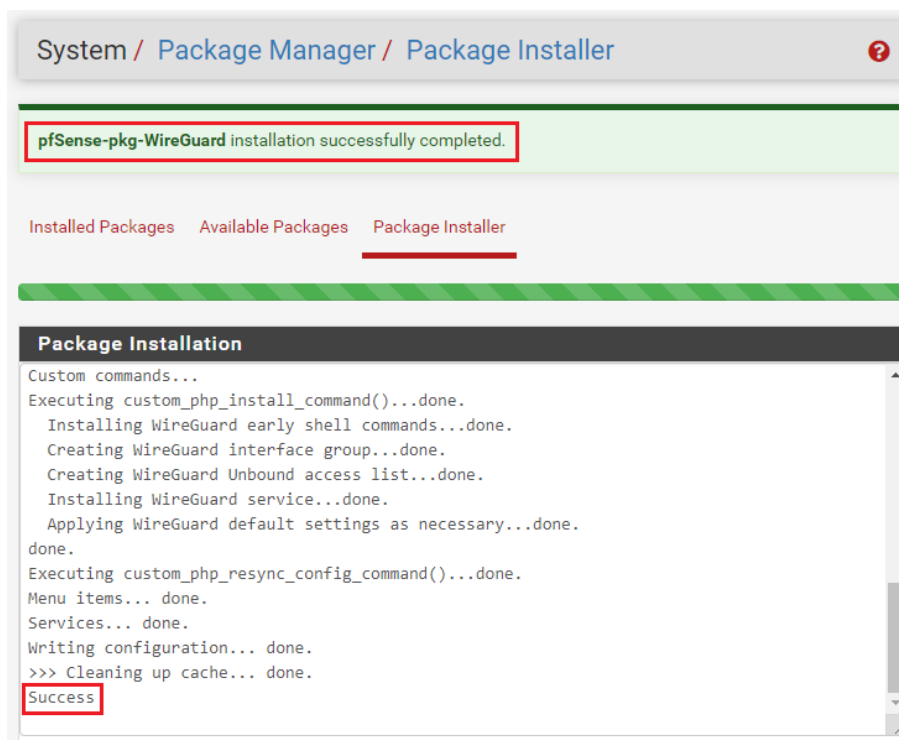


Figura 6.79: Instalación completada del paquete de WireGuard

Al igual que en los casos de los túneles anteriores, vamos utilizar como referencia el artículo de la guía oficial de sobre la configuración de un túnel WireGuard en modo site-to-site [42]. Sin embargo, a diferencia del resto de protocolos,

vamos a configurar a la vez ambos extremos, en vez de primero configurar uno completamente y luego el otro. Esto se debe a que las configuraciones de ambos extremos comparten muchos de los pasos a realizar, además en algunas fases de la configuración son necesarios datos obtenidos durante la configuración el otro extremo.

Comenzamos activando WireGuard en ambos cortafuegos, ya que por defecto está deshabilitado, accediendo a la sección VPN, seleccionamos WireGuard y en el apartado *Settings*, marcamos la opción *Enable WireGuard* y en seleccionamos *Only Unassigned Tunnels* como *Interface Group Membership* (ver figura 6.80). Guardamos y aplicamos los cambios.

VPN / WireGuard / Settings

Tunnels Peers Settings Status

### General Settings

**Enable**  **Enable WireGuard**  
Note: WireGuard cannot be disabled when one or more tunnels is assigned to a pfSense interface.

**Keep Configuration**  **Enable**  
Note: With 'Keep Configurations' enabled (default), all tunnel configurations and package settings will persist on install/de-install.

**Endpoint Hostname Resolve Interval**   
Interval (in seconds) for re-resolving endpoint host/domain names.  
Note: The default is 300 seconds (0 to disable).

**Track System Resolve Interval**  
Tracks the system 'Aliases Hostnames Resolve Interval' setting.  
Note: See System > Advanced > Firewall & NAT

**Interface Group Membership**   
Configures which WireGuard tunnels are members of the WireGuard interface group.  
Note: Group firewall rules are evaluated before interface firewall rules. Default is 'All Tunnels.'

Figura 6.80: Habilitar WireGuard en los ajustes de la VPN

A continuación, en ambos extremos, creamos dentro de la misma sección VPN, un nuevo túnel desde el apartado *Tunnels* utilizando *Add Tunnel*. En este túnel marcamos la opción *Enable* y configuramos una descripción como *Túnel WireGuard a pfSense2*, en el caso del *pfSense1*, o *Túnel WireGuard a pfSense1* en caso del *pfSense2*. Introducimos el puerto por defecto, es decir, 51820 y generamos una clave utilizando el botón *Generate* (ver figura 6.81). Copiamos las claves públicas generadas en cada uno de los extremos para utilizarla posteriormente, guardamos y aplicamos los cambios.

**Tunnel Configuration (tun\_wg0)**

**Enable**  **Enable Tunnel**  
 Note: Tunnel must be **enabled** in order to be assigned to a pfSense interface.

**Description**   
 Description for administrative reference (not parsed).

**Listen Port**   
 Port used by this tunnel to communicate with peers.

**Interface Keys**  
 Private key for this tunnel. (Required)   
 Public key for this tunnel. (Copy)   
 New Keys

Figura 6.81: Configuración del túnel WireGuard en pfSense1

Tras la creación del túnel, tendremos que crear un *Peer* para cada uno de los extremos. Para ellos, en cada uno de los cortafuegos editamos el túnel y añadimos el par con *Add Peer* (figura 6.82).





| Name      | Description                | Public Key                           | Address / Assignment | Listen Port | Peers | Actions   |
|-----------|----------------------------|--------------------------------------|----------------------|-------------|-------|---|
| > tun_wg0 | Túnel WireGuard a pfSense2 | 9cMWWRpKp/7Xngg8YTD7lh2lRRed1eYX6... | (none)               | 51820       | 0     |     |

Figura 6.82: Editar túnel WireGuard en pfSense1

Por un lado, en el *pfSense1* introducimos como descripción *Túnel a pfSense2 Peer*, desactivamos la opción *Dynamic Endpoint* y configuramos como *Endpoint* la dirección IP de la WAN del otro extremo, es decir, *192.168.254.2* y el puerto 51820 (ver figura 6.83). En cuanto a la clave pública, introducimos la clave generada en el otro cortafuegos, es decir, en *pfSense2* (figura 6.84).

**Peer Configuration**

**Enable**  **Enable Peer**  
 Note: Uncheck this option to disable this peer without removing it from the list.

**Tunnel**   
 WireGuard tunnel for this peer. (Create a New Tunnel)

**Description**   
 Peer description for administrative reference (not parsed).

**Dynamic Endpoint**  **Dynamic**  
 Note: Uncheck this option to assign an endpoint address and port for this peer.

**Endpoint**    
 Hostname, IPv4, or IPv6 address of this peer. Leave endpoint and port blank if unknown (dynamic endpoints).  
 Port used by this peer. Leave blank for default (51820).

Figura 6.83: Configuración del *Peer* WireGuard en pfSense1

**Public Key**   
 WireGuard public key for this peer.

Figura 6.84: Clave pública del *Peer* WireGuard en pfSense1



En la configuración de direcciones añadimos dos redes como *Allowed IPs*, una red que asignaremos para el túnel, igual que se realizó en la configuración de OpenVPN, en este caso la red será la *10.24.3.0/31* y la red local del pfSense2, es decir, la *10.24.2.0/24* (ver figura 6.85).

| Allowed IPs |  |   |    |  |
|-------------|--|---|----|--|
|             | 10.24.3.0  | / | 31 | Red del túnel  |
|             | 10.24.2.0  | / | 24 | Red local del pfSense2                                 |
|             | IPv4 or IPv6 subnet or host reachable via this peer. |   |    | Description for administrative reference (not parsed). |

**Figura 6.85:** Redes permitidas del *Peer WireGuard* en pfSense1

Por otro lado, en el cortafuegos *pfSense2*, introducimos como descripción *Túnel a pfSense1 Peer* y al igual que en el extremo anterior, desactivamos la opción de *Dynamic Endpoint* y configuramos manualmente la dirección IP *172.16.0.2* y el puerto *51820* como *Endpoint*, esta dirección coincide con la dirección WAN del *pfSense1*. Introducimos como clave pública la clave generada en la creación del túnel en el *pfSense1* (figura 6.86).

|                   |  |   |
|-------------------|--|---|
| <b>Endpoint</b>   | 172.16.0.2   | 51820   |
|                   | Hostname, IPv4, or IPv6 address of this peer.<br>Leave endpoint and port blank if unknown (dynamic endpoints). | Port used by this peer.<br>Leave blank for default (51820). |
| <b>Keep Alive</b> | Keep Alive   |   |
|                   | Interval (in seconds) for Keep Alive packets sent to this peer.<br>Default is empty (disabled).                |   |
| <b>Public Key</b> | 9cMWWRpKp/7Xngg8YTD7lh2lRed1eYX6vhFhs6rjcWc=   |   |
|                   | WireGuard public key for this peer.  |   |

**Figura 6.86:** Configuración y clave pública del *Peer WireGuard* en pfSense2

Al igual que que en el otro extremo, configuramos dos *Allowed IPs*, la red del túnel que es la misma en ambos extremos y la red local del *pfSense1*, es decir, la *10.24.1.0/24* (ver figura 6.87). En ambos cortafuegos guardamos y aplicamos los cambios.

| Allowed IPs |  |   |    |  |
|-------------|--|---|----|--|
|             | 10.24.3.0  | / | 31 | Red del túnel  |
|             | 10.24.1.0  | / | 24 | Red local del pfSense1                                 |
|             | IPv4 or IPv6 subnet or host reachable via this peer. |   |    | Description for administrative reference (not parsed). |

**Figura 6.87:** Redes permitidas del *Peer WireGuard* en pfSense2

Continuamos dirigiéndonos a *System* en ambos extremos, concretamente a *Routing* y ajustamos el *Default Gateway IPv4* a *WANGW*, guardamos y aplicamos los cambios (figura 6.88).





Figura 6.88: *Default gateway* en ambos pfSense

El siguiente paso también lo realizamos en ambos cortafuegos, vamos a asignar una nueva interfaz al túnel. Para esto, en la sección *Interfaces*, accedemos a *Assignments*, seleccionamos *tun\_wg0* (*tun\_wg0*) de entre los puertos de red disponibles y presionamos en *Add* para crear una nueva interfaz OPT (ver figura 6.89).

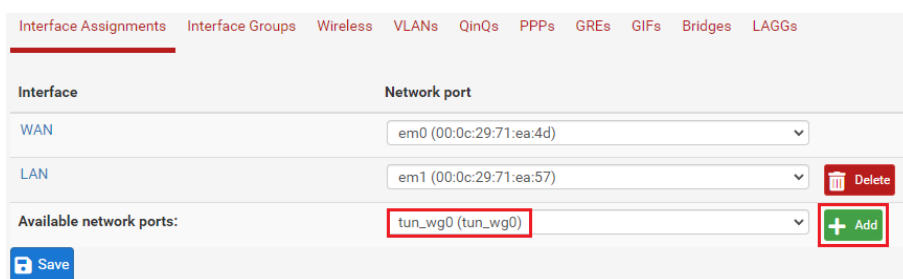


Figura 6.89: Añadir la nueva interfaz para WireGuard en ambos pfSense

Una vez creada, en *Interfaces*, seleccionamos la nueva *OPT1*, marcamos *Enable interface* para habilitarla, introducimos una descripción como *VPN\_a\_pfSense2* en el caso del *pfSense1* y *VPN\_a\_pfSense2* para el *pfSense2*, y seleccionamos *Static IPv4* como tipo de configuración IPv4 (figura 6.90).

