Diseño y despliegue de modelo genérico de infraestructura hardware y software basada en escritorio remoto que ofrece una solución informática para PYME's que trabajan en ambientes de oficina

TITULACIÓN: Grado en Ingeniería Informática

AUTOR: Carlos Santana Rodríguez

TUTORIZADO POR:
Francisco Alexis Quesada Arencibia

Fecha [12/2023]

Agradecimientos

Agradecer a todas las personas que me han acompañado en esta bonita etapa. A las que estuvieron pero ya no, a las que se unieron más tarde y a las que han estado en todo momento. Gracias, porque sin cualquiera de ustedes no sería quien soy ahora.

Gracias infinitas.

Resumen

Debido al inusual suceso pasado del COVID-19, la informatización de las empresas aumentó drásticamente al verse obligadas muchas de ellas al teletrabajo. Al igual que aumentó la informatización, también lo hicieron a la par los ataques informáticos, esto puede verse claro hoy día con las constantes noticias de empresas que son víctimas de ataques de tipo ransonware.

Con este Trabajo de Fin de Título se pretende crear un modelo base de infraestructura informática completa para que pequeñas empresas puedan incluir un servidor a su forma de trabajo que les permita la centralización de la información, menores costos en recursos y la posibilidad del trabajo en remoto teniendo siempre en cuenta la seguridad de toda la infraestructura.

El modelo constará de un equipo que virtualizará un firewall que proteja a toda la red y de un servidor Windows Server que implemente los servicios de Terminal Server y Directorio Activo.

Abstract

Due to the unsual past event of COVID-19, the computerization of companies increased drastically as many of them were forced to telework. Just as computerization increased, so did computer attacks. This can be seen clearly today with the constant news of companies that are victims of ransomware attacks.

This Final Degree Project aims to create a base model of a complete computer infraestructure so that small companies can include a server in their way of working that allows them to centralize information, lower resource costs and the possibility of remote work, always taking into account the security of the entire infraestructure.

The model will consist of a computer that will virtualize a firewall that protects the entire network and a Windows server that implements Terminal Server and Active Directory services.

Índice general

Índice de figuras

Índice de cuadros

Capítulo 1

Introducción

Vivimos en unos tiempos en los que podemos ver como la informática y la tecnología avanzan cada día a pasos agigantados, esto puede verse reflejado claramente en la sociedad. Si comparamos la sociedad de hace tan solo 10 años con la actual nos damos cuenta de que casi todo ha cambiado, todo tiene más y mejor tecnología que entonces era casi impensable para los tiempos de ahora. En las empresas este es un hecho más que evidente, casi todos los procesos de cualquier empresa del sector secundario y terciario pasan a través de sistemas informáticos.

Con toda la informatización actual, un aspecto importante a tener en cuenta es el nivel de seguridad que estos sistemas poseen. Dado que todo se encuentra informatizado, toda nuestra información se encuentra en constante flujo a través de internet, redes y sistemas que creemos seguros y confiamos en que así lo sea. Este aspecto es directamente proporcional al nivel de informatización, a mayor informatización mayor es la probabilidad de sufrir un ataque informático que ponga en peligro la seguridad de los sistemas y sus datos.

Tras las constantes noticias diarias de empresas que sufren ataques informáticos de tipo ransomware y robo de datos surge la preocupación de crear una infraestructura informática que pueda servir a pequeñas empresas con bajos presupuestos para proteger sus sistemas. La seguridad informática desgraciadamente es algo a la que las empresas no dedican los recursos necesarios ya sea por desconocimiento de los riesgos a los que se está expuesto, falta de presupuesto o inversión de estos en otros cosas o simplemente no darle la importancia que esta merece. Este proyecto busca de alguna manera proporcionar una solución de fácil instalación y mantenimiento y a un coste lo más reducido posible que permita a las empresas realizar su actividad de oficina poniendo siempre por delante la seguridad del propio sistema.

Capítulo 2

Estado actual y objetivos iniciales

2.1. Estado actual

No sorprende conocer que España se situó en el tercer puesto mundial entre los países que más ciber ataques reciben, llegando a la cifra de casi 375.000 ataques en 2022, lo que supone un incremento del 22 por ciento frente al año anterior [1].

Esta situación viene dada porque un gran número de las empresa no disponen de medidas de seguridad informática suficientes para proteger sus sistemas y la información que estos contienen. Otras tantas las tendrán pero o no han sido bien configuradas en su momento o han quedado obsoletas debido a la falta de mantenimiento y actualización. Realmente son pocas las empresas que comprenden los peligros a los que se enfrentan debido a la desprotección de sus sistemas y las consecuencias que puede acarrear sufrir un ataque, como pueden ser la pérdida del servicio, una mala reputación social o pérdidas económicas. Es por esas consecuencias que sufrir un ataque informático supone un duro golpe para cualquier empresa pero aún más a las pequeñas, dependiendo del ataque recibido son numerosas las empresas, exactamente 6 de cada 10 [2], que se han visto abocadas al cierre tras haber recibido un ataque tras la incapacidad de sobreponerse a este.

Cuando las empresas requieren de alguna implementación informática que pueda mejorar sus procesos deben contactar con proveedores de servicios informáticos privados, estos pueden ofrecerles distintas soluciones muy variadas con distintas implementaciones y presupuestos. Cuando una empresa se encuentra en la situación de qué empresa elegir esto puede generar cierta incertidumbre, ya que, ¿por qué elegir una solución y no otra? ¿Realmente cubren mis necesidades? ¿Qué aspectos de la seguridad informática están teniendo en cuenta?

Gracias a la infraestructura planteada se tendrá un modelo que pueda servir a un gran número de pequeñas empresas, a unos costes asequibles para sus presupuestos, que mejoren su flujo de trabajo, con capacidad de ser escalable y cuyo principal objetivo es mantener la máxima seguridad de los sistemas y su información.

2.2. Objetivos

El fin principal de este proyecto es crear un modelo base de infraestructura informática que aumente el nivel de informatización de las pequeñas empresas atendiendo a las necesidades técnicas propias de trabajos relacionados con ambientes de oficina pero teniendo como eje central la seguridad de todos sus activos. Este modelo deberá ser fácilmente aplicable y configurable a cualquier empresa del tipo descrito, que mantenga un coste que sea asequible para empresas pequeñas que cuentan con un presupuesto limitado, que permita una fácil gestión y que sea escalable.

Las empresas de hoy en día gestionan una gran cantidad de información a diario. Es de vital importancia que esa información se mantenga segura, por ello centralizarla en un solo lugar permite hacerlo de una manera más sencilla y más eficaz. El uso de un servidor permite almacenar toda la información en un solo lugar, consiguiendo así una mejor gestión y control de ella al no encontrarse distribuida en equipos distintos.

El uso de escritorio remoto está cada vez más extendido [3], esto es así por las enormes ventajas que proporciona este sistema. Con ello las empresas podrán recortar costes en hardware, tener una mayor seguridad al no quedar almacenada información en los equipos de los usuarios y dar la opción del teletrabajo a sus trabajadores, lo que puede incluso aumentar la satisfacción de los mismos con la empresa y por consecuencia su rendimiento.

Para lograr los objetivos descritos se ha llegado a la solución de utilizar un servidor Windows Server [4] y un firewall PfSense [5] virtualizados dentro de un solo equipo físico mediante el sistema operativo Proxmox [6] y al uso de escritorios remotos para que los usuarios tengan su entorno de trabajo. Al quedar todo centralizado en un mismo equipo se consigue que la gestión y protección del sistema sea mucho más sencilla, de esta manera la información no se encuentra distribuida en diferentes equipos, así como una reducción de costes dado que no harán falta grandes inversiones en equipos porque estos necesitarán de unas especificaciones muy básicas dado que solo se usarán para realizar la conexión remota al servidor.

Capítulo 3

Competencias cubiertas

3.1. Comunes a la Ingeniería Informática

3.1.1. CII01

"Capacidad para diseñar, desarrollar, seleccionar y evaluar aplicaciones y sistemas informáticos, asegurando su fiabilidad, seguridad y calidad, conforme a principios éticos y a la legislación y normativa vigente".

Para el desarrollo de proyecto se ha tenido como máxima prioridad la seguridad y el buen funcionamiento de toda la infraestructura, escogiendo las soluciones que mejor pudieran cubrir estos requerimientos.

3.1.2. CII04

"Capacidad para elaborar el pliego de condiciones técnicas de una instalación informática que cumpla los estándares y normativas vigentes".

En este mismo proyecto se especifican cuales son las condiciones y requerimientos para el montaje de la infraestructura.

3.1.3. CII05

"Conocimiento, administración y mantenimiento de sistemas, servicios y aplicaciones informáticas".

Para este proyecto será necesaria la administración y mantenimiento de los sistemas que la infraestructura informática del mismo comprende.

3.1.4. CII09

"Capacidad de conocer, comprender y evaluar la estructura y arquitectura de los computadores, así como los componentes básicos que los conforman".

El proyecto incluye una sección donde se especifican los componentes necesarios para la creación de la infraestructura, teniendo en cuenta la carga de trabajo y uso que se va a hacer de la misma.

3.1.5. CII11

"Conocimiento y aplicación de las características, funcionalidades y estructura de los sistemas distribuidos, las redes de computadores e Internet y diseñar e implementar aplicaciones basadas en ellas".

La infraestructura cuenta con servicios web qué, gracias a una configuración correcta de la red e Internet, podrán ser accedidos tanto desde redes internas como desde Internet.

3.2. Específicas a las Tecnologías de la Información(TI)

3.2.1. TI01

"Capacidad para comprender el entorno de una organización y sus necesidades en el ámbito de las tecnologías de la organización y las comunicaciones".

Ha sido necesario conocer los flujos de trabajo de una empresa para poder aportar un solución informática que mejore a estos y facilite el trabajo a sus trabajadores.

3.2.2. TI02

"Capacidad para seleccionar, diseñar, desplegar, integrar, evaluar, construir, gestionar, explotar y mantener las tecnologías de hardware, software y redes, dentro de los parámetros de coste y calidad adecuados".

Se ha intentado crear una infraestructura informática lo más completa posible manteniendo el menor coste para que este sistema sea asumible para las empresas.

3.2.3. TI04

"Capacidad para seleccionar, diseñar, desplegar, integrar y gestionar redes e infraestructuras de comunicaciones en una organización.".

La infraestructura cuenta con una configuración de red completa, que abarca tanto redes internas como externas que permiten la conexión de cualquier usuario autorizado a la misma.

3.2.4. TI05

”Capacidad para seleccionar, desplegar, integrar y gestionar sistemas de información que satisfagan las necesidades de la organización, con los criterios de coste y calidad identificados.”.

Este proyecto intenta mejorar los flujos de trabajo de una pequeña empresa gracias a la informatización atendiendo a sus necesidades técnicas y sus capacidades económicas.

3.2.5. TI06

”Capacidad de concebir sistemas, aplicaciones y servicios basados en tecnologías de red, incluyendo Internet, web, comercio electrónico, multimedia, servicios interactivos y computación móvil”.

La infraestructura cuenta con toda una configuración de red que interconecta todos los activos, tanto localmente como desde Internet, permitiendo así su uso desde cualquier equipo.

3.2.6. TI07

”Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos”.

Es el pilar fundamental de este proyecto, asegurar la máxima seguridad de la infraestructura informática.

Capítulo 4

Aportaciones

4.1. Entorno profesional

Con la implementación la infraestructura informática que se describe en este proyecto se consigue:

- ✔ Optimización de recursos: Al utilizar máquinas virtuales se aprovecha mejor el hardware del equipo anfitrión.
- ✔ Centralización: Dado que todos los servicios se encuentran en un mismo equipo, se pueden centrar los esfuerzos de mantenimiento, gestión y protección del sistema en un solo sitio.
- ✔ Copias de seguridad: Gracias al uso de máquinas virtuales y el estar todo centralizado se facilita la creación de copias de seguridad.
- ✔ Seguridad: La infraestructura cuenta con numerosas medidas de seguridad que protegen al sistema.

Gracias a lo descrito anteriormente las empresas pueden aumentar su nivel de informatización, consiguiendo con ello una mayor agilidad en los flujos de trabajo y manteniendo siempre un entorno que maximiza la seguridad.

Uno de los aspectos importantes de este proyecto es la implementación del servicio de Escritorio Remoto [7], mediante este servicio se obtienen grandes ventajas tanto para la empresa como para los trabajadores de la misma. La empresa reduce los costes en hardware, ya que no hará falta el uso de equipos que cumplan una serie de especificaciones que permitan trabajar con ellos, simplemente terminales ”tontas”[8] que tienen un coste bastante menor. También puede reducir costes de oficina ya que se podría permitir el trabajo remoto, con esta modalidad de trabajo los usuarios pueden reducir y evitar gastos de transporte y tiempo al poder trabajar desde su hogar, lo que puede aumentar la satisfacción de los empleados con su trabajo y por ende una mayor productividad.

4.2. Entorno personal

La realización de este proyecto ha conllevado la búsqueda, análisis y prueba de varios sistemas o distribuciones. Cada sistema ofrecía distintas funcionalidades que podían cuadrar más o menos con las necesidades que se pretendían cubrir, por tanto, fue necesaria una documentación y prueba exhaustiva de cada sistema hasta encontrar cuál se acercaba más a la solución deseada. Esto ha permitido conocer nuevos sistemas que, si bien fueron descartados para este proyecto, pueden ser interesante para ser aplicados a otros proyectos futuros.

Con el objetivo de crear una infraestructura lo más segura posible, fue necesario el estudio de los flujos de trabajo que siguen las empresas, cómo estos se podrían mejorar gracias a la informatización y cómo hacerlo manteniendo un estándar de seguridad y calidad, siempre teniendo en cuenta la facilidad de uso para el usuario.

Capítulo 5

Normativas y Legislación

A continuación se describen las licencias de las que hacen uso las tecnologías y servicios descritos en este proyecto.

5.1. Licencia GNU GPL

La Licencia Pública General [9] es ampliamente usada en el mundo del software libre y el código abierto. Esta garantiza la libertad de usar, estudiar, compartir y modificar el software. Esta licencia además protege al software de intentos de apropiación que restrinjan esas libertades a nuevos usuarios cuando la obra es distribuida, modificada o ampliada.

Esta es una licencia copyleft, cualquier software derivado de un trabajo que esté cubierto por esta licencia deberá ser distribuido con los mismos términos de la licencia. También se especifica que si se distribuye software cubierto por la misma se debe proporcionar el código fuente del software para permitir que los usuarios finales puedan modificarlo y redistribuirlo.

Esta licencia es usada por Proxmox, dado que integra KVM, por PfSense y por OpenVPN.

5.2. Licencia GNU APGL

La Licencia Pública General Affero de GNU versión 3 [10] es una licencia para software libre y con copyleft. Esta licencia es muy similar a la Licencia Pública General de GNU (GLP) pero esta posee un apartado extra que especifica que se debe proporcionar el código fuente si se modifica el software cubierto por la APGLv3 y si los usuarios interactúan remotamente a través de una red.

El objetivo de esta licencia es asegurar que el código fuente de cualquier software cubierto por esta licencia sea accesible para la comunidad, incluso aunque el software se utilice en un servidor de red.

Esta licencia es utilizada por Proxmox.

5.3. Licencia GNU LGPL

La Licencia Pública General Reducida de GNU [11] está basada en la GNU GPL, pero con la principal diferencia de que la LGPL permite que el software licenciado se combine con software propietario. Los usuarios pueden hacer uso de software licenciado en aplicaciones propietarias sin tener que compartir el código fuente de la aplicación.

Esta licencia es utilizada por KVM y PfSense.

5.4. Licencia BSD

La licencia Berkeley Software Distribution [12] es una licencia para software libre permisiva que se utiliza en gran medida para los sistemas BSD, un tipo de sistema operativo de tipo Unix. Esta licencia permite el uso, modificación y distribución libre de software.

A diferencia de otras licencias como la GLP, esta licencia permite el uso de código fuente en software no libre.

Esta licencia es usada por Proxmox y PfSense.

5.5. Licencia MIT

Esta es una licencia de software libre permisiva creada por el Instituto Tecnológico de Massachusetts (MIT) [13], por lo que se permite que una obra pueda ser distribuida tanto de forma libre como privada. Esta licencia permite una alta compatibilidad con otro tipo de licencias como podría ser con la GNU GPL pero no al contrario.

Esta licencia es usada por Proxmox y PfSense.

5.6. Licencia MPL

La licencia Mozilla Public License [14] es una licencia de tipo software y código libre que fue desarrollada por Mozilla. Se podría decir que es un híbrido entre las licencias BSD y GNU GPL, busca encontrar un equilibrio entre los intereses de los desarrolladores de código abierto y los propietarios.

Esta licencia es utilizada por noVNC, que se integra en Proxmox, y por PfSense.

5.7. Licencia CAL

La licencia CAL [15] es una licencia de Acceso de Usuario (CLient Access License) creada por Microsoft, permiten a los usuarios y dispositivos acceder a un servidor con Windows Server instalado. Las licencias CAL pueden ser del tipo usuario o de dispositivo.

Esta licencia es utilizada por Windows Server para su servicio de Escritorio Remoto.

5.8. Proxmox

Proxmox es un software de código abierto que se acoge a la licencia GNA AGPL. A pesar de ello, Proxmox ofrece planes de suscripción que otorgan acceso al repositorio empresarial, actualizaciones y soporte.

Para el caso que desarrollaremos nos bastará con la licencia gratuita de Proxmox.

5.9. PfSense

Pfsense también es un software de código abierto bajo la licencia AGPL. Al igual que Proxmox, PfSense también ofrece suscripciones de pago que incluyen soporte entre otras funcionalidades.

Usaremos la licencia gratuita de PfSense.

5.10. Ley RGPD

La RGPD es el Reglamento General de Protección de Datos [16] creado por la Unión Europea. Se diseño con el fin de proteger a las personas de todo lo que tenga que ver con el tratamiento de sus datos personales y la circulación de estos.

El incumplimiento de esta ley acarrea graves sanciones económicas, demandas legales y hasta incluso la suspensión o cierre de la empresa.

Esta ley se ha tenido en cuenta durante todo el desarrollo del proyecto con el objetivo de crear una infraestructura informática que proteja toda la información que por ella circule.

5.11. Ley LOPDGDD

Esta ley orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales es una ley española que adapta la ley RGPD al reglamento español.

Dado que por el sistema viajará información tanto de los empleados como usuarios del sistema como de los clientes de la empresa, es de vital importancia conocer esta ley y la RGPD. Estas leyes establecen sanciones de grandes sumas de dinero para las empresas que infrinjan cualquiera de ellas, si por una mala configuración del sistema o la falta de ella se expusieran datos sensibles la empresa se vería en grandes problemas. Es por ello que toda la configuración de la infraestructura se ha llevado a cabo siguiendo estas leyes.

Capítulo 6

Metodología de Trabajo y Planificación

6.1. Metodología de trabajo

Se ha elegido como metodología de trabajo para este proyecto la metodología incremental [17]. Este tipo de metodología divide el proyecto en partes más pequeñas del mismo llamadas iteraciones, tras cada iteración se consigue un incremento que añade funcionalidades al producto final. Cada iteración está compuesta por distintas etapas como podrían ser el análisis, desarrollo y la evaluación.

Gracias a esta metodología se consigue obtener una versión funcional del producto tras cada iteración que puede ser testeada antes de proseguir con la implementación de funcionalidades.

6.2. Planificación inicial

La planificación que se planteó en un inicio fue la siguiente (6.1).

Fases	**Duración Estimada (horas)**	**Tareas**
Estudio previo / Análisis	40	Tarea 1.1: Estudio del servicio de Terminal Server. Tarea 1.2: Estudio del servicio de Active Directory. Tarea 1.3: Estudio de los requisitos hardware del sistema según número de usuarios.
Diseño / Desarrollo / Implementación	180	Tarea 2.1: Montaje del host de virtualización. Tarea 2.2: Diseño del cluster. Tarea 2.3: Diseño de las redes. Tarea 2.4: Instalación del cluster. Tarea 2.5: Instalación y configuración de las redes. Tarea 2.6: Instalación y configuración de los servicios. Tarea 2.7: Instalación y configuración de los terminales que se conectarán al servidor.
Evaluación / Validación / Prueba	20	Tarea 3.1: Pruebas para validar la alta disponibilidad del clúster. Tarea 3.2: Pruebas para validar el buen funcionamiento de la UPS. Tarea 3.3: Comprobar el acceso remoto al servidor. Tarea 3.4: Comprobar que cada usuario solo puede acceder a los ficheros que tiene permiso. Tarea 3.5: Comprobar que las copias de seguridad se realizan correctamente y se pueden recuperar. Tarea 3.6: Comprobar que el cortafuegos gestiona las redes correctamente.
Documentación / Presentación	60	Tarea 4.1: Desarrollo de la documentación. Tarea 4.2: Preparación de la presentación y defensa del Trabajo de Fin de Título.

Cuadro 6.1: Planificación inicial del proyecto

La primera etapa del proyecto se basó en estudiar los sistemas y servicios que se pretendían implementar y calcular qué hardware era necesario para ello. Esto con el fin de poder dimensionar el sistema y no elegir un hardware que se viera recortado en cuanto a rendimiento o en caso contrario un hardware demasiado potente que hiciera que no se aprovechase al máximo, recayendo así en un sobre coste de hardware.

Una vez hecho todo el proceso de análisis previo se procedió al desarrollo, este se dividió en host anfitrión, máquina virtual servidor y máquina virtual firewall. Debido a incompatibilidades del diseño inicial con los sistemas y servicios elegidos finalmente no se implementó la característica de clúster pero se añadirá como mejora a futuro del proyecto.

