Universidad Politécnica
de Madrid

Escuela Técnica Superior de Ingenieros Informáticos

Grado en Ingeniería Informática

Trabajo Fin de Grado

Guía práctica de auditoría de seguridad de red en entornos corporativos simulados

Autor: MIGUEL GARCIA MONTERO
Tutor(a): NAZARIO FELIX GONZALEZ

Madrid, ENERO 2026

Este Trabajo Fin de Grado será depositado en la ETSI Informáticos de la Universidad Politécnica de Madrid para su defensa.

Trabajo Fin de Grado
Grado en Ingeniería Informática
Título: Guía práctica de auditoría de seguridad de red en entornos corporativos simulados
ENERO - 2026

Autor: MIGUEL GARCIA MONTERO
Tutor: NAZARIO FELIX GONZALEZ
ETSI Informáticos
Universidad Politécnica de Madrid

Resumen

En el presente Trabajo Fin de Grado se detalla el diseño, implementación y análisis de un laboratorio de auditoría de seguridad de red pensado para un entorno corporativo real. El objetivo de su desarrollo es evaluar la indefensión frente a vulnerabilidades y la eficacia de los controles de seguridad perimetral mediante la aplicación de principios de defensa en profundidad, segmentación de red y hardening de sistemas. Para exponer esa idea, se ha elaborado un nodo de red virtualizado que integra múltiples tecnologías y fabricantes, incluyendo firewalls de nueva generación, sistemas Linux vulnerables y herramientas profesionales de auditoría, permitiendo reproducir escenarios habituales basándonos en dispositivos que se pueden encontrar en cualquier cliente. Su diseño se ha creado separando claramente las zonas WAN, DMZ y LAN, y asignando a cada componente un rol específico dentro de la infraestructura.

En el desarrollo de la auditoria se ha aplicado una metodología estructurada que abarca desde la planificación y el reconocimiento inicial hasta el análisis de las vulnerabilidades encontradas junto a la propuesta de medidas de mitigación. Entre las acciones tomadas se han realizado escaneos con y sin autenticación utilizando herramientas especializadas, lo que ha permitido comparar la superficie de ataque en diferentes escenarios y analizar el impacto de las vulnerabilidades. Los resultados que se han obtenido han puesto de manifiesto la importancia de una correcta configuración de los dispositivos de seguridad, implementación de medidas perimetrales, además de la necesidad de complementarlas con políticas de segmentación y endurecimiento de sistemas. Finalmente se han realizado un conjunto de reflexiones técnicas y propuestas de mejora que ponen en relieve la idea de que una arquitectura bien diseñada, apoyada en buenas prácticas y estándares oficiales, puede reducir significativamente el riesgo y mejorar la postura de seguridad de un entorno de seguridad real.

Abstract

This Final Degree Project describes the design, implementation and subsequent analysis of a network security auditing laboratory intended to represent a real corporate environment. The main purpose of this work is to analyze the level of exposure to vulnerabilities and to assess how effective the perimeter security controls are applying defense-in-depth principles, network segmentation and system hardening techniques. To illustrate this objective, a virtualized network node was built, bringing together different technologies and vendors, this includes next-generation firewalls, deliberately vulnerable Linux systems and professional auditing tools, allowing the reproduction of common situations like those found in real customer infrastructures. The laboratory was designed with a clear separation between WAN, DMZ and LAN areas, with each element assigned a specific function within the overall architecture.

The audit itself followed a structured methodology, starting with planning and initial reconnaissance tasks and continuing through analyzing the vulnerabilities identified and the definition of possible mitigation measures. As part of the work, different scans were performed (authenticated and unauthenticated) using specialized tools, allowing the analysis of the exposed attack surface in several scenarios and making it easier to assess the relevance of the vulnerabilities identified. The results show the importance of the correct configuration of the security devices, the implementation of perimetral measures and the need to reinforce them with internal segmentation and basic system hardening practices. Finally, this work concludes with a series of technical considerations and improvement proposals, supporting the idea that a properly designed architecture, based on recognized standards and good practices, can considerably reduce risk and improve the security posture on a real operational environment.

Tabla de contenidos

1. Introducción y Metodología de la Auditoría

1.1. Justificación y Alcance

El presente Trabajo Fin de Grado se justifica por la necesidad que tienen las organizaciones de validar la eficacia real de su infraestructura de ciberseguridad. A pesar de implementar tecnologías robustas como firewalls (NGFW), el riesgo persiste en la configuración incorrecta y la falta de hardening en los sistemas internos, además del mal uso de las características proporcionadas por los mismos.

Este documento adopta un enfoque de análisis de vulnerabilidades y de red utilizando funcionalidades de hacking ético y auditoría de red perimetral. Este enfoque dual es esencial porque:

Identifica vulnerabilidades técnicas: Permite detectar debilidades en los sistemas operativos Linux y los servicios en red, las cuales pueden ser explotadas por atacantes externos o internos, pudiendo revisar vulnerabilidades reales en un entorno controlado.

Evalúa controles de seguridad: El trabajo que nos ocupa se centra en verificar si las reglas de los firewalls son efectivas, eliminando reglas redundantes o demasiado permisivas (en este caso se ha permitido cierta permisividad para permitir la explicación y el desarrollo del entorno) que incrementan el riesgo de ataque, además de en la aplicación de configuraciones vistas en entornos reales para la protección de los activos.

Promueve la mejora continua: Los hallazgos y las propuestas de mitigación servirán como una guía práctica básica de hardening de red además de un plan de acción para fortalecer la infraestructura y optimizar su rendimiento.

Pasamos a establecer el alcance y las restricciones del proyecto:

Activos Incluidos en la Auditoría
La auditoría se realizará sobre un laboratorio virtual aislado que simula una infraestructura empresarial simple con dos capas primarias de defensa de las que se documentará las ampliaciones necesarias para o añadir más o hacer esas dos más robustas. Los activos bajo alcance son:

Doble Capa de Seguridad Perimetral: Dos firewalls simulados (Palo Alto y Fortinet), permitiendo una auditoría de la segmentación de red y la correcta aplicación de políticas y configuraciones entre diferentes zonas (ej. WAN, DMZ, LAN).

Sistemas Internos: Servidores Linux que exponen servicios comunes de infraestructura (web, FTP, MYSQL, etc.), con vulnerabilidades intencionales para fines de prueba.

Red de Análisis: La infraestructura de enrutamiento, direccionamiento IP y configuración de NAT necesaria para la comunicación entre zonas.

Sistemas Externos: En las configuraciones entre capas (DMZ) se van a explicar y detallar una serie de servicios (DNS,LDAP,BALANCEADORES) que son propuestas de arquitectura avanzada y no están desplegados físicamente que permitirán darle riqueza a la topología y al estudio realizado, ayudando a ilustrar como se protegería en el mundo real y como ayudan a securizar aún más el servicio y los equipos internos.
Estos solo serán documentados como parte de las propuestas de mitigación en las conclusiones del informe.

Restricciones y Exclusiones
Para asegurar que el proyecto se centre en la seguridad de red y sea completado dentro del plazo de la Memoria de Seguimiento, se excluyen explícitamente las siguientes áreas:

Desarrollo de exploits o malware personalizados.

Pruebas de ingeniería social o seguridad física.

Auditoría de código fuente de aplicaciones web.

1.2. Marco Metodológico

Se va a establecer una metodología que consista en un ciclo de auditoria simple y adaptativo, enfocándolo en cuatro fases clave, desde el diseño inicial hasta la entrega de conclusiones definitivas

Fase de Auditoría	Tarea del TFG Asociada	Descripción y Objetivo (Libertad de Ejecución)
1. Planificación y Diseño	T1, T2 (Diseño del Laboratorio)	Consiste en establecer el alcance y el diseño lógico del entorno virtual. Esta fase finaliza con la creación de la infraestructura (PA, Fortinet, Linux) en la que se aplicarán todas las pruebas.
2. Detección y Escaneo	T5, T6 (Reconocimiento y Análisis)	Se utilizan herramientas de escaneo y mapeo (Nmap, Nessus) para descubrir activos, puertos y vulnerabilidades en la red. El objetivo es obtener una lista de hallazgos sobre los sistemas Linux y los servicios expuestos.
3. Análisis y Validación	T6 (Análisis de Vulnerabilidades)	Se evalúa la gravedad y el impacto de los fallos detectados. Esta fase incluye la validación controlada de una vulnerabilidad crítica para demostrar que el riesgo es real y no solo teórico, realizada

		desde el Kali.
4. Mitigación y Propuesta	T7 (Análisis de Riesgos y Mitigaciones)	Es la fase de seguridad defensiva. Se estudian el Hardening necesario para los sistemas utilizados, se diseñan las reglas óptimas en los firewalls (PA y Fortinet) y se documentan las propuestas de arquitectura avanzada para la mejora continua de la red.

1.3. Herramientas Fundamentales

Herramienta	Función Principal	Justificación Técnica y Metodológica
VMware Workstation	Plataforma para el diseño y aislamiento del laboratorio.	Esencial para crear un entorno de red controlado y seguro, permitiendo simular las diferentes zonas (LAN, DMZ) y aislar las pruebas de hacking ético de la red personal.
Firewalls Virtuales (PA/Fortinet)	Defensa Perimetral y Segmentación.	Permite la auditoría de configuración de reglas, NAT. Se utilizan para proponer y validar las medidas de mitigación.
Kali Linux	Sistema Operativo de Auditoría.	Plataforma base que incluye y preconfigura la mayoría de las herramientas necesarias para las fases de Recolección y Explotación (Nmap).
Nmap	Reconocimiento y Mapeo de Red.	Es la herramienta principal para la fase de Recolección de Información (T5), utilizada para el escaneo de puertos, la identificación de servicios y la huella digital de los sistemas operativos.
Nessus	Escaneo Automatizado de Vulnerabilidades.	Crucial para la fase de Análisis (T6). Proporciona un informe detallado y priorizado de fallos de configuración y vulnerabilidades de software conocidas en los sistemas Linux, que valida la necesidad de hardening.
Wireshark	Análisis Profundo de Tráfico.	Utilizado para la validación de controles. Permite capturar y analizar el tráfico de red, verificando si las políticas de seguridad del firewall están siendo violadas o si se están utilizando protocolos inseguros (ej. HTTP, FTP), su utilización ha sido puntual para validar problemas de conectividad y políticas no orientado a análisis forense completo

2. Diseño del Laboratorio y Entorno de Trabajo

2.1. Topología Lógica

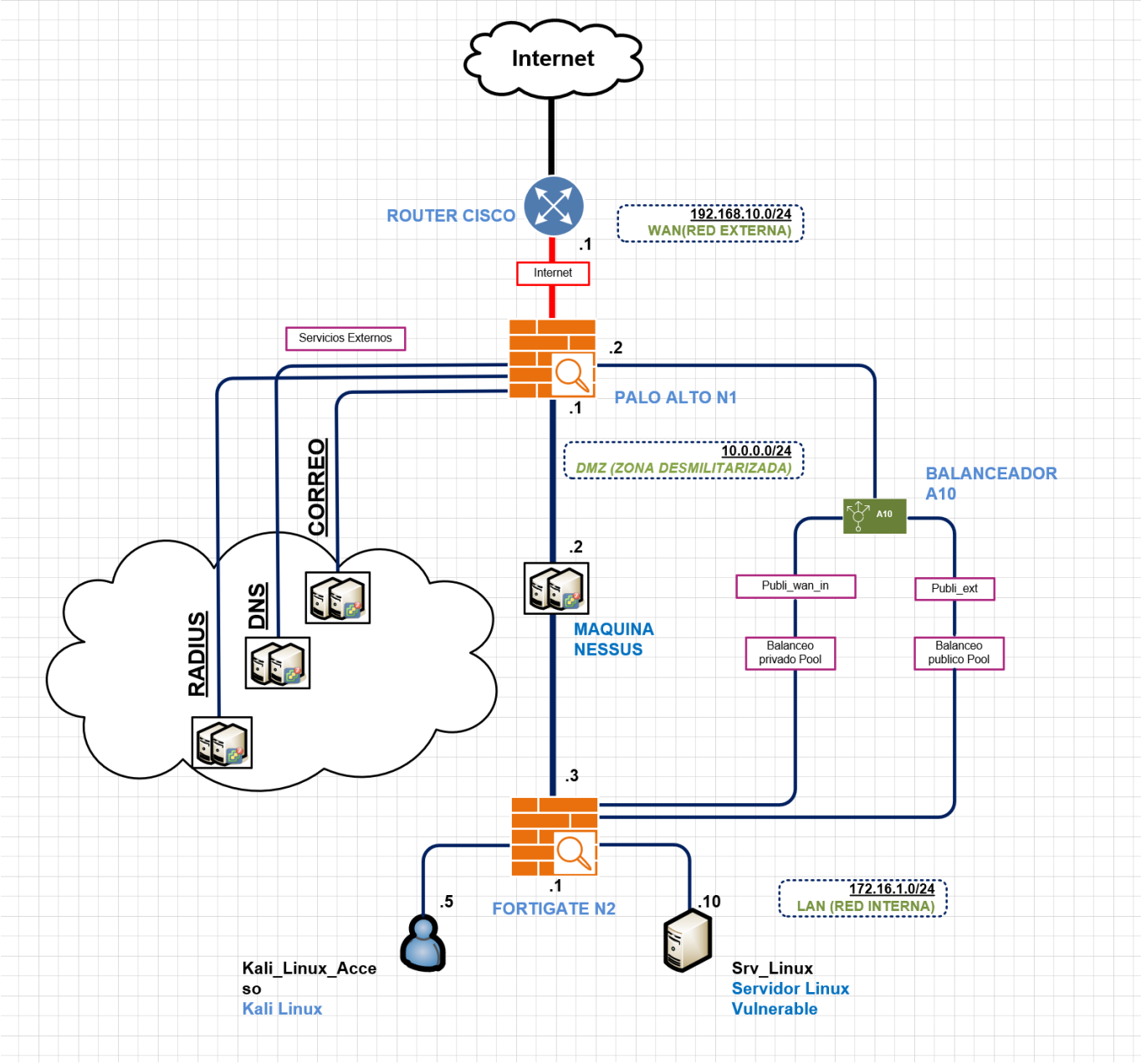


Figura 1 – Esquema de red de la Infraestructura

2.2. Esquema de Direccionamiento y Subredes

Subred (Segmento)	Rango de Dirección (Ejemplo)	Máscara	Propósito y Conexiones
WAN/Red Externa	192.168.10.0 - Teórica - (192.168.1.0/24 MGMT - Real)	/24	Simulación del Internet. Conecta el Router y la interfaz WAN del Palo Alto – (Para poder estructurarlo mejor y darle una funcionalidad más sencilla se le ha dado ip del router donde se ha montado 192.168.1.250 que es la ip del router personal coincidiendo con las de MGMT)
DMZ (Zona Desmilitarizada)	10.0.0.0	/24	Conecta la interfaz DMZ del Palo Alto con la interfaz WAN del Fortinet, es donde se encuentran los servicios como DNS, LDAP, A10, NESSUS que se documentarán.
LAN (Red Interna)	172.16.1.0	/24	Red interna principal. Contiene los Servidores Linux y la estación de auditoría (Kali).

