PLATAFORMA DE MONITORIZACIÓN Y ALERTAS PARA SERVIDORES DE EMPRESA

Mónica Prieto Cardeiro

2025/2026

1. Contextualización

1.1. Presentación del proyecto

El proyecto que se plantea consiste en la implantación de una plataforma de monitorización centralizada, está destinado a microempresas y PYMES que necesiten supervisar sus sistemas informáticos de una forma sencilla y eficaz.

Su propósito principal es garantizar la disponibilidad y seguridad de la infraestructura permitiendo detectar incidencias de forma rápida, generar alertas automáticas y aplicar medidas de seguridad y copias de respaldo que aseguren la continuidad del servicio.

Los requisitos básicos que deberá cumplir son:

- Ser accesible vía web para los usuarios autorizados.
- Monitorizar los recursos principales del servidor (CPU, memoria, disco, red) y los servicios desplegados en contenedores.
- Contar con un sistema de alertas configurables que notifique incidencias relevantes.
- Incluir medidas de seguridad y copias de respaldo.
- Ser escalable, permitiendo añadir más servidores o servicios en caso de crecimiento.

1.2. Contextualización

Para este trabajo tenemos como escenario una pequeña empresa que dispone en la actualidad de un servidor principal con diferentes servicios desplegados en contenedores y un NAS Synology, utilizado para almacenamiento y copias de seguridad. Situados en redes distintas y protegidos mediante un firewall Fortinet.

El modelo de negocio se centra en la optimización de procesos internos y asegurar que los sistemas informáticos sigan funcionando para que la empresa no tenga interrupciones en su trabajo diario.

A medio plazo, se espera que la infraestructura pueda ampliarse, añadiendo más servidores o abriendo servicios básicos para clientes, como páginas web o almacenamiento compartido.

La solución se desplegará en un nodo independiente, un equipo dentro de la red, que actuará como servidor de monitorización. En el servidor principal y en el NAS Synology se instalarán los exporters necesarios para enviar métricas. Esta arquitectura permite que, en caso de caída del servidor principal, el sistema de monitorización siga operativo y pueda generar alertas.

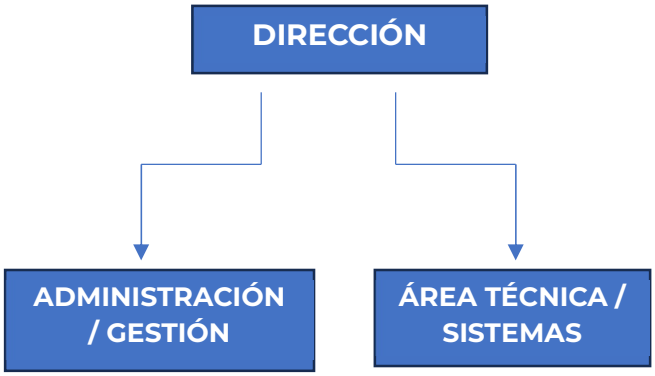
Además de la monitorización, contempla medidas de seguridad (bastionado y control de accesos), copias de respaldo y la posibilidad de gestión y acceso remoto seguro, reforzando la continuidad del servicio.

La plataforma está pensada para adaptarse a distintos tipos de organización.

Puede integrarse tanto en empresas del sector tecnológico como en compañías de otros ámbitos que necesiten supervisar sus sistemas de forma centralizada y segura.

La implantación estaría a cargo del área técnica o de sistemas.

A continuación, se muestra un organigrama genérico de implantación de la solución:



1.2.1. Descripción externa

La empresa no comercializa un producto al público general, sino que se centra en garantizar servicios internos que sean estables. El valor que aporta es la disponibilidad y seguridad de sus sistemas, lo que garantiza que la productividad de los empleados no se vea interrumpida por errores o caídas en los servicios.

1.2.2. Descripción interna

La empresa está formada por una única sede, con un equipo reducido de empleados. El área técnica está a cargo de un administrador de

sistemas, que es el que lleva el mantenimiento de la infraestructura. El resto del personal se dedica a funciones de gestión.

1.2.3. Viabilidad y expansión del negocio

La solución de monitorización es viable y escalable, ya que se apoya en herramientas libres y puede crecer en paralelo con la empresa.

- A corto plazo, permitirá controlar el servidor y sus servicios junto al NAS.
- A medio plazo, podrá incorporar otros servidores o servicios críticos.
- A largo plazo, la plataforma puede ampliarse para ofrecer servicios a clientes externos o integrarse con infraestructuras más grandes, sin necesidad de inversiones elevadas.

1.3. Descripción e objetivos del proyecto

La motivación de este proyecto surge de la falta de un sistema centralizado de monitorización en pequeñas empresas, que suelen depender de revisiones manuales o de que los usuarios reporten incidencias. Esto provoca retrasos en la detección de problemas, pérdidas de productividad y riesgo de indisponibilidad de servicios críticos.

En el mercado existen soluciones consolidadas como Zabbix o Nagios, que permiten cubrir estas necesidades, pero suelen estar orientadas a entornos más grandes y complejos, con despliegues pesados y funciones algo grandes para una pyme.