Tras la separación del desarrollo en 3 hitos se seleccionaron tareas más pequeñas dentro de cada uno. Así, con la consecución de todas las pequeñas tareas dentro de uno de los hitos se completaría el mismo y se procedería con el siguiente. El separar una tarea grande en otras más pequeñas permite que durante las iteraciones se puedan ir viendo incrementos en las funcionalidades.

A medida que las tareas se iban completando se procedía con su evaluación para comprobar que cada iteración cumplía con los resultados esperados y que todo el desarrollo de iteraciones previas seguía funcionando correctamente.

6.3. Ajustes de la planificación del proyecto

La planificación quedó de la siguiente manera (6.2) tras ajustar los tiempos de cada fase y establecer las tareas.

Fases	**Duración Estimada (horas)**	**Tareas**
Estudio previo / Análisis	40	Tarea 1.1: Estudio del sistema Proxmox. Tarea 1.2: Estudio del servicio de Escritorio Remoto. Tarea 1.3: Estudio del servicio de Active Directory. Tarea 1.4: Estudio del sistema PfSense. Tarea 1.5: Estudio de los requisitos hardware del sistema según número de usuarios.
Diseño / Desarrollo / Implementación	180	Tarea 2.1: Montaje del host anfitrión. Tarea 2.2: Configuraciones de red. Tarea 2.3: Montaje de la máquina virtual servidor. Tarea 2.4: Montaje de la máquina virtual firewall. Tarea 2.5: Implementación acceso remoto.
Evaluación / Validación / Prueba	20	Tarea 3.1: Comprobar accesos seguros. Tarea 3.2: Comprobar que las copias de seguridad se realizan correctamente y se pueden recuperar. Tarea 3.3: Comprobar el acceso remoto al servidor. Tarea 3.4: Comprobar permisos de usuario en el Directorio Activo. Tarea 3.5: Comprobar funcionamiento de las reglas del firewall.
Documentación / Presentación	60	Tarea 4.1: Desarrollo de la documentación. Tarea 4.2: Preparación de la presentación y defensa del Trabajo de Fin de Título.

Cuadro 6.2: Planificación ajustada

Capítulo 7

Tecnologías, herramientas e infraestructura hardware

7.1. Tecnologías

Existe un gran número de sistemas operativos, servicios y configuraciones posibles, es por ello que ha sido necesario realizar un arduo análisis y prueba de todas para poder seleccionar las que satisfagan en mayor medida las necesidades que se requerían en este proyecto. Las tecnologías que finalmente han sido seleccionadas se describen en las siguientes secciones.

7.1.1. Equipo anfitrión - Proxmox

El sistema operativo elegido como host anfitrión para las máquinas virtuales ha sido Proxmox VE. Proxmox es una plataforma de virtualización de código abierto que utiliza el hipervisor KVM para ello.

Proxmox posee una gran cantidad de características que lo hacen perfecto para su aplicación en este proyecto. Una de ellas es que provee de una interfaz web que permite la gestión total del sistema y las máquinas virtuales, esto permite poder monitorear el sistema remotamente.

Otra de las funcionalidades que implementa es la de las copias de seguridad, permite realizar copias de seguridad e incluso programarlas de manera nativa. La restauración de las copias es muy sencilla y eficaz.

Dado que se trabajará con máquinas virtuales, la posibilidad de crear y gestionar redes es otra gran funcionalidad.

Como se ha comentado en numerosas ocasiones, la seguridad del sistema es un pilar importante en este proyecto. Proxmox agrega funciones de seguridad tales como el cifrado de datos o la autenticación de dos factores que permiten aumentar la seguridad de toda la infraestructura en gran medida.

7.1.1.1. KVM

Kernel-based Virtual Machine [18] es una tecnología de virtualización específica para el kernel de Linux que lo transforma en un hipervisor. KVM virtualiza a nivel de hardware y lo hace en sistemas basados en Linux de una manera eficaz y eficiente, por ello es el elegido por Proxmox para la virtualización de sus máquinas virtuales.

7.1.1.2. noVNC

noVNc es un cliente VNC (Virtual Network Copmputing) [19] que permite acceder y gestionar máquinas virtuales remotamente a través de una interfaz web. Es por estas características que Proxmox integra esta tecnología para la gestión remota de sus máquinas virtuales gracias a que proporciona acceso gráfico a las consolas de las máquinas virtuales.

7.1.2. Máquina Servidor - Windows Server

Dados los servicios que se pretendían implementar, Directorio Activo y Escritorio Remoto, no cabía otra posibilidad que no fuera la de utilizar Windows Server como sistema operativo para nuestro servidor.

Windows Server se basa en el mismo sistema Windows para sistemas de escritorio, lo que hace que los usuarios estén muy familiarizados con su interfaz. Esta distribución de Windows específica para servidores incluye herramientas de administración y seguridad y un gran rendimiento.

El uso de este sistema está sujeto a la compra de una licencia dado que no es software libre.

7.1.2.1. Directorio Activo

Uno de los servicios que se ha decidido instalar en el servidor Windows es el de Directorio Activo [20]. Es uno de los servicios más implementados ya que gracias a este se permite la gestión de identidades y accesos. Permite crear usuarios, grupos, equipos o unidades organizativas formando así una jerarquía entre sí que se conoce como árbol de dominio.

Usaremos Directorio Activo para crear usuarios y autenticarlos en el servidor, se les asignarán permisos a cada uno para así gestionar el acceso a los recursos compartidos del servidor.

Además, Directorio Activo permite implementar políticas de seguridad basadas en usuarios y grupos que permitirá tener un mayor control sobre el uso que los usuarios hacen del servidor, impidiendo, por ejemplo, que los usuarios accedan a páginas web no permitidas, descarguen ficheros o instalen programas sin autorización, todo ello con el fin evitar cualquier tipo de vector de entrada de malware al sistema.

7.1.2.2. Escritorio Remoto

Con el servicio de Escritorio Remoto que proporciona Windows Server tendremos la posibilidad conectarnos a un servidor remoto y crear sesiones de usuario virtualizadas. Este servicio está basado en el protocolo Remote Desktop Protocol que establece una conexión segura entre el servidor y el usuario. Este protocolo es compatible con distintos sistemas como Windows, macOS o Linux, lo que hace posible obtener y trabajar en una sesión de un escritorio Windows desde cualquier tipo de sistema.

Mediante el uso de las sesiones remotas, toda la información queda almacenada en el servidor, lo que facilita en gran medida la realización de copias de seguridad así como se restauración.

Gracias a este servicio se puede aumentar la flexibilidad y productividad de los usuarios dado que les permite trabajar desde cualquier lugar. Además permite un servicio de resolución de problemas del usuario mejorado ya que no será necesario desplazarse hasta el puesto de este para poder gestionarlo.

7.1.3. Máquina firewall - PfSense

PfSense fue el sistema operativo elegido para la máquina virtual que hará de firewall. Esta es una distribución diseñada específicamente para hacer de firewall, por lo que ofrece una gran variedad de características para desarrollar esta función.

PfSense es una distribución de código abierto y gratuita por lo que se hace perfecta para este proyecto en el que se busca la mejor solución con el menor coste posible.

Al igual que Proxmox, PfSense también dispone de una interfaz web que permite su configuración y administración de una manera muy sencilla. Dadas todas las características que implementa se convierte en una opción con una gran flexibilidad, dadas todas sus opciones de configuración, y seguridad.

7.1.3.1. OpenVPN

PfSense [21] nos permite la instalación del servicio OpenVPN para la creación de una VPN privada. Este servicio es de código abierto y proporciona una gran seguridad.

Gracias a la VPN podremos acceder a la red interna de Proxmox y conectarnos al servidor a través del Escritorio Remoto.

7.2. Infraestructura hardware

Debido a las características del proyecto, el hardware utilizado para este proyecto no es el que se recomienda más adelante para ser usado. El hardware de laboratorio del que se ha hecho uso consta de:

- ✔ Router Huawei AX3.
- ✔ Switch TP-Link LSG105G, 5 puertos Ethernet.
- ✔ Ordenador con procesador Intel i5-9400f, 32GB de memoria RAM, tarjeta gráfica Nvidia 1050TI, 1 disco duro SSD de 240GB y 2 discos duros HDD de 1Tb cada uno.
- ✔ Portátil Lenovo Legion 5 para realizar las conexiones a Proxmox y al servidor Windows para su configuración y escritorio remoto.

El hardware que se sugiere para ser implementado, según las características del mismo y del proyecto, es el siguiente:

- ✔ Router TP-Link Archer C6 Gigabit
- ✔ Switch TP-Link LSTL-SG108E, 8 puertos Gigabit.
- ✔ Servidor Supermicro con CPU Intel Xeon Silver 4208, memoria RAM de 32Gb, 2 discos duros SSD de 1Tb cada uno, interfaz de red Dual LAN de 1Gbps.
- ✔ HP EliteDesk 800 G2 Desktop Mini con CPU i5, memoria RAM de 8Gb y disco duro SSD de 256Gb para la terminal tonta.

Capítulo 8

Presupuesto

Dado que este proyecto pretende crear una infraestructura que sea aplicable a pequeñas empresas, ha de tenerse en cuenta los gastos de instalación que supone, tanto por todo el equipamiento hardware como por las licencias de los sistemas usados, para que este sea viable para las mismas. Se ha buscado optimizar al máximo el hardware para sacar el mayor rendimiento con el menor costo posible, así como la utilización de sistemas operativos y servicios de uso gratuito, a excepción del sistema operativo Windows Server y sus servicios que por los requerimientos del proyecto se hacía necesario su uso.

8.1. Hardware

Como equipo que haga de host para instalar el sistema Proxmox y dentro de este las máquinas virtuales se recomienda el uso de un equipo servidor de la marca Supermicro que contenga las siguientes características:

- ✔ CPU: Intel Xeon Silver 4208 (8 núcleos y 16 hilos - 2,1Gz - 11Mb)
- ✔ Memoria RAM: 32Gb DDR4 2933Mhz (2 x 16Gb)
- ✔ Disco duros: 2 SATA SSD 1 Tb
- ✔ Interfaz de red: Dual LAN 1Gbps
- ✔ Placa base: X11SPM-F

Este equipo tiene un coste aproximado de 1965,00€ + IGIC. Adicionalmente se implementara otro disco duro SSD de 240Gb para la instalación del sistema Proxmox y el almacenaje de las imágenes ISO requeridas, dejando los otros dos discos de 1Tb nombrados previamente para el almacenamiento de las máquinas virtuales. Este disco SSD de 240Gb tiene un coste aproximado de 36€.

Además del equipo anfitrión, también será necesaria la compra de material hardware para la gestión de la red. Hará falta la implementación de un router, para la interconexión de

Internet con la red local, y de un switch para la distribución de la red local con los equipos físicos que se encuentren en la misma. Con estos dos componentes hardware existe una mayor flexibilidad en cuanto a los modelos que pueden ser utilizados, sin embargo se ponen ejemplos como podrían ser el router TP-Link Archer C6 Gigabit con un costo de 45€ aproximadamente y un switch TP-Link LSTL-SG108E, 8 puertos Gigabit con un costo de 32€.

Para reducir costes y gracias al uso del servicio de Escritorio Remoto, se puede hacer uso de equipos ”tontosçomo equipos físicos en la oficina dentro de la red local que permitan la conexión al servidor para obtener una sesión remota. Estos equipos cuentan con un hardware mínimo que permite la instalación de un sistema operativo con bajos requerimientos en cuanto a recursos, pues el único fin de estos es la conexión al servidor y estos no harán casi ningún tipo de procesamiento. Con este fin pueden usarse los equipos HP EliteDesk 800 G2 Desktop Mini que tienen un coste aproximado de 104€.

8.2. Software

El sistema operativo Proxmox y PfSense son sistemas de uso gratuito, estos tienen opciones de pago a modo de donación para sus creadores que dan acceso a obtener soporte pero que no es estrictamente necesaria su compra para el uso que queremos hacer. Por lo tanto, no se requerirá de ningún gasto para el uso de estos sistemas.

Para poder hacer uso del sistema operativo Windows Server 2022 habrá que obtener una licencia Standar Edition que tiene un coste de 960,00€ + IGCI. Además del pago por licencia de Windows Server, Microsoft también nos requiere la compra de licencias de usuarios para el uso del servicio de Escritorio Remoto, a este tipo de licencias se las llama licencias CAL y tienen un coste de 160,00€ + IGIC por usuario.

8.3. Presupuesto total

Tras el desglose de presupuestos en los apartados anteriores se procede a la creación de un presupuesto final que engloba tanto los gastos en equipo hardware como en licencias software. Este presupuesto se ha creado teniendo en cuenta que se usarán 5 licencias CAL de Windows Server y se tendrán 5 terminales tontos dispuestos en la oficina.

Concepto	Cantidad	Coste
Equipo Host	1	1965€
Disco Duro 240Gb SSD	1	36€
Terminal tonto	5	520€
Licencia Windows Server 2022	1	960€
Licencias CAL Windows Server	5	800€
Total		4281€

Cuadro 8.1: Presupuesto Total

Capítulo 9

Diseño

Como ya se ha hablado anteriormente, la infraestructura estará formada por equipo host con sistema Proxmox que contendrá dos máquinas virtuales, una máquina que hará de servidor gracias a Windows Server y otra máquina que hará de firewall gracias a PfSense. Para toda la configuración de red se hará uso de un router que conectará internet con el equipo host y de un switch que conectará el equipo host con los terminales tontos que se encuentren físicamente en la oficina.

El esquema de red de toda la infraestructura quedaría de la siguiente forma:

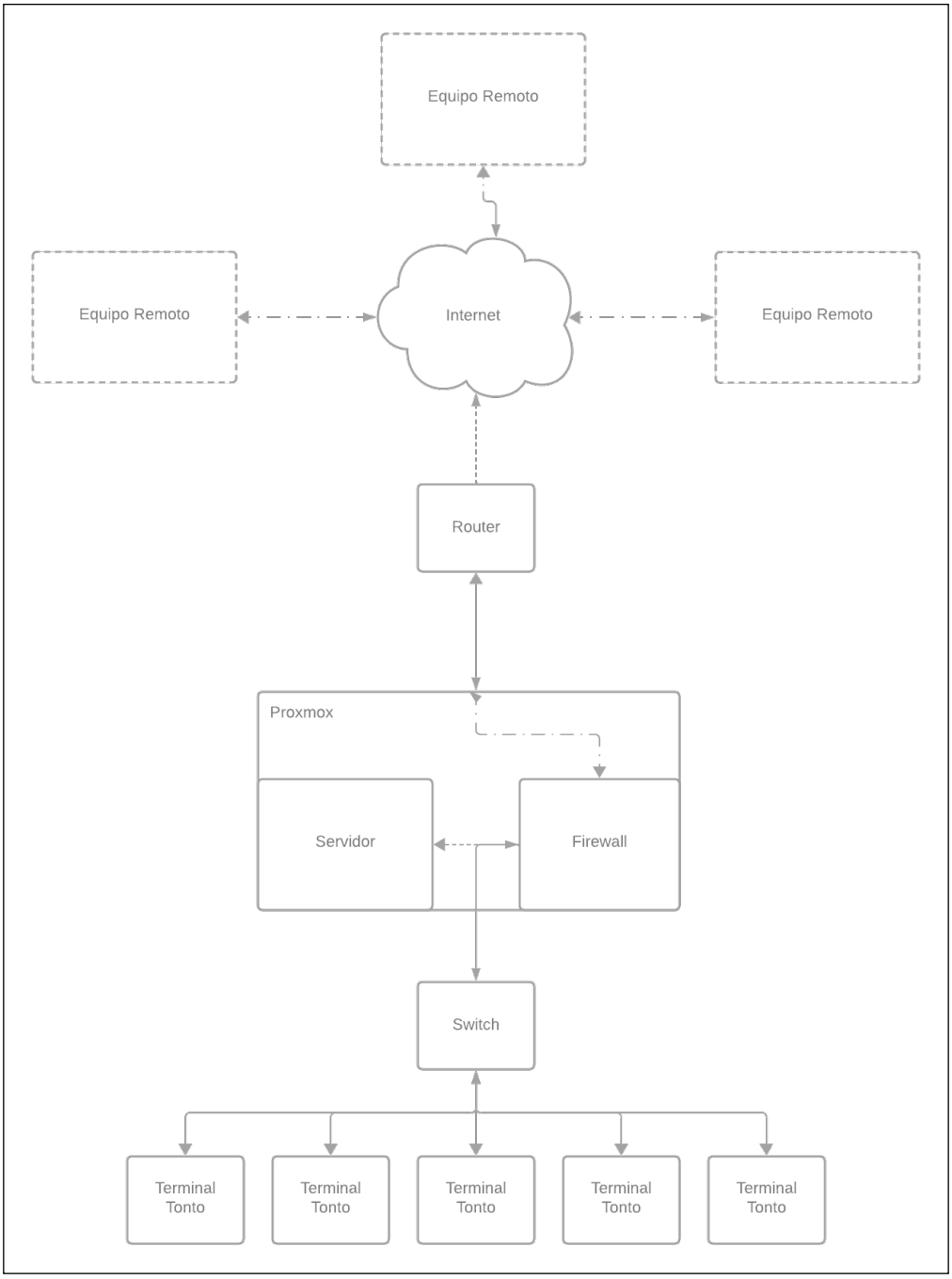

Ilustración 9.1: Inicio de sesión en Proxmox

Capítulo 10

Desarrollo

10.1. Sistema Operativo anfitrión

En esta sección se va realizar la configuración del sistema operativo anfitrión Proxmox, la instalación del mismo se especifica en el Anexo I. Este sistema está preparado para la virtualización, lo que nos brindará numerosas opciones para la instalación, configuración y monitoreo de las máquinas virtuales que se instalarán posteriormente que harán de servidor y firewall.

10.1.1. Configuración inicial

Haremos la configuración del sistema a través del entorno gráfico que Proxmox nos proporciona vía web. Desde un navegador en otro dispositivo conectado a la misma red introduciremos la URL que Proxmox nos proporciona.

Nos aparecerá un aviso diciendo que la conexión no es privada ya que carecemos de certificado para la web, pulsamos en configuración avanzada y aceptamos los riesgos. Ahora deberíamos poder ver el entorno gráfico de Proxmox que nos pedirá iniciar sesión (Ilustración 10.1), lo haremos introduciendo el usuario root y la contraseña elegida en la instalación. Al iniciar sesión nos saldrá un aviso diciendo que nuestra suscripción no es válida dado que estamos usando licencia de uso gratuito para este caso.

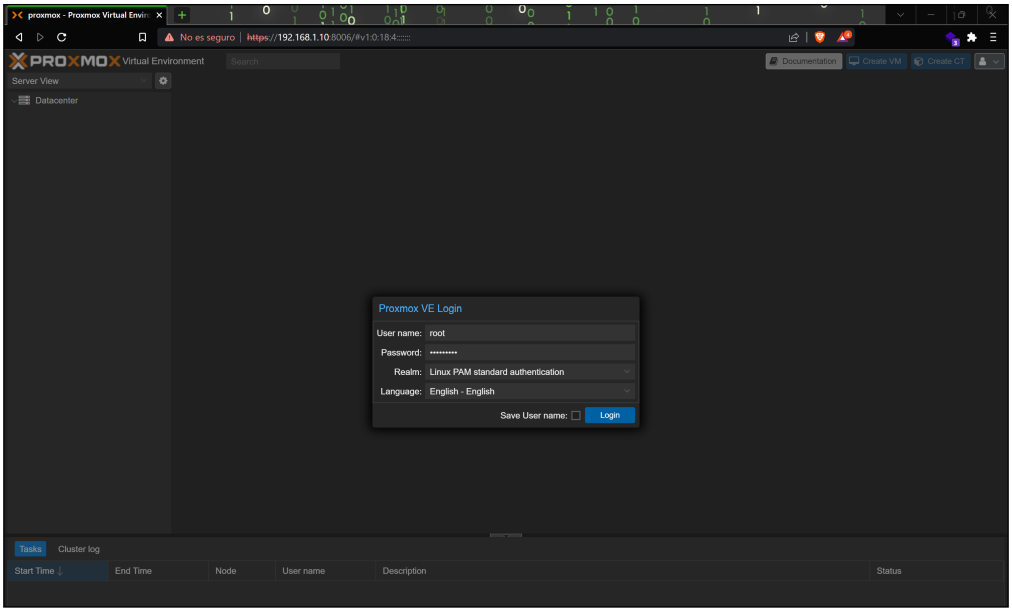

Ilustración 10.1: Inicio de sesión en Proxmox

Una vez hayamos iniciado sesión podemos pulsar en nuestro nodo **proxmox** (menú a la izquierda) y en el apartado **Summary** para ver un resumen del estado de los recursos del sistema. Esta pestaña (Ilustración 10.2) nos permite monitorizar el uso de discos, memoria o red entre otros parámetros.