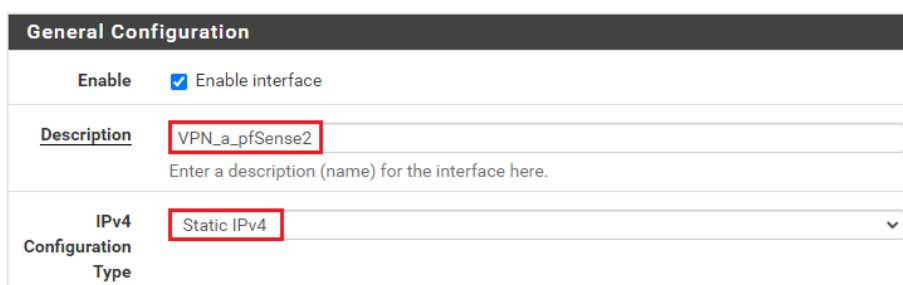


Figura 6.90: Configuración general de la nueva interfaz WireGuard en pfSense1

Respecto a esta configuración de IPv4, en el caso del *pfSense1*, tal y como se muestra en la figura 6.91, introducimos como dirección la *10.24.3.0/31* y añadimos un nuevo *IPv4 Upstream gateway* al que nombramos como *Gateway\_VPN\_a\_pfSense2* y asignamos *10.24.3.1* como *Gateway IPv4*, que será la dirección de la interfaz del otro extremo (ver figura 6.92).

| Static IPv4 Configuration |   |
|---------------------------|---|
| IPv4 Address              | 10.24.3.0 / 31  |
| IPv4 Upstream gateway     | Gateway_VPN_a_pfSense2 - 10.24.3.1 <span>+ Add a new gateway</span> |

**Figura 6.91:** Configuración IPv4 de la nueva interfaz WireGuard en pfSense1

### New IPv4 Gateway

Default  Default gateway

Gateway name: Gateway\_VPN\_a\_pfSense2

Gateway IPv4: 10.24.3.1

Description:

+ Add Cancel

**Figura 6.92:** Creación del nuevo IPv4 Gateway para la interfaz WireGuard en pfSense1

Para el *pfSense2*, tal y como se ha comentado, configuramos como dirección la *10.24.3.1* y creamos un *IPv4 Upstream gateway* nombrándolo como *Gateway\_VPN\_a\_pfSense1*, introduciendo como *Gateway IPv4* la dirección del extremo opuesto, es decir, *10.24.3.0* (ver figura 6.93). En ambos cortafuegos seleccionamos el *gateway* que hemos creado, guardamos y aplicamos los cambios.

| Static IPv4 Configuration |   |
|---------------------------|---|
| IPv4 Address              | 10.24.3.1 / 31  |
| IPv4 Upstream gateway     | Gateway_VPN_a_pfSense1 - 10.24.3.0 <span>+ Add a new gateway</span> |

**Figura 6.93:** Configuración IPv4 de la nueva interfaz WireGuard en pfSense2

Tras la creación de las interfaces comenzamos con la creación de las reglas necesarias. En ambos cortafuegos, nos dirigimos a *Firewall*, seleccionamos *Rules* y en el apartado WAN añadimos una nueva regla. Esta regla permitirá el acceso a la VPN, por tanto seleccionamos el protocolo UDP e introducimos como fuente la dirección WAN del extremo opuesto en cada caso, para el *pfSense1* introducimos la dirección *192.168.254.2* y para el *pfSense2*, la *172.16.0.2*. En cuanto al destino, en ambos casos seleccionamos *WAN address*, que representa a la WAN de cada uno de los cortafuegos respectivamente, y como puerto, escogemos *other* e introducimos el *51280* (ver figura 6.94). Para terminar la creación de la regla, marcamos la opción *Log*, elegimos una descripción como *Permitir tráfico al túnel WireGuard desde pfSense2* para el *pfSense1* y *Permitir tráfico al túnel WireGuard desde pfSense1* para el *pfSense2*, guardamos y aplicamos los cambios.

The screenshot shows the configuration for a firewall rule in pfSense. The 'Protocol' is set to 'UDP'. Under the 'Source' section, the 'Source' is set to 'Address or Alias' with the value '192.168.254.2'. A 'Display Advanced' button is visible. Under the 'Destination' section, the 'Destination' is set to 'WAN address'. The 'Destination Port Range' is set to 'From: (other) 51820' and 'To: (other) 51820', both with 'Custom' range type. A note at the bottom states: 'Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.'

**Figura 6.94:** Configuración de la regla permitir tráfico al túnel WireGuard desde pfSense2 a pfSense1

Al igual que en los túneles VPN anteriores, necesitamos crear una regla que permita el paso del tráfico a través del túnel, esta regla será idéntica en ambos extremos. Para ello, en la misma sección *Rules* nos dirigimos al apartado correspondiente a la nueva interfaz *VPN\_a\_pfSense2* o *VPN\_a\_pfSense1* respectivamente y añadimos una nueva regla. Esta regla se configurará, igual que en las VPN anteriores, de la forma más permisiva. Configuramos el puerto, la fuente y el destino como *any*, marcamos la opción *Log* y introducimos una descripción como *Permitir tráfico a través del túnel WireGuard*. Para terminar, guardamos y aplicamos los cambios.

Para finalizar la configuración del túnel con WireGuard, añadimos una ruta estática en cada uno de los cortafuegos que encamine el tráfico a través del túnel. Accedemos a *System*, seleccionamos *Routing* y en *Static Routes* añadimos una nueva ruta con *Add* (figura 6.95).

The screenshot shows the 'Static Routes' configuration page in pfSense. The breadcrumb navigation is 'System / Routing / Static Routes'. There are tabs for 'Gateways', 'Static Routes', and 'Gateway Groups'. Below the tabs is a table with columns: 'Network', 'Gateway', 'Interface', 'Description', and 'Actions'. A '+ Add' button is located at the bottom right of the table.

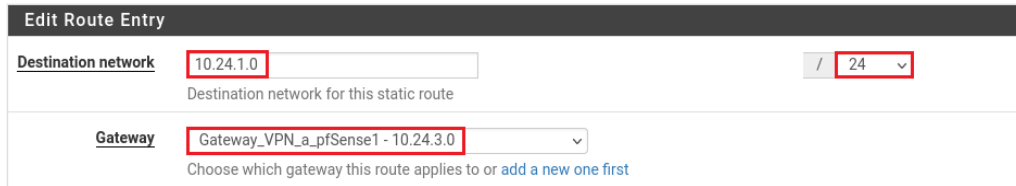
**Figura 6.95:** Añadir una ruta estática en ambos pfSense

En el caso del *pfSense1* introducimos como red destino, la red local del otro extremo, es decir, la *10.24.2.0/24* y seleccionamos como *Gateway* el *Gateway\_VPN\_a\_pfSense2 - 10.24.3.1*, correspondiente a la interfaz del túnel que hemos creado (ver figura 6.96).

The screenshot shows the 'Edit Route Entry' configuration page. The 'Destination network' is set to '10.24.2.0 / 24'. The 'Gateway' is set to 'Gateway\_VPN\_a\_pfSense2 - 10.24.3.1'. A note at the bottom states: 'Choose which gateway this route applies to or add a new one first'.

**Figura 6.96:** Configuración de la ruta estática en pfSense1

Mientras que para el *pfSense2*, configuramos como red destino la red local del *pfSense1*, es decir, la *10.24.1.0/24* y como *Gateway* el *Gateway\_VPN\_a\_pfSense1 - 10.24.3.0* (ver figura 6.97). En ambos casos, guardamos y aplicamos los cambios, con lo que terminamos la configuración del túnel WireGuard.



The screenshot shows the 'Edit Route Entry' interface in pfSense. It features two main sections: 'Destination network' and 'Gateway'. The 'Destination network' section has a text input field containing '10.24.1.0' and a dropdown menu for the subnet mask, currently set to '24'. The 'Gateway' section has a dropdown menu showing 'Gateway\_VPN\_a\_pfSense1 - 10.24.3.0'. Red boxes highlight the '10.24.1.0' text, the '24' dropdown, and the 'Gateway\_VPN\_a\_pfSense1 - 10.24.3.0' dropdown.

**Figura 6.97:** Configuración de la ruta estática en pfSense2

---

# CAPÍTULO 7

## Implantación

---

En esta sección se explicará como poner en funcionamiento cada uno de los túneles tras su configuración.

### 7.1 Puesta en marcha de la VPN con IPsec

---

En el caso del túnel VPN con IPsec, su puesta en funcionamiento es realmente sencilla ya que, si todo está correctamente configurado, solo se necesita crear tráfico que pase a través del túnel para que la conexión se establezca automáticamente.

En nuestro caso hemos realizado un *ping* desde el *PC1* a la dirección IP interna del *PC2*, es decir, la *10.24.2.51*. La ejecución de esta orden es suficiente para activar el túnel ya que en la regla hemos configurado que el tráfico, con cualquier protocolo, transmitido entre ambas redes locales pase a través de la VPN. Para comprobar que la conexión se ha establecido correctamente, desde cualquiera de los cortafuegos accedemos a la sección *Status*, seccionamos IPsec y en el apartado de *Overview* podemos observar el estado del túnel junto a toda la información de la conexión. Si nos aparece como *Established*, el túnel se ha podido establecer sin ningún problema (ver figura 7.1). Además en este apartado podemos conectar o desconectar manualmente la conexión sin necesidad de generar tráfico a través de ella, como se muestra en la figura 7.2.

| IPsec Status |                  |   |   |                 |  |  |  |
|--------------|------------------|---|---|-----------------|--|--|--|
| ID           | Description      | Local   | Remote  | Role            | Timers   | Algo   | Status   |
| con1 #1      | Túnel a pfSense2 | ID: 172.16.0.2<br>Host: 172.16.0.2:500<br>SPI: eb4b493e82d59a2d | ID: 192.168.254.2<br>Host: 192.168.254.2:500<br>SPI: 4f3449b6cd829b55 | IKEv2 Initiator | Rekey: 25370s (07:02:50)<br>Reauth: Disabled                                 | AES_CBC (256)<br>HMAC_SHA2_256_128<br>PRF_HMAC_SHA2_256<br>MODP_2048 | Established<br>14 seconds<br>(00:00:14) ago<br>Disconnect P1   |
| ID           | Description      | Local   | SPI(s)  | Remote          | Times  | Algo   | Stats  |
| con1: #2     | Túnel a pfSense2 | 10.24.1.0/24  | Local: c58fe928<br>Remote: c08abd2d                                   | 10.24.2.0/24    | Rekey: 3153s (00:52:33)<br>Life: 3586s (00:59:46)<br>Install: 14s (00:00:14) | AES_GCM_16 (256)<br>IPComp: None                                     | Bytes-In: 0 (0 B)<br>Packets-In: 0<br>Bytes-Out: 0 (0 B)<br>Packets-Out: 0<br>Installed<br>Disconnect P2 |

Figura 7.1: Comprobación del estado del túnel IPsec

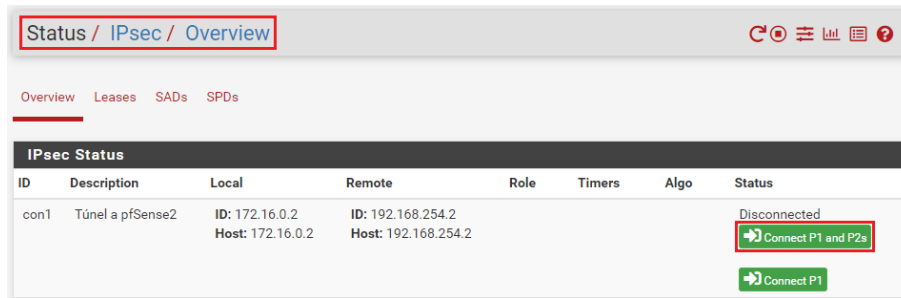


Figura 7.2: Conectar el túnel IPsec manualmente

A modo de comparación se ha realizado el mismo *ping* antes de configurar el túnel y como podemos observar en la figura 7.3, no logramos alcanzar el PC2 desde el PC1. Sin embargo, cuando el túnel está activo podemos llegar sin problemas tal y como se puede observar en la figura 7.4.