Activo	Interfaz	Dirección IP
Router de Borde	LAN	192.168.10.1 (192.168.1.1)
Palo Alto Firewall	WAN (Externa)	192.168.10.2 (192.168.1.250)
	DMZ (Interna)	10.0.0.1
Fortinet Firewall	WAN (Externa)	10.0.0.3
	LAN (Interna)	172.16.1.1
Metaspoitable 3 (Servidor Linux)	Única	172.16.1.10 (Servicios Web/SSH)
Kali Linux	Única	172.16.1.5 (Estación de Ataque)
Nessus	Única	10.0.0.2 (Escaneo de Vulnerabilidades)

Configuración de NAT

La gestión de NAT es un aspecto crítico de la auditoría y se divide por los roles específicos de los *firewalls* desplegados para garantizar la **Defensa en Profundidad**:

SNAT (Source NAT - Traducción de Origen)

El SNAT permite que el tráfico generado en las redes internas (LAN y DMZ) salga hacia la red WAN (Internet).

Palo Alto Firewall (Firewall de Perímetro): Dispositivo responsable de la salida hacia la red WAN (Internet). Su configuración ha sido realizada con reglas de SNAT con la intención de traducir el tráfico con origen en la red DMZ (10.0.0.0/24) hacia la WAN (utilizando la ip de la interfaz externa 192.168.1.250).

Este diseño permite que las direcciones IP internas no sean visibles desde el exterior, además de que el control del acceso a Internet esté centralizado en el firewall perimetral y que el retorno del tráfico se realice correctamente, sin necesidad de definir rutas adicionales en la WAN (lo cual no es posible).

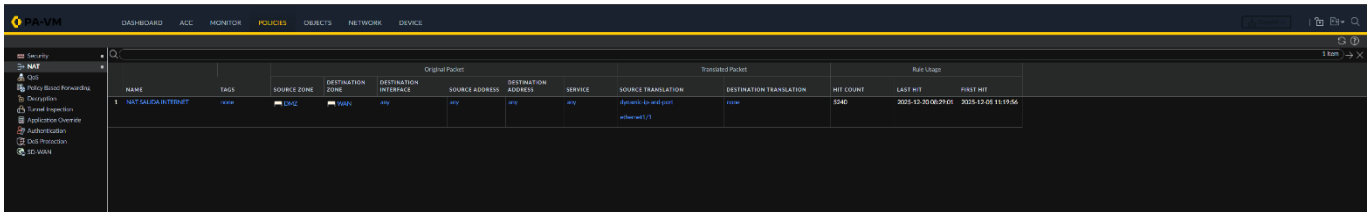


Figura 2 – NAT Salida a Internet del Palo Alto

Fortinet Firewall (Segmentación Interna): Dispositivo responsable de la segmentación y del control del tráfico interno entre redes. En el entorno desplegado se ha configurado con reglas de SNAT para el tráfico que sale de la LAN (172.16.1.0/24) hacia la DMZ (10.0.0.0/24), también siendo posible su implementación (en escenarios concretos) para comunicaciones específicas entre servidores internos cuando sea requerido por el servicio (no siendo necesario en este desarrollo al no tener segmentación interna en la LAN). En el contexto de este laboratorio, se ha habilitado SNAT en la política de salida de la LAN hacia la DMZ. Esta decisión técnica permite que los activos de la red interna (Kali y Metasploitable) alcancen los servicios de la DMZ y la red WAN sin necesidad de gestionar rutas de retorno de tráfico complejas en los firewalls en este entorno. Por el contrario, en el flujo inverso (DMZ hacia LAN), el NAT se mantiene deshabilitado con el objetivo de mantener la trazabilidad del tráfico y permitir que las políticas de seguridad del Fortinet identifiquen la dirección IP real de origen de los sistemas de auditoría como Nessus. Fortinet no realiza traducción de direcciones desde la DMZ hacia la WAN, delegando esta función en el firewall Palo Alto, que actúa como punto único de salida a Internet para la DMZ. De este modo, el Fortinet opera principalmente como firewall de segmentación interna, aplicando NAT únicamente en casos puntuales y debidamente justificados por requisitos específicos del entorno.

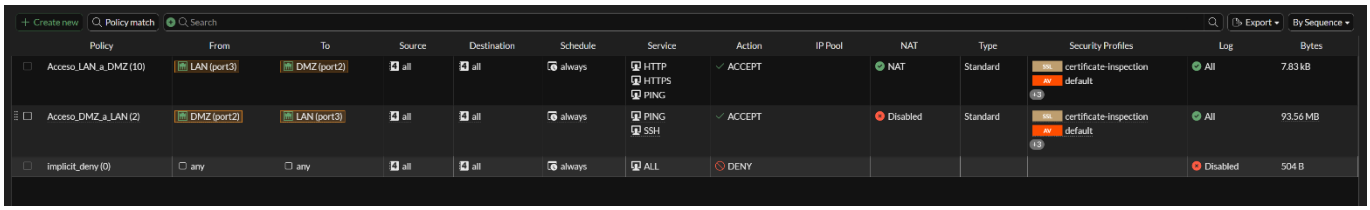


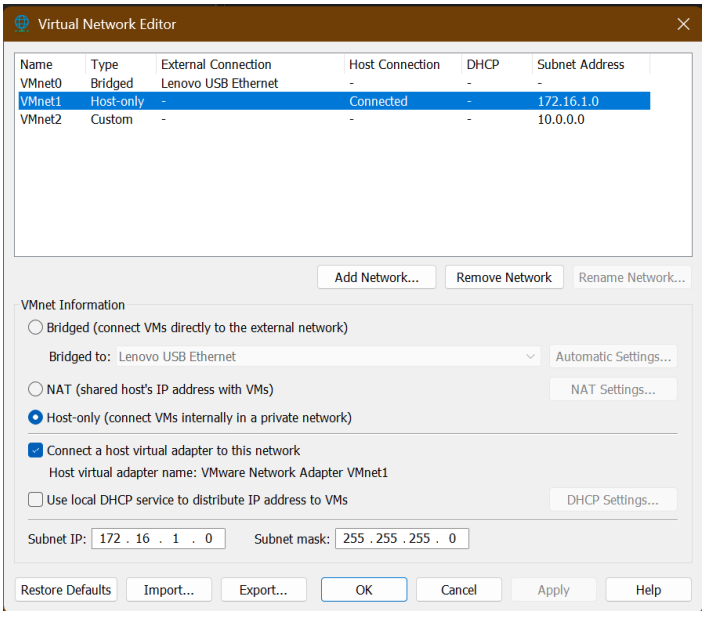
Figura 3 - Conjunto de Reglas y NAT configurados en Fortinet

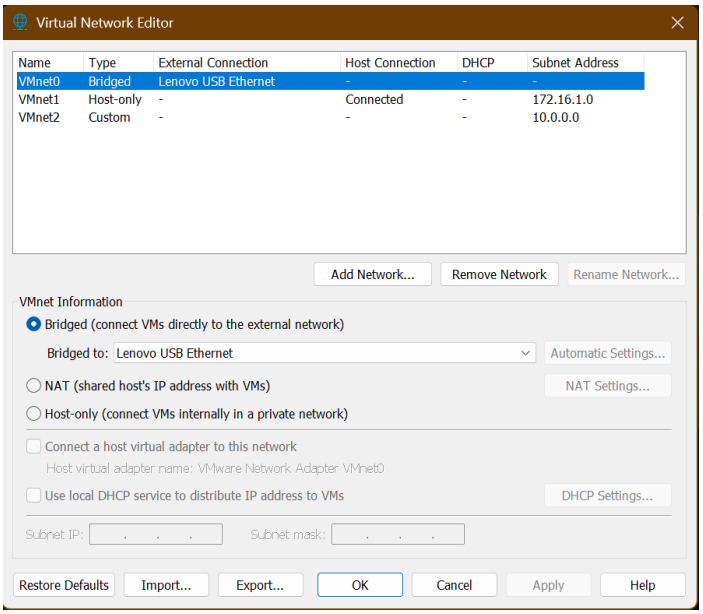
DNAT (Destination NAT - Traducción de Destino)
El DNAT se configura para permitir el acceso externo (desde la WAN) a los servicios alojados en las redes internas.
Palo Alto Firewall (Perímetro): Actúa como único punto de publicación de servicios hacia el exterior. Sería posible su configuración (se expone con objetivo teórico) con reglas de DNAT para traducir la dirección IP pública expuesta en la WAN hacia la dirección IP privada del servidor destino ubicado en la DMZ. Este firewall constituye el primer nivel de filtrado y control de seguridad frente a accesos externos. En entornos más desarrollados, y como se detallará posteriormente en el capítulo 8, esta traducción podría realizarse hacia la IP de un Virtual Server en el Balanceador A10 cuando se requiera balanceo de carga o alta disponibilidad para servicios alojados en la LAN o la DMZ.
Fortinet Firewall (Segmentación Interna): No realiza traducciones DNAT desde la WAN, ya que esta función se delega completamente en el firewall perimetral. Únicamente se aplicarían reglas DNAT en escenarios muy concretos, como cuando un servicio ubicado en la LAN (172.16.1.0/24) debe ser accesible desde la DMZ (por ejemplo, el acceso de un servidor Nessus a sistemas internos). En este laboratorio, y con el objetivo de mantener la trazabilidad del tráfico y facilitar el análisis, se han conservado las direcciones IP originales sin aplicar DNAT interno.

2.3. Plataforma de Virtualización

La implementación del laboratorio virtual se realizará utilizando una estrategia de único hipervisor para maximizar la estabilidad y la compatibilidad con los componentes críticos de la red. Esta aproximación, minimiza los problemas de NAT y enrutamiento entre los diferentes tipos de activos, optimizando la Tarea T3 (Despliegue y Configuración).

VMware Workstation (Firewalls y Router): Esta plataforma será la principal para el despliegue de los firewalls virtuales Palo Alto y Fortinet además de los equipos de la DMZ y la LAN. Ha sido seleccionado por su robustez en la configuración de redes virtuales complejas (VMnets) y por la compatibilidad optimizada con las imágenes virtuales de los firewalls de próxima generación (NGFW), garantizando la estabilidad de los nodos de seguridad más críticos.
Se configuraron 3 VMnet (Redes) en el Virtual Network Editor del hipervisor gracias a las capacidades de segmentación del mismo [4], la 0 siendo la de MGMT (Management o Gestión) funcionando como red de administración, la 1 siendo la red interna LAN (172.16.1.0/24) y la 2 siendo la red DMZ (10.0.0.0/24) de equipos corporativos, se adjuntan capturas con la configuración de cada una.





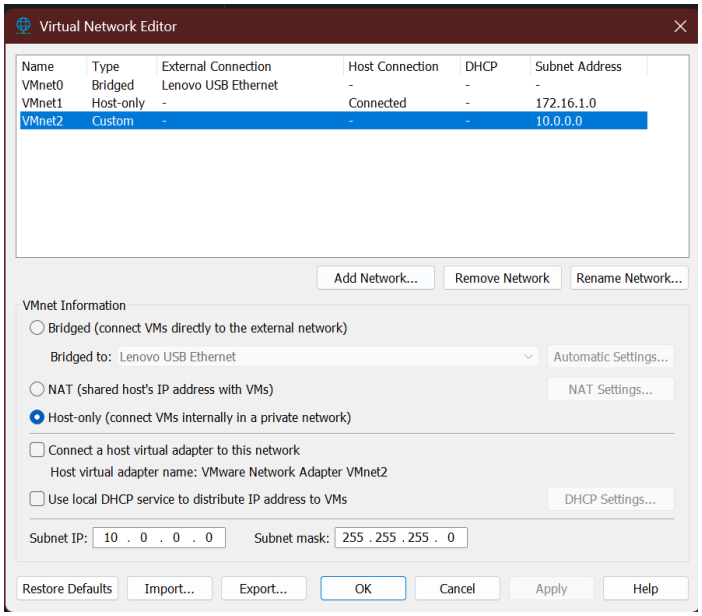


Figura 4 – Configuración de las Redes en VMware

Como detalle al final de las especificaciones de red se documenta que, para la gestión de todos los activos, independientemente del hipervisor en el que residan, se ha usado la toolbox MobaXterm. Esta herramienta es esencial para consolidar todas las conexiones de administración (SSH a Linux, consolas de Firewalls) en una sola interfaz, optimizando el flujo de trabajo durante las fases de configuración (T3) y auditoría (T5 y T6).