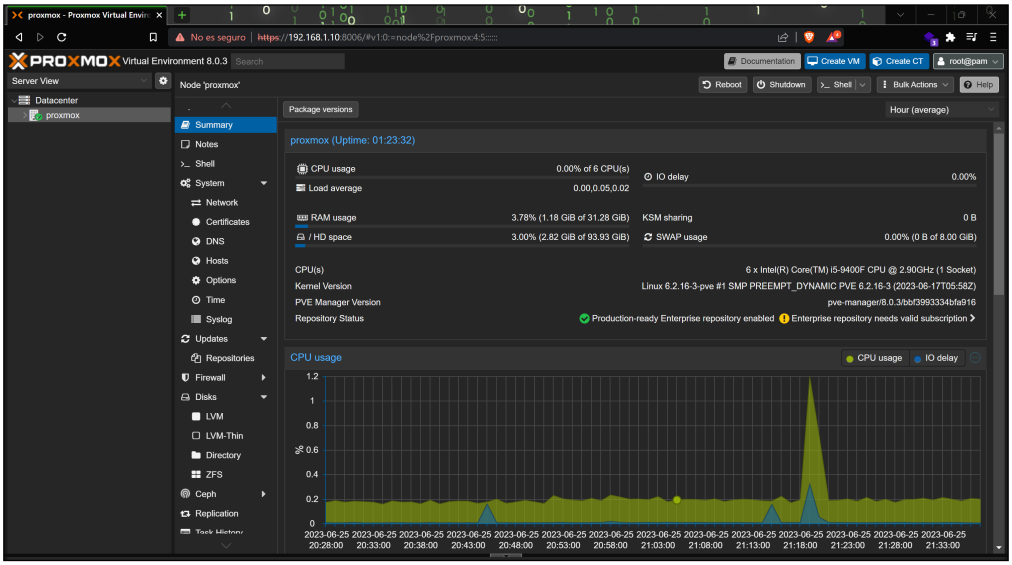

Ilustración 10.2: Pestaña resumen

Lo primero que haremos será actualizar el sistema, para ello pulsaremos en el nodo **proxmox**>**Shell** y se nos abrirá una consola como si estuviésemos en el propio equipo. Para actualizar el sistema introduciremos los siguientes comandos:

```
$ apt update #Para actualizar los paquetes
y
$ apt dist-upgrade #Para actualizar el sistema
```

Una vez actualizado completamente el sistema lo reiniciamos.

Si desplegamos la pestaña del nodo proxmox veremos que existen dos almacenamientos, **local** y **local-lvm**, el primero con solo 100Gb y el segundo con 343Gb. Esto es así porque Proxmox crea estos dos almacenamientos por defecto para separar el sistema del almacén de datos e imágenes de sistemas para las máquinas. Como disponemos de más discos en el equipo, procederemos a eliminar el volumen **local-lvm** y añadir ese espacio a **local**.

Vamos a **Datacenter>Storage**, seleccionamos el volumen a eliminar y pulsamos *remove*. Para añadir el espacio que acaba de quedar libre al otro volumen deberemos ir a la consola como anteriormente e introducir los siguientes comandos:

```
$ lvremove /dev/pve/data
$ lvresize -l +100%FREE /dev/pve/root
$ resize2fs /dev/mapper/pve-root
```

Después de hacerlo podremos observar como ahora solo existe un volumen con 462Gb. Ahora se deberá ir de nuevo a **Datacenter>Storage**, seleccionar el volumen y pulsar en editar, en la ventana que aparece, en la sección *content*, podremos seleccionar todo el tipo de contenido que acepta el volumen, que para este caso serán todas las opciones.

10.1.2. Configuración de discos duros

Para el caso de este equipo de laboratorio se procederá a crear un sistema RAID1 o Mirror [22] que contendrá las máquinas virtuales. El uso de un RAID nos permite asegurar la información en caso de fallo de uno de los discos a costa de sacrificar espacio de almacenamiento. Haremos uso de dos discos HDD de 1Tb, lo que nos proporcionará un RAID1 de 1Tb útil.

Dentro del nodo proxmox, en la sección de almacenamiento se encuentra **ZFS** [23]. Se ha elegido este nuevo tipo de sistema de archivos dado que es sólido, escalable y fácil de administrar. Haciendo click en *"Create ZFS"* nos aparecerá la pantalla que puede verse en la Ilustración 10.3.

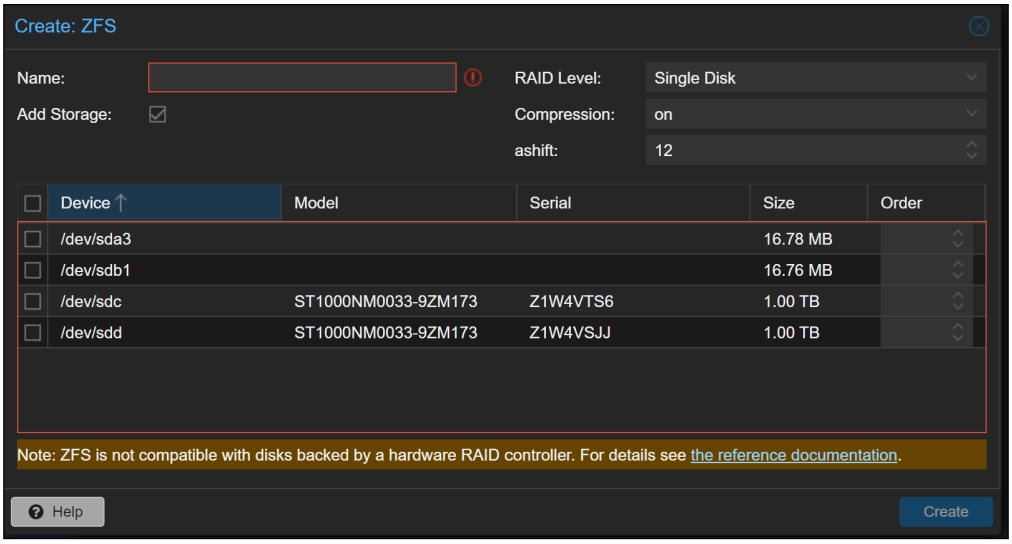

Ilustración 10.3: Ventana creación ZFS

Le pondremos un nombre al sistema de archivos, para el caso se ha elegido **ZFS01**, elegimos el nivel de RAID que como se ha dicho es de nivel 1 y se seleccionan los discos que lo formarán. Pulsamos en crear. Con esto ya tendremos listo nuestro sistema de archivos ZFS que contendrá los discos de las máquinas virtuales que creemos.

10.1.3. Configuración disco externo para backups

Se hará uso de un disco duro externo en el que se guardarán las copias de seguridad que hagamos de las máquinas virtuales. A pesar de que los discos internos formen un RAID1 y nos protejan frente a cualquier fallo en cualquiera de los discos, esto nos protege frente a la remota posibilidad de que ambos discos fallen pero sobretodo frente a un ataque de ransomware.

Esta es una buena práctica para evitar ataques de tipo ransomware ya que se usarán dos discos que se irán rotando según la política de seguridad establecida. Con ello se consigue tener siempre una copia de seguridad offline, en caso de sufrir un ataque de ransonware el disco offline no se vería afectado y podría restablecerse el sistema de forma rápida y sencilla, acortando en gran medida la parada del servicio de la empresa.

Para este caso se establecerá una política de seguridad con una copia incremental de lunes a jueves y una copia completa los viernes. De lunes a jueves el usuario mantendrá el primer disco duro externo conectado al equipo y los viernes lo cambiará al segundo.

Para crear el disco para backups primero tendremos que crear un directorio para poder montar nuestro disco duro externo. Accedemos a la consola de nuestro nodo proxmox e introducimos los siguientes comandos:

```
$ sudo mkdir /media/proxmox/BK_DISK
$ sudo mkfs.exfat -L BK_DISK /dev/sdf1
```

Con el primer comando se ha creado un directorio de nombre *BK_DISK* que será donde montemos el disco externo. Con el segundo creamos un sistema de ficheros exFAT en el disco externo y le asignamos la etiqueta *BK_DISK*.

Ahora debemos editar el fichero fstab para automontar el disco tras cada arranque:

```
$ sudo nano -B /etc/fstab
```

El parámetro -B sirve para crear un backup del fichero por si tuviésemos algún error con el fichero que vamos a editar. Introducimos la siguiente línea en el fichero fstab.

```
LABEL=BK_DISK /media/proxmox/BK_DISK exfat errors=remount-ro,defaults,users,noatime,nodiratime,umask=0 0 2
```

Montamos el disco y comprobamos que se ha montado correctamente:

```
$ sudo mount -a
$ lsblk -s
```

```
sde1        8:65   0  1007K  0 part
└─sde       8:64   0 447.1G  0 disk
sde2        8:66   0     1G  0 part
└─sde       8:64   0 447.1G  0 disk
sdf1        8:81   0 698.6G  0 part /media/proxmox/BK_DISK
└─sdf       8:80   0 698.6G  0 disk
pve-swap 253:0     0     8G  0 lvm  [SWAP]
└─sde3      8:67   0 446.1G  0 part
  └─sde     8:64   0 447.1G  0 disk
pve-root 253:1     0 438.1G  0 lvm  /
└─sde3      8:67   0 446.1G  0 part
  └─sde     8:64   0 447.1G  0 disk
root@proxmox:/media/proxmox#
```

Ilustración 10.4: Montaje correcto

A partir de ahora el disco se montará cada vez que el sistema se inicie, pero si queremos cambiar los discos en caliente (mientras el sistema sigue en funcionamiento) no se montará hasta que el sistema se reinicie. Por ello debemos crear un script que monte el disco externo y hacer que se ejecute de forma periódica gracias al fichero *cron*.

Crearemos el script que automonte el disco externo, deberemos guardarlo en un sitio seguro del sistema para evitar que nadie pueda acceder a este fichero y modificarlo. Se ha nombrado al script como **mount_external_drive.sh** y contendrá lo siguiente:

```
$ #!/bin/bash
$ mount /media/proxmox/BK_DISK
```

Le damos permisos de ejecución y pasamos a editar el fichero *cron* para que ejecute el script periódicamente, para el caso se ha elegido que la frecuencia sea cada 5 minutos. Introducimos la siguiente línea en el fichero *cron*:

```
$ */5 * * * * /ruta/al/script/mount_external_drive.sh
```

Con el disco montado y la configuración para que se automonte hecha ahora deberemos crear el directorio para los backups y añadirlo a Proxmox.

```
$ mkdir /media/proxmox/BK_DISK/VM_BK
```

En el entorno web vamos a **Datacenter>Storage>Add>Directory**. En la ventana emergente rellenamos los datos que nos piden, poniendo como ruta del directorio la que hemos creado anteriormente y lo creamos. Una vez hecho esto ya nos aparecerá este almacenamiento en Proxmox.

Más adelante se hará la configuración de las máquinas virtuales para que realicen las copias de seguridad en este disco duro externo que acabamos de configurar.

Ahora pasaremos a añadir una capa de seguridad extra para el acceso a nuestro sistema anfitrión. Como se vio anteriormente, para acceder al sistema simplemente se requiere de usuario y contraseña, si alguien obtuviese las credenciales tendría acceso completo al sistema y todo lo que ello conlleva, por eso es aconsejable la inclusión de un sistema de autenticación en dos pasos.

Para añadir la autenticación en dos pasos tendremos que ir a **Datacdenter > Permissions > Two Factor** y en el menú superior pulsaremos en Add. Se abrirá un menú despegable que nos dará varias opciones, elegimos la opción TOTP [24]. En el panel que nos aparece (10.5) seleccionaremos el usuario al que queremos añadirle la autenticación en dos pasos e introducimos una breve descripción. El mismo panel nos muestra un código QR, deberemos escanearlo con alguna aplicación de autenticación, como puede ser Google Authenticator, y al instante veremos como genera un código de 6 dígitos que ha de ser introducido en el apartado *Verify Code* del panel.

Ilustración 10.5: Panel configuración 2FA

Si el código introducido es correcto se cerrará el panel y ya tendremos configurado nuestro sistema de autenticación en dos pasos. A partir de ahora, cada vez que se quiera iniciar sesión con el usuario seleccionado pedirá usuario y contraseña como antes, pero si las credenciales son introducidas correctamente entonces pedirá el código generado por la aplicación que hemos usado anteriormente. Estos códigos que genera la aplicación son únicos y se generan y borran cada pocos segundos, lo que asegura que no se pueda robar dicho código para su posterior uso.

10.2. Acceso remoto a sistema anfitrión

Hasta el momento solo podemos acceder al sistema anfitrión si nos encontramos conectados a la misma red. El objetivo de este proyecto es poder administrar el sistema de manera remota por lo que en este apartado se va a proceder a hacer las configuraciones necesarias para ello.

10.2.1. Configuración router

Podemos observar que en la URL que proxmox nos proporciona para la conexión a través del navegador también se incluye un puerto, el puerto 8006. Para poder acceder a Proxmox deberemos conectarnos a la IP pública del router y que esté nos redirija a él. Accedemos a la configuración del router y vamos al apartado de **Reenvío de puertos**. Nos aparecerá un panel parecido al que se muestra en 10.6, en eset caso asignamos un nombre, seleccionamos la IP a la que queremos que se redirija (la IP del equipo anfitrión), protocolo que se usará para la conexión y los puertos. El puerto de entrada puede ser cualquier puerto que esté disponible, una buena práctica es elegir un puerto distinto al puerto por defecto del servicio ya que si algún atacante lanzase un escaneo contra nuestro router en busca de puertos típicos abiertos le sería más difícil detectarlo.

Ilustración 10.6: Port Forwarding

10.2.2. Obtención dominio

Con la configuración actual, para acceder remotamente a nuestro equipo anfitrión debemos de conectarnos al router a través de la IP pública del mismo, esto puede no ser lo más óptimo ya que puede ser difícil de recordar. Para solucionar este problema existen los dominios, el dominio es más fácil de recordar y cuando se introduzca en el navegador este traducirá a la IP pública de nuestro router.

Para obtener un dominio estos pueden comprarse a través de Internet, pero para este caso se hará uso de una plataforma llamada **NO-IP** que nos permite vincular nuestra IP pública con un subdominio de la web gratuitamente. Tendremos que crear una cuenta en la web, una vez logueados iremos al menú izquierdo y pulsaremos en **DNS Dinámico** > **No-IP Hostnames**. Pulsamos en **Crear nombre de host** y nos saldrá el siguiente panel (10.7):

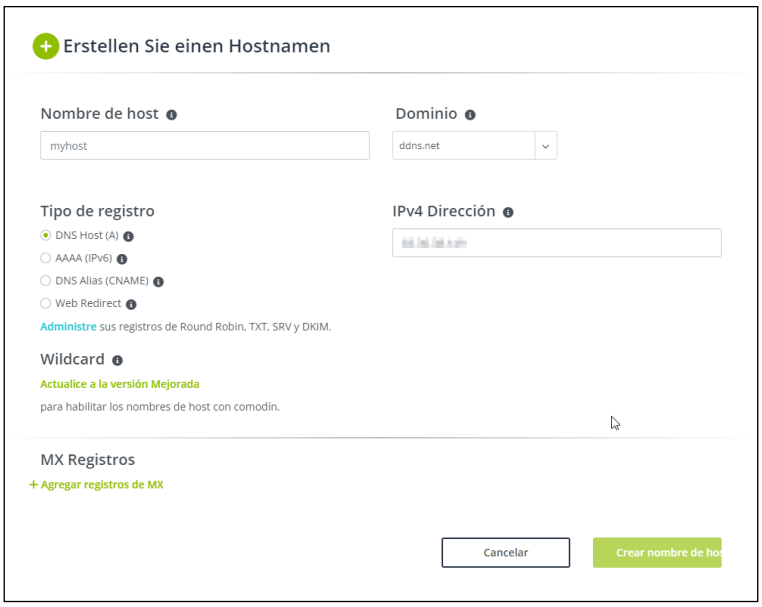

Ilustración 10.7: Port Forwarding

En el panel se nos da la opción de elegir el nombre del host y un dominio, se ha elegido como nombre para este caso **mytfgserver.ddns.net**. En el panel también nos aparecen los distintos tipos de registro disponibles, dejamos marcada la opción por defecto de DNS Host. El panel directamente nos detecta la IP Pública que estamos usando, si es la deseada podemos dejarla y guardar la configuración.

Con la configuración anterior ya podremos acceder al sistema anfitrión remotamente a través de la URL *https://mytfgserver.ddns.net:8006* al igual que si estuviésemos en la misma red.

10.3. Configuración inicial Windows Server

Ahora se procederá a realizar la instalación de la máquina virtual que hará de servidor gracias al sistema operativo Windows Server 2022. Antes de realizar esta configuración es necesario haber instalado primero la máquina virtual que actuará de firewall como se explica en el Anexo II.

Tras haber instalado el sistema Windows Server 2022 como se especifica en el Anexo IIIpodemos proceder a la configuración del mismo.

Lo primero que deberemos hacer es asignar un nombre que identifique a nuestro servidor y que además servirá de nombre del controlador de dominio. Para ello deberemos acceder a *Sistema* y pulsar en **Cambiar el nombre de este equipo**. En este caso se ha seleccionado como nombre para el servidor ”THEOFFICE”. Se nos dirá que para establecer este cambio es necesario reiniciar el sistema, pero omitiremos esto y lo haremos más adelante para poder continuar con la configuración.

Ahora configuraremos la red, vamos a asignarle una IP fija. Accedemos a las propiedades del adaptador de red y modificamos la IPv4. Seleccionamos una IP dentro de la red LAN que configuramos previamente en el Anexo II y asignamos como gateway la IP del firewall para que así este pueda filtrar el tráfico, debe quedar como en 10.8:

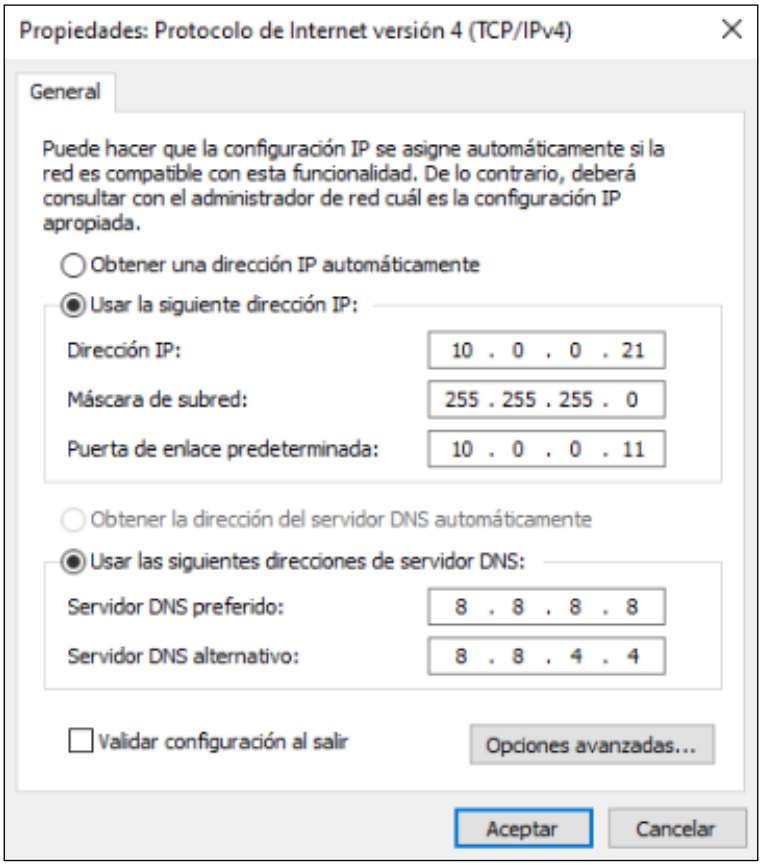

Ilustración 10.8: Configuración de red Windows Server

Es necesario configurar las actualizaciones para que posteriormente este no se reinicie inesperadamente o instale actualizaciones que puedan afectar a los servicios que se encuentren corriendo. Configuramos las horas activas del servidor para que entre esas horas el servidor no instale ninguna actualización, fijamos el horario entre las 6:00 y las 23:00.

10.4. Directorio Activo

Con la red configurada ya podremos conectarnos a Internet y realizar las siguientes configuraciones. Procederemos a instalar el **Directorio Activo**, para ello tendremos que acceder al *Administrador del Servidor*, que se abre automáticamente cuando el sistema se inicia, pulsar en en *Administrar* que se encuentra en el menú superior y hacer click en *Agregar roles y características* en el menú desplegable que saldrá.

Aparecerá el *Asistente para agregar roles y características* (10.9) que nos guiará con la instalación. En el apartado *Tipo de instalación* seleccionamos **Instalación basada en características o roles** y continuamos. En *Selección del servidor* dejamos la opción marcada de **Seleccionar un servidor del grupo de servidores** que nos asigna por defecto al servidor que estamos configurando actualmente. Siguiendo en el apartado *Roles del servidor* nos aparecerán todos los roles disponibles para su instalación, buscamos el rol llamado **Servicios de dominio de Active Directory** y lo marcamos, se abrirá otro panel que nos pregunte si queremos agregar las características necesarias para el rol de Directorio Activo, le decimos que sí y seguimos. Llegaremos al apartado de *Características*, como previamente ya hemos añadido las características para el Directorio Activo podemos continuar. Como estamos instalando el rol de Directorio Activo aparecerá un nuevo apartado nombrado *AD DS*, este apartado simplemente nos explicará algunas especificaciones de este rol, continuamos al apartado de *Confirmación* en el que se nos hará un resumen de lo que se va a instalar, pulsamos la casilla de **Reiniciar automáticamente el servidor de destino en caso necesario** para que se instalen y apliquen todos los cambios necesarios, una vez se haya reiniciado el servidor ya tendremos el Directorio Activo correctamente instalado.