Por eso se propone una solución más ligera, modular y escalable adaptada al contexto de microempresas y pymes.

Estas medidas garantizan que la plataforma no solo detecte problemas, sino que también contribuya a mantener la continuidad del servicio y la resiliencia de la infraestructura

Esta solución es una posible oportunidad de negocio ya que se puede replicar en otras microempresas y pymes.

Se podría hacer una implantación on-premise o por suscripción (SaaS).

1.3.1. Necesidades que cubre el proyecto

1.3.2. Objetivo general

Implantar una plataforma de monitorización centralizada y segura que ayude a microempresas y pymes a controlar en tiempo real el estado de sus servidores y servicios. Además, la solución permitirá recibir alertas automáticas cuando haya incidencias, aplicar medidas básicas de seguridad y resiliencia, y contar con copias de seguridad y procedimientos de restauración que aseguren que la empresa pueda seguir trabajando sin interrupciones.

1.3.3. Objetivos específicos

- Monitorizar los recursos básicos del servidor (CPU, memoria, disco, red).
- Monitorizar servicios desplegados en contenedores y el NAS de almacenamiento.
- Configurar un sistema de alertas que notifique incidencias críticas (caída de servicio, uso excesivo de CPU, espacio en disco insuficiente, latencia elevada).
- Establecer diferentes roles de usuario con control de accesos y permisos diferenciados, acceso remoto al servidor.
- Aplicar medidas de bastionado: firewall, cierre de puertos no utilizados, contraseñas robustas y claves seguras.
- Implementar un sistema de copias de seguridad y realizar al menos una prueba de restauración.
- Documentar la instalación, la operación de la plataforma y los procedimientos de respuesta ante incidentes.
- *(Opcional)* Evaluar el uso de una herramienta ligera de monitorización en tiempo real (Netdata) como complemento de la solución principal.

La solución se basará en herramientas de software libre utilizadas habitualmente en la administración de sistemas y en la monitorización de infraestructuras TI. Se empleará un sistema operativo Linux como base para el despliegue, junto con servicios de contenedorización (por ejemplo, Docker y Docker Compose) que permitan un entorno reproducible y seguro.

Para la parte de monitorización y alertas se utilizarán plataformas de recogida y visualización de métricas (como Prometheus, Grafana o soluciones equivalentes), así como sistemas de notificación de incidencias. Se incorporarán también medidas de

seguridad y bastionado (firewall, políticas de contraseñas y copias de seguridad) que garanticen la continuidad de los servicios.

2. Análisis

2.1. Requisitos de la solución técnica

A continuación, se describen los requisitos técnicos y operativos que debe cumplir la plataforma de monitorización.

- **Plataforma de monitorización centralizada**

La solución deberá permitir monitorizar en tiempo real los servidores y servicios de la empresa, integrando en un mismo panel las métricas de rendimiento, consumo de recursos y estado de los servicios críticos.

- **Sistema de alertas y notificaciones**

La plataforma deberá generar alertas automáticas cuando se produzcan incidencias relevantes como pueden ser: caída de un servicio, uso excesivo de CPU, falta de espacio en disco, latencia elevada, se notifica al administrador mediante diferentes canales configurables.

- **Seguridad y control de acceso**

Se implementarán medidas de bastionado y control de acceso. El acceso al servidor y a los paneles de monitorización se realizará mediante autenticación segura (clave SSH), restringiendo los permisos según el rol de cada usuario.

- **Copias de respaldo y recuperación**

La solución deberá incluir políticas de copia de seguridad, almacenando las copias en el NAS Synology y verificando su correcta restauración.

- **Despliegue en contenedores**

El sistema se ejecutará sobre contenedores Docker, utilizando Docker Compose para simplificar la instalación, mantenimiento y reproducibilidad del entorno.

▪ **Herramientas**

Se emplearán herramientas libres como Prometheus, Grafana, Alertmanager por su compatibilidad con entornos de contenedores y su carácter open source, así se evitan costes de licencia y facilita la escalabilidad en el futuro.

▪ **Infraestructura y red**

La implantación se realizará en entorno on-premise, en un nodo independiente dentro de la red local de la empresa, conectado al servidor principal y al NAS Synology.
El NAS será monitorizado mediante protocolo SNMP, y los contenedores se comunicarán entre sí a través de una red privada definida en Docker.

▪ **Autenticación y usuarios**

Los usuarios tendrán diferentes perfiles de acceso. La autenticación será local, aunque se prevé la posibilidad de integración futura con un servicio de directorio (LDAP o Active Directory).

▪ **Escalabilidad y resiliencia**

El sistema deberá poder adaptarse fácilmente al crecimiento de la infraestructura, en caso de que se añadan nuevos servidores o servicios.

▪ **Políticas de software y licencias**

Todas las herramientas utilizadas serán de código abierto, lo que garantiza libertad de uso, modificación y distribución, reduciendo costes y favoreciendo la sostenibilidad del proyecto.

3. Planificación temporal y de recursos

3.1. Identificación de las actividades

Se detallan a continuación las principales actividades del proyecto

Fase 1 – Preparación

Revisión y análisis del entorno existente (servidor Proxmox, NAS, Fortinet) y definición de los servicios a monitorizar.