2.4. Descripción de las maquinas

El laboratorio se estructura como un conjunto de máquinas virtuales diseñadas para montar un nodo de interconexión sencillo pero realista, incorporando principios básicos de segmentación de red, separación de funciones y defensa en profundidad; acercándonos de una manera básica (con algunas secciones documentadas) a la forma de trabajar de un entorno real.
Cada sistema implicado tiene un rol específico dentro del nodo, permitiendo realizar diferentes funciones desde analizar la superficie de ataque o la aplicación de medidas de mitigación.
Se han utilizado credenciales de administración robustas y diferenciadas por cada sistema, no documentándolas en este análisis por motivos de seguridad y buenas practicas académicas.

2.4.1 FortiGate VM

FortiGate es el firewall de segmentación interna del laboratorio, funcionando como punto central del paso de tráfico entre la red LAN y la red DMZ. La función que posee es la de controlar el movimiento entre sistemas internos y hacia la DMZ además de proporcionar un primer punto de salida hacia internet usando para ello políticas de firewall basadas en servicios, aplicaciones y perfiles de seguridad.

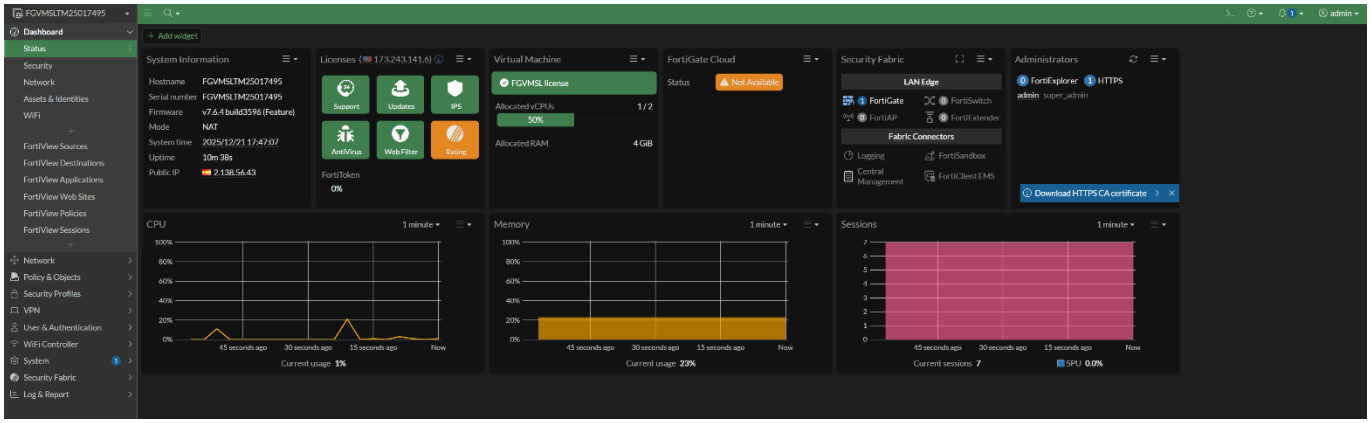


Figura 5 – Panel principal de Firewall Fortinet

Tiene configuradas tres interfaces:

Interfaz de gestión (MGMT): utilizada exclusivamente para la administración del dispositivo mediante HTTPS y SSH desde la red de gestión (192.168.1.0/24).
Interfaz LAN (172.16.1.0/24): conecta los equipos internos del laboratorio, como Kali Linux y Metasploitable.
Interfaz DMZ (10.0.0.0/24): conecta servicios estructurales del nodo como el servidor Tenable/Nessus (entre otros) además de servir como red de unión con el firewall perimetral Palo Alto.

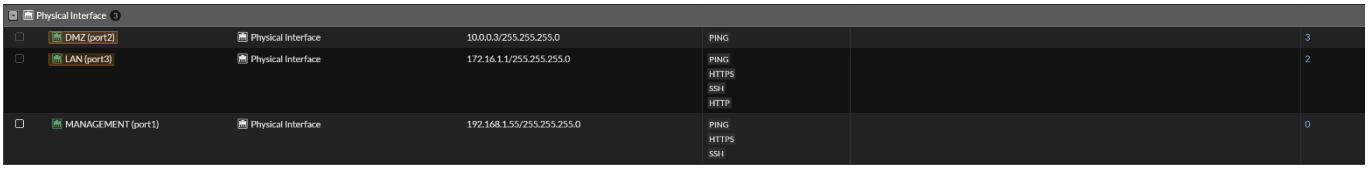


Figura 6 – Interfaces Configuradas en el Firewall de Fortinet

En su configuración (realizada con el apoyo de la documentación oficial de Fortinet [2]) se han aplicado políticas de restricción de tráfico, perfiles de seguridad por defecto (Antivirus, IPS, Control de Aplicaciones, Web Filtering) y medidas de hardening como la limitación de servicios de gestión, el bloqueo por intentos fallidos de autenticación y el uso de inspección de certificados (reflejado en el Capítulo 6).
Es importante comentar que no actúa como salida directa a Internet, esa función la realiza el firewall perimetral de Palo Alto.

2.4.2 Palo Alto VM-Series

El Palo Alto se utiliza como firewall perimetral, representando el punto de salida principal hacia Internet del laboratorio. Su rol principal en el laboratorio es controlar y proteger el tráfico entre la DMZ y la red externa (también entre la WAN y la DMZ como rol secundario a nivel de política de seguridad), aplicando políticas basadas en aplicaciones (App-ID), perfiles de seguridad avanzados y reglas de traducción de direcciones (NAT).

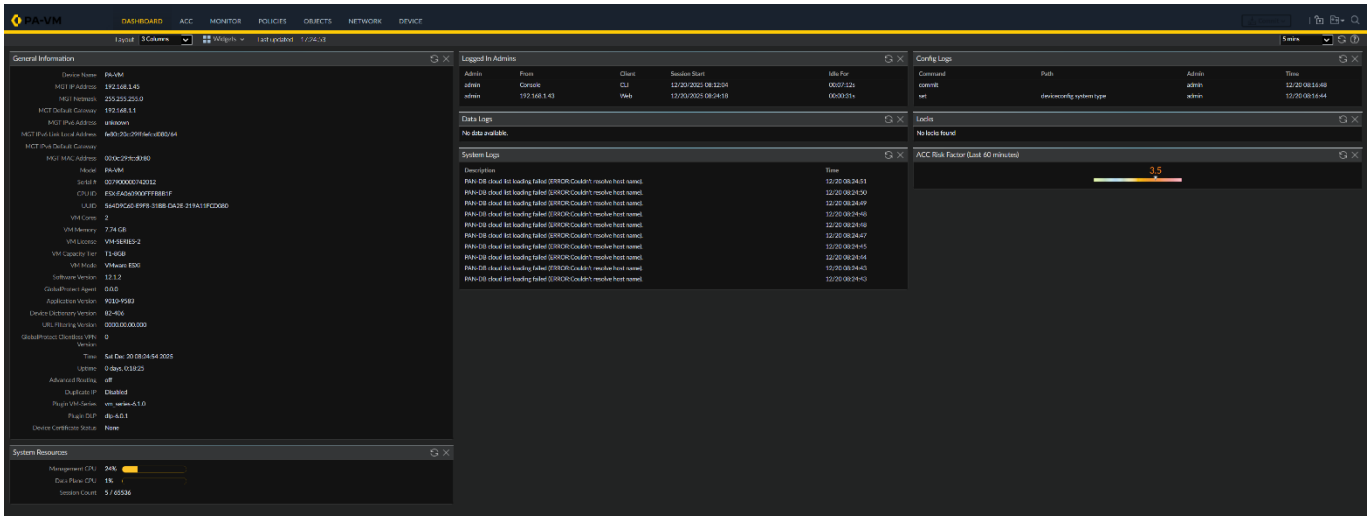


Figura 7 – Panel principal de Firewall Palo Alto

Tiene configuradas 2 interfaces y una de MGMT:

Interfaz de gestión: usada para tareas de administración (192.168.1.0/24).
Interfaz DMZ (10.0.0.1/24): donde se encuentran los servicios estructurales del nodo de interconexión, se encuentra conectada al Fortigate en el otro extremo.
Interfaz WAN: conectada a la red externa simulada (192.168.1.0/24) para proporcionar acceso a Internet.

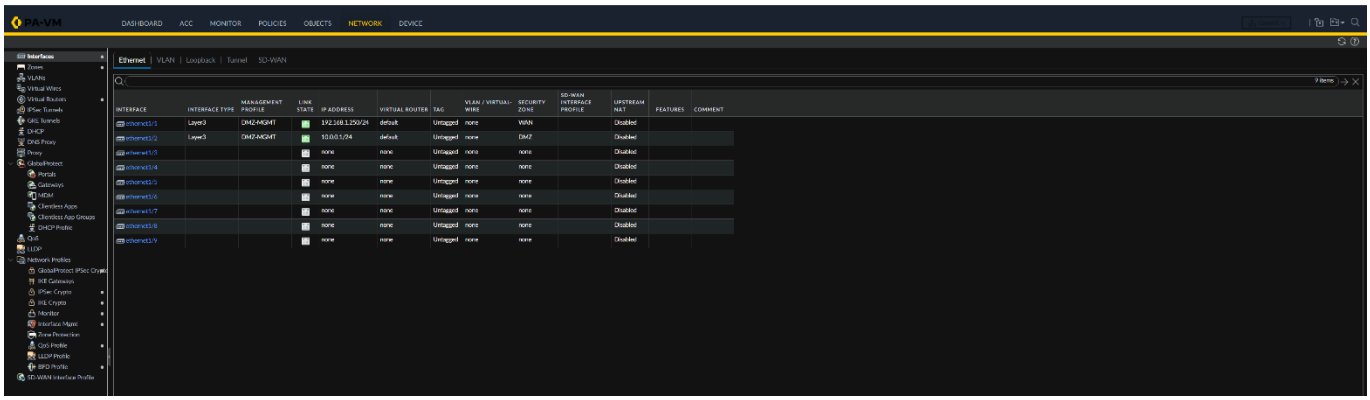


Figura 8 – Interfaces Configuradas en el Firewall de Fortinet

Se ha procedido dentro de las mitigaciones realizadas a la configuración (realizada con el apoyo de la documentación oficial de Palo Alto [1]) de reglas de seguridad con perfiles en modo default (personalizables en un entorno real) de Antivirus, Vulnerability Protection, Anti-Spyware, URL Filtering y WildFire, así como reglas de SNAT para garantizar la salida hacia internet y el correcto retorno del tráfico. Además, como medida de análisis y seguridad, se ha implementado Certificate Inspection para el estudio del tráfico TLS sin necesidad de realizar Deep Inspection (también realizable, pero se deja para entornos más avanzados), manteniendo la compatibilidad y la simpleza del nodo de interconexión.

2.4.3 Kali Linux

Kali Linux es una de las máquinas de la LAN utilizada como estación de trabajo para pruebas de seguridad además de representar el rol de un atacante interno dentro de la red. Desde él se realizan tareas de reconocimiento y validación de vulnerabilidades detectadas durante los escaneos de auditoria realizados desde el Nessus.

Tiene configuradas dos interfaces:

Interfaz de gestión: usada para tareas de administración (192.168.1.0/24).
Interfaz en la red LAN (172.16.1.0/24), desde la cual interactúa con los

sistemas restantes dentro de la misma red o para la salida hacia el Fortinet por ejemplo si tuviera que acceder a internet o a otros elementos de la DMZ.

No expone servicios en escucha por defecto, reduciendo su superficie de ataque.
Como medida de seguridad (revisando la documentación disponible [8]) y muestra se ha aplicado un hardening básico mediante firewall local (UFW), permitiendo únicamente tráfico saliente y accesos controlados desde la LAN. No se han aplicado medidas restrictivas que limiten las herramientas de auditoría, confiando su mitigación a las reglas creadas en el firewall y a la segmentación de red.

2.4.4 Metasploitable

Metasploitable es una máquina que ha sido intencionadamente diseñada para ser vulnerable y así, simular un sistema con mala configuración dentro de una red empresarial. En el nodo de interconexión actúa como objetivo principal de los ataques, lo que permite validar técnicas de explotación y analizar el impacto de vulnerabilidades críticas, medias y locales documentadas con el Tenable Nessus.
Se halla situada en la red LAN (172.16.1.0/24) y posee numerosos servicios inseguros, entre los que se encuentran FTP, MySQL o servicios web vulnerables. Esta configuración permite la demostración de ataques como ejecución remota de código, denegación de servicio o la escalada de privilegios, y permite la evaluación de cómo las políticas de firewall y los perfiles de seguridad mitigan o limitan dichos ataques.
No dispone de interfaz de gestión independiente con el objetivo de proteger a los otros activos de la estructura, reforzando el escenario planteado y evidenciando la importancia de la segmentación y el control del tráfico.

2.4.5 Tenable / Nessus

Tenable / Nessus se usa como herramienta para el descubrimiento y la evaluación de vulnerabilidades en la estructura. Esta localizado en la DMZ (10.0.0.0/24) y tiene igual acceso a la LAN como a los firewalls para realizar escaneos tanto autenticados como no autenticados.