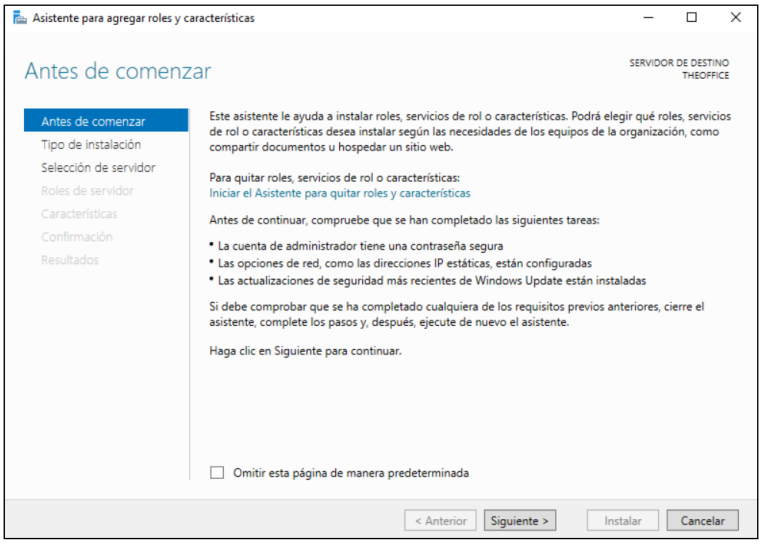

Ilustración 10.9: Asistente agregar roles y características

Cuando el servidor se vuelva a iniciar y se abra el *Asistente del servidor*, en la parte superior nos aparecerá un aviso. Como hemos instalado el rol de Directorio Activo se nos pedirá que promovamos el servidor a controlador de dominio, por lo que pulsando el aviso se abrirá el *Asistente para configuración de Servicios de dominio de Active Directory* (10.10). En la primera sección de este nos saldrán varias opciones y elegiremos *Agregar un nuevo bosque* ya es el primer dominio que creamos, debemos introducir un nombre para el nuevo dominio, se ha elegido **DUNDERMIFFLIN.LOCAL**. La especificación de *.LOCAL* es una recomendación de Microsoft ya que poner otras terminaciones de dominio como puede ser ".es.º ".com"puede generar conflictos. En la siguiente sección nos aparecerán las opciones del controlador de dominio, deberemos fijar los niveles funcionales al más actual que se nos permita, dado que no tenemos otros servidores, y elegiremos la contraseña para el modo de restauración de

servicios de directorio, este modo sirve para recuperar nuestro Directorio Activo en caso de que surgiera algún fallo. El resto de opciones que nos aparezcan dejaremos todo por defecto hasta que nos permita hacer la instalación, una vez se termine se reiniciará el servidor.

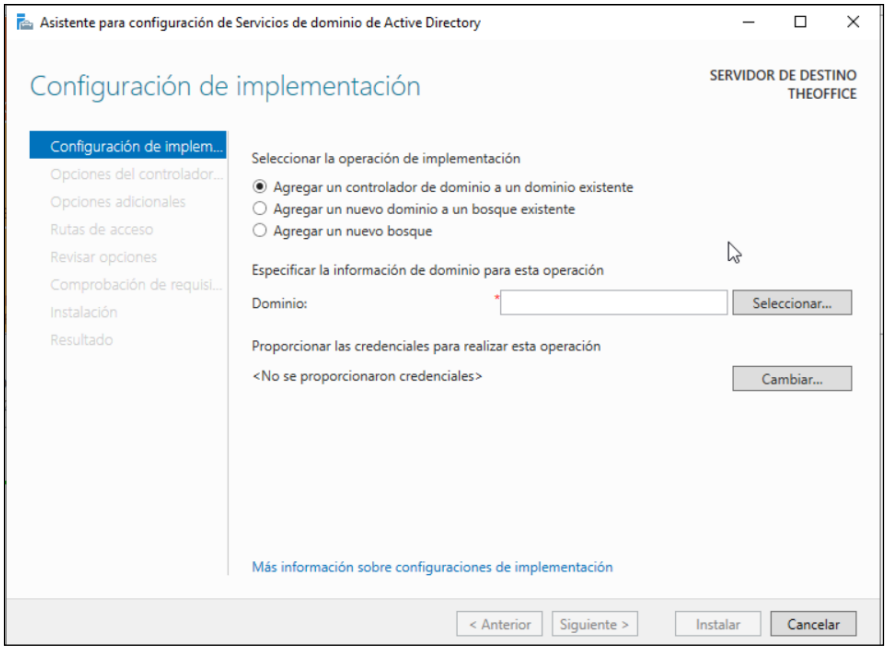

Ilustración 10.10: Asistente servicios de dominio Active Directory

Ahora cuando el servidor se vuelva a iniciar podremos ver como en el inicio de sesión nos aparecerá el nombre de usuario del administrador precedido del nombre del dominio que hemos elegido 10.11.

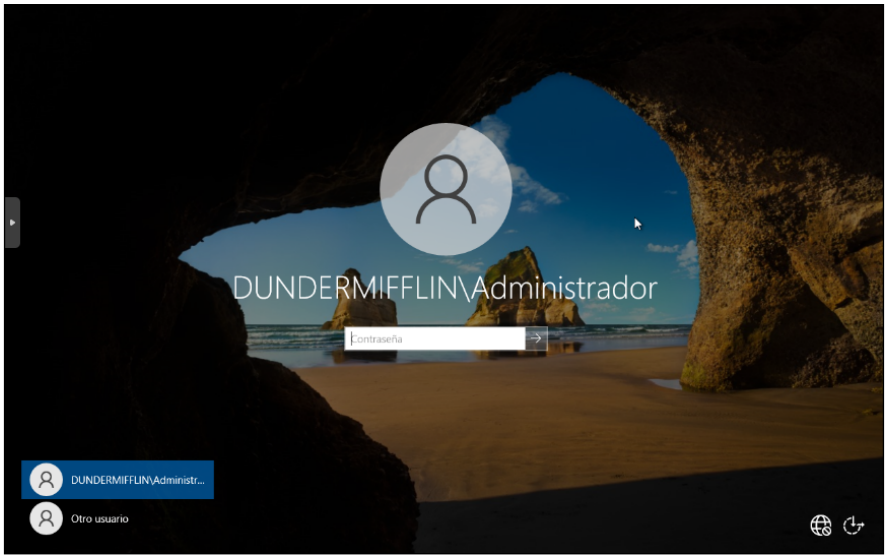

Ilustración 10.11: Inicio de sesión en dominio

Iniciamos sesión igual que hacíamos anteriormente y cuando se inicie el *Administrador del servidor* podremos ver los nuevos roles que hemos instalado. Ahora crearemos algunos usuarios para el servidor y unidades organizativas en las que distribuiremos a esos usuarios según sus puestos en la empresa, para ello deberemos abrir el *Centro de administración de Directorio Activo*. Haciendo click en la raíz del dominio podemos crear las unidades organizativas como se ve en 10.12.

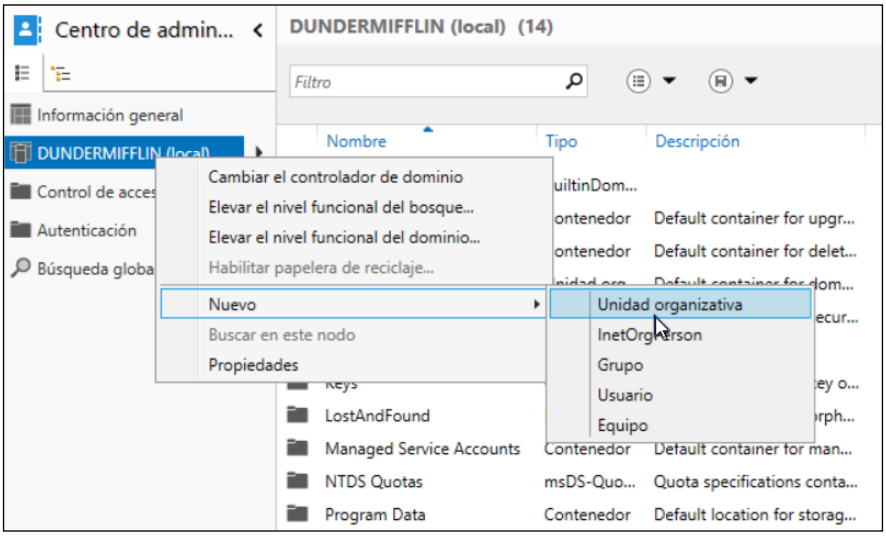

Ilustración 10.12: Añadir unidad organizativa

Se nos abrirá una ventana en la que deberemos rellenar los datos. Para este caso hemos creado una unidad organizativa llamada *Scranton*, que contendrá otras unidades organizativas. Las unidades organizativas que se encuentran dentro de *Scranton* se han organizado de la siguiente manera:

- ✔ Equipos: contiene los equipos físicos de la oficina
- ✔ Impresoras: contiene las impresoras de la oficina
- ✔ Usuarios: contiene a todos los usuarios que irán a su vez dentro de otras unidades organizativas para clasificarlos.

Para este caso, la distribución de las unidades organizativas a quedado de la siguiente forma:

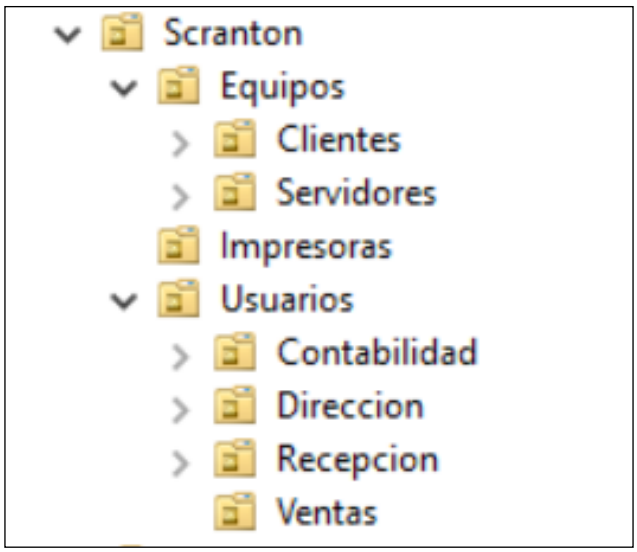

Ilustración 10.13: Árbol unidades organizativas

Con las unidades organizativas ya creadas ahora podremos ir añadiendo los usuarios a las unidades que correspondan con sus puestos en la empresa. Además dentro de cada unidad organizativa deberemos de crear un grupo con el mismo nombre que la unidad. Para la creación de un usuario haremos click derecho sobre la unidad organizativa donde queremos añadirlo y seleccionamos **Nuevo** > **Usuario**. Aparecerá una ventana en la que podremos completar los datos del usuario.

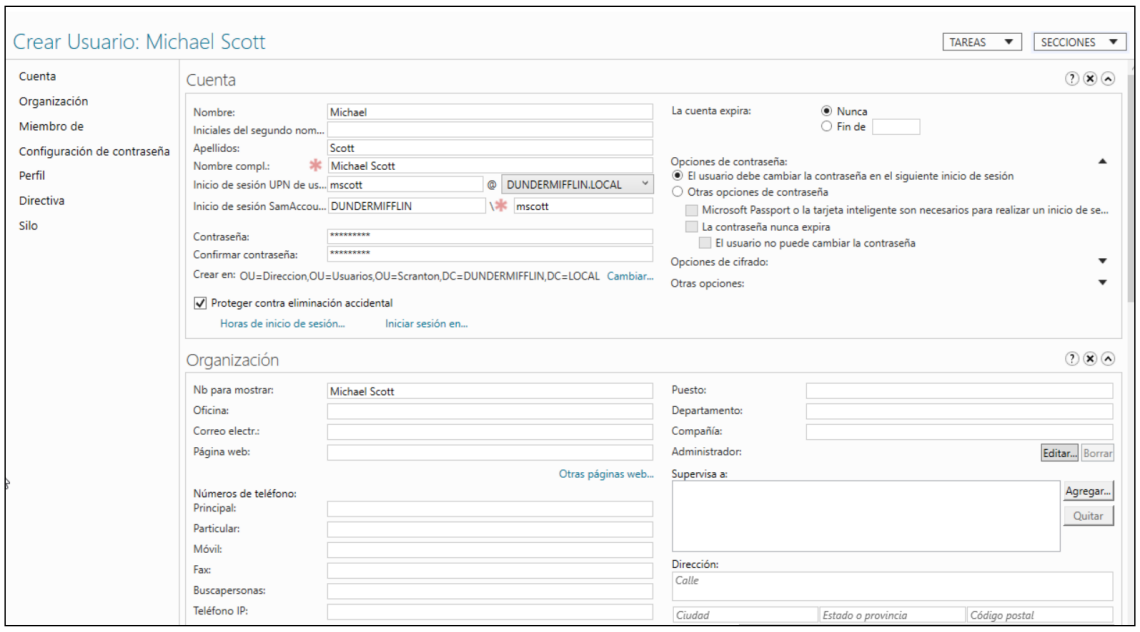

Ilustración 10.14: Creación usuario

Para la creación de un usuario será necesario especificar su nombre, apellido y nombre de inicio de sesión. Para los nombre de inicio de sesión se ha optado en este caso por una

política de *flast* (primera letra del nombre seguida del apellido). También se nos pedirá una contraseña, tenemos la opción de elegir si queremos que el usuario cree una contraseña nueva después del primer inicio sesión, así solo el propio usuario conocerá su contraseña.

Una opción que se nos ofrece en este panel es la de *Horas de inicio de sesión*. Con esta opción podemos seleccionar las horas en las que un usuario puede conectarse, esto puede servir para fijar un horario de trabajo y fomentar la desconexión del trabajo así como para evitar ataques realizados fuera de las horas de trabajo si se comprometiese algún usuario.

Una vez tengamos creados los grupos y usuarios, probemos a iniciar sesión con uno de los usuarios creados.

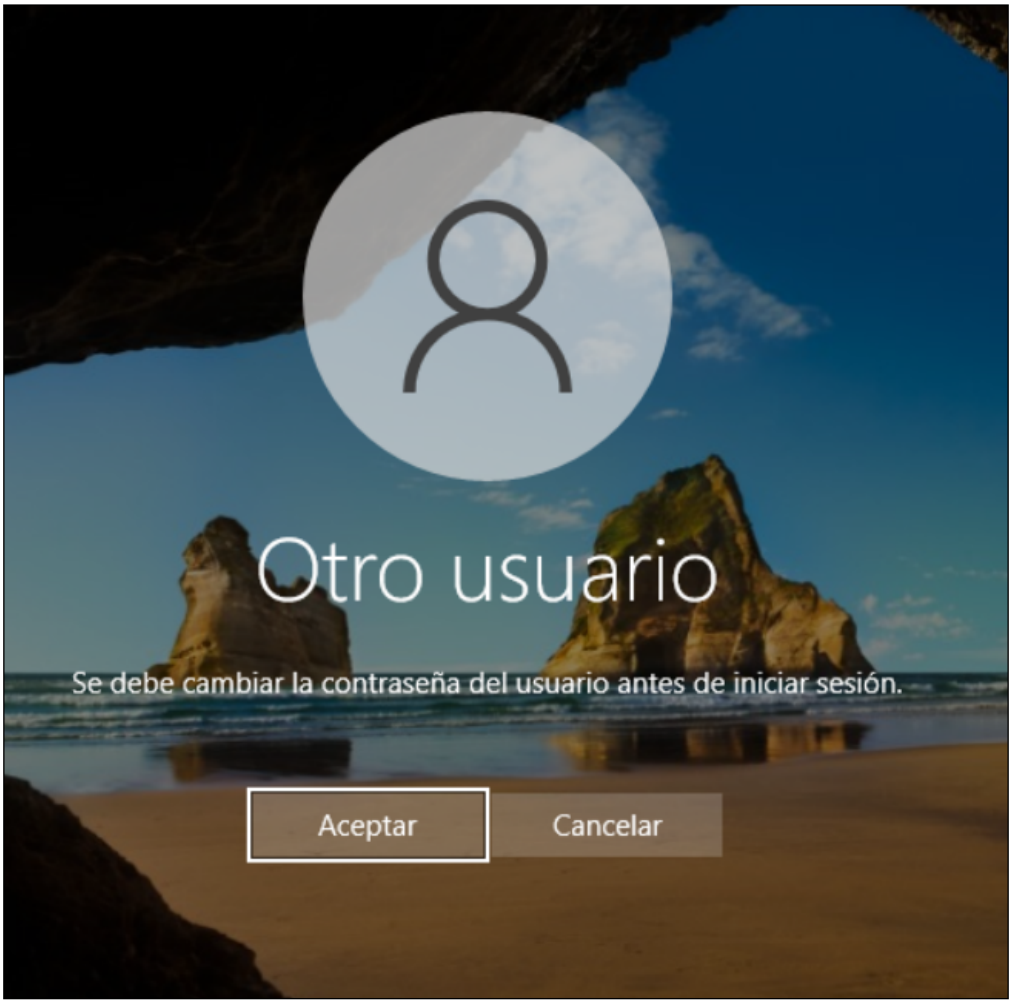

Ilustración 10.15: Creación contraseña nueva tras primer inicio de sesión

Como se observa, el inicio de sesión fue correcto y nos pide que introduzcamos una contraseña nueva para el usuario. Este inicio de sesión lo estamos haciendo directamente desde la máquina servidor pero en este proyecto lo que se pretende es que cada usuario inicie una sesión remota, por ello ahora se procederá a instalar el rol de escritorio remoto.

10.5. Máquina Firewall

Se va a proceder a configurar la máquina que hará de firewall con el sistema pfSense tras la instalación del mismo en el Anexo II.

10.5.1. Configuración Inicial pfSense

Como se explica en el Anexo II, PfSense ofrece una interfaz web. Para acceder a la interfaz web simplemente deberemos introducir la IP de la máquina PfSense en el buscador del navegador web desde otro equipo en la misma red, desde el servidor por ejemplo. Si todo se ha hecho correctamente nos aparecerá la siguiente pantalla de inicio de sesión.

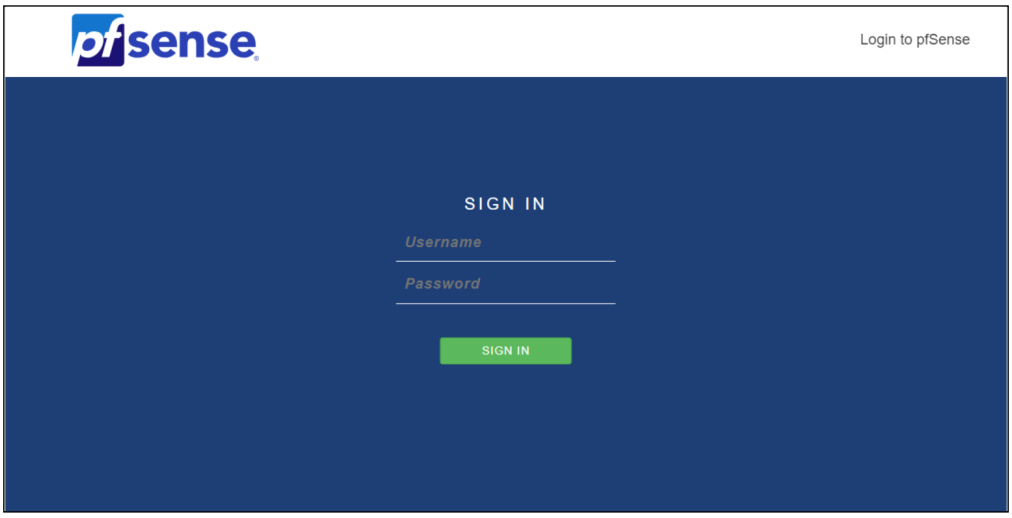

Ilustración 10.16: Inicio de sesión PfSense

Cuando iniciemos sesión con las mismas credenciales que hicimos desde la propia máquina comenzará el setup de PfSense para hacer una configuración inicial rápida. Dado que ya hemos configurado previamente la máquina podemos omitir mucho de los pasos que aparecerán. Tendremos que establecer una contraseña de administración que nos servirá para iniciar sesión en la web y para el acceso a través del protocolo SSH.

Lo primero que tendremos que hacer es asociar nuestra IP del firewall con el hostname *mytfg-server.ddns.net* que hemos obtenido anteriormente para que en configuraciones posteriores podamos hacer referencia a este y no a la IP. Para ello deberemos ir a **Services** > **Dynamic DNS** > **Dynamic DNS CLients** > **Edit**, aparecerá un formulario como se ve en la figura 10.17 que nos pedirá con qué servicio tenemos el DNS dinámico, qué interfaz queremos usar (usaremos la WAN) y nuestro nombre de hostname. Si hemos puesto todo correctamente, al guardar la configuración nos deberá aparecer como se observa en la figura 10.18, nos detectará automáticamente la IP pública que se esté usando. Esto permite que si por la razón que sea se modifica la IP pública de nuestro servidor no tengamos que reconfigurar nuestro firewall, ya que este hace referencia al hostname que no varía.