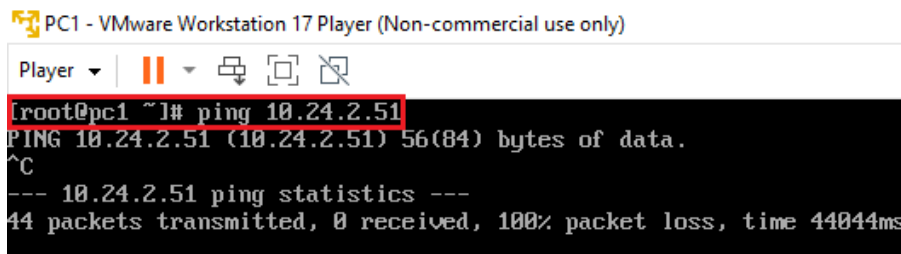


Figura 7.3: Orden *ping* desde el PC1 al PC2 antes de crear el túnel IPsec

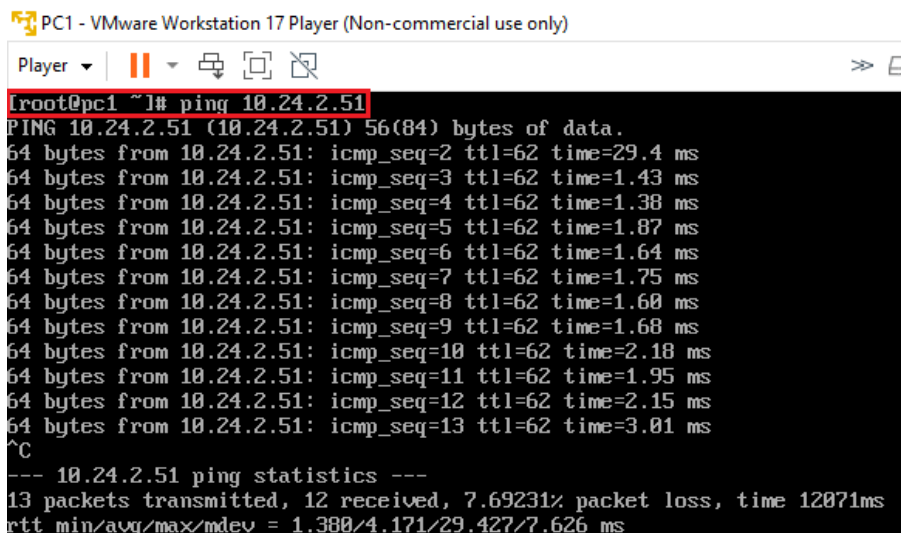


Figura 7.4: Orden *ping* desde el PC1 al PC2 con el túnel IPsec creado y establecido

## 7.2 Puesta en marcha de la VPN con OpenVPN

El túnel OpenVPN se activa automáticamente tras terminar su configuración, si no hay errores, no es necesaria ninguna acción concreta para que el túnel comience a funcionar. Podemos comprobar el estado de este accediendo a la sección *Status* y seleccionando OpenVPN. Si el estado es *Connected* (*Success*) como se

muestra en la figura 7.5, la conexión se ha establecido correctamente. Podemos realizar un *ping* entre los *PCs* para comprobar que se pueden alcanzar entre ellos sin problemas.

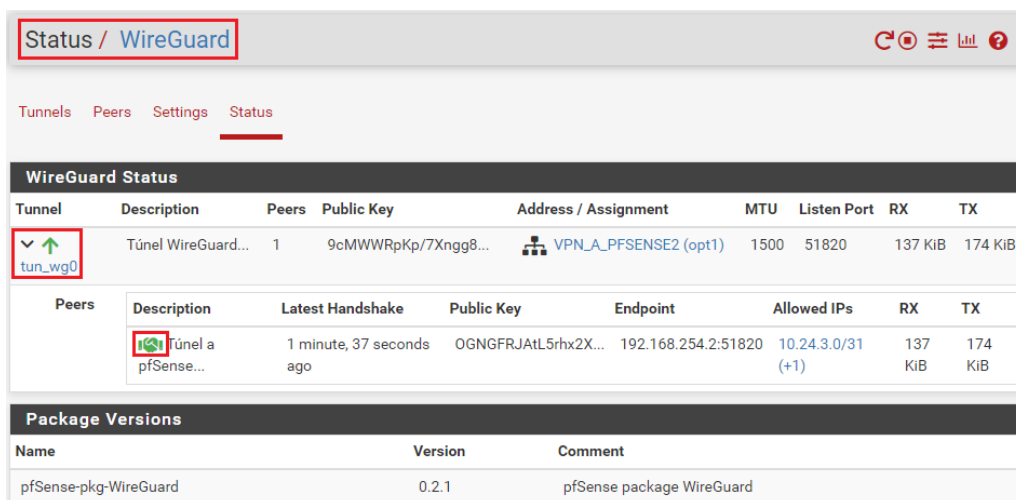


| Name                                       | Status                 | Last Change               | Local Address       | Virtual Address | Remote Host     | Bytes Sent | Bytes Received | Service |
|--|------------------------|---------------------------|---------------------|-----------------|-----------------|------------|----------------|---------|
| ovpnc1<br>Túnel OpenVPN a<br>pfSense1 UDP4 | Connected<br>(Success) | Sat Jun 8 0:41:51<br>2024 | 192.168.254.2:18581 | 10.24.3.2       | 172.16.0.2:1194 | 7 KiB      | 6 KiB          |         |

Figura 7.5: Comprobación del estado del túnel OpenVPN

## 7.3 Puesta en marcha de la VPN con WireGuard

La VPN con WireGuard, al igual que con OpenVPN, comienza a funcionar directamente tras terminar su configuración, sin realizar ninguna acción específica. Para comprobar el estado de la conexión podemos acceder a la sección *Status* y seleccionar WireGuard. Como se muestra en la figura 7.6, podemos observar los diferentes datos y parámetros del túnel, como el tráfico transmitido y recibido a través de él. Si nos aparece la flecha verde situada junto al nombre del túnel, la conexión se ha establecido correctamente. Podemos realizar un *ping* entre los *PCs*, al igual que en los casos anteriores, y comprobar como el tráfico alcanza perfectamente su destino utilizando el túnel.



| Tunnel  | Description        | Peers | Public Key          | Address / Assignment  | MTU  | Listen Port | RX      | TX      |
|---------|--------------------|-------|---------------------|-----------------------|------|-------------|---------|---------|
| tun_wg0 | Túnel WireGuard... | 1     | 9cMWWRpKp/7Xngg8... | VPN_A-PFSENSE2 (opt1) | 1500 | 51820       | 137 KiB | 174 KiB |

| Peers | Description           | Latest Handshake            | Public Key          | Endpoint            | Allowed IPs          | RX         | TX         |
|-------|-----------------------|-----------------------------|---------------------|---------------------|----------------------|------------|------------|
|       | Túnel a<br>pfSense... | 1 minute, 37 seconds<br>ago | OGNGFRJAtL5rhx2X... | 192.168.254.2:51820 | 10.24.3.0/31<br>(+1) | 137<br>KiB | 174<br>KiB |

| Name                  | Version | Comment                   |
|-----------------------|---------|---------------------------|
| pfSense-pkg-WireGuard | 0.2.1   | pfSense package WireGuard |

Figura 7.6: Comprobación del estado del túnel WireGuard





---

---

# CAPÍTULO 8

## Pruebas

---

Con la finalidad de analizar el correcto funcionamiento de la solución y comparar el rendimiento entre cada una de las configuraciones, se realizarán distintas pruebas. Estas pruebas se dividirán en dos secciones. Por una parte, se confirmará que el tráfico se trasmite correctamente entre las redes locales de cada uno de los cortafuegos y se comparará el rendimiento de cada uno de los protocolos VPN utilizados. Por otra parte, se analizará el tráfico que fluye por los túneles para observar el encapsulado realizado por cada uno de los protocolos.

### 8.1 Pruebas de conectividad y rendimiento de los túneles VPN

---

Para comparar el rendimiento entre los distintos túneles configurados en la solución se realizarán dos pruebas que a su vez funcionarán como comprobación del correcto flujo del tráfico entre ambas redes. Primero se medirá el ancho de bando máximo en cada túnel VPN utilizando la herramienta *iperf3*. A continuación, se comparará el tiempo necesario para transferir un archivo relativamente pesado a través de los distintos túneles con el comando *scp*.

Cabe destacar que los resultados de ambas pruebas estarán limitados en comparación a una implementación real de la solución. Estas limitaciones se deben al entorno virtual utilizado combinado con las restricciones a niveles de uso de recursos del sistema por parte de cada una de las máquinas virtuales. Sin embargo, los resultados seguirán siendo suficientemente representativos de los que obtendríamos en un entorno real.

#### 8.1.1. Medida de ancho de banda con *iperf3*

*iperf* es una herramienta de código abierto y gratuita que sirve para evaluar el rendimiento de una red en tiempo real. Este software destaca en la medición del máximo ancho de banda alcanzable en una red, que es en lo que se centrarán nuestras pruebas [43]. Concretamente se empleará la última versión, la *iperf3*.

Para poder realizar las pruebas, instalamos la herramienta en ambos PCs con el comando *sudo yum install iperf3*. A continuación, necesitamos determinar cual

de las máquinas se comportará como servidor y cual como cliente. En nuestro caso utilizaremos el *PC2* como servidor y el *PC1* como cliente, ya que como el *PC1* no cuenta con interfaz gráfica, realiza un consumo menor de los recursos disponibles, permitiendo que la herramienta pueda utilizar más recursos para generar más tráfico hacia el servidor. De esta forma, podemos conseguir unos resultados mejores y más próximos a los de una implementación real.