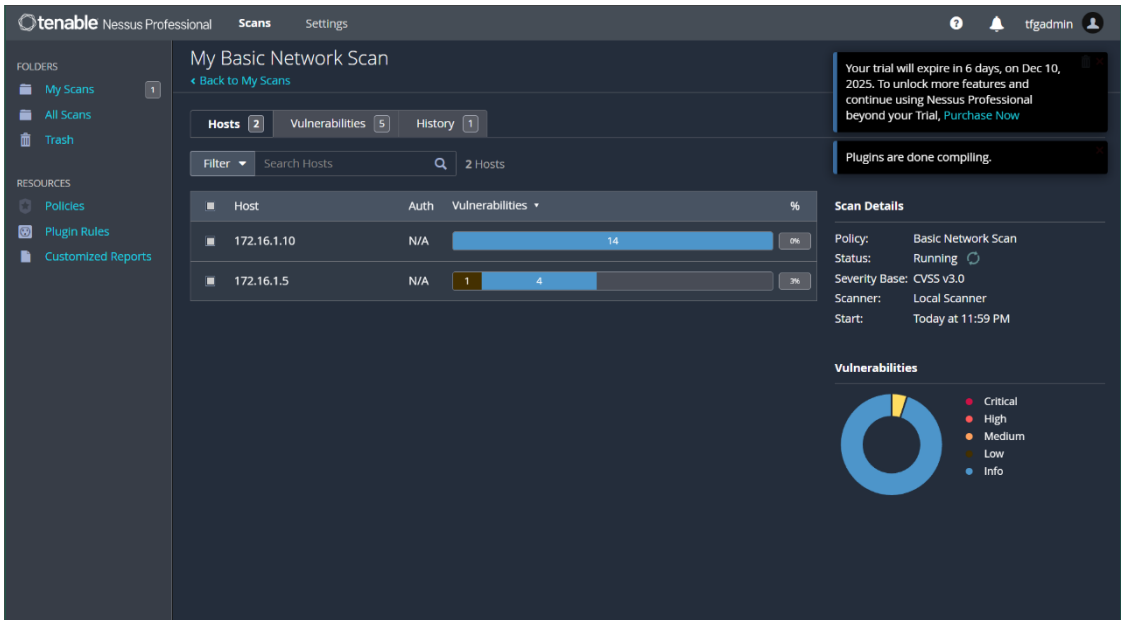


Figura 9 - Panel Principal del Tenable Nessus

En las pruebas ejecutadas se han realizado varios tipos de escaneos:

- No autenticados, donde no se han especificado las credenciales.
- Autenticados, donde si se han introducido en una lista dentro del sistema las credenciales de todos los equipos, proporcionando una visión más informativa y real del estado de los sistemas.
- Escaneos de red y de dispositivos de seguridad:

Teniendo en cuenta que la licencia de evaluación limita la exportación de informes (en las imagen siguientes (Figuras 10 y 11) se pueden ver la licencia usada y su fecha de fin, además de la pantalla de descarga de informes desde donde bloqueaba su generación por falta de funciones), los resultados obtenidos han permitido identificar vulnerabilidades críticas, altas y medias,

que posteriormente se han utilizado como base para el análisis y la creación inicial de las medidas de mitigación reseñadas en este documento.

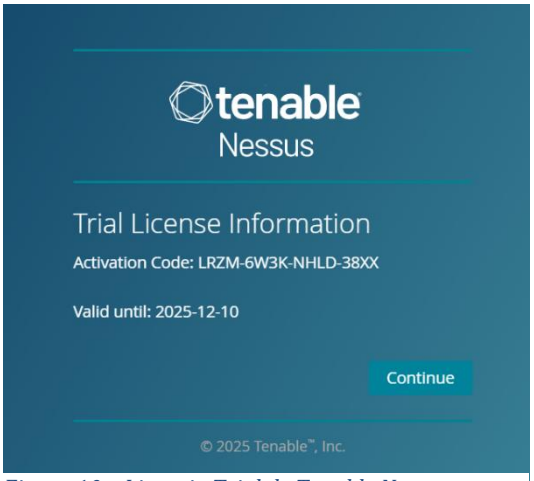


Figura 10 – Licencia Trial de Tenable Nessus

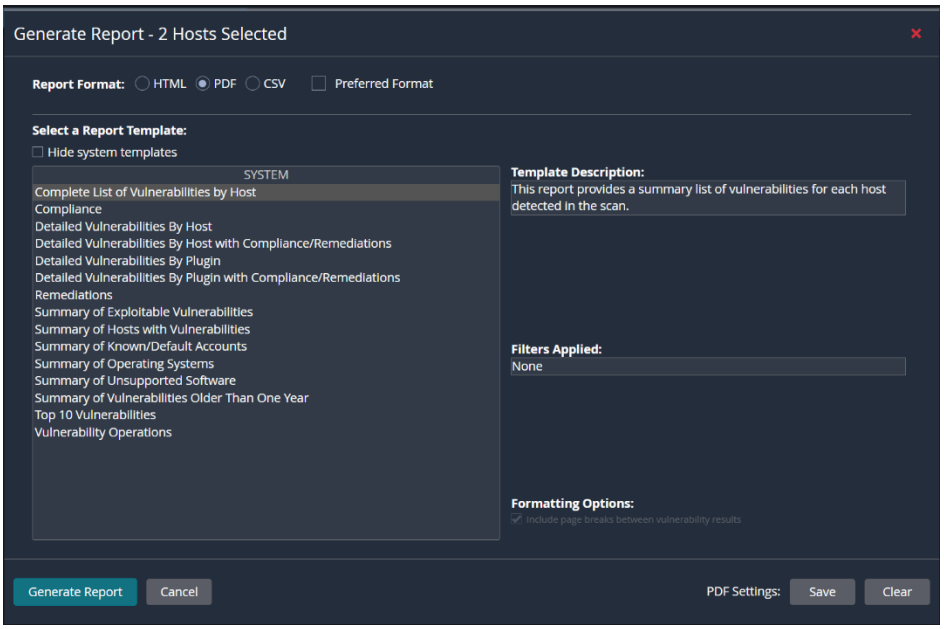


Figura 11 – Menú de exportación de reportes de Tenable Nessus

3. Despliegue del Laboratorio

El desarrollo y montaje de las maquinas dentro del nodo se realizó de una manera controlada, primero se montó la parte del firewall de segmentación Fortinet junto a las maquinas del Kali y Metasploitable porque fueron las primeras disponibles debido a que eran las más claras de montar junto a la disponibilidad de la licencia, posteriormente se procedió a montar el Palo Alto cuando se pudo licenciar, para pasar una vez desplegado al conexionado de todos los elementos priorizando siempre una correcta pero simple y explicativa segmentación de red antes de proceder al análisis de las vulnerabilidades,

mitigación y hardening de los mismos.
Esta forma de desarrollarlo permitió validar cada fase del laboratorio de manera independiente, permitiendo ver los fallos de conectividad, licenciamiento y configuración que iban ocurriendo y corrigiéndolos en el momento.

3.1 Instalación y licenciamiento de FortiGate

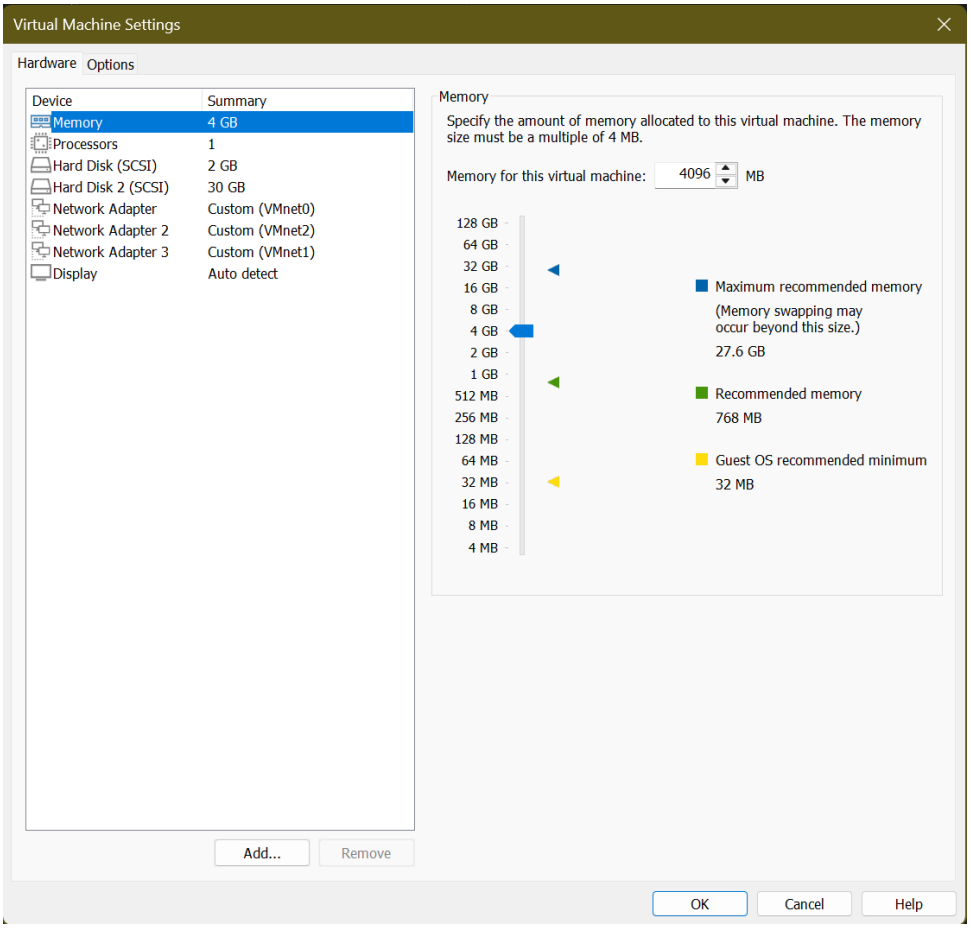


Figura 12 – Configuración en VMware Workstation de la máquina virtual del Firewall Fortinet

El despliegue de la máquina de Fortigate en WMware se hizo en primer lugar ya que fue el primer dispositivo del que se disponía licencia, primero se utilizó de forma incorrecta una .ova de FortiFirewall no siendo la opción válida para montar lo que se requería, posteriormente investigando más en la web de soporte se intentó desplegar otra .ova incorrecta como es (FGT_VM64_VMX-v7.2.12) que finalmente después de investigar se vio que era una imagen para entornos de virtualización KVM (Kernel-based Virtual Machine), lo que por último se pudo ver que era la causa de los problemas de compatibilidad y licenciamiento. Tras realizar un estudio más profundo de las imágenes disponibles en la web de soporte del fabricante se vio que la correcta era FGT_VM64-v7.6.4.F-build3596, compatible con el entorno del que se disponía permitiendo su licenciamiento correcto.

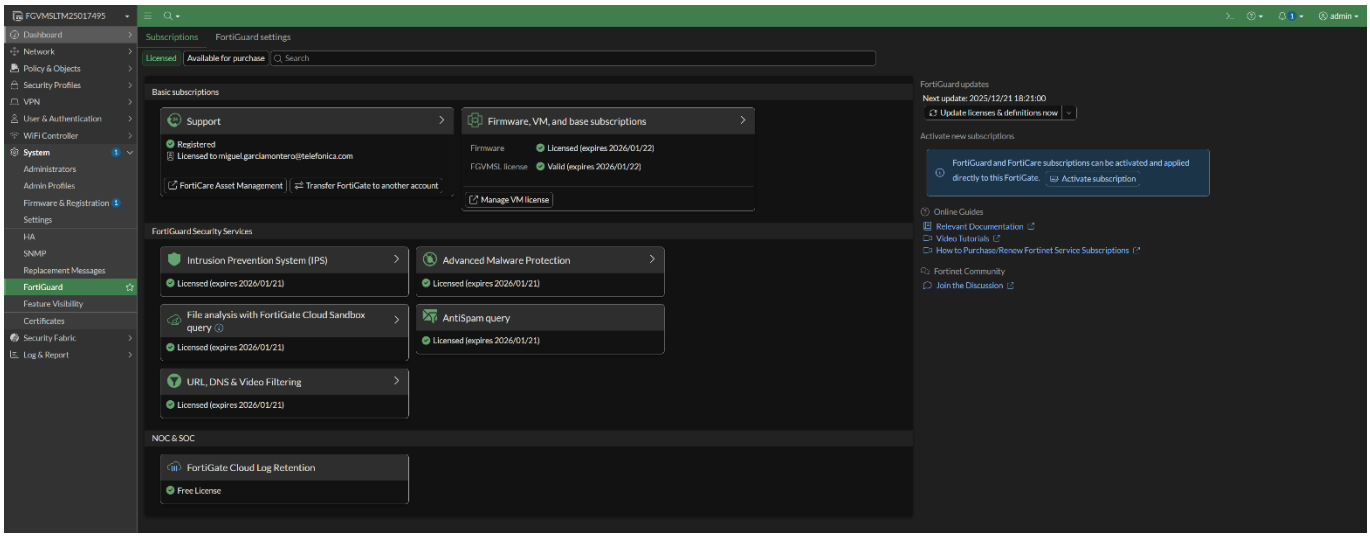


Figura 13 – Panel de licenciamiento del Firewall de Fortinet

Procedemos a detallar de manera resumida algunos de los problemas encontrados en el despliegue de este fabricante:

- Dimensionamiento de recursos:

Inicialmente la maquina venia configurada con 2 GB de RAM, al iniciarla nos notificaba que aunque quedaba pendiente el licenciamiento los recursos no eran los adecuados, revisando la información disponible y los foros de documentación del fabricante se vio que era necesario que tuviera como mínimo 4 GB para el correcto funcionamiento de los motores de seguridad (IPS, Antivirus y Control de Aplicaciones), con ello se consiguió hacer la interfaz más fluida, evitar inestabilidades durante la carga de firmas además del correcto funcionamiento de características como packet inspection (IPS/APP Control) y SSL Decryption

- Gestión de credenciales:

En el primer acceso a la GUI se produjo un conflicto con la contraseña de administrador por lo que fue necesario reiniciarla desde la CLI (Consola de Comandos) con el comando config system admin, restaurando el acceso por interfaz gráfica desde la red de MGMT.