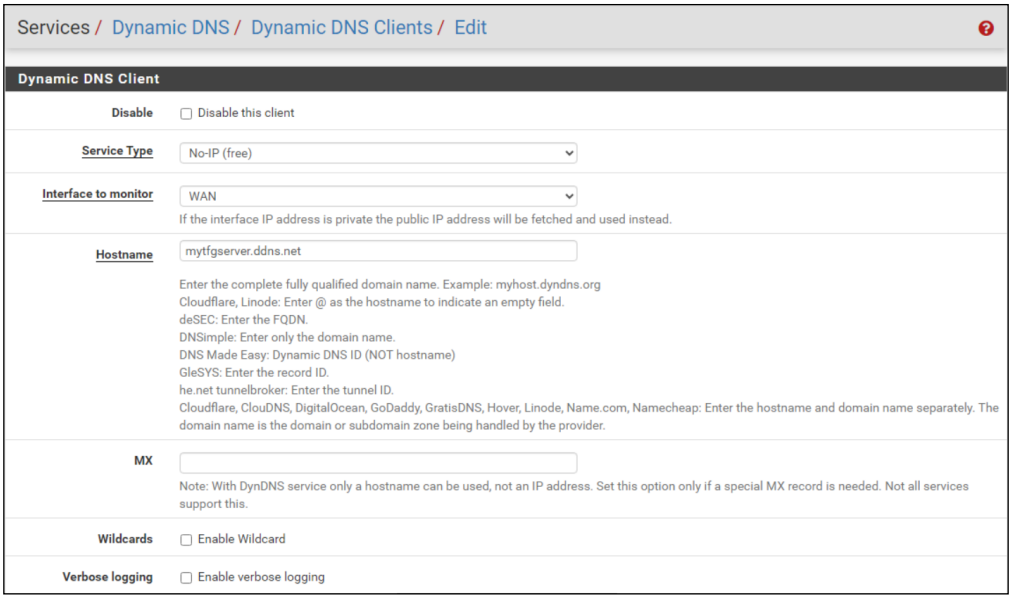

Ilustración 10.17: Formulario DNS dinámico

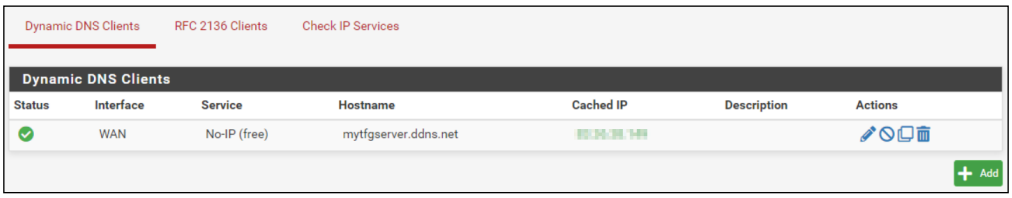

Ilustración 10.18: DNS dinámico configurado correctamente

10.5.2. Creación VPN

Nuestra máquina servidor se encuentra en una red interna dentro de Proxmox tras el firewall por lo que ahora mismo no podemos acceder remotamente al servidor. Una opción para solventar este problema sería abrir puertos en el PfSense y crear reglas que nos permitan llegar hasta el servidor, pero esto puede generar brechas de seguridad si no se hace una configuración correcta además de que no permite una gran versatilidad al no tener un acceso completo a la red. La solución que implementaremos será la creación de una VPN propia, lo haremos mediante OpenVPN que viene integrado en PfSense. Gracias a la VPN tendremos acceso completo a la red interna de PfSense desde cualquier lugar y podremos conectarnos desde cualquier equipo, con la ventaja de que al crear un túnel entre nuestro equipo y la red interna sólo nosotros navegaremos ahí y la posibilidad de implementar autenticación basada en certificados y usuario/contraseña.

Para asegurar la seguridad de nuestra VPN haremos uso de certificados, se generará un certificado por cada usuario. Para iniciar sesión en la VPN será necesario que el usuario introduzca sus credenciales y además que posea su certificado, con ello nos protegemos frente a inicios de sesión fraudulentos en caso de sufrir un robo de credenciales.

Lo primero que debemos crear es una unidad certificadora, para ello nos dirigimos a **System > Certificate Manager > CAs** y pulsamos en Add. Aparecerá un formulario que nos pedirá que introduzcamos un nombre para la nueva unidad certificadora, el método dejamos el que aparece por defecto y el resto de campos los rellenamos según se ve en la figura 10.19.

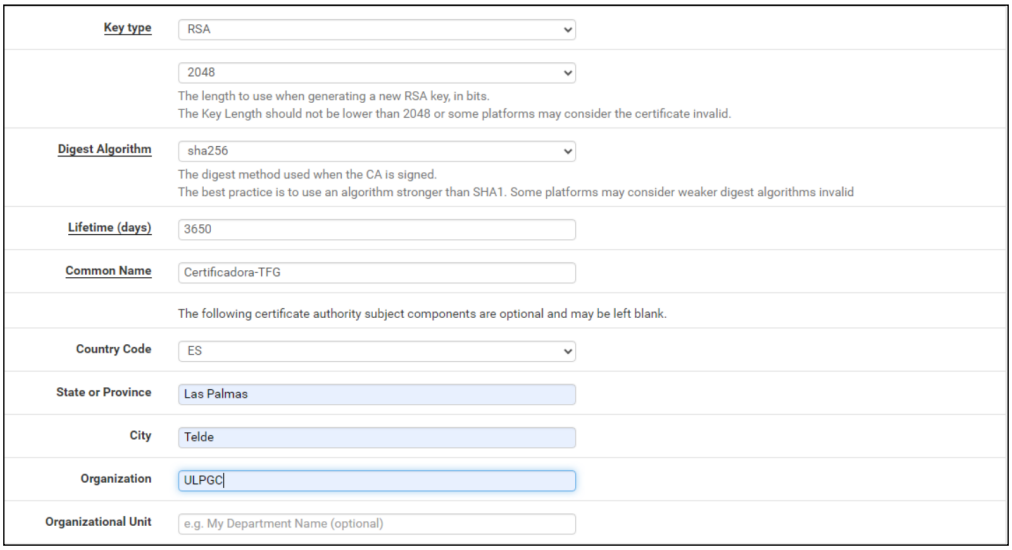

Ilustración 10.19: Creación unidad certificadora

Con la unidad certificadora creada ahora es paso de crear los certificados, necesitamos de un certificado para el servidor OpenVPN y certificados de usuarios. Para la creación del certificado del servidor iremos a **System > Certificate Manager > Certificates** y creamos uno nuevo. Deberemos dejar todo por defecto a excepción del nombre que le daremos al certificado y seleccionar el tipo de certificado como *Certificado de Servidor*.

Para la creación de los certificados de los usuarios podría hacerse de la misma manera pero seleccionando como tipo de certificado *Certificado de usuario*, pero tendríamos que crear uno a uno. Para simplificar este paso lo que haremos será crear los usuarios y con ello se generarán los certificados propios a la vez. Para crear los usuarios nos dirigimos a **System > User Management > Users** y creamos tantos usuarios como usuarios del servidor necesiten de acceso remoto. PfSense nos pedirá nombre y contraseña del usuario como datos obligatorios, deberemos marcar las casilla **Click to create a new user certificate** para que se genere el certificado del usuario como se nombró anteriormente.

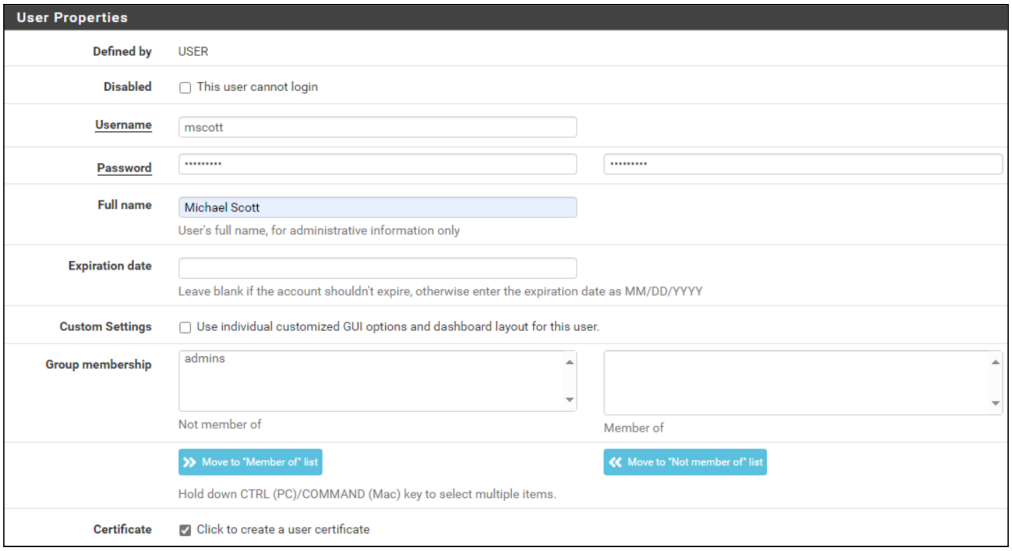

Ilustración 10.20: Creación usuario VPN

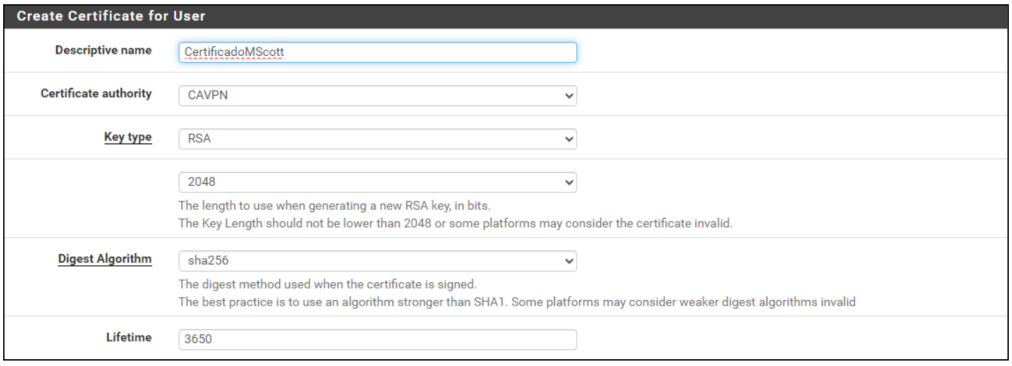

Ilustración 10.21: Certificado usuario

Con la unidad certificadora y los certificados creados ahora sí podemos proceder a crear la VPN. En el menú superior vamos a **VPN** > **OpenVPN** y en la pestaña **Servers** creamos uno. En el modo de servidor seleccionamos **Remote Access (SSL/TLS + User auth)**, de está manera se necesitará del certificado de usuario y credenciales para acceder a la VPN como se mencionó anteriormente. En el campo **Interface** introduciremos la interfaz que estará escuchando, como accederemos remotamente deberemos seleccionar la interfaz WAN, el puerto por defecto que utiliza OpenVPN es el 1194 que habrá que abrirlo posteriormente en el router. Usaremos llaves TLS que generaremos automáticamente, seleccionamos la unidad certificadora, el certificado de servidor que creamos previamente y elegimos los algoritmos de encriptación que se ven en la figura 10.22. Deberemos introducir una red para nuestro servidor VPN, esta red tendrá acceso completo a la red interna de PfSense, el único requisito de esta red es que no puede estar contenida en el PfSense, por lo que en este caso se seleccionó la red 10.0.1.0/24. Guardamos la configuración del servidor OpenVPN.

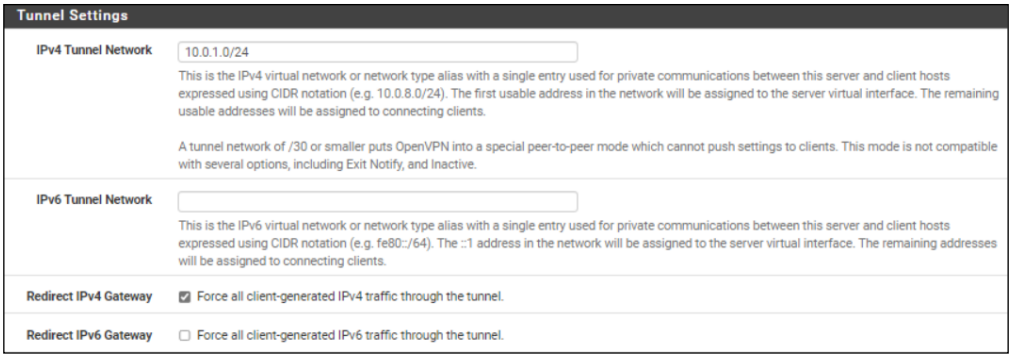

Ilustración 10.22: Creación VPN

Ya tenemos nuestro servidor OpenVPN creado pero primero deberemos configurar algunas reglas en PfSense para permitir el tráfico de la VPN. Accedemos a **Firewall** > **Rules** > **WAN** y creamos una regla nueva. La acción de la regla será **Pass** ya que queremos que permita el tráfico, la interfaz cláramente será la WAN y usaremos el protocolo UDP. Como **Source** dejaremos .Any"para poder acceder desde cualquier lado y como **Destination** también seleccionamos .Any"pero seleccionando como puertos el puerto 1194 que es el que utiliza OpenVPN para la conexión. Es importante marca activos los logs para llevar un registro de las conexiones de la VPN para que si surgiese algún error o en caso de sufrir un ataque poder hacer un seguimiento del accidente.

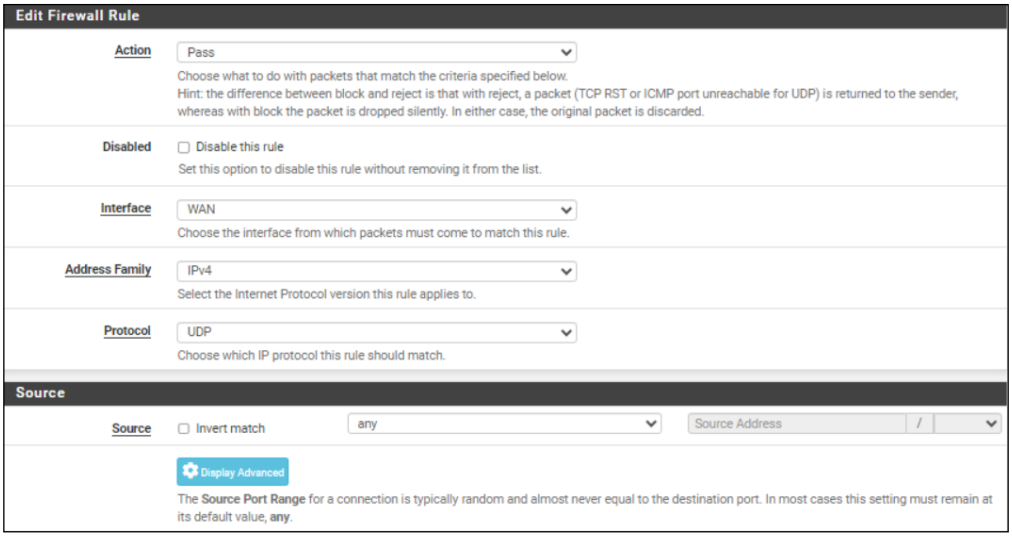

Ilustración 10.23: Regla firewall para OpenVPN

En este punto ya podremos conectarnos a nuestra VPN y obtener acceso a la red interna de PfSense pero no tendremos ningún tipo de conexión, por lo que deberemos crear otra regla que nos permita la conexión desde la VPN, accedemos a **Firewall** > **Rules** > **openVPN** y creamos una regla nueva. Para esta regla deberemos seleccionar como interfaz OpenVPN, protocolo .Anyz tanto en **Source** como en **Destination** pondremos .Any"también.

Con esto ya tenemos nuestra VPN configurada y permitiendo cualquier tipo de conexión desde ella. Más adelante se pueden añadir reglas al firewall para limitar el acceso y el tráfico de la VPN, como por ejemplo sólo permitir el acceso desde España, limitar las conexiones a únicamente el servidor Windows o bloquear el acceso a ciertas webs que puedan ser peligrosas o que no queremos que los usuarios accedan.

10.5.3. Acceso VPN

Como se comentó en el apartado anterior, para acceder a la VPN cada usuario necesita de su certificado. Para exportar los certificados y poderlos entregar a los usuarios deberemos instalar un paquete en PfSense. Deberemos acceder a **System** > **Package Manager** > **Available Packages** e instalar el paquete **openvpn-client-export**, este paquete nos permitirá exportar de una manera sencilla las configuraciones de los clientes de OpenVPN para distintos sistemas incluyendo los certificados de cada usuario. Una vez se haya instalado nos dirigimos a **VPN** > **OpenVPN** > **Client Export**, al final de la página nos aparecerán todos los usuarios que hayamos creado y diferentes clientes de OpenVPN listos para descargar (10.24). Simplemente deberemos descargar el cliente adecuado para el sistema del usuario y se lo haremos llegar.

Ilustración 10.24: Clientes OpenVPN

Dependiendo del sistema que utilicen los usuarios estos tendrán distintas opciones para conectarse a la VPN. Si se trata de un sistema Linux, por ejemplo una distribución Ubuntu, desde el propio administrador de red nos permite importar el cliente que previamente le hemos hecho llegar al usuario (10.25). Una vez importado simplemente activando la VPN nos pedirá las credenciales del usuario y nos dará acceso a la red interna de PfSense. Ya dentro de la red interna de PfSense podremos conectarnos a una sesión remota del servidor Windows tal como se explicará en siguientes apartados.

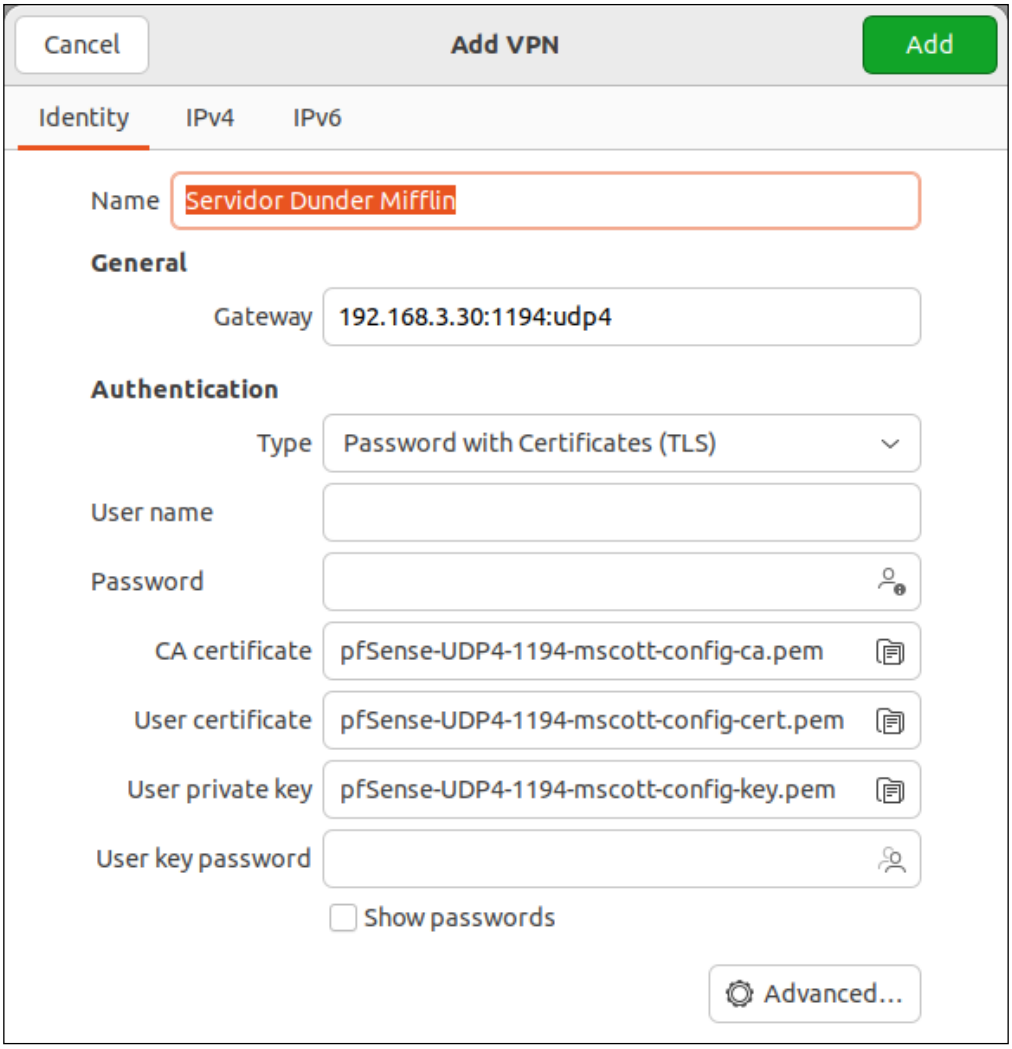

Ilustración 10.25: Cliente VPN importado

Para otros sistemas que no permitan la importación del cliente VPN de manera nativa o se prefiere otra opción, a través de la propia web de OpenVPN se ofrece la descarga de un cliente para todos los sistemas, el usuario deberá descargar e instalar el cliente adecuado para su sistema. Una vez instalado, el cliente de OpenVPN, al igual que el sistema Ubuntu anteriormente, permite la importación del cliente que le hemos hecho llegar la usuario. Al conectarse nos pedirá las credenciales del usuario y accederemos a la red interna de PfSense (10.26).

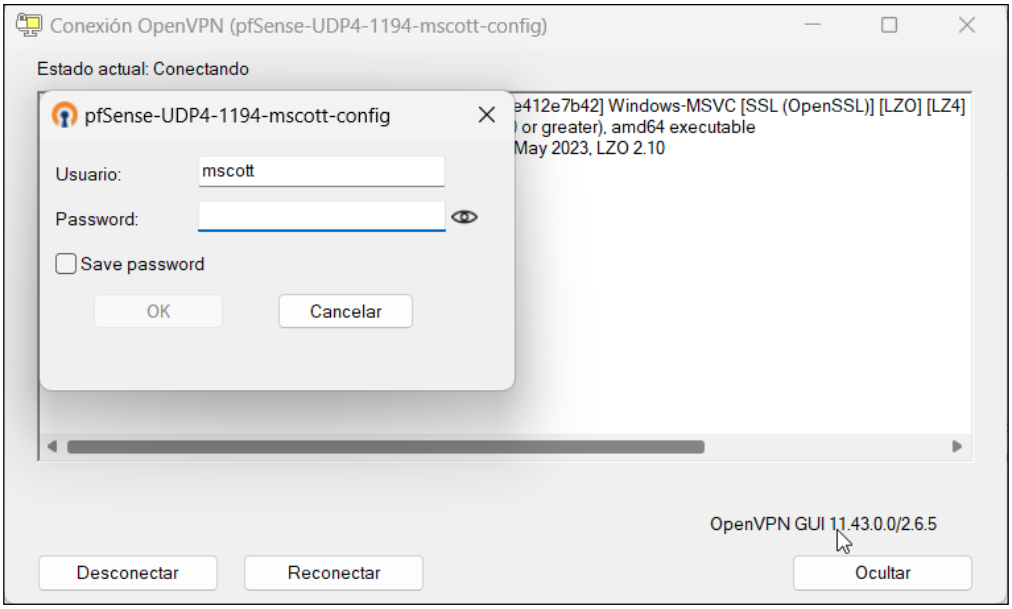

Ilustración 10.26: Cliente OpenVPN

Cuando OpenVPN nos confirme que la conexión ha sido exitosa podremos comprobar que efectivamente estamos dentro de la red interna de PfSense observando la IP que estamos usando y realizando un ping al servidor. Como se ve en las figuras 10.27 y 10.28, se nos ha asignado una IP dentro del rango de red que configuramos para OpenVPN y realizando un ping a la IP del servidor Windows este nos contesta, por tanto la configuración y conexión a la VPN ha sido correcta.