Duración estimada -> 2 jornadas

Fase 2 – Implementación del entorno base

Configuración del host de monitorización. Instalación del sistema operativo (Debian/Ubuntu) y dependencias.

Duración estimada -> 1 jornada

Fase 3 – Seguridad

Configuración SSH con clave pública y acceso seguro entre host monitor y servidor.

Duración estimada -> media jornada

Fase 4 – Integración y configuración

- Instalación de exporters, Node, Blackbox y SNMP exporters en los equipos monitorizados (servidor Proxmox, NAS y contenedores).

Duración estimada -> dos jornadas

- Configuración de alertas y canales de notificación. Reglas en Prometheus y Alertmanager (CPU, RAM, disco, servicios).

Duración estimada -> 1 jornada

- Creación de dashboards en Grafana. Paneles personalizados para servidores, servicios y métricas.

Duración estimada -> dos jornadas

Fase 5 – Pruebas y documentación

- Pruebas de rendimiento y verificación, comprobación de alertas, métricas y backups.

Duración estimada -> 1 jornada

- Documentación final

Duración estimada -> 3 jornadas

Duración total estimada: 16 jornadas (128 horas de trabajo).

3.2. Identificación de recursos

Recursos de personal

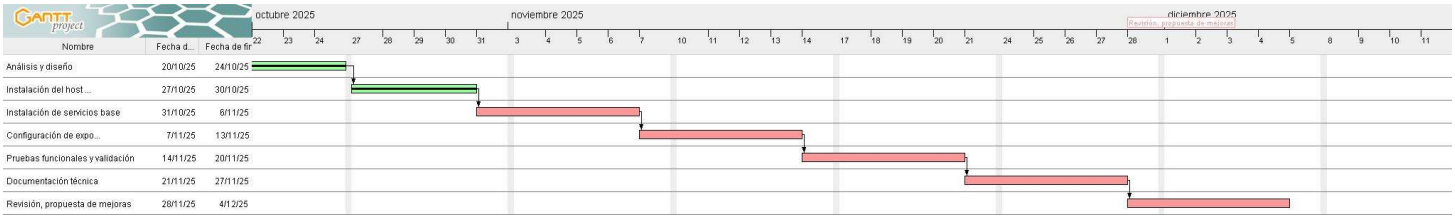
ROL	TAREAS PRINCIPALES	CUALIFICACIÓN
Administrador de sistemas	Análisis, diseño, instalación, configuración, pruebas y documentación.	Técnico Superior en Administración de Sistemas Informáticos en Red

Recursos materiales

TIPO	DESCRIPCIÓN	OBSERVACIONES
Servidor Principal (PROXMOX)	Host físico donde están los contenedores monitorizados.	CPU 8 núcleos, RAM 16 GB, almacenamiento 1 TB SSD.
NAS Synology	Almacenamiento de copias de seguridad y métricas.	IP 172.16.4.2 (subred separada, gestionada por Fortinet).
Equipo de monitorización	PC o mini servidor con Prometheus, Grafana, Alertmanager.	IP 192.168.20.21, conectado por Wifi a la LAN, en este escenario en concreto
Firewall Fortinet	Segmentación de redes y control de acceso.	Permite comunicación segura entre subredes.
Software	Prometheus, Grafana, Alertmanager, Docker, Docker Compose, Debian/Ubuntu.	Todo software libre y multiplataforma.

3.3. Planificación temporal

A continuación, se muestra el diagrama de Gantt que refleja la planificación del proyecto.



3.4. Presupuesto

Este proyecto se ha diseñado para ser implementado íntegramente con software libre y aprovechando infraestructura existente, esto hace que los costes sean más bajos.

Se incluye también una estimación del coste en un escenario real de empresa en el que fuera necesario adquirir por ejemplo un miniservidor para la monitorización.

Coste de recursos humanos

El proyecto ha sido realizado por una única persona con perfil de administradora de sistemas, estimando una dedicación total de 128 horas de trabajo (16 jornadas).
Se aplica una tarifa profesional media de 20 €/hora, lo que equivale a:

128 h × 20 €/h = 2.560 €

Coste de recursos materiales

ELEMENTO	DESCRIPCIÓN	COSTE	OBSEVACIONES
Servidor principal (Proxmox)	Ya existe en la empresa	0€	No se requiere inversión
NAS Synology	Almacenamiento de copias de seguridad		Equipo ya disponible
Equipo de monitorización	Mini servidor	500€	
Firewall Fortinet	Equipo ya disponible.		Equipo ya disponible
Software	Prometheus, Grafana, Alertmanager, Docker, Debian, SNMP, etc		Todo software libre
Electricidad y mantenimiento	Consumo estimado durante las pruebas y funcionamiento	40€	
Total recursos :		**540€**	

Recursos humanos -> 2560€

Recursos materiales -> 540 €

Total -> 3100€

4. Diseño de la solución

4.1. Diseño general del sistema

En el siguiente esquema se muestra cómo se conectan los distintos elementos: el servidor principal con sus contenedores, el NAS Synology donde se almacenan las copias, el firewall Fortinet que protege las redes y el equipo de monitorización desde el que se controlan todos los servicios.