Por tanto, ejecutamos la herramienta en el *PC2* como servidor con el comando *iperf3 -s*, quedando a la espera de que un cliente establezca la conexión (figura 8.1). Mientras que, en el *PC1*, utilizamos el comando *iperf3 -c 10.24.2.51* para que realice la función de cliente comenzando la comunicación con el servidor (figura 8.2).

```

root@pc2:~# iperf3 -s
-----
Server listening on 5201
-----
Accepted connection from 10.24.1.52, port 48876
[ 5] local 10.24.2.51 port 5201 connected to 10.24.1.52 port 48886
[ ID] Interval           Transfer             Bitrate
[ 5]  0.00-1.00   sec    12.4 MBytes    104 Mbits/sec
[ 5]  1.00-2.00   sec    14.5 MBytes    122 Mbits/sec
[ 5]  2.00-3.01   sec    13.2 MBytes    109 Mbits/sec
[ 5]  3.01-4.00   sec    13.0 MBytes    110 Mbits/sec
[ 5]  4.00-5.00   sec    13.5 MBytes    113 Mbits/sec
[ 5]  5.00-6.00   sec    13.6 MBytes    114 Mbits/sec
[ 5]  6.00-7.00   sec    13.8 MBytes    116 Mbits/sec
[ 5]  7.00-8.01   sec    13.5 MBytes    112 Mbits/sec
[ 5]  8.01-9.00   sec    10.5 MBytes    89.0 Mbits/sec
[ 5]  9.00-10.00  sec    11.0 MBytes    92.3 Mbits/sec
[ 5] 10.00-10.04  sec     419 KBytes    95.6 Mbits/sec
-----
[ ID] Interval           Transfer             Bitrate
[ 5]  0.00-10.04  sec    129 MBytes    108 Mbits/sec
receiver

```

Figura 8.1: Ejecución de *iperf* como servidor en el PC2

```

PC1 - VMware Workstation 17 Player (Non-commercial use only)
Player
root@pc1 ~# iperf3 -c 10.24.2.51
Connecting to host 10.24.2.51, port 5201
[ 5] local 10.24.1.52 port 48886 connected to 10.24.2.51 port 5201
[ ID] Interval           Transfer             Bitrate      Retr  Cwnd
[ 5]  0.00-1.00   sec    16.7 MBytes    140 Mbits/sec   73   465 KBytes
[ 5]  1.00-2.00   sec    13.8 MBytes    115 Mbits/sec   25   130 KBytes
[ 5]  2.00-3.00   sec    12.5 MBytes    105 Mbits/sec    0   191 KBytes
[ 5]  3.00-4.00   sec    13.8 MBytes    115 Mbits/sec    6   175 KBytes
[ 5]  4.00-5.00   sec    13.8 MBytes    115 Mbits/sec   11   143 KBytes
[ 5]  5.00-6.00   sec    13.8 MBytes    115 Mbits/sec    0   204 KBytes
[ 5]  6.00-7.00   sec    13.8 MBytes    115 Mbits/sec    5   174 KBytes
[ 5]  7.00-8.00   sec    12.5 MBytes    105 Mbits/sec    7   185 KBytes
[ 5]  8.00-9.00   sec    11.2 MBytes    94.4 Mbits/sec   25   100 KBytes
[ 5]  9.00-10.00  sec    11.2 MBytes    94.3 Mbits/sec   20   103 KBytes
-----
[ ID] Interval           Transfer             Bitrate      Retr
[ 5]  0.00-10.00  sec    133 MBytes    111 Mbits/sec  172
[ 5]  0.00-10.04  sec    129 MBytes    108 Mbits/sec
sender
iperf Done.
receiver

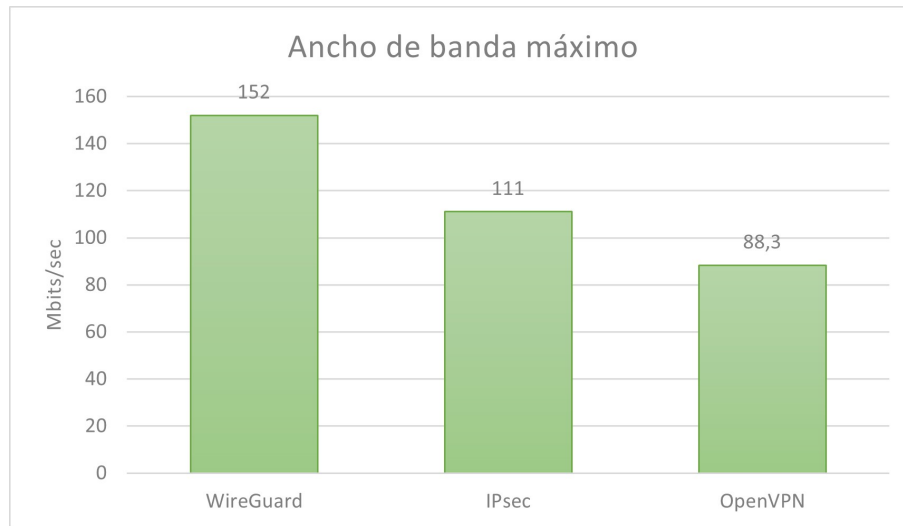
```

Figura 8.2: Ejecución de *iperf* como cliente en el PC1

Tras la ejecución de la herramienta, esta indica los distintos resultado para diez intervalos de un segundo y presenta un resultado final con el ancho de banda promedio para los diez segundo de ejecución totales. Este último dato, que

aparece como *Bitrate*, es el que se utilizará para poder comparar los distintos túneles.

Los resultado de ancho de banda promedio de la ejecución de *iperf3* en cada una de las configuraciones se muestran en la figura 8.3 a modo de gráfico.



**Figura 8.3:** Gráfico de anchos de banda máximos de los túneles

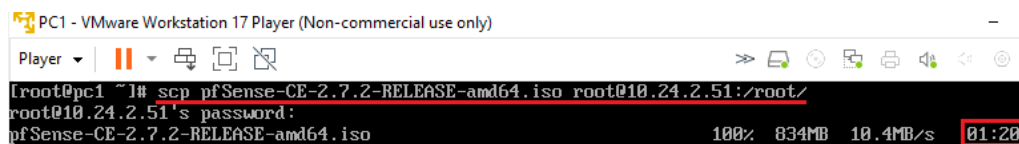
Analizando los resultados se observa que WireGuard toma la delantera en lo que a rendimiento se refiere. Este resultado coincide con lo esperado tras el análisis teórico realizado en apartados anteriores del trabajo, ya que dado a el uso de un cifrado más ligero este protocolo consigue aumentar la velocidad de la VPN. El segundo lugar lo ocupa IPsec, obteniendo un ancho de banda considerablemente alto a pesar de que el protocolo de cifrado utilizados es AES-256, que supone un alto nivel de seguridad pero utilizando un elevado nivel de computo. En último lugar se encuentra OpenVPN, que ha resultado ser el más irregular de los tres ya que a lo largo de diversas ejecuciones se han obtenido anchos de banda desde los casi los 100 Mbits/sec hasta debajo de los 70 Mbits/sec, dejando como promedio el resultado que se muestra en el gráfico.

### 8.1.2. Transferencia de archivos con scp

A modo de segunda prueba, como ya se ha mencionado anteriormente, se va a medir el tiempo necesario transferencia para un archivo utilizando *scp*. Este comando de Linux permite realizar una transferencia de archivos a través de la red de forma segura [44]. El tiempo de ejecución del comando *scp* no incluye solamente la transferencia del archivo por la red, sino que también incluye el almacenado del archivo en el disco entre otras operaciones internas. Sin embargo, como se va a realizar la transferencia bajo las mismas condiciones para cada uno de los túneles, es decir, el mismo archivo entre las mismas máquinas origen y destino, las diferencias en cuanto al tiempo de ejecución recaen en las prestaciones de la red.

Para realizar las pruebas se transferirá desde el *PC1* al *PC2* un archivo con un tamaño considerable, en este caso, se ha escogido la imagen ISO de pfSense

que tiene un peso de 834MB. Se podría haber utilizado cualquier otro archivo siempre y cuando se utilice el mismo para las pruebas en los tres túneles. Para realizar esta transferencia ejecutamos en el *PC1* el comando `scp pfSense-CE-2.7.2-RELEASE-amd64.iso root@10.24.2.51:/root/`. Una vez termine la ejecución, el tiempo que ha tardado en realizar la transferencia se muestra al final de la línea de salida de la orden (ver figura 8.4).



```
PC1 - VMware Workstation 17 Player (Non-commercial use only)
Player
[root@pc1 ~]# scp pfSense-CE-2.7.2-RELEASE-amd64.iso root@10.24.2.51:/root/
root@10.24.2.51's password:
pfSense-CE-2.7.2-RELEASE-amd64.iso 100% 834MB 10.4MB/s 01:20
```

Figura 8.4: Ejecución de *scp* en el *PC1*

Los tiempos resultantes de ejecutar el comando utilizando cada uno de los túneles se muestra en el gráfico de la figura 8.5.

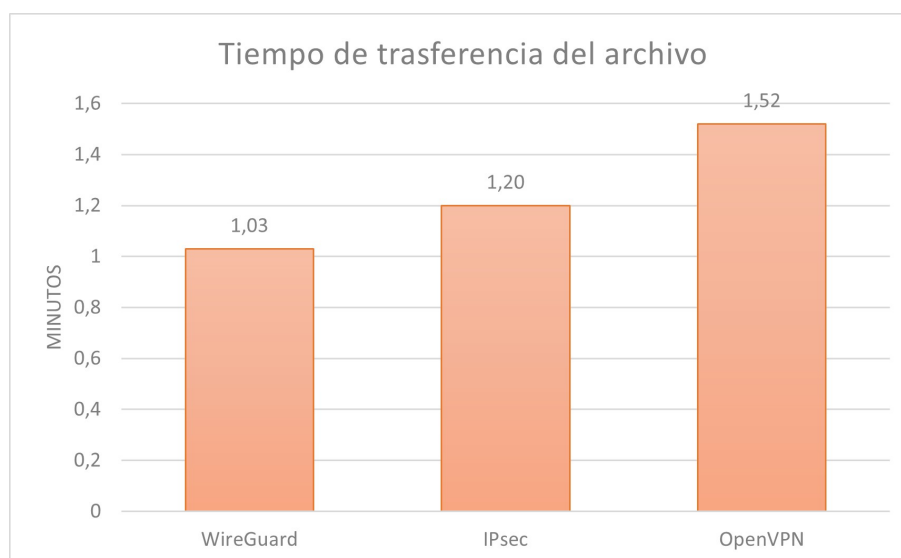


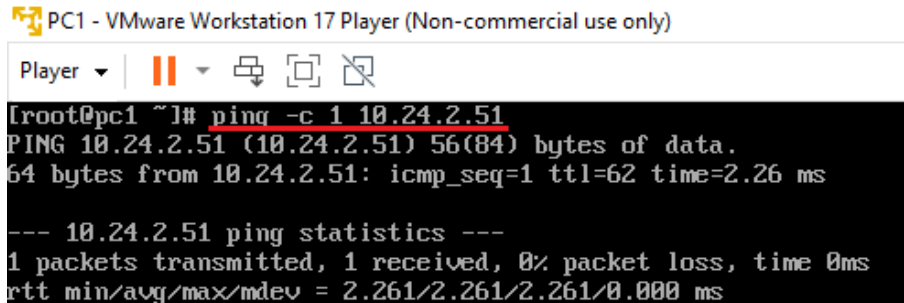
Figura 8.5: Gráfico de tiempos de transferencia del archivo en los túneles

Los tiempos de transferencia obtenidos reafirman los resultados obtenidos con la herramienta *iperf*. El rendimiento observado sitúa a WireGuard como la VPN más rápida, seguida por IPsec y dejando OpenVPN de nuevo en último lugar. A lo largo de la transferencia del archivo se han observado nuevamente irregularidades de ancho de banda para este último protocolo, mientras que WireGuard y IPsec se han mantenido estables durante la transmisión.