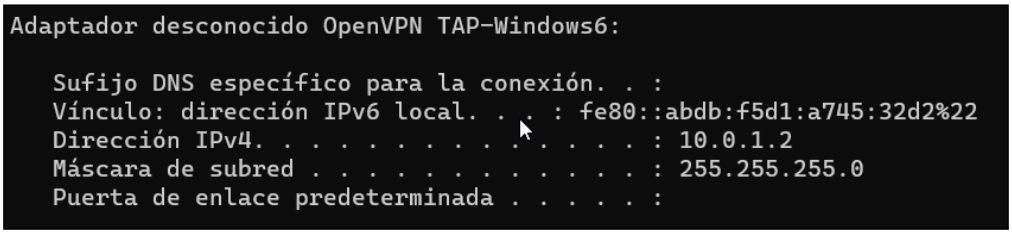

Ilustración 10.27: IP OpenVPN

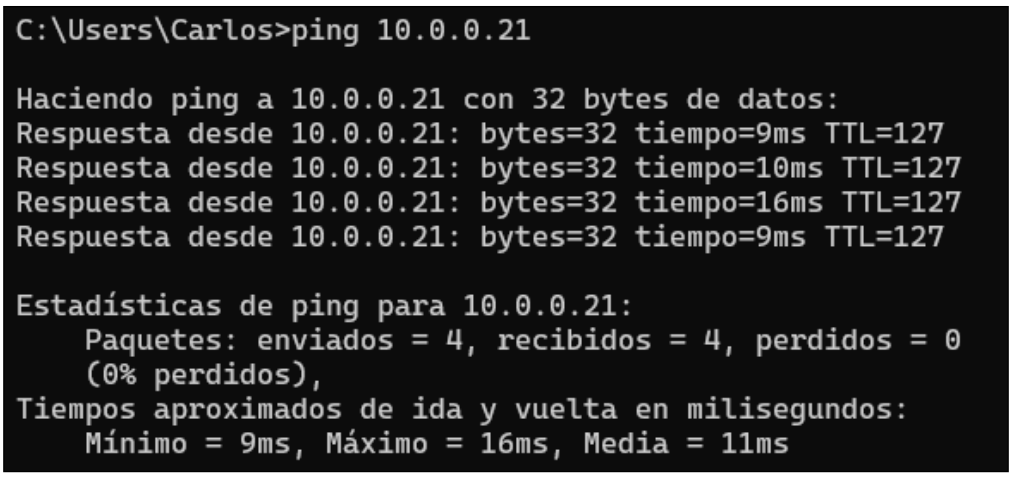

Ilustración 10.28: Ping al servidor exitoso

10.6. Escritorio Remoto

Ahora, que gracias a la VPN tenemos acceso remoto al servidor Windows, procederemos a instalar el rol de **Escritorio Remoto**.

10.6.1. Instalación y configuración servicio Escritorio Remoto

La instalación será igual que hicimos con el directorio activo, en este caso en el panel de instalación, en la sección *Tipo de instalación*, deberemos seleccionar **Instalación de Servicios de Escritorio Remoto**. Como tipo de implementación seleccionamos *Inicio rápido*, ya que solo estamos utilizando un servidor y no queremos instalar cosas innecesarias y en el siguiente apartado de *Escenario de implementación* marcaremos la opción **Implementación de escritorio remoto basada en sesión**, tras esto seleccionamos el servidor donde se instalará. Al finalizar se nos hará un resumen de la instalación y se avisa que el servidor puede reiniciarse para poder aplicar los cambios, pulsamos en implementar y acabamos con la instalación.

Con el rol de *Escritorio Remoto* ya instalado ahora tendremos que gestionar las licencias CAL para los usuarios. Como nos encontramos en un servidor de evaluación, Windows nos proporciona licencias gratuitas que podrán usarse durante 180 días pero para el servidor en producción habrá que adquirirlas, el proceso de activación es igual. Volveremos a *Agregar roles y características*, seleccionamos *Instalación basada en roles y características* y en la página de roles seleccionamos **Servicios de Escritorio Remoto**, de los roles que se incluyen en este paquete deberemos de instalar el rol de **Administración de licencias de Escritorio Remoto**, continuamos hasta el final e instalamos. En el *Administrador del Servidor* nos dirigimos a la pestaña de **Servicios de Escritorio Remoto** > **Servidores**. Haciendo click derecho sobre el servidor nos permitirá acceder al **Administrador de licencias de Escritorio Remoto**, una vez dentro deberemos seleccionar el servidor y **Acción** > **Activar**

servidor, aceptamos todo e introducimos los datos que nos pide sobre la empresa. Ahora seleccionamos **Acción** > **Revisar configuración** > **Añadir al grupo** y aceptamos, hará falta introducir las credenciales de algún administrador del servidor.

Habrá que darle permisos a los usuarios para que puedan conectarse al escritorio remoto. Durante la configuración del Directorio Activo, por cada unidad organizativa creamos un grupo que contenía a los usuarios/unidades del mismo nivel, podemos darle acceso a todos los usuarios si agregamos el grupo *Usuarios del sistema* como miembro del grupo *Usuarios de Escritorio Remoto* o solo hacer miembros de dicho grupo a los grupos que queramos, también se puede dar acceso individual a un usuario. Para ello habrá que dirigirse al administrador de *Usuarios y equipos de Active Directory* y seleccionar el grupo o usuario que queramos que use el servicio, haciendo click derecho y pulsando **Propiedades** veremos una pestaña llamada **Miembro de**, dentro de esa pestaña deberemos de añadir el grupo *Usuarios de Escritorio Remoto* (10.29).

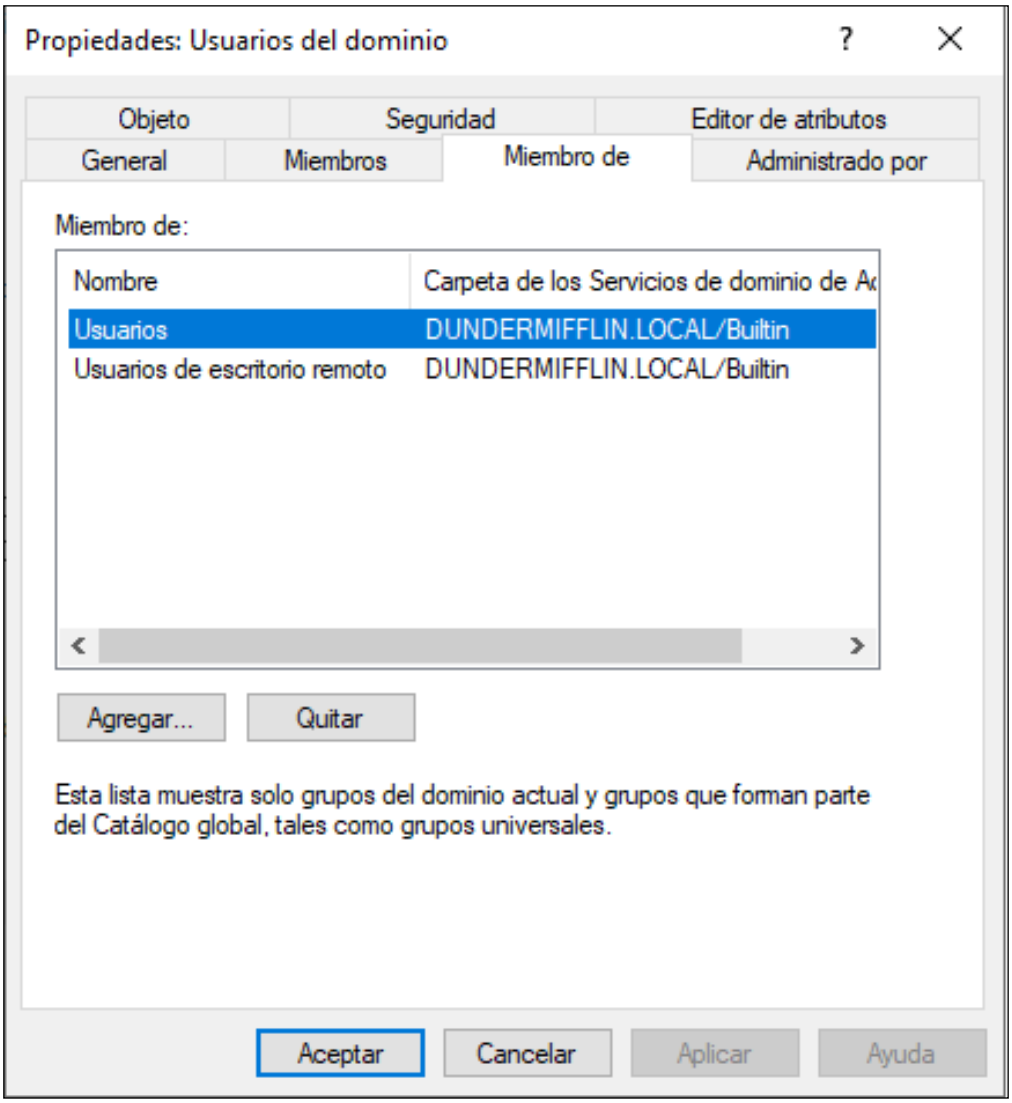

Ilustración 10.29: Grupo miembro de otro grupo

10.6.2. Sesión remota desde sistema Windows

Con los permisos dados ya podemos probar a iniciar una sesión remota, lo primero siempre será conectarse a la VPN como previamente se explicó. Si nos encontramos en un equipo Windows podremos usar la aplicación de **Conexión a Escritorio Remoto** que el propio sistema nos implementa. Nos pedirá que introduzcamos la IP del servidor, que en nuestro caso es la **10.0.0.21** y también podemos agregarle el dominio y usuario que queremos usar, así lo guardará para próximas conexiones y solo tendremos que agregar la contraseña del usuario (10.30).

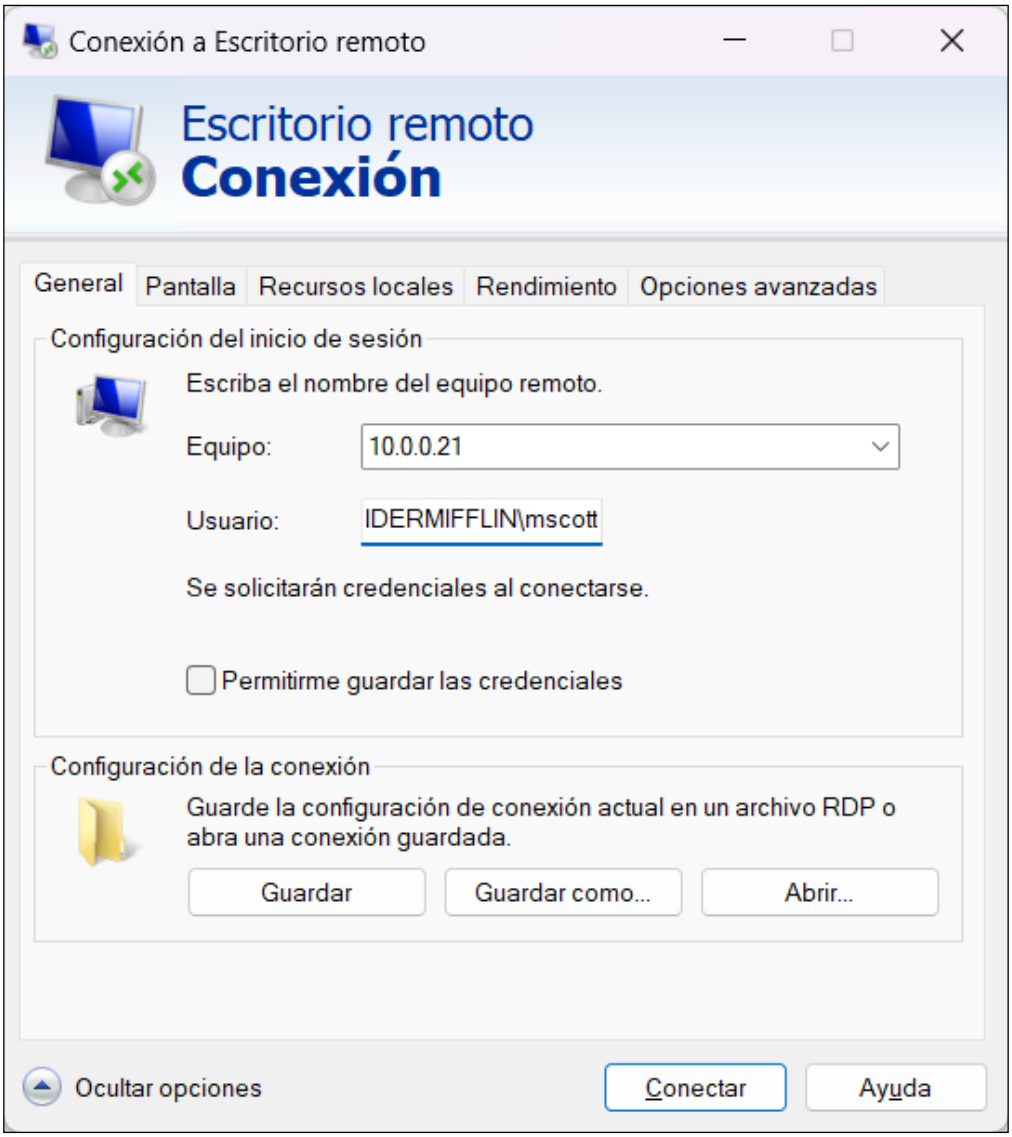

Ilustración 10.30: Conexiópn RDP

Si hemos realizado la configuración del servicio de *Escritorio Remoto* correctamente entonces se abrirá una ventana en la que veremos como se inicia sesión con el usuario que hemos

introducido, como si iniciásemos sesión en cualquier equipo físico con sistema Windows, a partir de ahí el usuario puede trabajar en la sesión remota como lo haría normalmente.

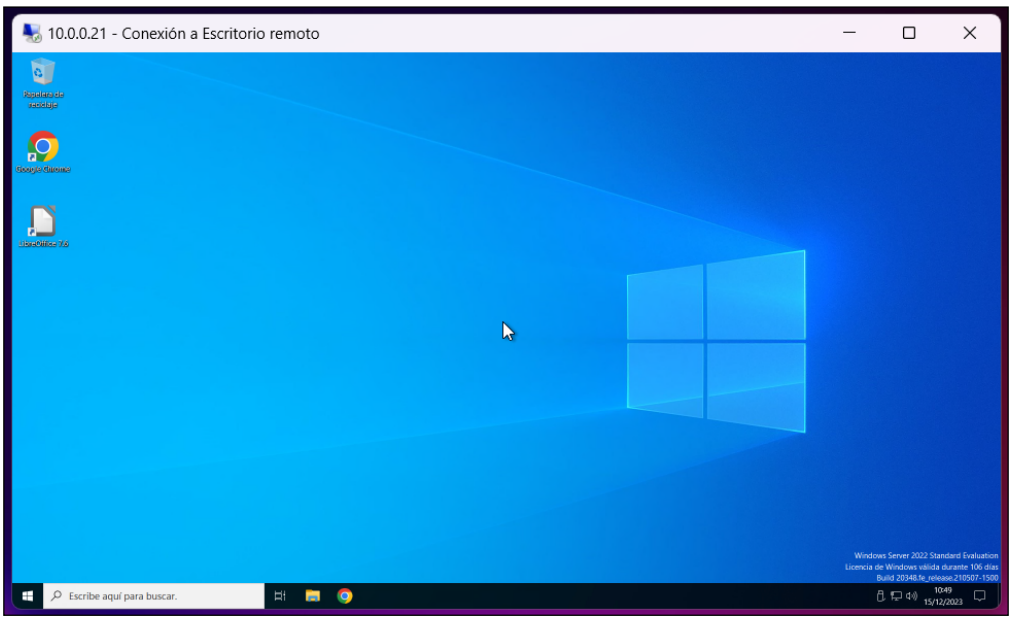

Ilustración 10.31: Sesión remota

10.6.3. Sesión remota desde sistema Linux

En los sistemas Linux, como en los terminales "tontos"de la oficina o si el usuario usase Linux en su equipo, habrá que instalar una aplicación llamada **Remmina** [25]. Remmina es una de las alternativas más usadas como software de escritorio remoto en sistemas Linux, esto gracias a la gran cantidad de opciones que ofrece. Este software es gratuito, implementa varios protocolos que permiten la conexión remota como puede ser RDP, SSH o VNC.

Por normal general, Reminna viene incluido en los repositorios de la mayoría de distribuciones, para la instalación de Remmina nos basaremos en Lubuntu, la distribución que tendrán instalados los equipos "tontos"de la oficina. Lo primero será actualizar los repositorios para seguidamente hacer la instalación.

```
$ apt update
$ apt install remmina
```

Así de sencillo tendremos instalado Remmina en los equipos. Al ejecutar el programa veremos la pantalla 10.32. Como se observa, por defecto nos entra con el protocolo RDP, para conectarnos a la sesión remota simplemente habría que introducir la IP del servidor pero si queremos que la configuración de la conexión se guarde para conexiones futuras podemos pulsar el botón de arriba a la izquierda y completar los datos que se nos piden, Para conexiones futuras simplemente habrá que hacer click sobre el nombre que hayamos elegido para la conexión y se intentará realizar la conexión con los datos guardados.

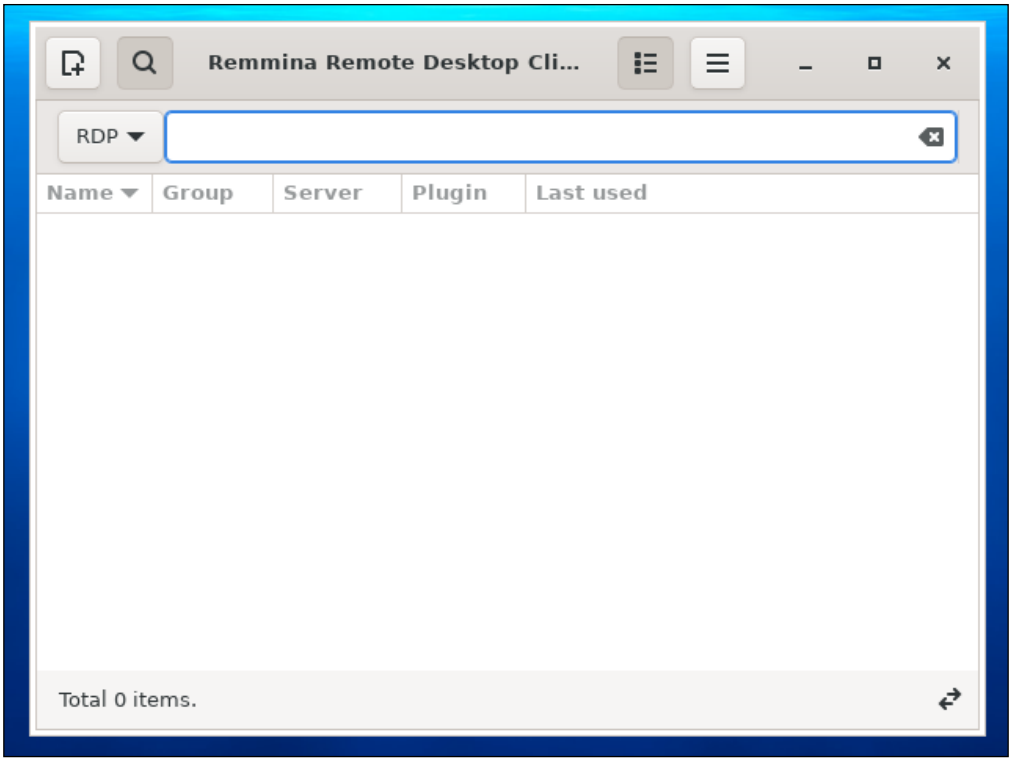

Ilustración 10.32: Remmina dashboard

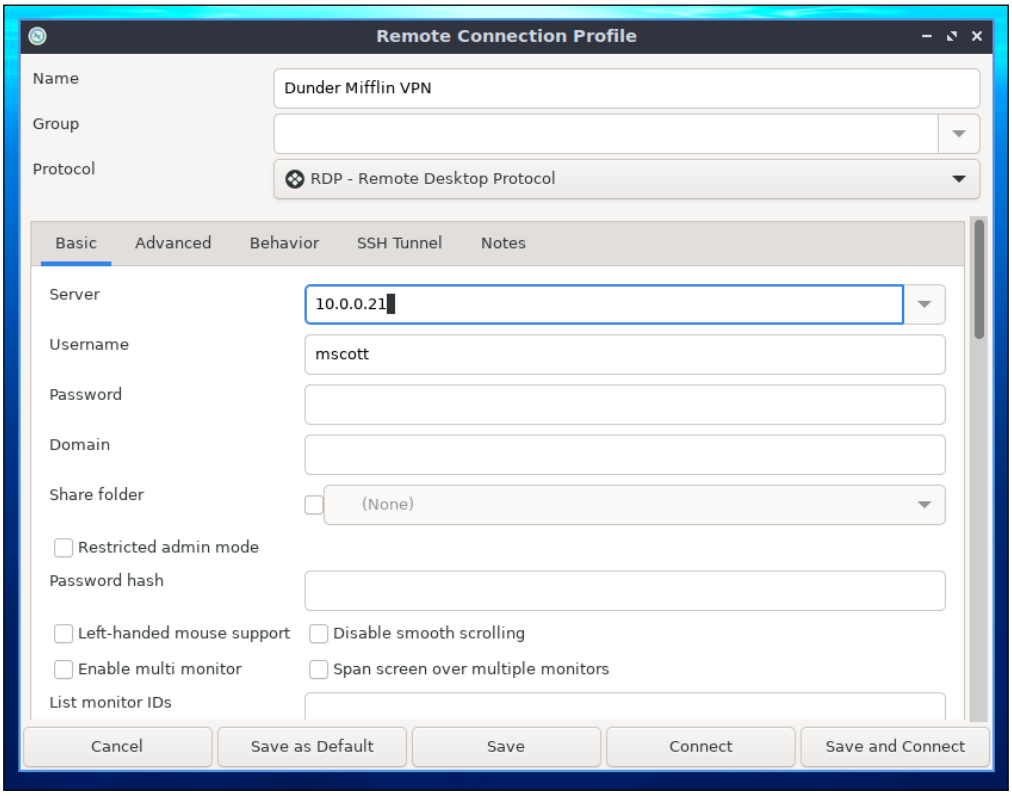

Ilustración 10.33: Remmina conexión guardada

Si los datos de la conexión se han introducido correctamente, al igual que en Windows se abrirá una ventana con la sesión remota del servidor Windows.