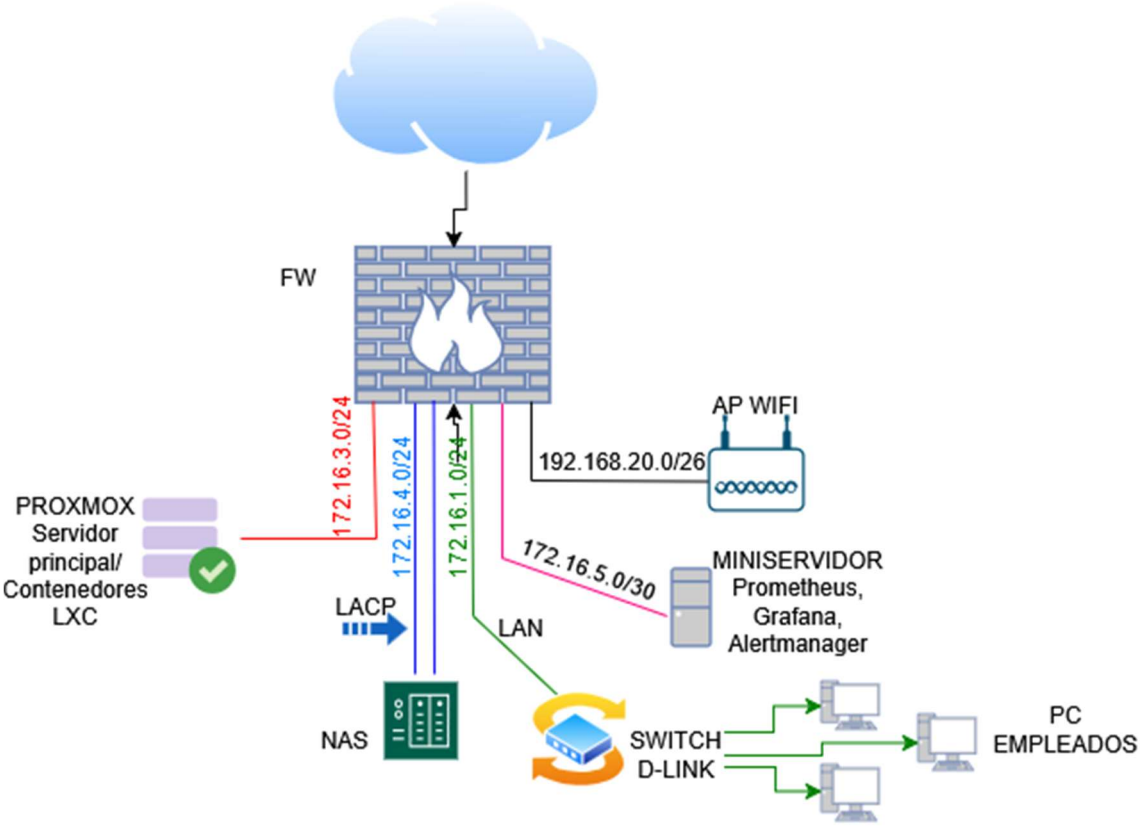


Figura 1. Arquitectura general del sistema

En la Figura 1 se muestra la arquitectura general del sistema. Vemos la segmentación de la red en cuatro subredes principales:

- **172.16.3.0/24**: red para los servidores, en este caso solo se dispone de uno, Proxmox, con los contenedores LXC que ejecutan los distintos servicios corporativos.
- **172.16.4.0/24**: red de almacenamiento, la utiliza el NAS Synology para las copias de seguridad y el almacenamiento de métricas.

- **192.168.20.0/26**: red de administración, a la que se conecta el equipo de monitorización mediante Wi-Fi, desde el cual se ejecutan Prometheus, Grafana y Alertmanager.
- **172.16.5.0/30:** red de monitorización, dedicada al miniservidor donde se ejecutan Prometheus, Grafana y Alertmanager, garantizando una conexión estable y aislada del resto de redes.
- **172.16.1.0/24**: red corporativa, conecta los equipos de los empleados, impresoras y otros dispositivos de trabajo. El firewall controla el acceso de esta red hacia los servicios internos.

El firewall Fortinet actúa como punto de control del tráfico entre redes y acceso a Internet, garantizando la seguridad y el aislamiento de los distintos segmentos.

El sistema permite que el equipo de monitorización recopile métricas del servidor principal y del NAS incluso si alguno de los servicios deja de estar disponible, asegurando la continuidad de la supervisión y la generación de alertas.

En un entorno empresarial real, el equipo de monitorización debería conectarse por cable en una vlan independiente para garantizar mayor estabilidad y seguridad.

5. Manual de implantación

5.1. Preparación del entorno

Antes de empezar con la instalación de los servicios de monitorización, se prepara el entorno de trabajo en el miniservidor.

En esta parte se configuraron las redes necesarias, se activó el acceso seguro por SSH y se instalaron las herramientas básicas que servirán para montar Prometheus, Grafana y Alertmanager dentro de contenedores Docker.