## 8.2 Validación del encapsulado del tráfico en los túneles VPN

Con la finalidad de analizar el funcionamiento de cada uno de los túneles y observar el distinto encapsulado proporcionado por cada uno de ellos se van a realizar las capturas de un mismo paquete tanto fuera como dentro del túnel.

Para ello, se utilizará el comando `ping` con la opción `-c 1` para enviar un único paquete ICMP desde el *PC1* al *PC2* (ver figura 8.6). Este orden realizará el envío de un paquete *ICMP request* desde el *PC1* al *PC2* que será respondido por un *ICMP reply* en sentido inverso.



```

PC1 - VMware Workstation 17 Player (Non-commercial use only)
Player | [Pause] [Copy] [Paste] [Close]
[root@pc1 ~]# ping -c 1 10.24.2.51
PING 10.24.2.51 (10.24.2.51) 56(84) bytes of data:
64 bytes from 10.24.2.51: icmp_seq=1 ttl=62 time=2.26 ms

--- 10.24.2.51 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 2.261/2.261/2.261/0.000 ms
  
```

Figura 8.6: Orden `ping -c 1` en el PC1

Para capturar estos paquetes dentro del túnel, utilizaremos la herramienta *Packet Sniffer* del router MikroTik seleccionando la interfaz *ether3* en el que se encuentran conectado el cortafuegos *pfSense2* por su interfaz WAN, permitiéndonos recoger el tráfico que pasa el túnel (ver figura 8.7). Al iniciar la herramienta, esta generará un archivo de captura con extensión *.pcap*, que descargaremos en el *PC anfitrión* y, posteriormente, analizaremos utilizando el software *Wireshark*.

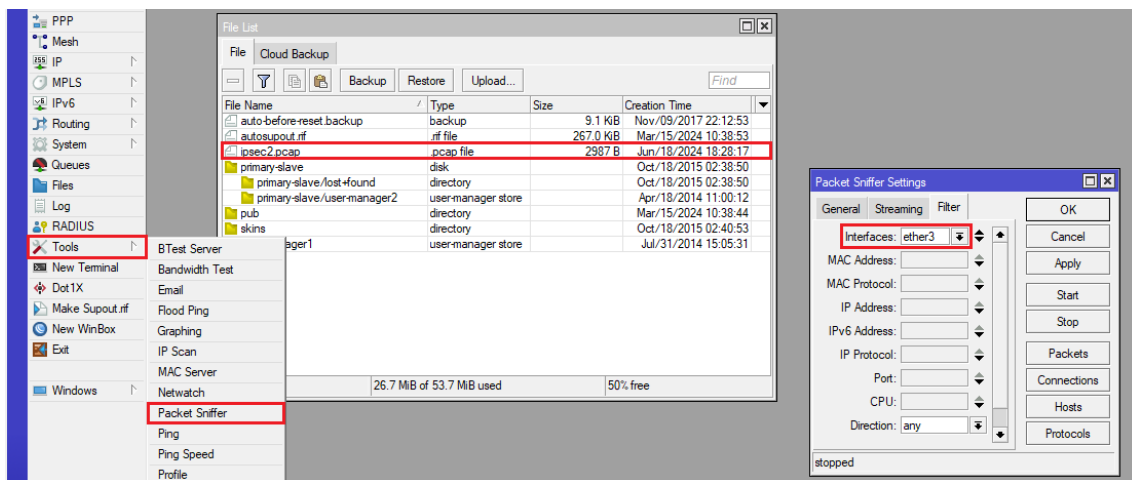


Figura 8.7: Orden `ping -c 1` en el PC1

Mientras que para capturar los paquetes fuera del túnel, utilizaremos directamente desde el *PC2*, el programa *Wireshark* para recoger y analizar el tráfico que pasa por la interfaz *ens37*. De esta forma podemos observar el tráfico sin encapsular ya que fluye por la red interna.

En el caso de IPsec, podemos ver en la figura 8.8 como capturamos ambos paquetes del protocolo ICMP mencionados previamente. Podemos observar que estos paquetes tienen como fuente y destino las direcciones IP privadas de cada uno de los PCs, a pesar de que pertenecen a dos redes locales diferentes. De esta forma, confirmamos que el túnel establece la interconexión entre estas redes.

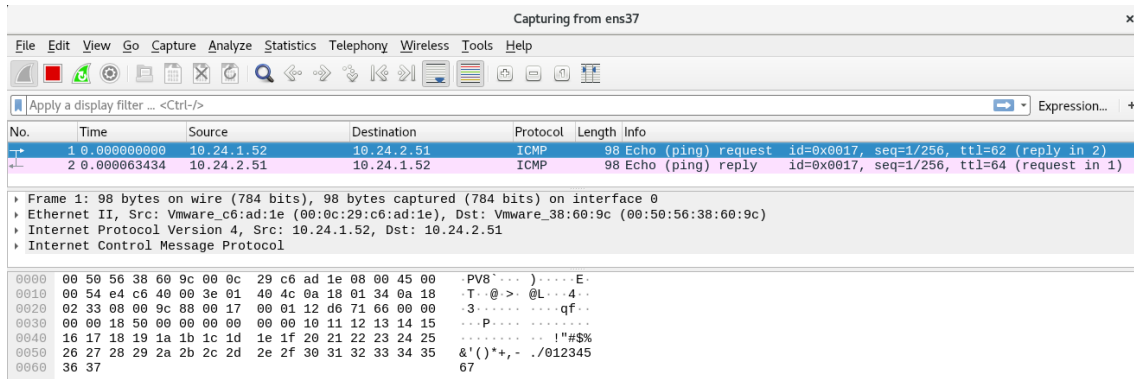


Figura 8.8: Captura Wireshark en la interfaz *ens37* del PC2 para IPsec

Mientras que si analizamos el contenido de la captura realizada sobre esos mismos paquetes pasando a través del túnel, observamos dos paquetes que han sido encapsulados por el protocolo *ESP* (*Encapsulating Security Payload*) (ver figura 8.9). Este protocolo se seleccionó durante la configuración de la fase 2 del túnel IPsec y es el encargado de encapsular y proteger el contenido que se trasmite por túnel (figura 6.57). Además, observando las direcciones origen y destino, vemos como el primero de los paquetes corresponde al *ICMP request* ya que se envían desde el *pfSense1* (172.16.0.2) al *pfSense2* (192.168.254.2) y el segundo paquete encapsula el *ICMP reply* ya que se trasmite en sentido opuesto (ver figura 8.9).

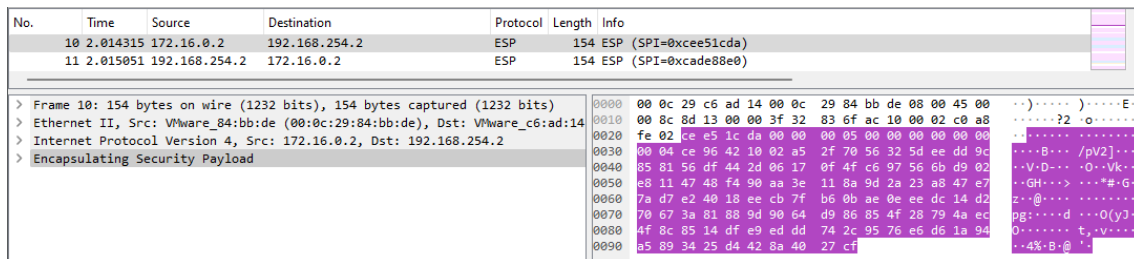


Figura 8.9: Captura Wireshark en la interfaz *ether3* del MikroTik para IPsec

Con lo que respecta a OpenVPN observamos un compartimiento equivalente al protocolo anterior. En la figura 8.10 se muestran los paquetes ICMP capturados desde el *PC2* y en la figura 8.11 podemos ver estos mismos paquetes encapsulados dentro del túnel. En este caso el protocolo utilizado para encapsular los paquetes es OpenVPN. También en la figura 8.11, podemos observar como los paquetes encapsulados aparecen como *MessageType: Unknown Message type [Malformed Packet]*. Esto es causado por el propio software *Wireshark* ya que no es capaz de analizar e interpretar algunos formatos de paquetes de ciertas versiones de protocolos, tal y como explica un desarrollador de la compañía **Netgate** en un foro oficial de acerca de este error [45]. Además, podemos descartar que se trate de un fallo en el protocolo OpenVPN ya que los cortafuegos son capaces de encapsular y desencapsular (cifrar y descifrar) correctamente el contenido que se trasmite, permitiendo el correcto flujo de paquetes por el túnel.

| No. | Time        | Source     | Destination | Protocol | Length | Info  |
|-----|-------------|------------|-------------|----------|--------|---|
| 1   | 0.000000000 | 10.24.1.52 | 10.24.2.51  | ICMP     | 98     | Echo (ping) request id=0x000c, seq=1/256, ttl=62 (reply in 2) |
| 2   | 0.000048182 | 10.24.2.51 | 10.24.1.52  | ICMP     | 98     | Echo (ping) reply id=0x000c, seq=1/256, ttl=64 (request in 1) |

Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0  
 Ethernet II, Src: Vmware\_c6:ad:1e (00:0c:29:c6:ad:1e), Dst: Vmware\_38:60:9c (00:50:56:38:60:9c)  
 Internet Protocol Version 4, Src: 10.24.1.52, Dst: 10.24.2.51  
 Internet Control Message Protocol

```

0000  00 50 56 38 60 9c 00 0c 29 c6 ad 1e 08 00 45 00  -PV8^... )....E
0010  00 54 20 19 40 00 3e 01 04 fa 0a 18 01 34 0a 18  -T @:>.....4..
0020  02 33 08 00 cf 2c 00 0c 00 01 85 c7 71 66 00 00  -3...>.....qf..
0030  00 00 64 c5 0e 00 00 00 00 00 10 11 12 13 14 15  -...d.....
0040  16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  -.....!""#%$
0050  26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  -&'()*+,-./012345
0060  36 37                                     67
  