- Licenciamiento:

Para permitir que se habilitara completamente el acceso al firewall con su plano de datos completamente accesible y la descarga de actualizaciones de seguridad además de mantenerlo conectado a los servidores de Fortiguard (Servicio que permite la actualización de firmas de IPS, Antivirus, etc..), el dispositivo tuvo que ser licenciado hasta el 29 de Enero de 2026 con una licencia de evaluación (para la que conté con la ayuda de un antiguo compañero de trabajo al que desde aquí agradezco), paso muy importante para

avanzar y permitir los primeros pasos de configuración.

Configuración base:
Como parte del hardening inicial, se procedió a configurar la zona horaria del sistema y se instaló la autoridad certificadora (CA) de Fortinet en el equipo, evitando errores de certificado SSL durante la gestión segura del firewall mediante su ip de MGMT.

3.2 Instalación y licenciamiento de Palo Alto

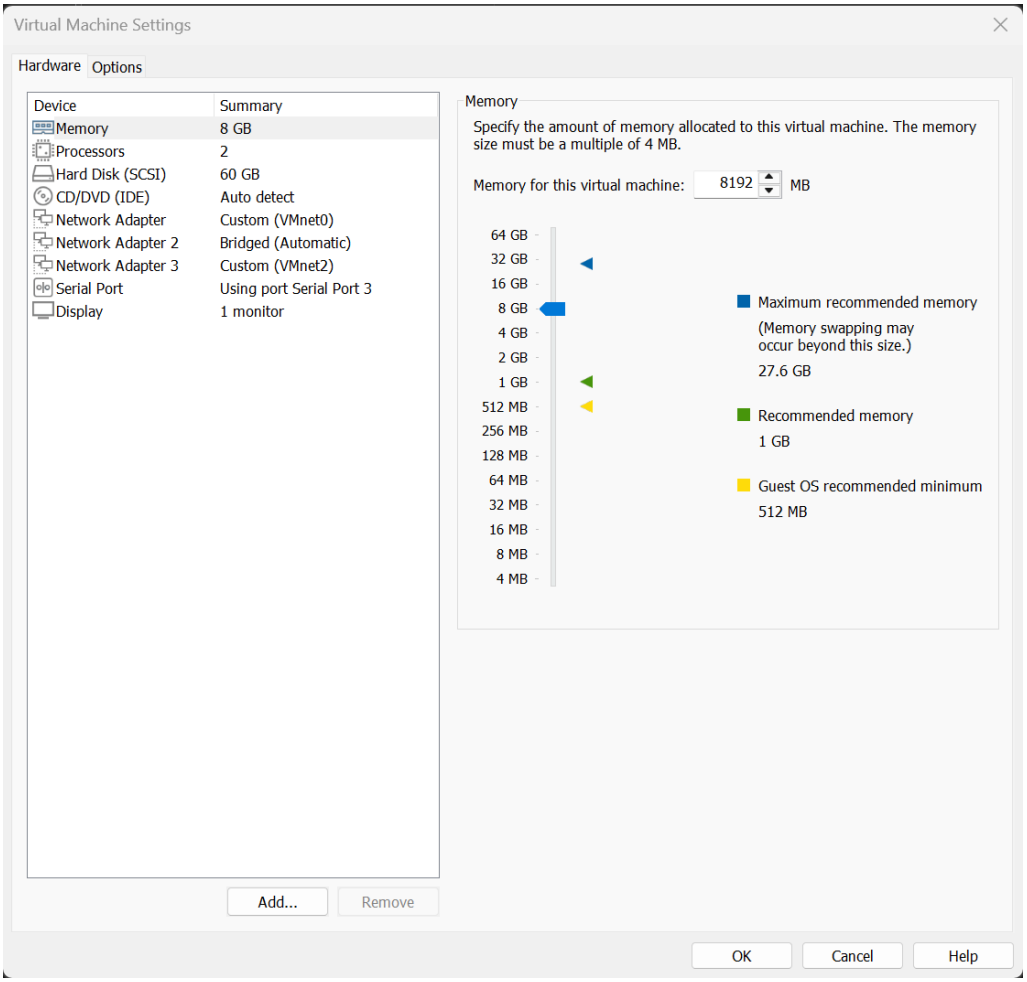


Figura 14 – Configuración en VMware Workstation de la máquina virtual del Firewall Palo Alto

La puesta en marcha del firewall perimetral de Palo Alto se realizó prestando especial atención a la correcta inicialización del Data Plane (siendo posible cuando se tuvo disponibilidad de la licencia que fue entregada mediante un authcode habilitando la configuración de las interfaces), elemento esencial para el funcionamiento del tráfico.

- Despliegue de imagen:

Igual que con despliegues anteriores se estudió la documentación del

fabricante [1] para poder determinar qué .ova usar, en ese estudio hubo cierta confusión con que imagen iba con cada supervisor teniendo que revisar detenidamente las que eran de VMware Workstation o las de ESX que son para entornos empresariales (similar a lo ocurrido con el firewall de Fortinet), finalmente se usó PA-VM-ESX-12.1.2 configurándola con 5,5 GB de memoria RAM y un disco de 60 GB, siguiendo las recomendaciones del fabricante para entornos de laboratorio, al igual que en máquinas anteriores para mejorar la fluidez y viendo recomendaciones del fabricante se subió la RAM a 8 GB.

- Activación de licencia:

Se aplicó una licencia de evaluación mediante un authcode (proporcionado por otro compañero de trabajo al que agradezco desde aquí), que habilitó el dataplane del equipo además de los servicios de Threat Prevention, URL Filtering y WildFire hasta el 10 de noviembre de 2026, permitiendo el uso completo del equipo para el tratamiento del tráfico además del funcionamiento de las medidas de seguridad de este (Perfiles de Seguridad).

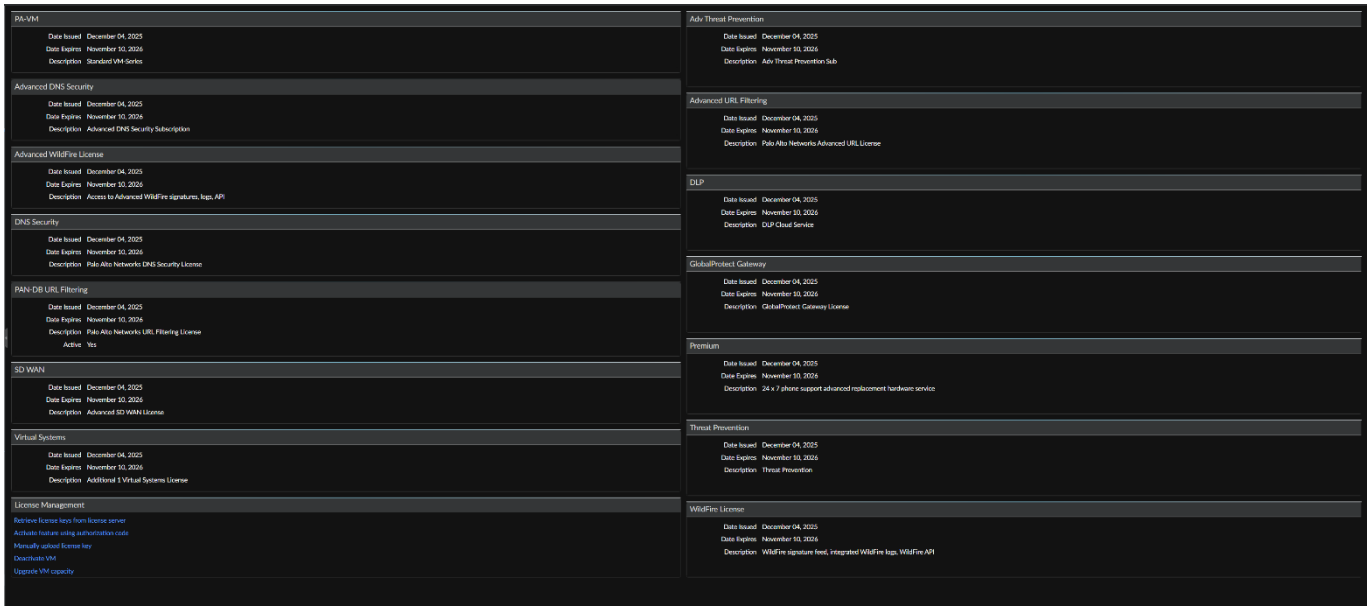


Figura 15 – Panel de licenciamiento del Firewall de Palo Alto

- Configuración de gestión:

Se fijó la IP de MGMT de forma estática mediante el comando de la CLI set deviceconfig system type static, evitando problemas derivados de asignaciones dinámicas por DHCP (configuración de inicio de la interfaz) y garantizando un acceso estable al equipo.

- Resolución del Data Plane:

Un aspecto importante durante el despliegue de la maquina en el hipervisor fue la ausencia inicial de interfaces al ejecutar el comando show interface all, llevando a un estudio detallado en la documentación del fabricante sobre cómo hacer que aparecieran para su configuración. Este comportamiento es

normal en Palo Alto, ya que las interfaces físicas no se activan primero hasta que no se licencia el equipo mediante el authcode (código de licencia), para posteriormente asignarles un modo (Layer 3), una zona de seguridad y un router virtual desde la GUI (Interfaz Web). Una vez que quedo todo configurado, las interfaces se mostraron con el comando inmediatamente.

3.3 Configuración de interfaces y rutas

Cuando ya se habían licenciado los firewalls y montado el resto de los equipos, se procedió a definir la topología de red creada y la lógica de enrutamiento necesaria para garantizar la comunicación entre zonas y la salida a Internet.

- Configuración de interfaces en FortiGate

Port 1 – MGMT: 192.168.1.55/24
Utilizada para la gestión del equipo, en ella se habilitaron los servicios HTTPS, SSH y PING.

Port 2 – DMZ: 10.0.0.3/24
Conexión a la red donde se encuentra el equipamiento corporativo, su salida es el firewall perimetral Palo Alto.

Port 3 – LAN: 172.16.1.1/24
Configurada como puerta de enlace para los equipos internos del laboratorio (LAN).

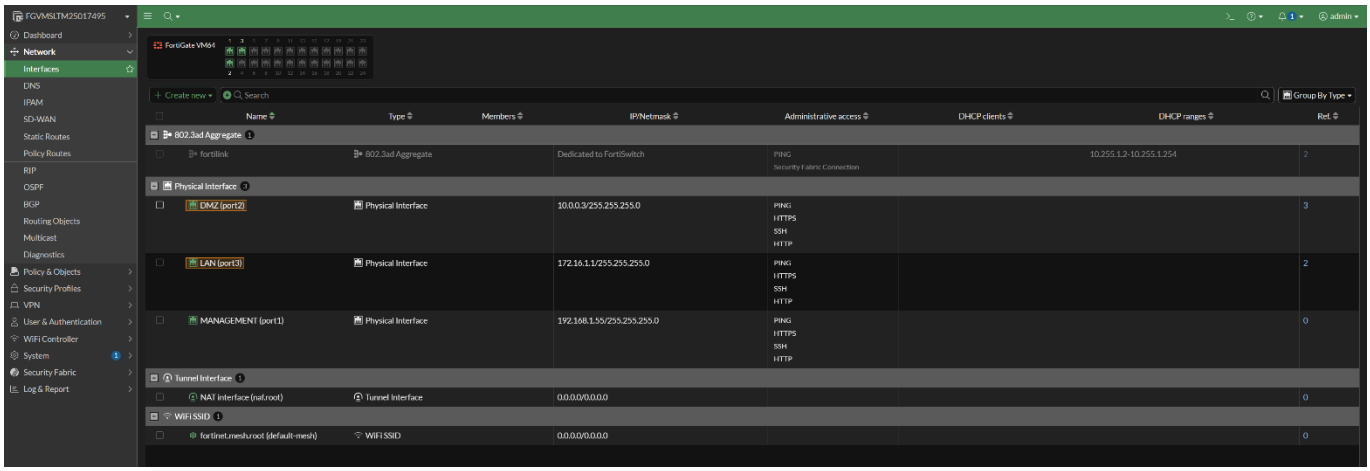


Figura 16 – Interfaces configuradas en el Firewall de Fortinet

- Configuración de interfaces en Palo Alto:

Ethernet1/1 – WAN: 192.168.1.250/24
Simula la salida a la red externa (Internet / WAN) a través del router del laboratorio.

Ethernet1/2 – DMZ: 10.0.0.1/24
Conexión a la red donde se encuentra el equipamiento corporativo, su salida es el firewall de segmentación interna de Fortinet.