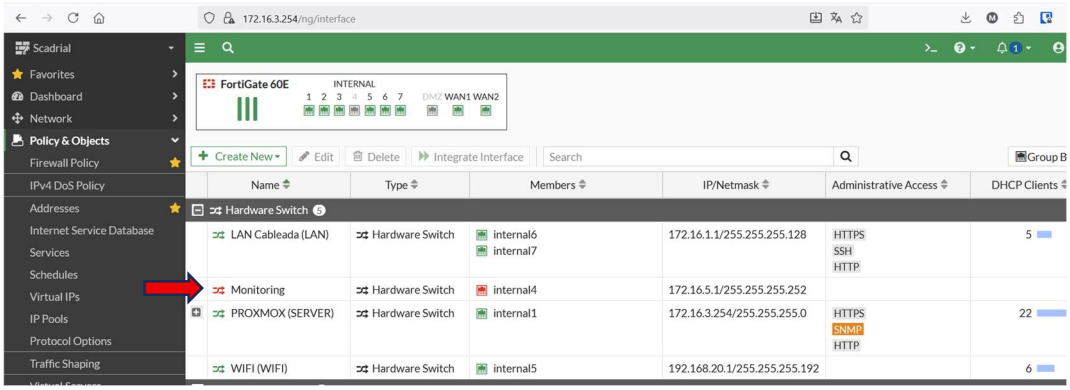
Se creó una estructura de directorios en el sistema para organizar todos los archivos del proyecto.

5.1.1. Configuración de red y direccionamiento

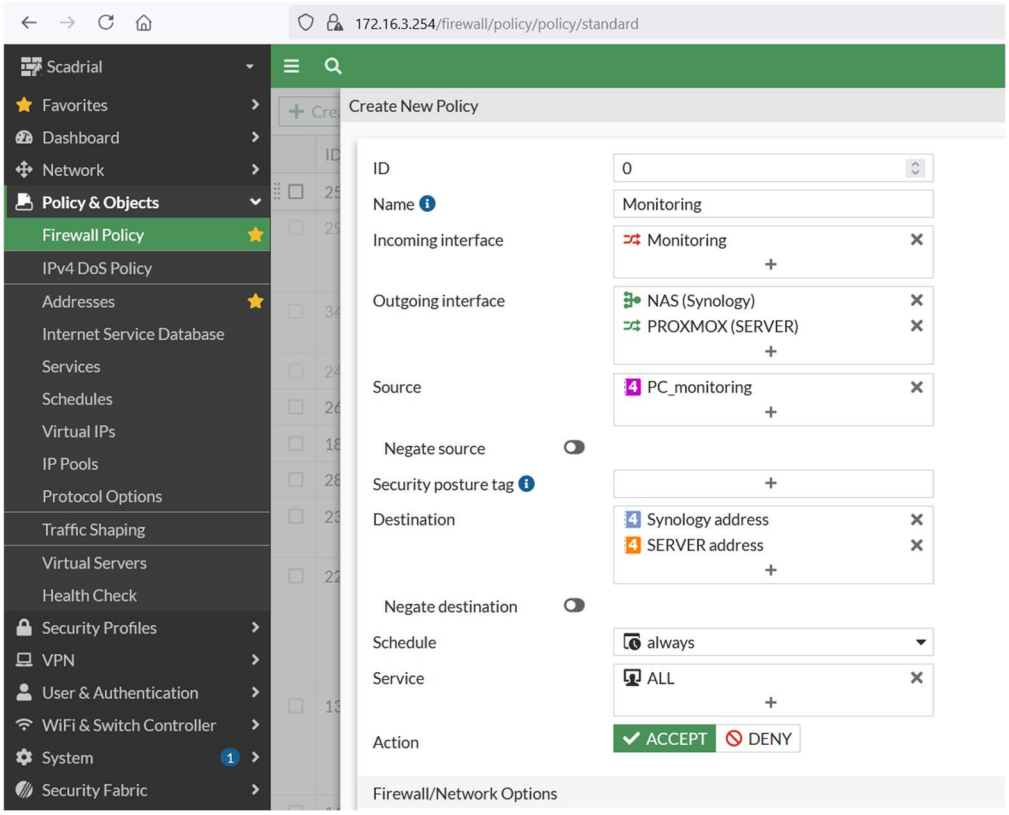
Se creó en el firewall Fortinet una nueva red dedicada (172.16.5.0/30) destinada al miniservidor de monitorización, asegurando una conexión cableada e independiente.