```

Figura 8.10: Captura Wireshark en la interfaz *ens37* del PC2 para OpenVPN

| No. | Time     | Source        | Destination   | Protocol | Length | Info   |
|-----|----------|---------------|---------------|----------|--------|--|
| 22  | 4.522771 | 172.16.0.2    | 192.168.254.2 | OpenVPN  | 186    | MessageType: Unknown MessageType[Malformed Packet] |
| 23  | 4.523787 | 192.168.254.2 | 172.16.0.2    | OpenVPN  | 186    | MessageType: Unknown MessageType[Malformed Packet] |

Frame 22: 186 bytes on wire (1488 bits), 186 bytes captured (1488 bits)  
 Ethernet II, Src: Vmware\_84:bb:de (00:0c:29:84:bb:de), Dst: Vmware\_c6:ad:14  
 Internet Protocol Version 4, Src: 172.16.0.2, Dst: 192.168.254.2  
 User Datagram Protocol, Src Port: 1194, Dst Port: 19678  
 OpenVPN Protocol  
 [Malformed Packet: OpenVPN]

```

0000  00 0c 29 c6 ad 14 00 0c 29 84 bb de 08 00 45 00  -).....?.....E
0010  00 ac 6e ed 00 00 3f 11 a1 96 ac 10 00 02 c0 a8  -n.....?.....
0020  fe 02 04 aa 4c de 00 98 4b 71 6e cb 97 02 e8 25  -L...K...%
0030  05 84 ad 01 98 a3 d8 21 12 1c 4a d6 25 03 56 5c  -.....:..J.%V
0040  58 04 9c 81 09 83 40 55 c8 6f 91 57 47 50 84 cb  -X.....@..o..MGP
0050  13 ef c8 5f 7e 5f 67 d2 25 06 c2 92 34 39 e3 98  -.....g %...49
0060  a3 83 eb b8 2d e4 96 67 3b 4e 53 ea 68 4c de d5  -.....;MS..hL
0070  9c 30 b8 71 76 6c 8f e6 f1 74 9e c1 9e be 3a f9  -0..qv1...t.....
0080  db d7 16 3e 7c 99 ed a4 5e ae c6 e5 13 14 6b 6b  ->|.....kk
0090  de 93 ce 60 2d 1d 35 48 5c 9e 8e b6 af fe 4d 39  -...>..5H \.....M9
00a0  30 e7 85 0a 10 fe c6 b9 10 0e 1b d5 1b 26 25 d7  -0.....5H \.....M9
00b0  81 33 27 33 7e ce ae 4c 80 26                                     -3'3...L &
  
```

Figura 8.11: Captura Wireshark en la interfaz *ether3* del MikroTik para OpenVPN

En cuanto al protocolo WireGuard, podemos observar en la figura 8.12, como al capturar el tráfico desde el *PC2*, la dirección IP origen de la petición ICMP y, por tanto, también la dirección destino de la respuesta, han sido sustituidas por la dirección de la interfaz virtual que se configuró para el túnel en el *pfSense1* (figura 6.91). Esto se debe a que en ambos extremos se configuraron rutas para que el tráfico dirigido al túnel se enviase por esta nueva interfaz. Sin embargo, la dirección IP del *PC2* no es sustituida por la de la interfaz para el túnel del *pfSense2* porque estamos analizando el tráfico desde dentro de la red privada del mismo. Si analizásemos el tráfico desde el *PC1*, entonces, sería la dirección del *PC2* la que estaría sustituida.

| No. | Time        | Source     | Destination | Protocol | Length | Info  |
|-----|-------------|------------|-------------|----------|--------|---|
| 1   | 0.000000000 | 10.24.3.0  | 10.24.2.51  | ICMP     | 98     | Echo (ping) request id=0x313a, seq=1/256, ttl=62 (reply in 2) |
| 2   | 0.000067340 | 10.24.2.51 | 10.24.3.0   | ICMP     | 98     | Echo (ping) reply id=0x313a, seq=1/256, ttl=64 (request in 1) |

Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0  
 Ethernet II, Src: Vmware\_c6:ad:1e (00:0c:29:c6:ad:1e), Dst: Vmware\_38:60:9c (00:50:56:38:60:9c)  
 Internet Protocol Version 4, Src: 10.24.3.0, Dst: 10.24.2.51  
 Internet Control Message Protocol

```

0000  00 50 56 38 60 9c 00 0c 29 c6 ad 1e 08 00 45 00  -PV8^... )....E
0010  00 54 34 78 40 00 3e 01 ee ce 0a 18 03 00 0a 18  -T4x@>.....
0020  02 33 08 00 3f 8c 31 3a 00 01 b0 ce 71 66 00 00  -3?>1:.....qf..
0030  00 00 a3 30 03 00 00 00 00 00 10 11 12 13 14 15  -...0.....
0040  16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  -.....!""#%$
0050  26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  -&'()*+,-./012345
0060  36 37                                     67
  
```

Figura 8.12: Captura Wireshark en la interfaz *ens37* del PC2 para WireGuard

No obstante, si analizamos el tráfico capturado dentro del túnel como se muestra en la figura 8.13, observamos más de dos paquetes, esto se debe al envío constantes de paquetes realizado por el protocolo WireGuard. Estos paquetes, conocidos como *Keepalive*, son utilizados para mantener la conexión establecida y detectar posibles desconexiones, optimizando así el rendimiento de la VPN. Para distinguir estos paquetes de los que nos competen, podemos examinar su tamaño, ya que los paquetes enviados para mantener la conexión tiene un tamaño de 106 bytes. De esta forma, podemos distinguir dos paquetes de 170 bytes que



corresponden a la petición y la respuesta ICMP encapsuladas (marcados con un rectángulo rojo en la figura 8.13). Además, encontramos como, en esta ocasión, el encapsulado de estos paquetes se realiza utilizando el propio protocolo WireGuard.

| No. | Time     | Source        | Destination   | Protocol  | Length | Info   |
|-----|----------|---------------|---------------|-----------|--------|--|
| 47  | 3.900287 | 172.16.0.2    | 192.168.254.2 | WireGuard | 170    | Transport Data, receiver=0xC35E3135, counter=162, datalen=96 |
| 48  | 3.901072 | 192.168.254.2 | 172.16.0.2    | WireGuard | 170    | Transport Data, receiver=0x09C0F608, counter=162, datalen=96 |
| 49  | 3.975324 | 192.168.254.2 | 172.16.0.2    | WireGuard | 106    | Transport Data, receiver=0x09C0F608, counter=163, datalen=32 |
| 50  | 3.975789 | 172.16.0.2    | 192.168.254.2 | WireGuard | 106    | Transport Data, receiver=0xC35E3135, counter=163, datalen=32 |

```

> Frame 47: 170 bytes on wire (1360 bits), 170 bytes captured (1360 bits) on 0
  0000 00 0c 29 c6 ad 14 00 0c 29 84 bb de 08 00 45 00 ..).....).....E
  0010 00 9c b2 12 00 00 3f 11 5e 81 ac 10 00 02 c0 a8 .....?..^.....
  0020 fe 02 ca 6c ca 6c 00 88 47 10 04 00 00 00 35 31 ...l.l.G....51
  0030 5e c3 a2 00 00 00 00 00 00 00 ec a2 b9 33 a0 95 .....Q....3..
  0040 84 7e 98 06 b3 1c cb 51 47 50 09 af 0a da f6 ff .....n...jpp...
  0050 10 42 66 7c 7d c3 41 90 5b 3f b1 a4 5b cc 34 83 .Bf]}.A.[?..[.4
  0060 32 88 82 ab 39 2a 69 7b d1 62 9f 9b d7 c6 25 68 2...9*(i{[b...%h
  0070 db b3 e7 13 90 9e 93 a6 ea bf 36 47 1f 9a 09 39 .....6G...9
  0080 88 76 fc f6 69 78 6b e3 e3 95 a5 0d b4 f0 68 bc .v..ixk...*...h
  0090 ef 11 26 21 70 07 f7 ee e7 0a ...&!p... ..
  00a0

```

Figura 8.13: Captura Wireshark en la interfaz *ether3* del MikroTik para WireGuard



---

## CAPÍTULO 9

# Conclusiones

---

A lo largo del trabajo se han presentado y analizado, desde un punto de vista teórico, las distintas alternativas para la interconexión segura de redes, comparando las conexiones VPN más utilizadas actualmente.

Además, se ha planteado un esquema de red virtual en el que se conectan dos redes entre si, utilizando dos cortafuegos pfSense bajo tres configuraciones distintas. También, se han configurado las máquinas virtuales VMware implicadas simulando un entorno real. Cada una de las tres configuraciones realizadas utiliza un protocolo VPN distinto para establecer la conexión, de forma que nos ha permitido comparar estos protocolos de forma empírica. Los protocolos utilizados han sido IPsec, OpenVPN y WireGuard.

Se han realizado distintas pruebas para comprobar el correcto funcionamiento de los túneles establecidos y comparar su rendimiento mediante las herramientas *iperf* y *scp*. Observando los resultados se ha concluido que WireGuard es la opción más rápida y, por tanto, la más recomendada si se buscan altas velocidades en la VPN. Le sigue IPsec, mostrando un buen balance entre rendimiento y elevados niveles de seguridad, utilizando los algoritmos de cifrado que se consideran más seguros actualmente. Lo que coloca este protocolo como una opción adecuada si se busca estabilidad y velocidad, a la vez que elevados niveles de seguridad. En último lugar, encontramos OpenVPN, para el cual se ha observado un ancho de banda inestable y unos bajos niveles de seguridad. Cabe destacar que para aumentar la seguridad de esta VPN se requiere de la configuración de certificados, incrementando considerablemente la complejidad de configuración. Este motivo sumado a la inestabilidad en cuanto rendimiento, convierten a este protocolo en una opción no recomendable para la solución propuesta.

Adicionalmente, se han realizado pruebas para verificar que el encapsulado realizado por los protocolos utilizados es correcto, analizando el tráfico dentro y fuera del túnel con el software Wireshark.

Con todo lo comentado, podemos concluir que se ha logrado alcanzar los distintos objetivos propuestos. Consiguiendo plantear, ejecutar y evaluar una solución que permite la interconexión segura de redes utilizando cortafuegos pfSense. Esta solución supone una alternativa segura, eficiente y de coste reducido para proporcionar conectividad en pequeñas empresas.

---

## 9.1 Relación del trabajo desarrollado con los estudios cursados

---

Las tareas que se han realizado a lo largo de este proyecto han puesto en práctica numerosos conocimientos adquiridos en el transcurso del grado en Ingeniería Informática. Concretamente, los principales conceptos aplicados se encuentran relacionados con la seguridad de redes y sistemas. Los conocimientos clave para llevar a cabo este trabajo han sido los fundamentos sobre conexiones VPN, proporcionados principalmente por la asignatura *Redes Comparativas*. Además, se ha requerido de conocimientos sobre los distintos protocolos de red, el encapsulamiento de paquetes y la configuración de redes de área local, los cuales han sido adquiridos en distintas asignaturas como *Redes* y *Diseño y configuración de redes de área local*.

Además, la asignatura *Seguridad de redes y sistemas informáticos* proporcionó las nociones necesarias acerca del funcionamiento de los cortafuegos y la seguridad de una red.

Por último, cabe mencionar que la elaboración de este proyecto ha aportado en el desarrollo de algunas competencias transversales, entre las cuales se encuentran la planificación y gestión del tiempo, el análisis y resolución de problemas y el conocimiento de problemas contemporáneos.