10.6.4. Administración sesiones

En el servidor Windows, si vamos al *Administrador del Servidor* > *Servicio de Escritorio Remoto* > *QuickSessionCollections* podremos ver a la derecha las sesiones remotas activas (10.34). En dicha apartado se pueden observar los usuarios que tienen sesiones remotas abiertas, se diferencian entre sesiones activas o desconectadas, las sesiones activas son sesiones abiertas y que están en uso y las desconectadas son sesiones que no están en uso pero no están siendo usadas, así como si suspendiéramos la sesión.

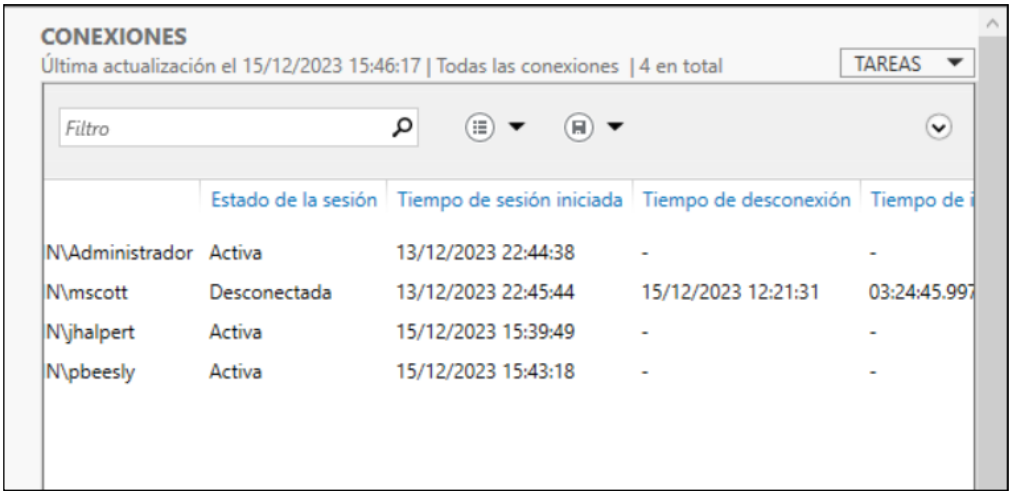

Ilustración 10.34: Sesiones remotas activas

Si hacemos click sobre un usuario nos aparecerán varias opciones, una de ellas es la sombra. Como administradores del servidor, podemos hacer sombra a un usuario para observar o tomar control de su sesión y así poder solucionar algún si surgiese.

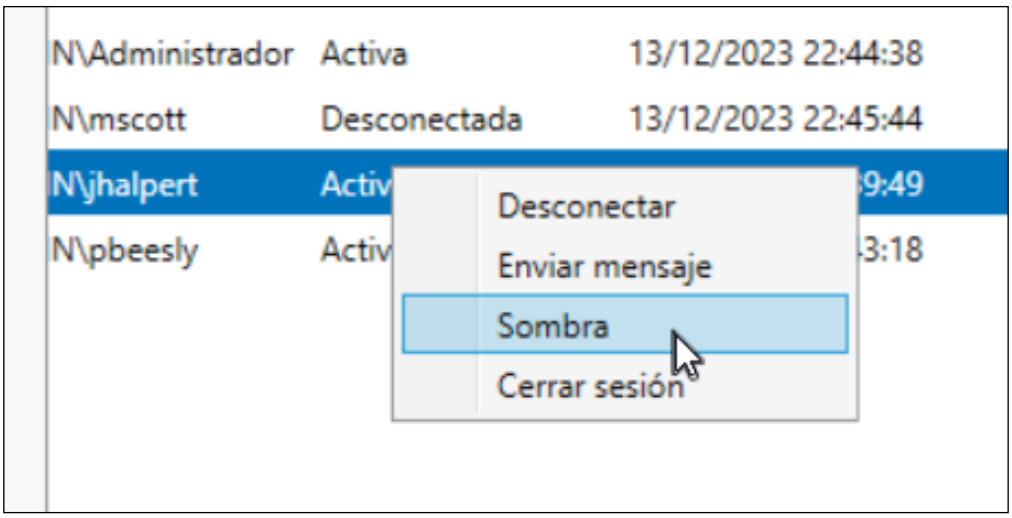

Ilustración 10.35: Opción de sombra

10.7. Rendimiento

Para comprobar que el sistema es capaz de soportar una carga de trabajo adecuada al uso que se quiere hacer de este se han abierto 5 sesiones remotas. Estas 5 sesiones de escritorio remoto simulan a usuarios conectados al servidor, para cada sesión se han abierto múltiples ventanas en el navegador Chrome y se han ejecutado programas de ofimática del paquete Libre Office.

Igual que se explicó en el apartado de *Escritorio Remoto*, si accedemos a este servicio desde el *Administrador del servidor* podremos ver las sesiones abiertas que existan en ese momento e interactuar con ellas, pero si queremos ver el uso de recursos que hace cada sesión entonces habrá que hacer uso del *Administrador de Tareas*. En el *Administrador de Tareas* habrá que entrar en la pestaña de *Usuarios*, ahí se mostrarán todos los usuarios que poseen una sesión abierta en el servidor igual que podíamos ver desde el *Administrador del servidor* pero con la diferencia de que en este caso se muestra el uso de CPU y memoria RAM total del sistema y específico de cada usuario.

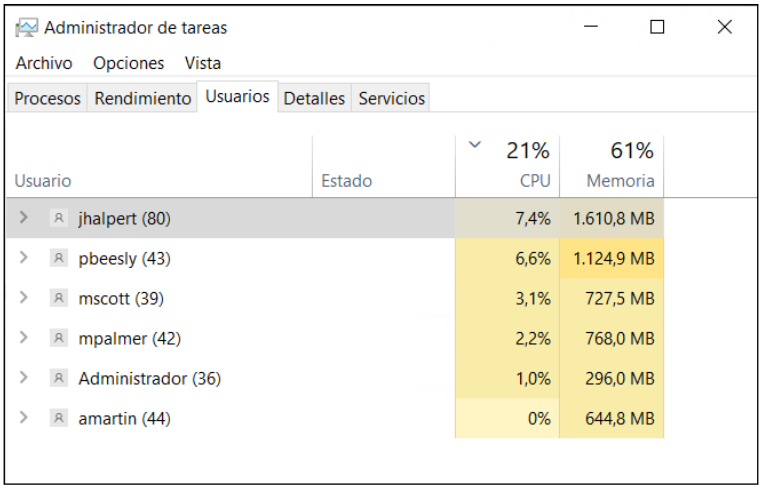

Ilustración 10.36: Uso de recursos del servidor

Como puede observarse en la ilustración 10.36, el servidor tiene un uso de recursos óptimos y no se encuentra sobrecargado. Las sesiones remotas se ejecutan correctamente y de forma fluida, no notando ninguna diferencia respecto al uso de un equipo físico para abrir la sesión. Dada la carga del servidor, este aún podría soportar el uso de programas que requieran de un mayor uso de recursos o incluso soportar más sesiones activas conjuntamente.

Si en algún momento notásemos que el sistema está sobrecargado puede deberse al uso excesivo de recursos por parte de un usuario, ya sea por el uso de programas que requieren de grandes recursos o por el fallo de algún programa que lo haga usar más recursos de los esperados. Si se da el caso podemos desplegar la sesión de cada usuario y observar qué programas está corriendo cada uno para detectar cuál es el que está ahogando al sistema.

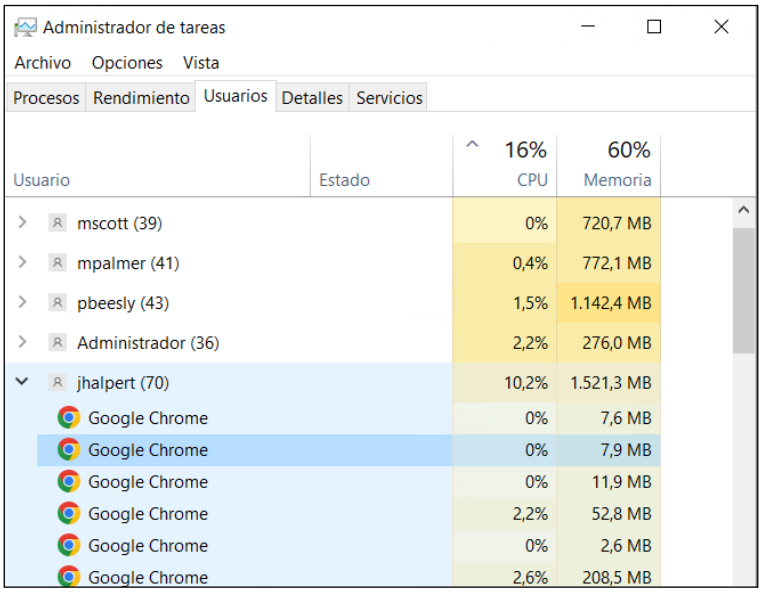

Ilustración 10.37: Tareas por usuario

En el caso mostrado en la ilustración 10.37, no existe ningún programa que esté haciendo un uso excesivo de recursos, pero si así fuese simplemente bastaría con seleccionarlo, click derecho y finalizar su ejecución.

10.8. Medidas adicionales

Tras la instalación y configuración de la infraestructura ahora se pasará a comentar otras medidas adicionales que ayudarán a que el sistema sea todavía más seguro.

Como primera medida se recomienda el uso de programas antivirus, gracias a estos el sistema se encuentra en constante monitoreo que, en caso de detectar patrones de actuación propios de un malware lo bloquearán al instante evitando así que se propague por el sistema causando problemas.

Otra medida y la más importante de todas, mas allá de todas las configuraciones que se han realizado en la infraestructura, es la formación de los usuarios. Actualmente el principal vector de entrada de los ciberataques son los propios usuarios del sistema, mediante ataques de phishing [26] o de ingeniería social [27] los atacantes son capaces de engañar a los usuarios para conseguir las credenciales de estos.

Cada vez son más las empresas que son conscientes de los peligros a los que se encuentran expuestos y deciden invertir en seguridad informática, esto es un quebradero de cabeza para los ciber criminales pues se encuentran con más sistemas que implementan más y mejores medidas de seguridad. A pesar de la mejora en las medidas de seguridad, el vector que siempre es olvidado es la formación de los usuarios del sistema, esto es aprovechado por los atacantes ya que requiere de bastante menos esfuerzo que intentar burlar las medidas de seguridad.

Capítulo 11

Resultados, mejoras futuras y conclusiones

11.1. Resultados

Una vez acabada la implementación de toda la infraestructura, se ha conseguido cumplir con los objetivos propuestos. Se ha conseguido crear una infraestructura informática completa que brinda los servicios de Escritorio remoto y Directorio Activo a sus usuarios disponiendo de unos controles de seguridad que frenan en gran medida la posibilidad de sufrir algún tipo de ataque.

Gracias a esta implementación ahora los usuarios podrán desarrollar su trabajo desde cualquier equipo, ya sea en la oficina o sus casas, sin diferencia alguna en el servicio.

Para las empresas esto supone un ahorro en costes, una mayor tranquilidad al disponer de un entorno de trabajo seguro y la posibilidad de ofrecer a sus usuarios unas mejores condiciones laborales al existir la capacidad del trabajo en remoto.

11.2. Mejoras futuras

Al tratarse de un entorno virtualizado, este permite una gran escalabilidad. Si el número de usuarios crece con el tiempo tan sólo haría falta contratar más licencias CAL para el servidor y si los recursos del servidor se viesen al límite sería tan sencillo como aumentarlos en el equipo host, como podría ser aumentar la capacidad de los discos duros, aumento de la memoria RAM o incluso hacer uso de un procesador más potente, y posteriormente desde Proxmox actualizar los recursos de las máquinas virtuales a los nuevos recursos del equipo host.

Otra opción de escalabilidad es la de implementar un clúster. Proxmox dispone nativamente de la opción de creación de un clúster, para ello se necesitan dos nodos proxmox. Si se tuviesen

dos equipos hosts con Proxmox instalado podría utilizarse esta opción que podría brindar balanceo de carga entre los nodos o alta disponibilidad de los servicios que estos contengan.

11.3. Conclusiones

Como se ha podido observar, la configuración de una infraestructura informática completa que implemente medidas de seguridad es algo que está al alcance de cualquier empresa que decida invertir en proteger su información frente a los ciber delincuentes. Gracias a este proyecto, esas medidas pueden ser aplicadas de una manera rápida, sencilla y asequible.

Con la creación de este proyecto se espera concienciar sobre los peligros a los que se encuentra expuesto cualquier sistema y de la importancia de protegerlos debidamente.

Capítulo 12

Anexo I

12.1. Instalación Proxmox

Para la instalación del sistema anfitrión Proxmox deberemos tener una imagen ISO del sistema en una unidad de almacenamiento externa desde la que arrancaremos el equipo. La imagen puede descargarse desde la web de Proxmox, se deberá descargar la versión **'Proxmox Virtual Environment'**, en este caso hemos descargado la **versión 8.0.3**. Con la imagen ISO descargada tendremos que montarla en la unidad externa, para ello pueden utilizarse herramientas como 'Rufus' o 'Balena Etcher'. Con la imagen ISO del sistema Proxmox ya montada en la unidad externa ya podemos proceder a introducirla en el equipo en el que queremos instalarla.

Con la unidad externa insertada en el equipo podemos arrancar el mismo, mientras se inicia deberemos pulsar la combinación de teclas necesarias para acceder a la BIOS y configurar como unidad de arranque la unidad externa que contiene la imagen Proxmox. Con esta configuración realizada podemos guardar los cambios y reiniciar el arranque.Una vez arrancado el sistema, si hemos hecho todos los pasos previos correctamente, nos aparecerá la siguiente pantalla de bienvenida (Ilustración 12.1) en la que seleccionaremos **'Install Proxmox VE (Graphical mode)'**.

Nos saldrá el 'Acuerdo de Licencia para el usuario final', simplemente pulsamos en **'I Agree'**. Ahora nos preguntará en qué disco queremos instalar el sistema, en este caso se ha elegido el disco */sde*, que para este caso es un disco de 500Gb, y hacemos click en el botón de siguiente.

Lo siguiente será seleccionar nuestra localización y zona horaria, introducimos la que corresponda y seguimos. Nos pedirá que añadamos una contraseña de *root*, que servirá para acceder al sistema más adelante, y un correo electrónico que puede ser configurado para recibir alertas.

Tras hacer lo anterior, pasaremos a hacer la configuración de red con los siguientes parámetros:

* Tarjeta de red: eno01

Ilustración 12.1: Pantalla inicial Promox

* Hostname: proxmox.local
* Dirección IP: 192.168.3.10/24
* Servidor DNS: 8.8.8.8 (Google)

Una vez hayamos configurado todo lo mencionado anteriormente nos aparecerá una pantalla con el resumen de la configuración para que podamos comprobar que hemos introducido todos los datos correctamente. Si todo está bien, seleccionamos la casilla de **'Automatically reboot after successful installation'** y procederemos a instalar el sistema. Cuando se termine la instalación el sistema se reiniciará, cuando vuelva a iniciar nos encontraremos la siguiente pantalla (Ilustración 12.2).

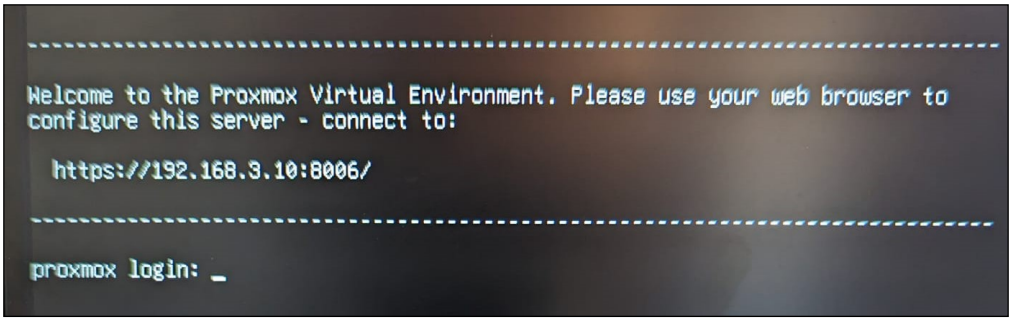

Ilustración 12.2: Shell Proxmox

El sistema nos da la bienvenida y nos proporciona una URL (https://192.168.3.10:8006 para el caso) desde la que podremos gestionar el sistema de manera gráfica a través de un navegador web desde cualquier equipo externo que se encuentre en la misma red. Además, nos proporciona una shell desde la que podremos iniciar sesión y gestionar el sistema a través de línea de comandos.

Capítulo 13

Anexo II

13.1. Instalación PfSense

Para la creación de la máquina virtual que hará de firewall gracias al sistema PfSense primero tendremos que tener una imagen del mismo en Proxmox, para ello desplegamos el nodo proxmox seleccionamos el volumen *local* y entre los distintos tipos de archivos que nos aparecen en el menú de la izquierda seleccionamos **ISO Images**. Se nos da la opción tanto de subir la imagen ISO desde el equipo que estamos conectados a Proxmox como de descargarla directamente a través de su URL. La imagen puede obtenerse desde la web de PfSense, para este caso se ha usado la versión 2.7.0 para la arquitectura amd64. Con la imagen subida ya podemos proceder con la creación de la máquina.

Arriba a la derecha existe un botón llamado **Create VM**, hacemos click y nos aparecerá un panel para la creación de la máquina como el que se muestra en 13.1.

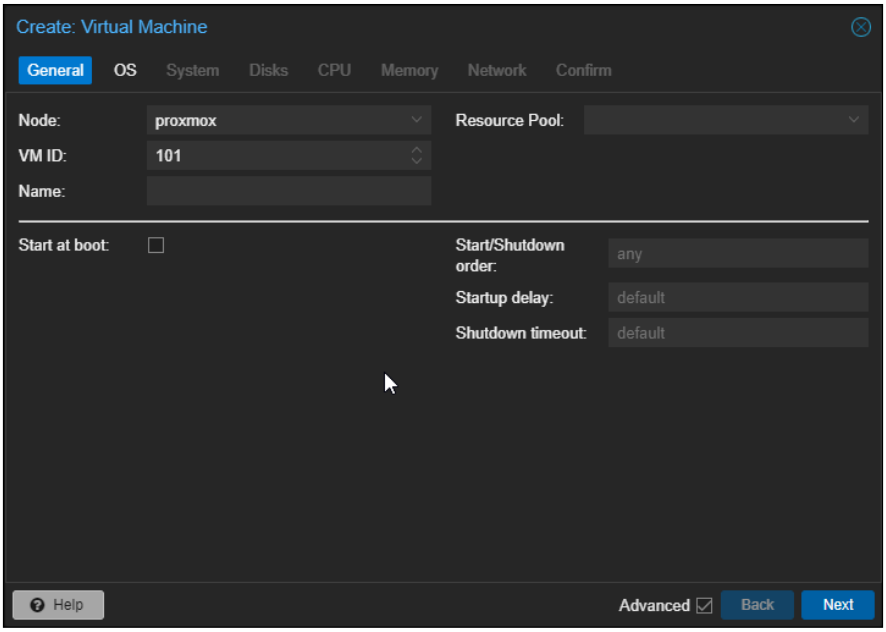

Ilustración 13.1: Panel creación máquina virtual

En el apartado de *General* le asignamos un ID a la máquina, elegimos su nombre (se ha seleccionado *PfSense* en este caso) y podemos elegir si queremos que la máquina se inicie automáticamente cuando el sistema Proxmox se inicie, dejaremos esta última opción desmarcada por el momento hasta que el firewall no esté completamente configurado.