Al miniservidor se le asignó la IP fija 172.16.5.2, con acceso controlado únicamente a las redes de servidores (172.16.3.0/24) y almacenamiento (172.16.4.0/24)

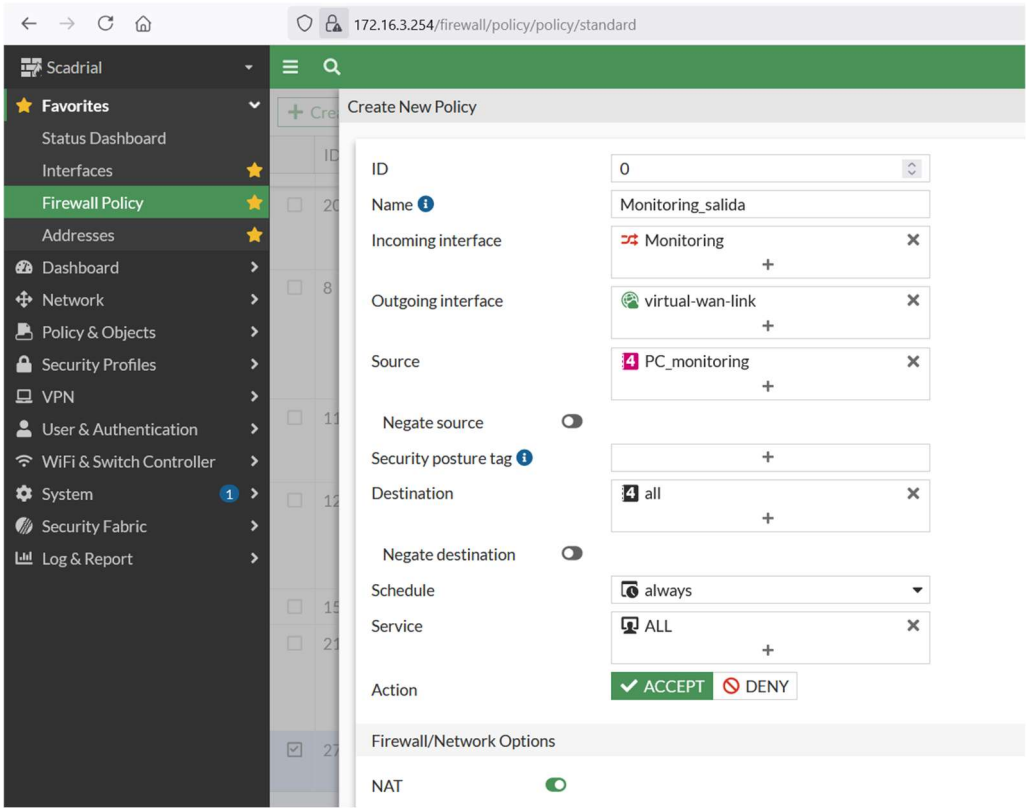
Se configura la red 172.16.5.1/30

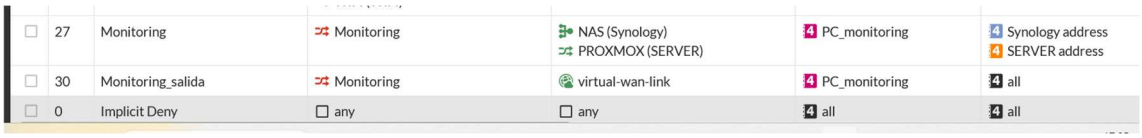


Posteriormente creamos una política de acceso en el Fortinet para permitir visibilidad entre las redes internas, de forma que el miniservidor pueda acceder al servidor Proxmox y al NAS.



Creamos también una regla específica que permite el acceso a Internet desde el equipo de monitorización.





5.1.2. Instalación de Docker y dependencias

Actualización sistema.

Antes de instalar Docker, se actualiza el sistema y se instalan las utilidades necesarias para asegurar las descargas y la verificación de paquetes:

sudo apt update && sudo apt upgrade

Para garantizar la seguridad de las conexiones HTTPS y las descargas desde repositorios externos, se instalaron los certificados actualizados del sistema mediante:

sudo apt install ca-certificates curl gnupg

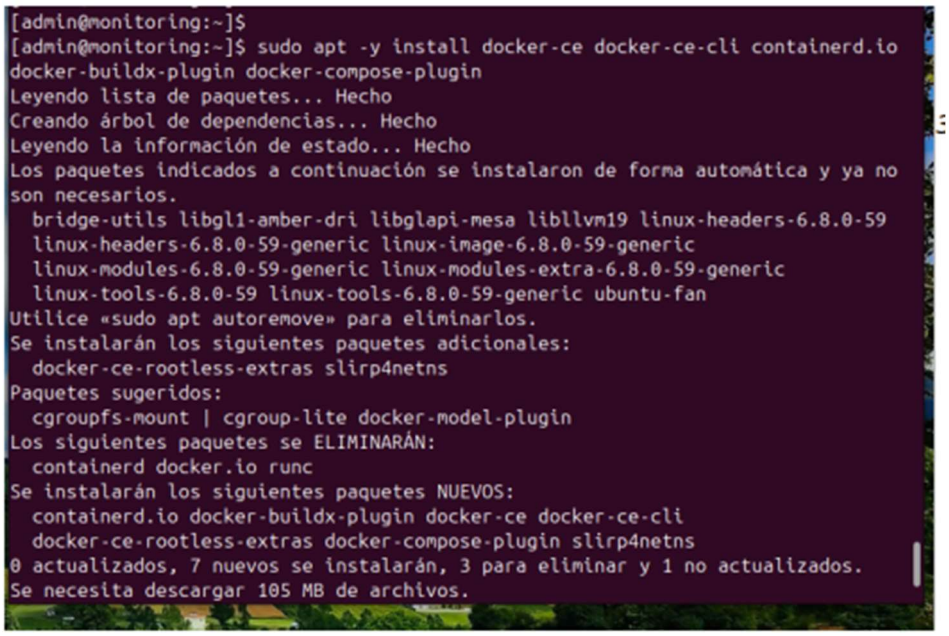
Ca-certificates -> garantizan que las conexiones HTTPS sean seguras.