# Bibliografía

---

- [1] Wikipedia. pfSense, 29/05/2024. Consultado en <https://es.wikipedia.org/wiki/PfSense>.
- [2] Cloudflare. ¿Qué es un firewall de nueva generación (NGFW)?, 2024. Consultado en <https://www.cloudflare.com/es-es/learning/security/what-is-next-generation-firewall-ngfw/>.
- [3] Gartner. Network Firewalls Reviews and Ratings, 2024. Consultado en <https://www.gartner.com/reviews/market/network-firewalls>.
- [4] Mario Montoya. FIREWALLS DE HARDWARE VS FIREWALLS DE SOFTWARE, 25/05/2021. Consultado en <https://blog.netdatanetworks.com/firewalls-de-hardware-vs-firewalls-de-software>.
- [5] ITcSystem. Firewall de hardware vs. Firewall de software: ¿Cuál es la mejor opción?, 02/03/2023. Consultado en <https://www.itcsystem.es/firewall-de-hardware-vs-firewall-de-software-cual-es-la-mejor-opcion/>.
- [6] Zenarmor. What Are The Best Open Source Firewalls?, 25/03/2024. Consultado en <https://www.zenarmor.com/docs/network-security-tutorials/best-open-source-firewalls>.
- [7] Emily Nemchick. Protocolos VPN: descripción y comparación, 22/09/2023. Consultado en <https://www.avast.com/es-es/c-vpn-protocols>.
- [8] Álvaro Marín García. Creación de un nodo multi-VPN en la nube para el ámbito empresarial, 17/07/2023. Consultado en <https://riunet.upv.es/handle/10251/196618>.
- [9] José Alapont Casañ. Cortafuegos y VPN para pymes con Raspberry, 15/07/2022. Consultado en <https://riunet.upv.es/handle/10251/186020>.
- [10] Jesús Melo Solanes. Introducción de aspectos de seguridad en una vivienda inteligente, 15/07/2015. Consultado en <https://riunet.upv.es/handle/10251/54076>.
- [11] TrustRadius. Best Virtualized Next-Generation Firewalls - VM Series Alternatives for Small Businesses, 2024. Consultado en <https://www.trustradius.com/products/paloalto-networks-virtualized-next-generation-firewalls/competitors>.

- 
- [12] Amal Joby. Best Firewall Software, 2024. Consultado en <https://www.g2.com/categories/firewall-software>.
- [13] Cloudflare. ¿Qué es la tunelización? | Tunelización en redes, 2024. Consultado en <https://www.cloudflare.com/es-es/learning/network-layer/what-is-tunneling/>.
- [14] Fortinet. Remote Access VPN, 2024. Consultado en <https://www.fortinet.com/resources/cyberglossary/remote-access-vpn>.
- [15] Perimeter 81. Remote Access vs. Site-To-Site VPN: Which One Is Better?, 26/11/2023. Consultado en <https://www.perimeter81.com/blog/network/remote-access-vs-site-to-site-vpn>.
- [16] GeeksforGeeks. Difference between site to site VPN and remote access VPN, 18/03/2023. Consultado en <https://www.geeksforgeeks.org/difference-between-site-to-site-vpn-and-remote-access-vpn/>.
- [17] Palo Alto Networks. What Are the Different Types of VPN Protocols?, 2024. Consultado en <https://www.paloaltonetworks.com/cyberpedia/types-of-vpn-protocols>.
- [18] VPN.com. All Of The VPN Protocols Explained, 07/05/2024. Consultado en <https://www.vpn.com/privacy/vpn-protocols/>.
- [19] Monique Danao. 6 Common VPN Protocols Explained, 06/06/2024. Consultado en <https://www.forbes.com/advisor/business/software/vpn-protocols/>.
- [20] KIO. Conoce los tipos de VPN y sus protocolos, 2024. Consultado en <https://www.kio.tech/blog/data-center/tipos-de-vpn-y-sus-protocolos>.
- [21] Tim Mocan. Cifrado de VPN (Todo lo Que Necesita Saber), 29/08/2019. Consultado en <https://www.cactusvpn.com/es/la-guia-para-principiantes-de-vpn/cifrado-de-vpn/>.
- [22] Netgate. pfSense Documentation, 31/05/2024. Consultado en <https://docs.netgate.com/pfsense/en/latest/>.
- [23] WunderTech. pfSense vs. OPNsense: Complete Firewall Comparison, 10/05/2024. Consultado en <https://www.wundertech.net/pfsense-vs-opnsense/>.
- [24] Deciso. Welcome to OPNsense's documentation!, 2024. Consultado en <https://docs.opnsense.org>.
- [25] Antanas Rimeikis. ¿Qué es el cifrado de una VPN y cómo funciona?, 12/06/2023. Consultado en <https://surfshark.com/es/blog/vpn-cifrado>.
- [26] Wikipedia. Hipervisor, 02/11/2023. Consultado en <https://es.wikipedia.org/wiki/Hipervisor>.

- 
- [27] StackScale. Hipervisores: definición, tipos y soluciones, 13/03/2024. Consultado en <https://www.stackscale.com/es/blog/hipervisores/>.
- [28] Andrea Flores. VMware vs. VirtualBox: ¡descubre cuál es el mejor virtualizador de sistemas operativos!, 30/01/2022. Consultado en <https://www.crehana.com/blog/transformacion-digital/vmware-vs-virtualbox/>.
- [29] Revolution Soft. VIRTUALBOX VS VMWARE: ¿CUÁL OFRECE MEJOR RENDIMIENTO?, 2023. Consultado en <https://blog.revolutionsoft.net/virtualbox-vs-vmware/>.
- [30] Māris B. RouterOS license keys, 08/02/2024. Consultado en <https://help.mikrotik.com/docs/display/ROS/RouterOS+license+keys>.
- [31] Normunds R. RouterOS Documentation, 16/04/2024. Consultado en <https://help.mikrotik.com/docs/display/ROS/RouterOS>.
- [32] Normunds R. Bridging and Switching, 13/05/2024. Consultado en <https://help.mikrotik.com/docs/display/ROS/Bridging+and+Switching>.
- [33] AlmaLinux. About AlmaLinux Wiki, 2024. Consultado en <https://wiki.almalinux.org>.
- [34] StackScale. 31 distribuciones de Linux populares, 29/06/2023. Consultado en <https://www.stackscale.com/es/blog/distribuciones-linux-populares/>.
- [35] pfSense. Download, 2024. Consultado en <https://www.pfsense.org/download/>.
- [36] Netgate. Installation Walkthrough, 29/06/2022. Consultado en <https://docs.netgate.com/pfsense/en/latest/install/install-walkthrough.html>.
- [37] MikroTik. Software Downloads, 2024. Consultado en <https://mikrotik.com/download>.
- [38] AlmaLinux. Obtener AlmaLinux OS, 2024. Consultado en [https://almalinux.org/es/get-almalinux/#ISO\\_Images](https://almalinux.org/es/get-almalinux/#ISO_Images).
- [39] AlmaLinux. AlmaLinux installation guide (ISOs), 09/02/2023. Consultado en <https://wiki.almalinux.org/documentation/installation-guide.html>.
- [40] Netgate. IPsec Site-to-Site VPN Example with Pre-Shared Keys, 03/04/2024. Consultado en <https://docs.netgate.com/pfsense/en/latest/recipes/ipsec-s2s-psk.html>.
- [41] Netgate. OpenVPN Site-to-Site Configuration Example with Shared Key, 03/04/2024. Consultado en <https://docs.netgate.com/pfsense/en/latest/recipes/openvpn-s2s-psk.html>.

- [42] Netgate. WireGuard Site-to-Site VPN Configuration Example, 03/04/2024. Consultado en <https://docs.netgate.com/pfsense/en/latest/recipes/wireguard-s2s.html>.
- [43] Aaron Kili. iPerf3 – Test Network Speed/Throughput in Linux, 09/05/2023. Consultado en <https://www.tecmint.com/test-network-throughput-in-linux/>.
- [44] Gustavo B. Cómo usar el comando SCP para transferir archivos, 15/05/2024. Consultado en <https://www.hostinger.es/tutoriales/comando-scp>.
- [45] jimp. Malformed packet in protocol OpenVPN after sniffing, 30/03/2020. Consultado en <https://forum.netgate.com/topic/151858/malformed-packet-in-protocol-openvpn-after-sniffing>.

---

# APÉNDICE A

## Configurar un cortafuegos pfSense sin utilizar la interfaz web

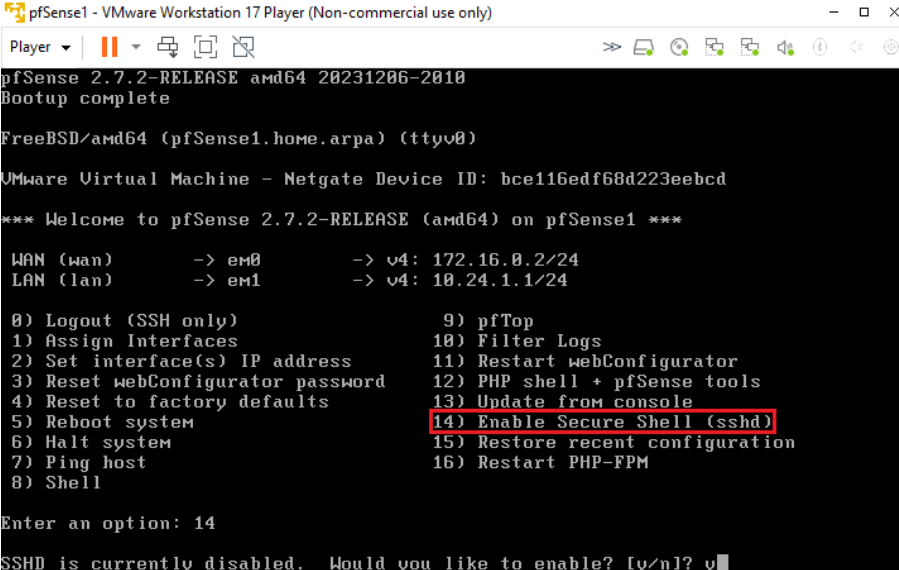
---

El software pfSense está orientado a la configuración vía interfaz web, sin embargo, existe la posibilidad de realizar configuraciones sin necesidad de tener acceso a un navegador o a otro equipo conectado al cortafuegos.

Este método consiste en editar directamente el archivo de configuración del sistema. Para ello, podemos acceder directamente a él desde la interfaz de consola de la propia máquina virtual del pfSense o utilizar una máquina externa para acceder al cortafuegos y modificarlo. En nuestro caso utilizaremos esta segunda opción, ya que nos permite simular como sería configurar el *pfSense1* desde el *PC1* que no cuenta con interfaz gráfica.

A modo de ejemplo, vamos a realizar las configuraciones necesarias para permitir el *ping* a través de la interfaz WAN, tal y como se realizó vía web en la configuraciones iniciales.