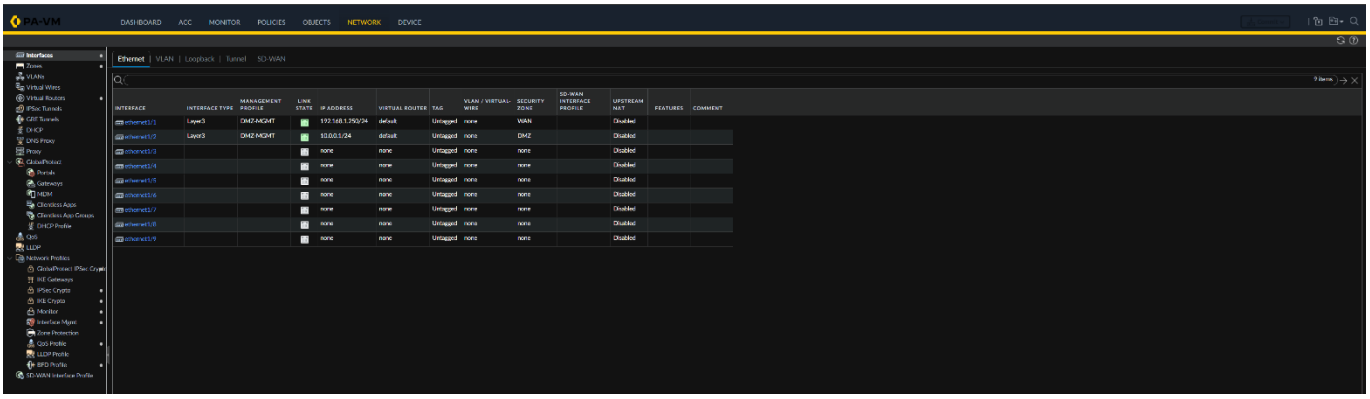


Figura 17 – Interfaces configuradas en el Firewall de Palo Alto

Port MGMT: 192.168.1.45/24
Utilizada para la gestión del equipo, en ella se habilitaron los servicios HTTPS, SSH PING

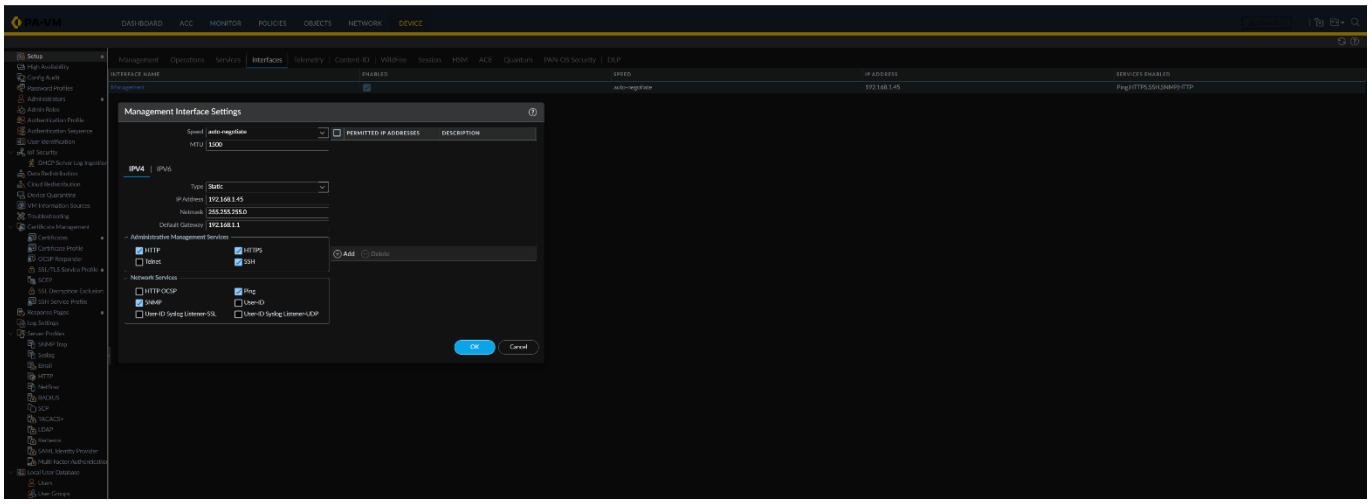


Figura 18 – Configuración de la Interfaz de Management en el Firewall de Palo Alto

Se ha definido un Interface Management Profile llamado DMZ-MGMT (utilizado para MGMT y posteriormente para el resto de los elementos), aplicado a las interfaces del firewall, que limita el acceso administrativo del firewall exclusivamente a HTTPS, SSH y ping, limitando los puertos accesibles de las interfaces.

Lógica de enrutamiento:
Para permitir que el tráfico interno que va hacia internet se canalice hacia el Palo Alto en el FortiGate, se configuró una ruta por defecto con el gateway definido con la ip 10.0.0.1 (Palo Alto) a través del puerto 2.

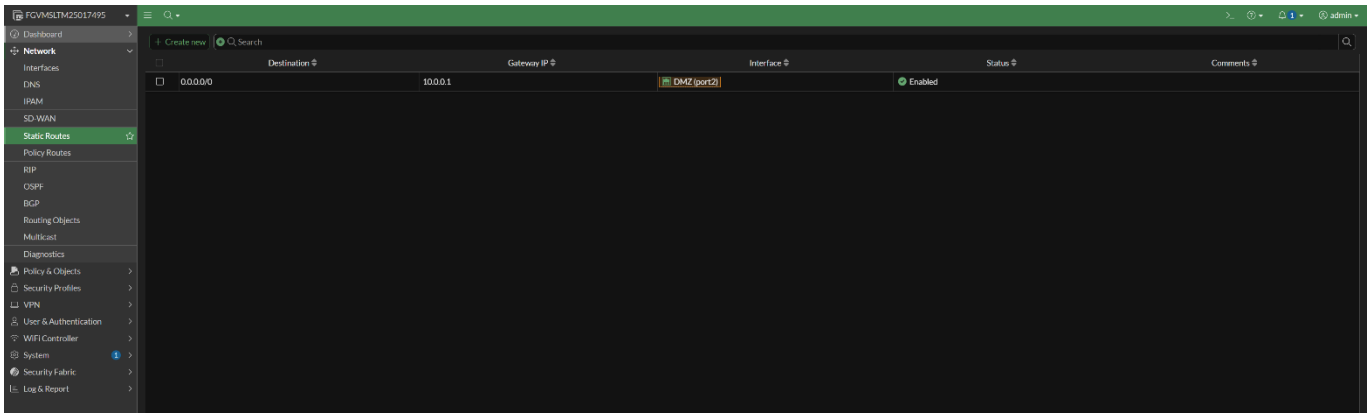


Figura 19 – Ruta por defecto en el Firewall de Fortinet para la salida por el Palo Alto

Acompañando esa configuración y para permitir la salida hacia internet en el Palo Alto, se definió la ruta por defecto utilizando como gateway 192.168.1.1 que es el gateway del router principal.
Ya que se necesitaba garantizar el tráfico de retorno hacia la red interna, se procedió a añadir rutas estáticas en el Palo Alto hacia 172.16.1.0/24 (LAN), utilizando la interfaz de la DMZ del FortiGate (10.0.0.3) como gateway.
De esta forma se crea una arquitectura clara de defensa en profundidad, donde el Palo Alto actúa como firewall perimetral y el FortiGate como firewall de segmentación interna, permitiendo la aplicación de controles de seguridad diferenciados en cada nivel.

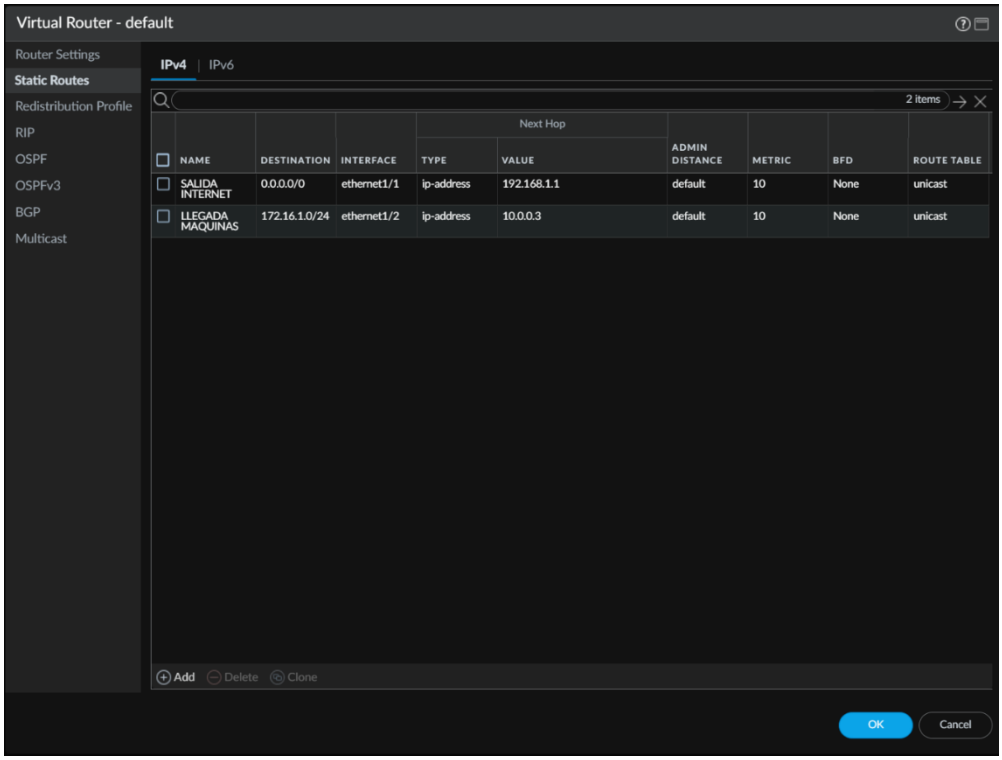


Figura 20 – Rutas en el Firewall de Palo Alto para la salida hacia internet y la llegada a las máquinas de la LAN.

3.4 Integración entre FortiGate y Palo Alto

Cuando ya se había realizado la configuración básica de cada firewall, junto al despliegue del resto de componentes, se procedió a la interconexión de los firewalls con el objetivo de establecer un flujo de tráfico en un modelo de defensa en profundidad, donde cada dispositivo tiene un rol especifico.

- Configuración del enlace DMZ

Se procedió a conectar el Fortigate con el Palo Alto a través de las interfaces de la DMZ (port2 para el Fortigate 10.0.0.3, ethernet1/2 para el Palo Alto 10.0.0.1) actuando este enlace como punto de comunicación entre los firewall de segmentación interna y el perimetral, funcionando en un escenario futuro como zona donde se encuentran los servicios corporativos del nodo (no configurados actualmente (referenciados en el capítulo 8) como por ejemplo LDAP, DNS, etc..), siendo donde está actualmente el Nessus para los análisis de auditoría.

- Lógica de enrutamiento entre firewalls

Con la idea de permitir que el tráfico originado en la red LAN alcance el firewall de perímetro, se configuro en el Fortigate una ruta estática por defecto con gateway el Palo Alto 10.0.0.1 (como se puede ver en la figura 19) para que todo el tráfico con destino externo sea canalizado por el firewall perimetral, en escenarios futuros se dividiría esa ruta para permitir los accesos necesarios a los equipos corporativos, pero para efectos de este laboratorio se ha definido así.

- Ruta de retorno en Palo Alto

Para asegurarnos en la especificación simple realizada del laboratorio de que el Palo Alto conociera la red LAN (172.16.1.0/24), se tuvo que crear una ruta especifica usando como gateway la ip 10.0.0.3 que es la del Fortigate para la DMZ, necesario para asegurar el retorno del tráfico (como se puede ver en la figura 20).

- Activación del Data Plane

Cuando se produjo la activación de la licencia mediante el authcode en el Palo Alto, se activó el dataplane haciendo que aparecieran las interfaces como se ha especificado antes, posteriormente se pasó a configurarles la ip y asociarlas al virtual router correspondiente, pasando después de este proceso ha estado activo (UP) cuando ya están configuradas completamente.

3.5 Resolución de incidencias de conectividad

Durante la fase de despliegue y finalización del laboratorio, surgieron diversas incidencias técnicas que requirieron tareas de troubleshooting de nivel de capa 2 y 3, siendo importante reseñar que en las maquinas Linux los cambios realizados se limitaron a direccionamiento y rutas para su funcionamiento sin alterar la configuración de seguridad de estos hasta la aplicación de mitigaciones:

- Discrepancia de redes virtuales en VMware (Capa 2)

En los primeros pasos del despliegue, no se lograba la conectividad entre las máquinas de la LAN y el FortiGate pese a estar configurados en el mismo rango IP. Después de estudiarlo se pudo analizar que las interfaces virtuales estaban conectadas a switches virtuales distintos (VMnet1 y VMnet2), impidiendo la resolución ARP. La incidencia se resolvió unificando ambos adaptadores y revisando que tuvieran la correspondencia correcta.

- Conflicto de rutas en el plano de gestión del Palo Alto

Cuando se estaba configurando el Palo Alto este no resolvía dominios ni descargaba actualizaciones de contenido. Realizando un estudio de los logs se pudo ver que el tráfico de administración se estaba enviando por el plano de gestión, el cual no disponía de una ruta válida hacia Internet. La solución después del análisis realizado se vio que era configurar las service routes en la GUI del firewall de "Use Management Interface" a "Customize" usando la ethernet 1/1 (Interfaz hacia la WAN / Internet) para forzar que servicios como DNS y NTP utilizaran el dataplane, además de definir servidores DNS públicos (8.8.8.8 y 8.8.4.4), este proceso de análisis evidencio la importancia de diferenciar entre el plano de gestión y el de datos.