Curl -> permiten la descarga de archivos

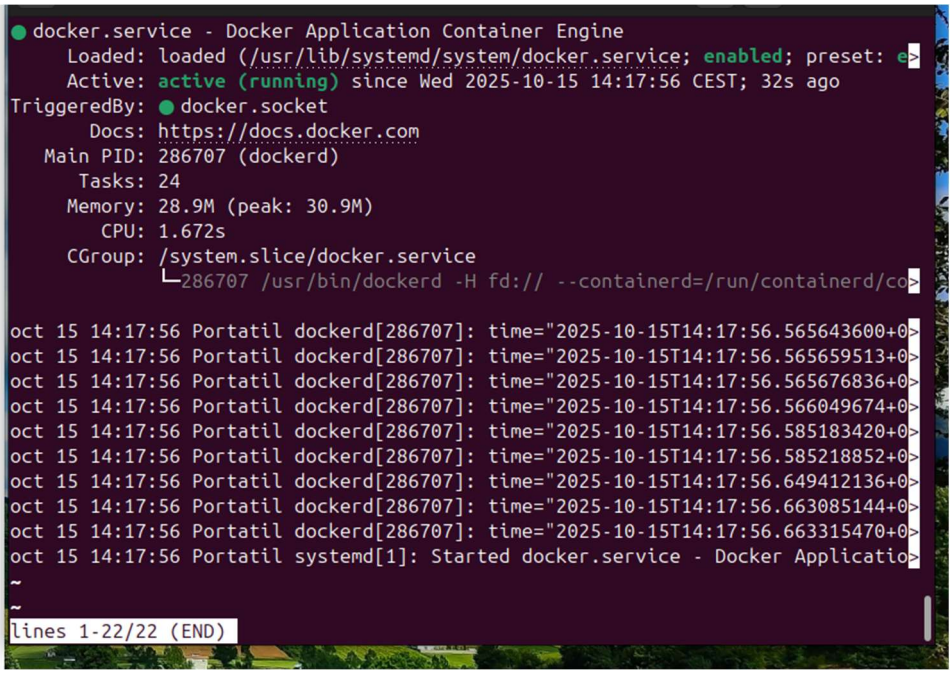
Gnupg -> gestionan las claves de firma digital para validar la autenticidad del repositorio oficial de Docker.

Instalación Docker y Sistemas.

Se añadió el repositorio oficial y se instaló Docker y Docker Compose



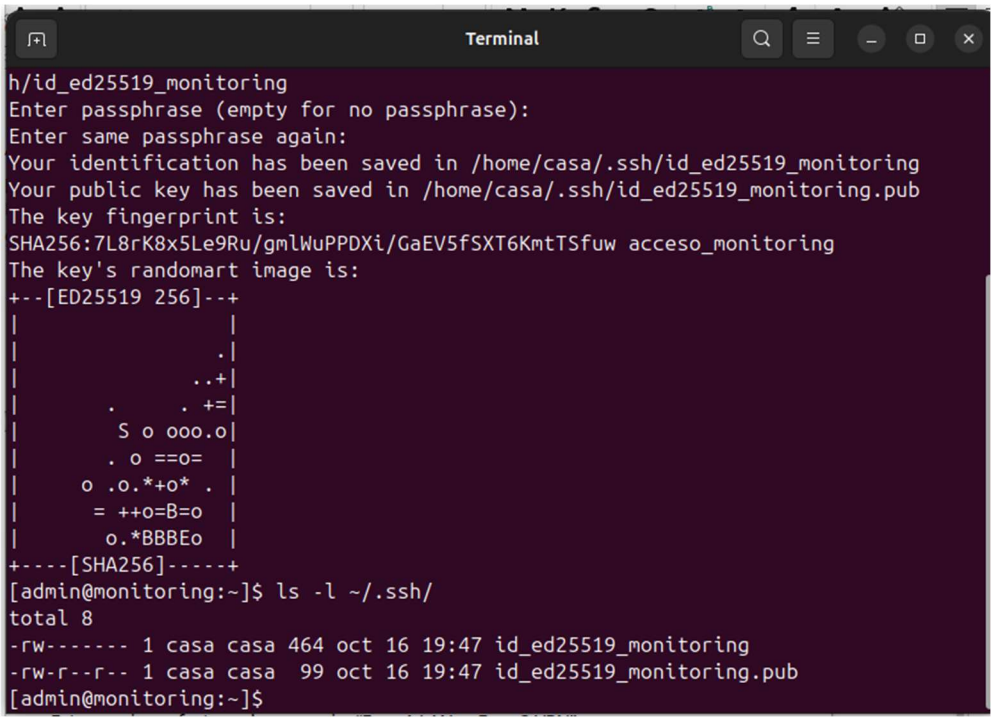
Comprobación del sistema.