Para conseguir esto, primero necesitamos activar el acceso vía el protocolo SSH en el *pfSense1*. En la interfaz de consola, escogemos la opción 14) *Enable Secure Shell (sshd)* y confirmamos que queremos habilitar el servicio (ver figura A.1).



```
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete

FreeBSD/amd64 (pfSense1.home.arp) (ttyv0)

VMware Virtual Machine - Netgate Device ID: bce116edf68d223eebcd

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense1 ***

WAN (wan)      -> em0      -> v4: 172.16.0.2/24
LAN (lan)      -> em1      -> v4: 10.24.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option: 14

SSHd is currently disabled. Would you like to enable? [y/n]? y
```

Figura A.1: Habilitar SSH en el pfSense1

Una vez permitido podemos acceder al cortafuegos desde el *PC1* utilizando la orden `ssh admin@10.24.1.1` e introduciendo la contraseña que asignamos al *pfSense1*. A continuación, seleccionamos la opción *8) Shell* para obtener una consola de comando en el pfSense y descargamos, con el comando `pkg install nano`, la herramienta *nano* para facilitarnos la edición del archivo (ver figura A.2).

```

PC1 - VMware Workstation 17 Player (Non-commercial use only)
Player
root@pc1 ~]# ssh admin@10.24.1.1
Password for admin@pfSense1.home.arpa:
VMware Virtual Machine - Netgate Device ID: bce116edf68d223eebcd

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense1 ***

WAN (wan)    -> em0      -> v4: 172.16.0.2/24
LAN (lan)    -> em1      -> v4: 10.24.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults    13) Update from console
5) Reboot system               14) Disable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: 8

[2.7.2-RELEASE][admin@pfSense1.home.arpa]/root: pkg install nano

```

Figura A.2: Acceder a pfSense1 desde PC1 vía SSH e instalar *nano*

Después, utilizamos el comando `cd ..` para ir a la carpeta raíz del sistema y `cd conf` para seleccionar la carpeta de configuración. Dentro de esta carpeta se encuentra el archivo `config.xml` que editamos utilizando `nano config.xml` (ver figura A.3).

```

[2.7.2-RELEASE][admin@pfSense1.home.arpa]/root: cd ..
[2.7.2-RELEASE][admin@pfSense1.home.arpa]/: cd conf
[2.7.2-RELEASE][admin@pfSense1.home.arpa]/conf: ls
backup                               pkg_log_pfSense-pkg-WireGuard.txt
config.xml                           rules.debug.old
copynotice_version                   upgrade_log.txt
copyright
[2.7.2-RELEASE][admin@pfSense1.home.arpa]/conf: nano config.xml

```

Figura A.3: Editar el archivo `config.xml` con *nano*

En este archivo se almacena toda la configuración del equipo pfSense, podemos inspeccionarlo para buscar la configuración que estamos buscando. En nuestro caso, para permitir el *ping* en la interfaz WAN necesitamos realizar dos modificaciones, desactivar las dos opciones de bloqueo a redes reservadas en dicha interfaz (figura 6.34) y añadir una regla que permita el paso de todo el tráfico ICMP (figura 6.37).

Por una parte, para desactivar los bloqueos de redes privadas y *bogon networks* buscamos el apartado de interfaces y, dentro de la configuración de la WAN, eliminamos las líneas `<blockpriv></blockpriv>` y `<blockbogons></blockbogons>` (ver figura A.4).



```

GNU nano 7.2                                config.xml
<interfaces>
  <wan>
    <enable></enable>
    <if>em0</if>
    <descr><![CDATA[WAN]]></descr>
    <ipaddr>172.16.0.2</ipaddr>
    <subnet>24</subnet>
    <gateway>WANGW</gateway>
    <ipaddrv6>dhcp6</ipaddrv6>
    <dhcp6-duid></dhcp6-duid>
    <dhcp6-ia-pd-len>none</dhcp6-ia-pd-len>
    <adv_dhcp6_prefix_selected_interface>wan</adv_dhcp6_prefix_selected_interface>
    <blockpriv></blockpriv>
    <blockbogons></blockbogons>
    <spooftmac></spooftmac>
  </wan>

```

Figura A.4: Desactivar bloqueo de redes reservadas en *config.xml*

Por otra parte, para añadir la regla que permita el tráfico ICMP nos dirigimos al apartado *filter* y añadimos una nueva regla incluyendo las líneas de código que se muestran en la figura A.5. Una vez modificado el archivo, guardamos con *CTRL + O* y salimos con *CTRL + X*.

```

GNU nano 7.2                                config.xml
<rule>
  <id></id>
  <tracker>1712689201</tracker>
  <type>pass</type>
  <interface>wan</interface>
  <ipprotocol>inet</ipprotocol>
  <tag></tag>
  <tagged></tagged>
  <max></max>
  <max-src-nodes></max-src-nodes>
  <max-src-comm></max-src-comm>
  <max-src-states></max-src-states>
  <statetimeout></statetimeout>
  <statetype><![CDATA[keep state]]></statetype>
  <os></os>
  <protocol>icmp</protocol>
  <icmptype>any</icmptype>
  <source>
    <any></any>
  </source>
  <destination>
    <any></any>
  </destination>
  <descr></descr>
  <updated>
    <time>1712689201</time>
    <username><![CDATA[admin@10.24.1.52 (Local Database)]]></username>
  </updated>
  <created>
    <time>1712689201</time>
    <username><![CDATA[admin@10.24.1.52 (Local Database)]]></username>
  </created>
</rule>

```

Figura A.5: Añadir regla para permitir el *ping* en *config.xml*

Por último, tenemos que aplicar los cambios. Para ello, borramos la cache, situándonos en la raíz del sistema y ejecutando la orden *rm /tmp/config.cache* y reiniciamos el cortafuegos (ver figura A.6).

```

[2.7.2-RELEASE][admin@pfSense1.home.arpa]/conf: cd ..
[2.7.2-RELEASE][admin@pfSense1.home.arpa]/cf: cd ..
[2.7.2-RELEASE][admin@pfSense1.home.arpa]/: rm /tmp/config.cache
[2.7.2-RELEASE][admin@pfSense1.home.arpa]/: _

```

Figura A.6: Borrar la cache de configuración en pfSense1



---

## APÉNDICE B

# Objetivos De Desarrollo Sostenible

---

Objetivos De Desarrollo Sostenible

Grado de relación del trabajo con los Objetivos de Desarrollo Sostenible (ODS).

| Objetivos de Desarrollo Sostenible               | Alto | Medio | Bajo | No<br>procede |
|--|------|-------|------|---------------|
| ODS 1. Fin de la pobreza.                        |      |       | X    |               |
| ODS 2. Hambre cero.                              |      |       |      | X             |
| ODS 3. Salud y bienestar.                        |      |       |      | X             |
| ODS 4. Educación de calidad.                     |      |       |      | X             |
| ODS 5. Igualdad de género.                       |      |       |      | X             |
| ODS 6. Agua limpia y saneamiento.                |      |       |      | X             |
| ODS 7. Energía asequible y no contaminante.      |      |       | X    |               |
| ODS 8. Trabajo decente y crecimiento económico.  |      |       |      | X             |
| ODS 9. Industria, innovación e infraestructuras. | X    |       |      |               |
| ODS 10. Reducción de las desigualdades.          |      |       |      | X             |
| ODS 11. Ciudades y comunidades sostenibles.      |      |       |      | X             |
| ODS 12. Producción y consumo responsables.       |      | X     |      |               |
| ODS 13. Acción por el clima.                     |      |       |      | X             |
| ODS 14. Vida submarina.                          |      |       |      | X             |
| ODS 15. Vida de ecosistemas terrestres.          |      |       |      | X             |
| ODS 16. Paz, justicia e instituciones sólidas.   |      |       |      | X             |
| ODS 17. Alianzas para lograr objetivos.          |      |       |      | X             |

Reflexión sobre la relación del TFG/TFM con los ODS y con el/los ODS más relacionados.

Los objetivos de desarrollo sostenible fueron establecidos en 2015 por la Asamblea General de las Naciones Unidas. Estos propósitos buscan abordar los distintos retos sociales, económicos y medioambientales del mundo actual de una forma sostenible. Se va examinar como la solución propuesta en este proyecto puede contribuir con estos objetivos.

Analizando los ODS, encontramos que la propuesta tiene impacto en el *ODS 9. Industria, innovación e infraestructuras* porque la solución ofrece la posibilidad de facilitar y mejorar las comunicaciones seguras en entornos empresariales. De esta forma, las empresas pueden conectar sus redes privadas a pesar de encontrarse en ubicaciones geográficamente diferentes, mejorando su infraestructura de comunicaciones y protegiendo la información que se transmite. Esto puede agilizar la colaboración entre distintas sedes de una misma organización o entre distintas organizaciones.

Además, podemos relacionar el proyecto con el *ODS 12. Producción y consumo responsables* debido a que el uso de cortafuegos software en entornos virtualizados permite aprovechar en mayor medida los recursos físicos dedicados a alojar servidores. Esto elimina la necesidad de disponer de equipos de seguridad físicos dedicados a realizar la función que se aborda con la solución y, de esta forma, reduce el consumo energético.

Indirectamente el uso de servicios en la nube para alojar los sistemas utilizados para desarrollar la solución puede contribuir con el *ODS 7. Energía asequible y no contaminante*. Dado que muchos de los centros de datos utilizados para alojar estos servicios están realizando cambios enfocados al uso de energías más renovables, suponiendo una opción más asequible y menos contaminante que las instalaciones propias.

También, encontramos una relación en menor medida con el *ODS 1. Fin de la pobreza* ya que las tecnologías utilizadas en solución propuesta ofrecen una alternativa con costes reducidos. Esto se debe a que se utilizan cortafuegos software y de código abierto en lugar de equipos físicos que requieran de la compra de licencias para su uso. Permitiendo que pequeñas empresas, que no pueden disponer de equipos de seguridad como cortafuegos, puedan establecer sus conexiones de forma segura.

Sin embargo, cabe destacar que no todos los ODS están relacionados de alguna manera con el proyecto desarrollado. Este es el caso de objetivos que se centran en algunas necesidades sociales como el *ODS 2. Hambre cero*, *ODS 3. Salud y bienestar*, *ODS 4. Educación de calidad*, *ODS 5. Igualdad de género*, *ODS 8. Trabajo decente y crecimiento económico*, *ODS 10. Reducción de las desigualdades* y *ODS 11. Ciudades y comunidades sostenibles*. Tampoco encontramos relación con algunos de los objetivos dedicados a la protección del medio ambiente como el *ODS 6. Agua limpia y saneamiento*, *ODS 13. Acción por el clima*, *ODS 14. Vida submarina* y *ODS 15. Vida de ecosistemas terrestres*.

De igual manera, el proyecto realizado no tiene ningún impacto en los objetivos con carácter gubernamental como el *ODS 16. Paz, justicia e instituciones sólidas* y *ODS 17. Alianzas para lograr objetivos*.

En conclusión, la solución propuesta tienen impacto en algunos de los Objetivos de Desarrollo Sostenible en diferente medida. La relación más directa la encontramos, dada la finalidad del proyecto, con el objetivo número 9. Además, localizamos una relación parcial con otros objetivos como el 12, 1 y 7 debido a los sistemas y tecnologías utilizadas para llevar a cabo la solución.