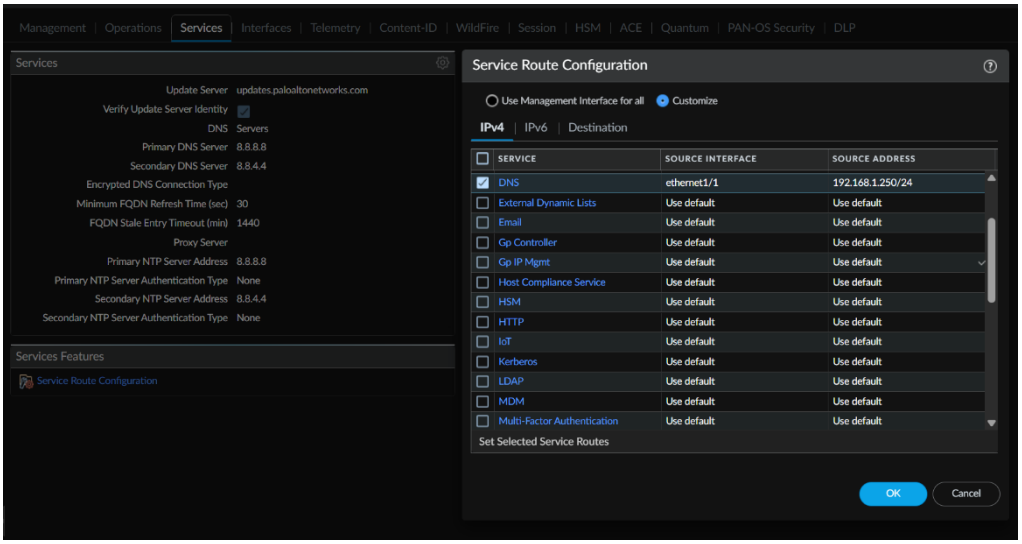


Figura 21 – Panel del Firewall de Palo Alto donde se muestran las Service Routes cambiadas

- Bloqueo de tráfico ICMP por políticas App-ID

Una vez que se comenzó a realizar las reglas de seguridad en los firewalls se vio que en las pruebas de conectividad finales no llegábamos por ping a algunas de las interfaces, por ello en el Palo Alto se volvió a habilitar en la interfaz de MGMT el ping, y en las reglas se puso la aplicación ping también que se había quitado en las mitigaciones realizadas por seguridad dejando solo entre otras el DNS, comprobado mediante nslookup y el comando ping las pruebas fueron satisfactorias.

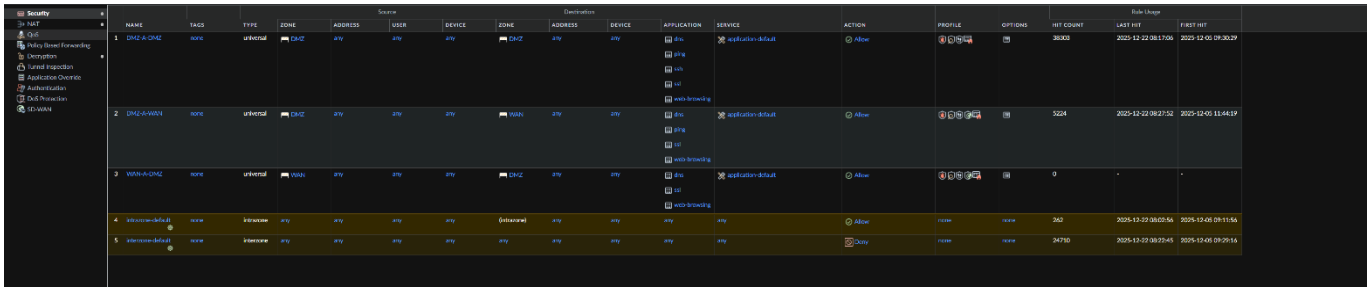


Figura 22 – Políticas de Seguridad configuradas en el Firewall de Palo Alto

- Persistencia de la IP de gestión

Se produjeron cambios al en la IP de MGMT del Palo Alto debido a que se tenía configurado que se diera el direccionamiento por DHCP, por ello la fijamos como estática mediante el comando de la CLI set deviceconfig system type static lo que permitió poder definirla como la 192.168.1.45 sin más problemas futuros.

- Problemas de conectividad de Kali

Durante las diferentes pruebas de conectividad realizadas pudimos ver que la maquina Kali tenía rutas asociadas a la interfaz eth2, provocando esto que el tráfico que iba hacia el Fortigate 172.16.1.1 se fuera por una interfaz que no estaba operativa, para ello procedimos a deshabilitar eth2, limpiar las rutas y forzar la salida por eth1, aunque la interfaz eth1 tenía IP correcta y mostraba enlace, el sistema mantenía rutas asociadas a eth2.
Los comandos utilizados para ello fueron:
sudo ip link set eth2 down
sudo ip route del default
sudo ip route add default via 172.16.1.1 dev eth1

- Duplicación Ip de Gestión Fortigate

En la configuración del Nessus no se estableció ya que la licencia era muy corta una ip de MGMT fija se entraba con la que se daba por DHCP esto provoco que en una ocasión tuviera la .55 que es la misma que el Fortigate con lo cual no se podía entrar a la GUI del firewall, después de ver que si se llegaba por ping y revisando toda las ips de MGMT de las maquinas levantadas ya fuera por DHCP o fijas se vio la inconsistencia y al apagar el Nessus que no se necesitaba en ese momento se recuperó el acceso al Fortigate.

3.6 Verificación de conectividad entre zonas

Una vez que se había procedido a la resolución de las incidencias que habían ido ocurriendo, se realizaron unas pruebas de conectividad para validar la sencilla segmentación realizada, el enrutamiento y las políticas de seguridad:

Origen	Destino	Herramienta	Resultado	Observación
LAN (Kali)	Gateway (Fortigate)	ping	Éxito	Comunicación de Capa 3 validada.
LAN (Kali)	DMZ (Nessus)	nmap	Éxito	El FortiGate aplica SNAT y permite el paso.
LAN (Kali)	WAN (Internet)	ping 8.8.8.8	Éxito	Tráfico atraviesa ambos firewalls y sale por el PA.
DMZ (Nessus)	LAN (Targets)	ping	Éxito	Enrutamiento y Políticas Correctas
PA (Management)	Internet	ping google.com	Éxito	DNS y Service Routes operativos.

Una vez superadas estas pruebas se pudo determinar que la parte de firewalls se encontraba operativa y preparada para las siguientes etapas, permitiendo evaluar la superficie de ataque como la eficacia de las medidas de seguridad implementadas.

3.7 Despliegue y configuración de las máquinas objetivo y de auditoría

Kali Linux

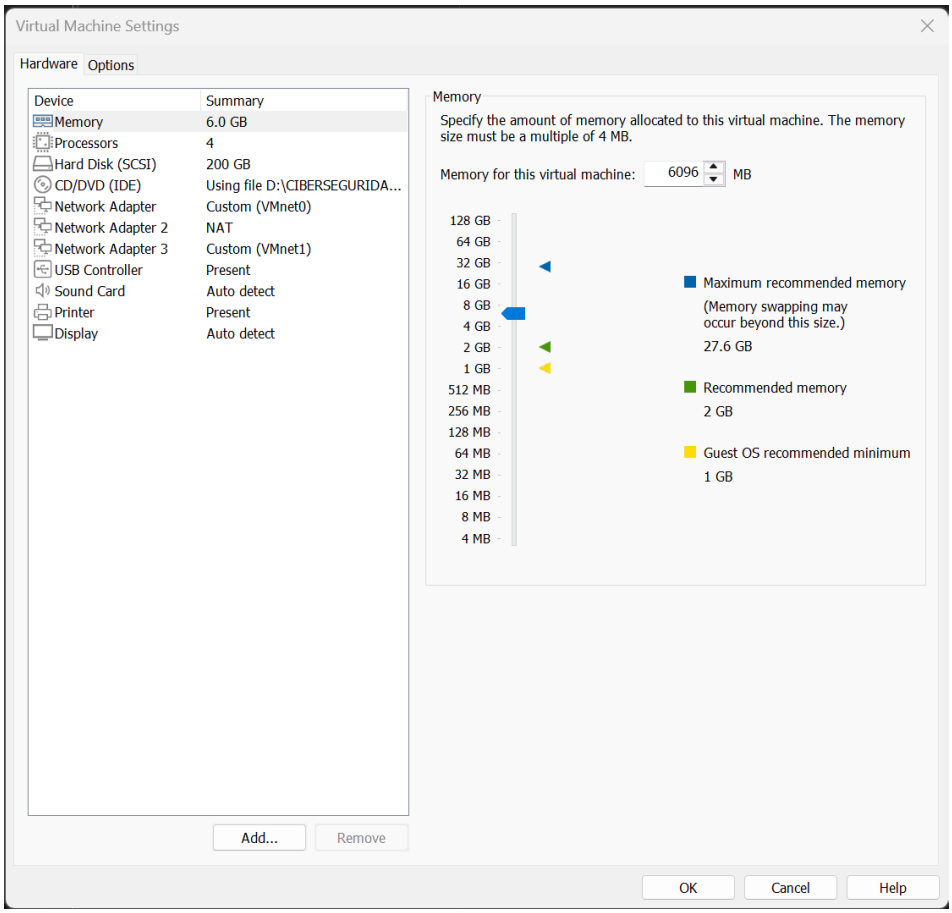


Figura 23 – Configuración en VMware Workstation de la máquina virtual de Kali Linux

Kali Linux es la estación principal de auditoría del nodo representando el rol de atacante interno, desde el se realizan tareas de reconocimiento, enumeración y las pruebas de penetración que irían dirigidas contra los equipos o servidores desplegados en la LAN y en la DMZ

- Configuración de red

Dispone de dos interfaces de red:
Interfaz de gestión (MGMT): perteneciente a la red de MGMT (192.168.1.0/24), con dirección IP 192.168.1.200, utilizada para la gestión de la maquina fuera del hipervisor aunque siempre se ha usado dentro del mismo.
Interfaz LAN: posee la dirección Ip 172.16.1.5 perteneciente a la red LAN (172.16.1.0/24), situándose en la zona interna del laboratorio donde también se encuentra el Metasploitable y el resto de los servidores potenciales.

Con ello hemos realizado una separación que es algo habitual en los entornos profesionales, la red administración de la red interna.

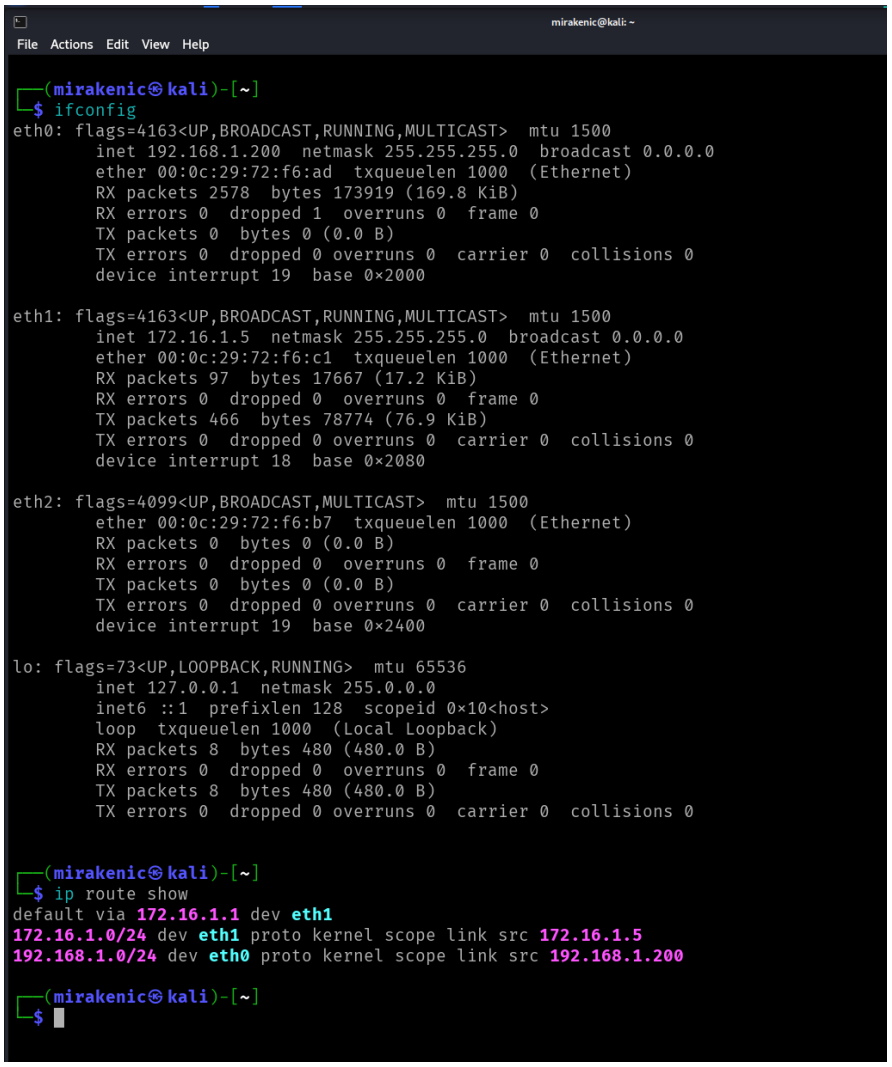


Figura 24 – Interfaces y Rutas configuradas en la maquina Kali Linux

- Estado de seguridad

En el hardening realizado vimos con el comando ss -tuln (Capitulo 6, Figura 60) que la maquina no exponía servicios hacia la red, reduciendo la superficie de ataque, además aplicamos otra capa de endurecimiento mediante la activación del firewall local ufw (Capitulo 6, Figura 59), poniendo que por defecto denegara el tráfico entrante y que permitiera el tráfico de la LAN.

- Justificación

Se eligió esta máquina porque nos permitía encontrar gran cantidad de información sobre su uso, además de la simulación de un escenario realista donde podemos tener un atacante comprometido dentro de la red interna o directamente un equipo con capacidad de poder comprobar vulnerabilidades, evaluar riesgos de otros dentro de cada red del nodo además de poder comprobar la falta de microsegmentación.