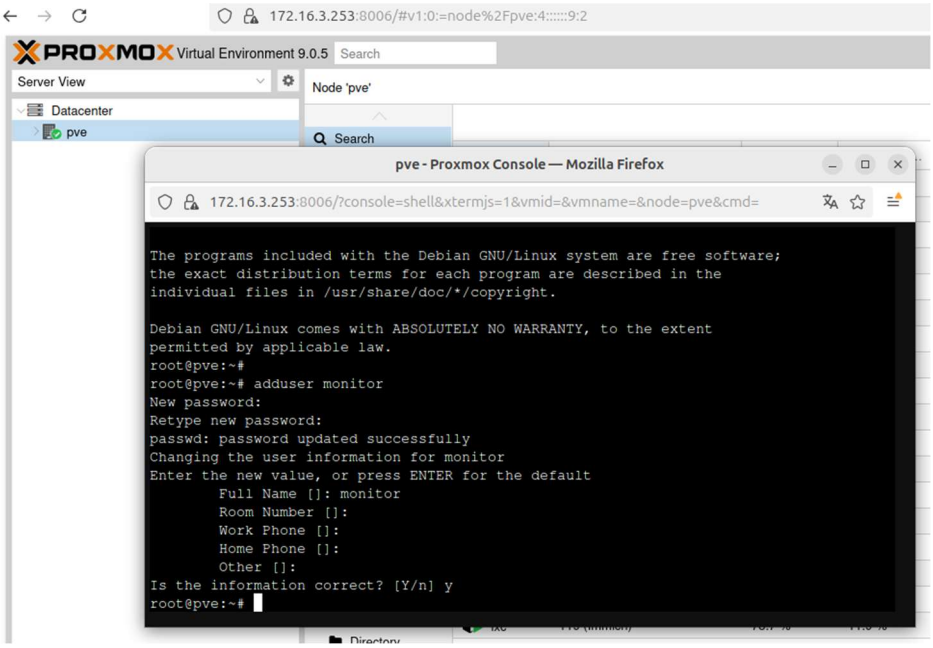
5.1.3. Seguridad básica

Generamos clave SSH en el pc desde el cual vamos a monitorizar y conectarnos al servidor. Se optó por el uso de autenticación SSH mediante clave pública en lugar de contraseña, debido a su mayor seguridad y comodidad en la automatización**.**

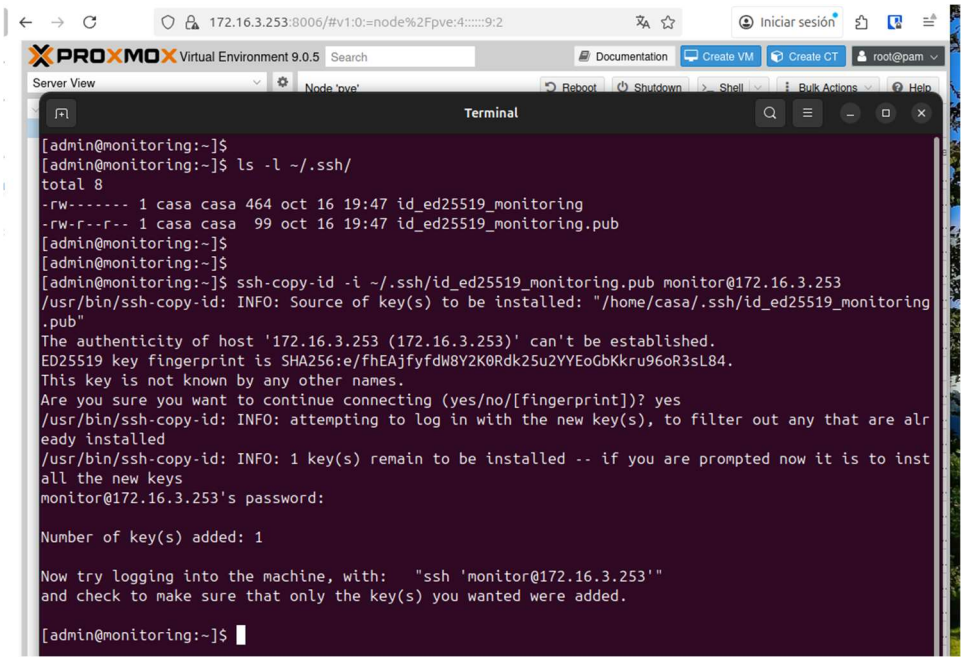
Este método elimina la necesidad de introducir contraseñas manualmente en cada conexión, evita ataques de fuerza bruta y permite una integración directa con las herramientas de monitorización



Tras generar las claves en el pc, procedemos a crear un usuario en proxmox:



Copiamos desde nuestro pc la clave ssh al servidor



Ajustamos permisos en el servidor

root@pve:~# chmod 700 ~/.ssh

root@pve:~# chmod 600 ~/.ssh/authorized_keys

Dentro del archivo de configuración del servidor: nano /etc/ssh/sshd_config

modificamos los siguientes parámetros para mayor seguridad.

```
PubkeyAuthentication yes

PasswordAuthentication no
PermitRootLogin no
```

Tras aplicar los cambios, se reinició el servicio SSH con:

sudo systemctl restart ssh