Siguiendo al apartado del sistema operativo le indicaremos la imagen ISO que queremos usar y dejamos seleccionada la opción del kernel que nos aparece por defecto que es *Linux 6.x - 2.6 Kernel*.

Continuando a Sistema dejamos todo por defecto y activamos el Qemu Agent. El Quemu Agent mejora la comunicación entre el host y la maquina virtual como por ejemplo para conocer información del sistema operativo invitado, controlar el apagado y reinicio o gestionar las instantáneas de las máquinas virtuales entre otras cosas.

Ahora en Discos veremos como por defecto nos aparece el volumen ZFS01 que creamos como almacenamiento, seleccionamos el número de GB de almacenamiento que queremos asignar a la máquina y, en caso de estar usando discos SSD, activamos la casilla *SSD Emulation*, que no es nuestro caso.

Para el apartado CPU seleccionaremos 1 socket y 2 cores para este caso y continuamos con la memoria. De memoria bastará con 2Gb.

En la sección de Memoria es importante marcar la casilla de **No Network Device** para este caso ya que manualmente añadiremos nosotros las interfaces de red. Con esto ya habremos terminado con la creación de la máquina, el último apartado es un resumen de toda la configuración que hemos hecho. Si está todo correcto podemos darle a *Finish*.

Como se nombró anteriormente, ahora procederemos a asignar las interfaces de red manual-

mente. Por defecto, Proxmox crea una red virtual asociada a cada interfaz física que nombra como *vmbr0, vmbr1, ... , vmbrX* así según el número de interfaces de red físicas instaladas, podemos ver las interfaces accediendo al nodo **proxmox** > **Network**. Como esta máquina servirá de servidor serán necesarias dos redes, una para el tráfico externo y otra para el interno. La red que usamos como externa tendrá asignada ya la IP que configuramos durante la instalación de proxmox, pero deberemos de asignarle una IP a la interfaz de red interna. Para este caso se ha asignado la IP 10.0.0.10/24.

En el menú de la izquierda ya aparecerá la máquina que acabamos de crear, pulsamos en ella y vamos a la sección de hardware, nos aparecerá un resumen del hardware de la máquina. Pulsamos en añadir y seleccionamos **Network Device**, nos saldrá un panel como el que se ve en 13.2. Deberemos de seleccionar una de las interfaces de red virtuales que están asociadas al equipo físico, en el modelo usaremos Intel E1000 para que no paravirtualice la interfaz y utilice el dispositivo del host directamente.

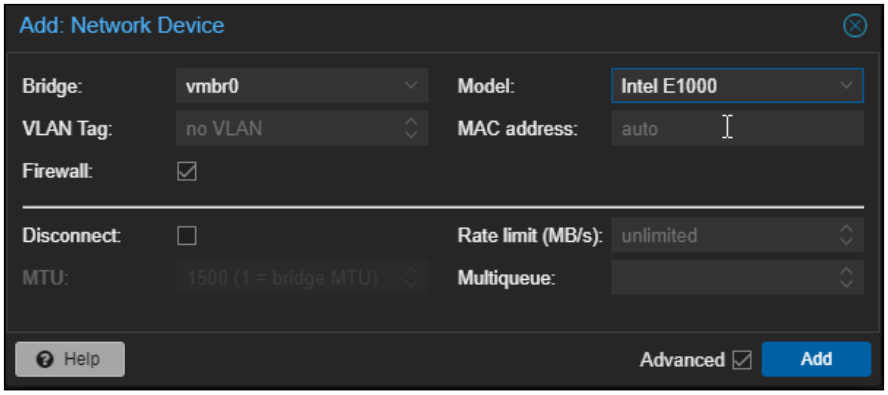

Ilustración 13.2: Asignación interfaces de red a máquina virtual

Una vez añadidas las dos redes el resumen del hardware nos debe de quedar de la siguiente manera:

Memory	2.00 GiB
Processors	2 (1 sockets, 2 cores) [x86-64-v2-AES]
BIOS	Default (SeaBIOS)
Display	Default
Machine	Default (i440fx)
SCSI Controller	VirtIO SCSI single
CD/DVD Drive (ide2)	local:iso/pfSense-CE-2.7.0-RELEASE-amd64.iso,media=cdrom,size=747284K
Hard Disk (scsi0)	ZFS01:vm-102-disk-0,iothread=1,size=32G
Network Device (net0)	e1000=AE:59:8B:DC:4C:79,bridge=vmbr0,firewall=1
Network Device (net1)	e1000=E2:6B:92:96:7D:10,bridge=vmbr1,firewall=1

Ilustración 13.3: Resumen hardware máquina firewall

Vamos al apartado *Console* y nos aparecerá la pantalla del sistema pfSense que nos ofrecerá diferentes opciones, seleccionamos **Install pfSense**. La instaliópn es bastante sencilla, dejaremos todo copn las opciones que se nos dan por defectos y al llegar a la ventana titulada

ZFS Configuration activaremos *QEMU HARDDISK*. Cuando hayamos terminado nos pedirá reiniciar, aceptamos.

Cuando el sistema ya inicie con pfSense instalado podremos ver lo siguiente:

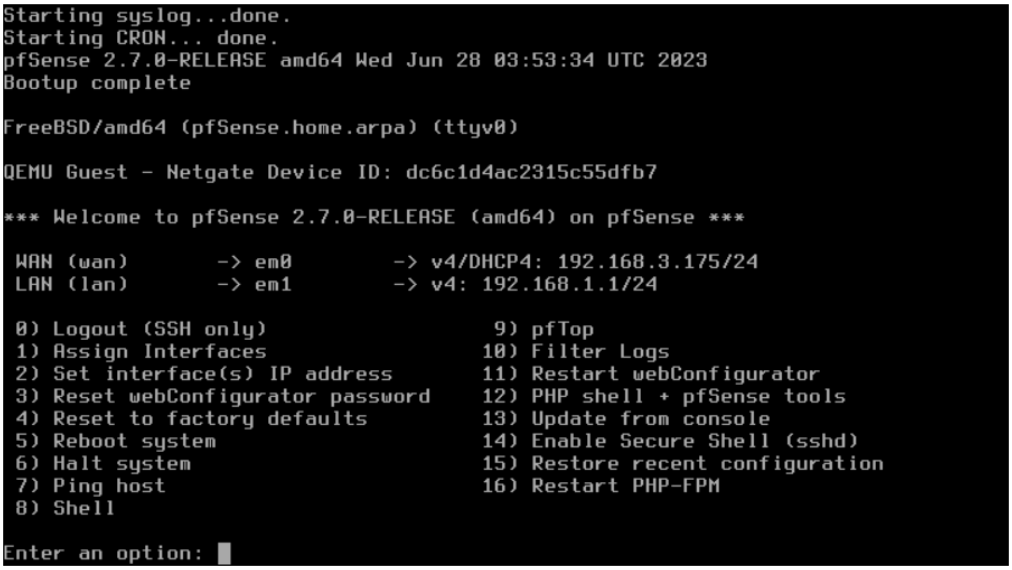

Ilustración 13.4: Pantalla inicial pfsense

Como se puede observar en 13.4, pfSense ha detectado automáticamente las dos interfaces de red, las ha asignado como WAN y LAN correctamente y asignado una IP para cada una. La red WAN ha obtenido su IP a través del protocolo DHCP, esto no nos interesa ya que si la máquina se reiniciase podría cambiar la IP y fallar toda la configuración que hagamos en breve, por ello debemos modificar la red WAN para que tenga IP fija y además también modificaremos la red LAN para asignarle la red que deseemos.

pfSense nos porporciona hasta 16 opciones que se pueden ver en 13.4, nos interesa la opción 2 **Set interface(s) IP address**. Seleccionamos la opción y nos pedirá que introduzcamos la interfaz a la que queramos modificar la IP, comenzaremos con la red WAN. La primera pregunta que nos hará será si queremos configurar la IP a través de DHCP, anteriormente hemos dicho que esto no nos interesa así que le indicamos que no, entonces nos pedirá que introduzcamos la IP fija que le queremos asignar a la interfaz, en este caso se ha elegido la IP 192.168.3.30 para la interfaz WAN. Nos pedirá que indiquemos la máscara de subred, como es una red de tipo C indicamos 24 y ahora nos preguntará por el gateway, el gateway será nuestro router así que en este caso introducimos 192.168.3.1.Nos preguntará si queremos configurar la IPv6 por DHCP, indicamos que no y para terminar, nos pregunta si queremos desactivar el servidor DHCP para la interfaz WAN, indicamos que si. Nos hará una última pregunta sobre si queremos cambiar al protocolo HTTP el configurador web, deberemos seleccionar que no ya que si no luego se nos puede dificultar el acceso al entorno web de pfSense.

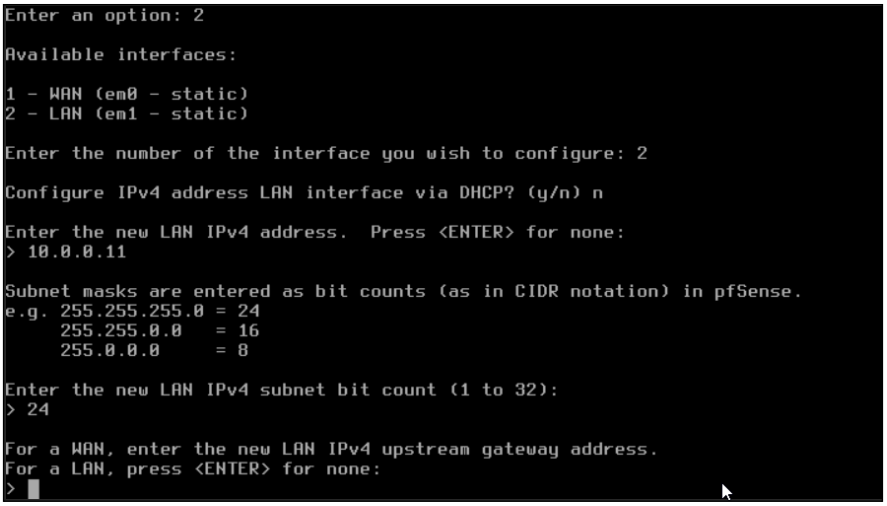

Ilustración 13.5: Configuración LAN - 1

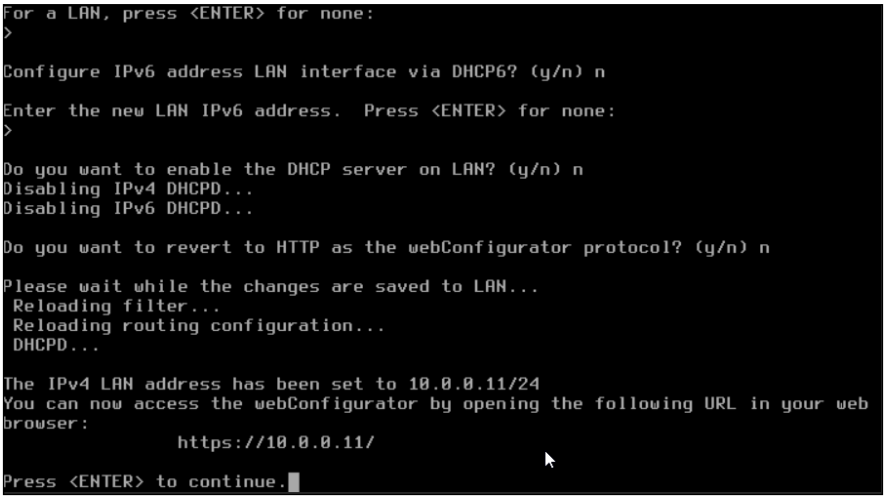

Ilustración 13.6: Configuración LAN - 2

Ahora haremos lo mismo para la interfaz LAN. Seguiremos el mismo procedimiento a diferencia de que como ahora es una interfaz para la red interna no configuraremos el gateway, le asignamos la IP 10.0.0.11. A través de esa IP será por donde accedamos al panel de configuración web que nos proporciona pfSense como lo hace Proxmox.

Capítulo 14

Anexo III

14.1. Instalación Windows Server

Se va a proceder a crear una máquina virtual e instalar en ella el sistema Windows Server 2022, esta máquina hará de servidor. Para este apartado deberemos de haber descargado y subido a proxmox, como se explica en el Anexo II, dos imágenes ISO, una del sistema Windows Server y otra de los drivers necesarios. La imagen del sistema Windows Server puede obtenerse a través de la web de Microsoft, podemos descargar una versión de evaluación desde el centro de evaluación de Microsoft. Los drivers se puieden encontrar en RELLENAR.

Creamos la máquina de la misma manera que hicimos en el Anexo II. Para el caso de esta máquina que llevará el sistema Windows Server tendremos que hacer algunas modificaciones durante la creación de la máquina respecto a cómo lo hicimos para pfSense. En este caso:

- ✔ Apartado OS: Seleccionar OS *Microsoft Windows 11/2022*.
- ✔ Apartado System: Desactivar la casilla **Add TPM** y seleccionar como *EFI Storage* el volumen ZFS01 que hemos creado.
- ✔ -Apartado Disks: Seleccionar como *Bus/Device* **VirtIO Block** y seleccionar la caché como **Write back**.
- ✔ Apartado CPU: En este caso se han elegido 2 sockets y 2 cores, resultando en un total de 4 cores. Elegir el *Type* como **host**.
- ✔ Apartado Memory: Elegir la RAM deseada, en este caso se han seleccionado 16Gb.
- ✔ Apartado Network: Deberemos elegir la interfaz que tengamos configurada para la LAN, en este caso *vmbr1*.

Tras crear la máquina con las especificaciones anteriores ahora debemos de añadirle un disco con la imagen de los drivers. Al igual que hicimos con la máquina pfSense para añadirle las interfaces de red, nos dirigimos a *Hardware*, pulsamos en *Add* y seleccionamos *CD/DVD Drive*. Nos saldrá un panel como el de 14.1, simplemente seleccionamos la imagen ISO de los

drivers que deberemos de haber subido previamente y ya tendremos la máquina virtual lista para arrancarla.

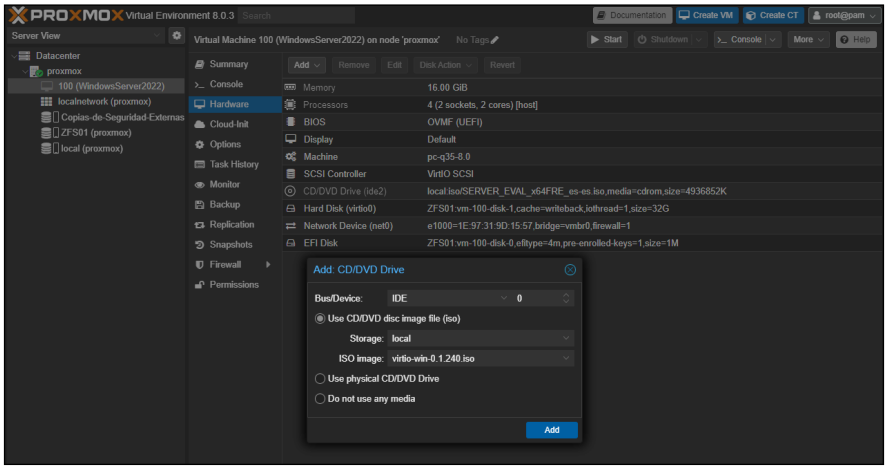

Ilustración 14.1: Añadir disco drivers

Iniciamos la máquina y al dirigirnos a *Console* veremos la pantalla de la máquina que nos muestra el panel de instalación típico de Windows. Iniciamos la instalación como lo haríamos con cualquier sistema Windows y en algún momento nos preguntará qué sistema queremos usar, seleccionaremos **Windows Server 2022 Standard Evaluation** con la experiencia de escritorio. Seguimos con la instalación y cuando nos pregunte qué tipo de instalación queremos seleccionaremos personalizada. En este punto deberemos pulsar en cargar controlador y examinar para poder elegir los controladores y que nos detecte el disco en el que instalaremos el sistema. Desplegamos el disco *VirtIO*, desplegamos *amd64* y seleccionamos la carpeta *2k22*, una vez cargue el driver hacemos click en siguiente y procederá a su instalación, una vez terminada nos aparecerá el disco en el que podremos instalar el sistema. Tras esto se comenzará a instalar el sistema.

Con el sistema instalado nos pedirá que creemos una contraseña para el usuario Administrador y ya nos dejará iniciar sesión. Para poder instalar los drivers iremos al explorador de archivos, accedemos al disco *VirtIO* y ejecutamos **virtio-win-guest-tools**, una vez hecho deberemos reiniciar. Con todo lo anterior realizado ya tendremos nuestro sistema listo para su configuración.

Capítulo 15

Bibliografía

[1] Ministerio del Interior, "España registró 374.737 ciberdelitos en 2022"(en línea. 20 de octubre de 2023).
Disponible en: https://www.interior.gob.es/opencms/es/detalle/articulo/Espana-registro-374.737-ciberdelitos-en-2022/

[2] Cope, "España es el tercer país del mundo que más ciberataques recibe"(en línea. 21 de septiembre de 2023).
Disponible en: https://www.cope.es/actualidad/sociedad/noticias/espana-tercer-pais-del-mundo-que-mas-2908999

[3] ChannelE2E, "Global Remote Desktop Market Sees 15 per cent Growth: Report"(en línea. 8 de mayo de 2023).
Disponible en: https://www.channele2e.com/news/global-remote-desktop-market-sees-15-growth-report

[4] Microsoft, "Windows Server 2022"(en línea. 22 de diciembre de 2023).
Disponible en: https://www.microsoft.com/es-ES/evalcenter/evaluate-windows-server-2022

[5] Netgate, "pfSense Documentation"(en línea. 22 de diciembre de 2023).
Disponible en: https://docs.netgate.com/pfsense/en/latest/

[6] Proxmox, "Proxmox Virtual Environment"(en línea. 22 de diciembre de 2023).
Disponible en: https://www.proxmox.com/en/proxmox-virtual-environment/overview

[7] Microsoft, "Servicios de Escritorio remoto"(en línea. 13 de junio de 2023).
Disponible en: https://learn.microsoft.com/es-es/windows/win32/termserv/terminal-services-portal

[8] ICM, "Thin Client ¿qué es y para qué sirve?"(en línea. 23 de julio de 2019).
Disponible en: https://www.icm.es/2019/07/23/thin-client/

[9] GNU, "GNU General Public License"(en línea. 22 de diciembre de 2023).
Disponible en: https://www.gnu.org/licenses/gpl-3.0.html

[10] GNU, "GNU Affero General Public License"(en línea. 22 de diciembre de 2023).
Disponible en: https://www.gnu.org/licenses/agpl-3.0.html

[11] GNU, "GNU Lesser General Public License"(en línea. 22 de diciembre de 2023).
Disponible en: https://www.gnu.org/licenses/lgpl-3.0.html

[12] AppMaster, "¿Qué es la licencia BSD"(en línea. 25 de enero de 2023).
Disponible en: https://appmaster.io/es/blog/que-es-la-licencia-bsd

[13] Licen.cc "Licencia MIT"(en línea. 22 de diciembre de 2023).
Disponible en: https://www.licen.cc/es/licencias/mit/

[14] Universidad Complutense de Madrid, "Licencia MPL"(en línea. 18 de noviembre de 2017).
Disponible en: https://wikis.fdi.ucm.es/ELP/Licencias_MPL

[15] Microsoft, "Licencias de acceso de cliente y licencias de administración"(en línea. 22 de diciembre de 2023).
Disponible en: https://www.microsoft.com/es-xl/licensing/product-licensing/client-access-license

[16] Jefatura del Estado, "Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales "(en línea. 6 de diciembre de 2018).
Disponible en: https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf

[17] OBS Business School, "Características y fases del modelo incremental"(en línea. 22 de diciembre de 2023).
Disponible en: https://www.obsbusiness.school/blog/caracteristicas-y-fases-del-modelo-incremental

[18] Red Hat, "¿Qué son las KVM?"(en línea. 22 de diciembre de 2023).
Disponible en: https://www.redhat.com/es/topics/virtualization/what-is-KVM

[19] noVNC, "noVNC - the Open Source VNC Client"(en línea. 22 de diciembre de 2023).
Disponible en: https://novnc.com/info.html

[20] Microsoft, "Introducción a Active Directory Domain Services"(en línea. 9 de marzo de 2023).
Disponible en: https://learn.microsoft.com/es-es/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview

[21] OpenVPN, "Secure access and network connectivity reimagined"(en línea. 22 de diciembre de 2023).
Disponible en: https://openvpn.net/

[22] Intel, "Definición de volúmenes RAID para la tecnología Intel® de almacenamiento rápido"(en línea. 17 de octubre de 2017).
Disponible en: https://www.intel.la/content/www/xl/es/support/articles/000005867/technologies.html

[23] Oracle, "Definición de ZFS"(en línea. 22 de diembre de 2023).
Disponible en: https://docs.oracle.com/cd/E19253-01/820-2314/zfsover-2/index.html

[24] KeepCoding, "¿Qué es TOTP?"(en línea. 22 de diciembre de 2023).
Disponible en: https://docs.oracle.com/cd/E19253-01/820-2314/zfsover-2/index.html

[25] Remmina, "Remote access screen and file sharing to your desktop"(en línea. 22 de diciembre de 2023).
Disponible en: https://remmina.org/l

[26] Incibe, "Phishing"(en línea. 22 de diciembre de 2023).
Disponible en: https://www.incibe.es/aprendeciberseguridad/phishing

[27] Incibe, "Ingeniería Social"(en línea. 22 de diciembre de 2023).
Disponible en: https://www.incibe.es/aprendeciberseguridad/ingenieria-social#:~:text=El%20Concepto,comprar%20en%20sitios%20web%20fraudulentos.