Metasploitable

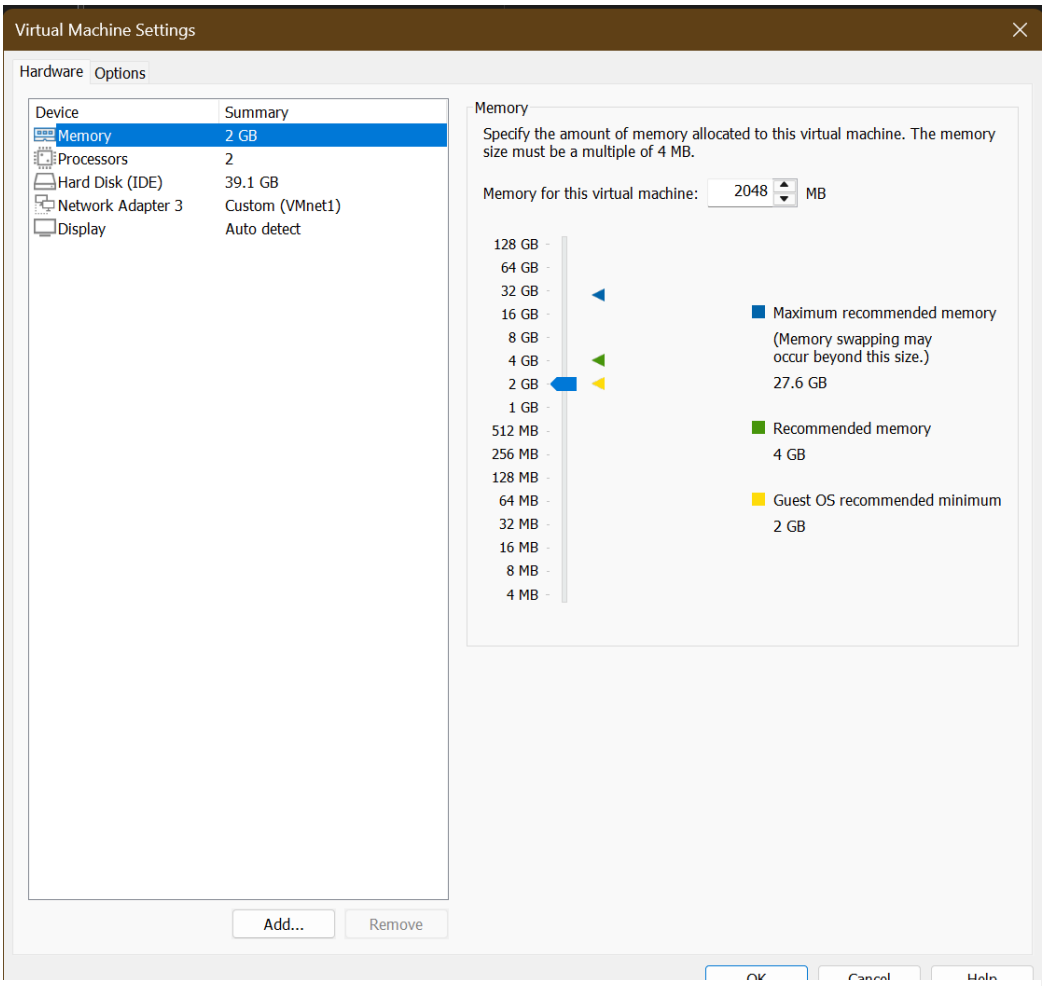


Figura 25 – Configuración en VMware Workstation de la máquina virtual de Metasploitable

Metasploitable se ha configurado en el entorno por tener la utilidad de ser un sistema cuya base ya viene con vulnerabilidades, una maquina intencionalmente mal configurada que sirve como blanco de escaneos y pruebas de explotación en las auditorias.

- **Configuración de red**

Dispone de una única interfaz que es la que está conectada a la red LAN (172.16.1.0/24) con ip 172.16.1.10 siendo la puerta de enlace la (172.16.1.1) que es el Firewall Fortigate, no cuenta con interfaz de gestión con la idea de reducir su exposición a la red interna

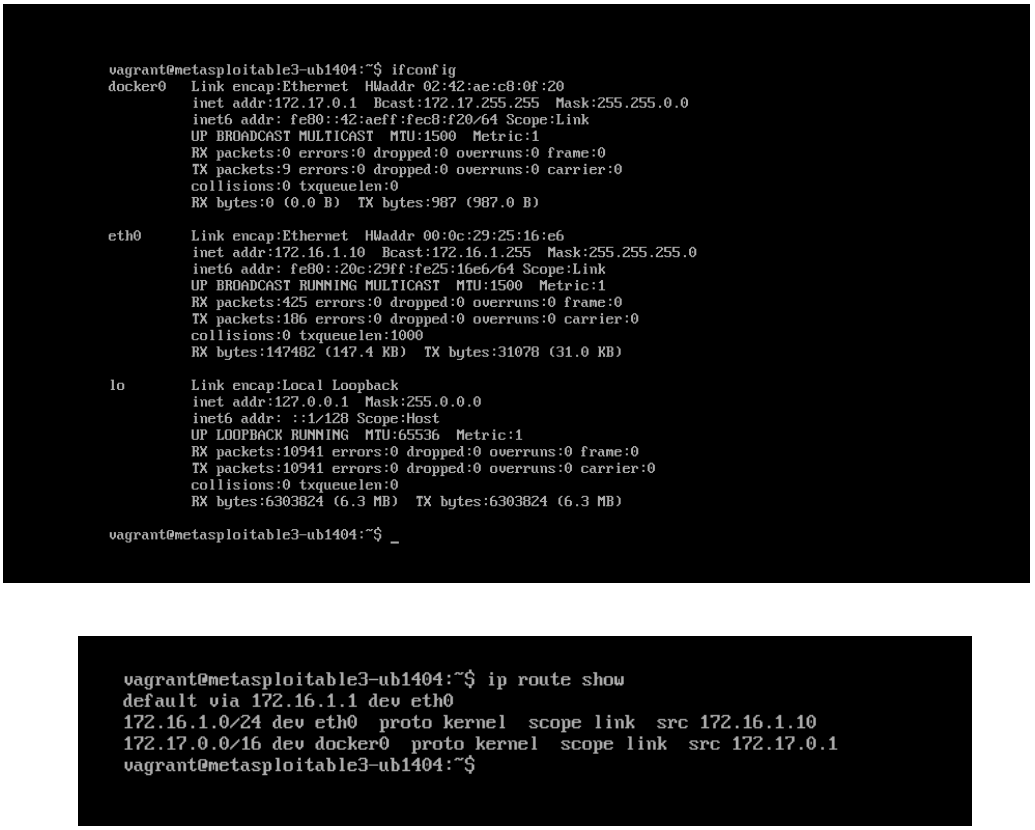


Figura 26 – Interfaces y Rutas configuradas en la maquina Metasploitable

- **Estado de seguridad**

Expone múltiples servicios inseguros intencionadamente, como FTP, MySQL y otros que están obsoletos, sin ninguna medida de hardening aplicada, lo que permite la identificación de vulnerabilidades al realizar escaneos con herramientas como Nessus.

- **Justificación**

Su inclusión permite demostrar las diferentes formas de atacar y reconocer vulnerabilidades de un sistema inseguro y como estas pueden ser encadenadas para alcanzar un control remoto del mismo.

Tenable / Nessus

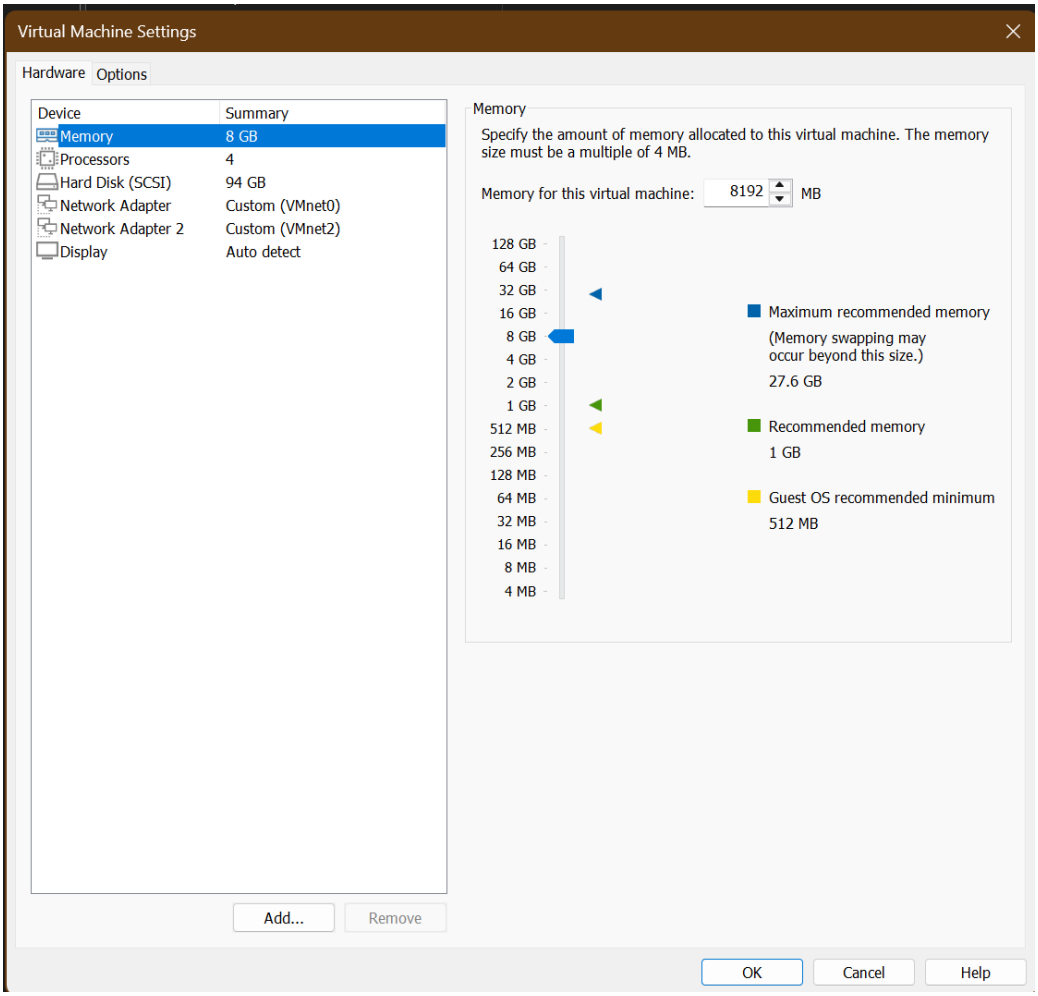


Figura 27 – Configuración en VMware Workstation de la máquina virtual de Tenable Nessus

Tenable Nessus es una herramienta profesional para la gestión y análisis de vulnerabilidades, desplegada como la solución Tenable Core junto a la integración del motor de Nessus.

- Ubicación estratégica

Se procedió a situarlo en la DMZ (10.0.0.0/24) donde se encuentran los servicios corporativos del nodo con la ip 10.0.0.2, todo su tráfico de análisis y reconocimiento de vulnerabilidades (en principio el análisis se enfoca contra equipos de la red LAN también se podría validar vulnerabilidades en equipos de la DMZ) es inspeccionado por el Fortigate (si el escaneo se hace contra equipos de la red LAN como es el que nos ocupa) donde tiene su gateway en la 10.0.0.3. permitiendo aplicar políticas y perfiles de seguridad.

- Metodología de auditoría

Nessus se ha utilizado para ejecutar:
Escaneos no autenticados, simulando un análisis de vulnerabilidades sin credenciales.
Escaneos autenticados vía SSH, proporcionando una visibilidad profunda del sistema objetivo, paquetes instalados y configuraciones internas.
Esta manera de realizar los escaneos resulta valiosa para identificar y comparar diferentes tipos de vulnerabilidades además de la exposición de los sistemas a escanear.

- Limitaciones técnicas

Se utilizó en este caso una licencia de prueba (Trial) de 7 días (Capitulo 2, Figura 10) ya que, aunque se intentó no se pudo acceder a una completa como en el caso del resto de dispositivos , lo que impuso una serie de restricciones como la de poder descargar los informes en PDF. Para solucionarlo, se realizaron una serie de capturas directas desde la interfaz web de Nessus (Capitulo 5, Figuras 29,30,31,34 y 35).

4. Auditoría de Seguridad

La auditoría de seguridad constituye un elemento importante y estructural del trabajo expuesto en este documento, permitiendo evaluar el estado real de los sistemas para la aplicación posterior de medidas correctoras, en su desarrollo se han analizado servicios expuestos, configuraciones inseguras y vulnerabilidades conocidas afectando a diversos sistemas del nodo, lo que nos ha permitido obtener una visión realista del riesgo que se encuentra en la infraestructura, usando para ello escaneos con o sin credenciales para poder ver el estado con y sin acceso inicial al sistema objetivo.

4.1 Metodología de escaneo

Para la realización de la evaluación de seguridad (dada la experiencia laboral adquirida anteriormente además de ser una de las soluciones de análisis de vulnerabilidades más usadas y con más información) se ha utilizado **Tenable Nessus** (herramienta que basa sus detecciones en bases de datos públicas como la National Vulnerability Database (NVD) [3][6])**,** desplegado en la red DMZ, lo que permite simular una posición intermedia con visibilidad para la búsqueda de vulnerabilidades en los equipos de la infraestructura, tanto hacia la red interna (LAN) como hacia los dispositivos de seguridad.

Los escaneos han sido realizados en varias fases:

Descubrimiento de activos: identificación de los hosts en las redes LAN (172.16.1.0/24) y DMZ (10.0.0.0/24).

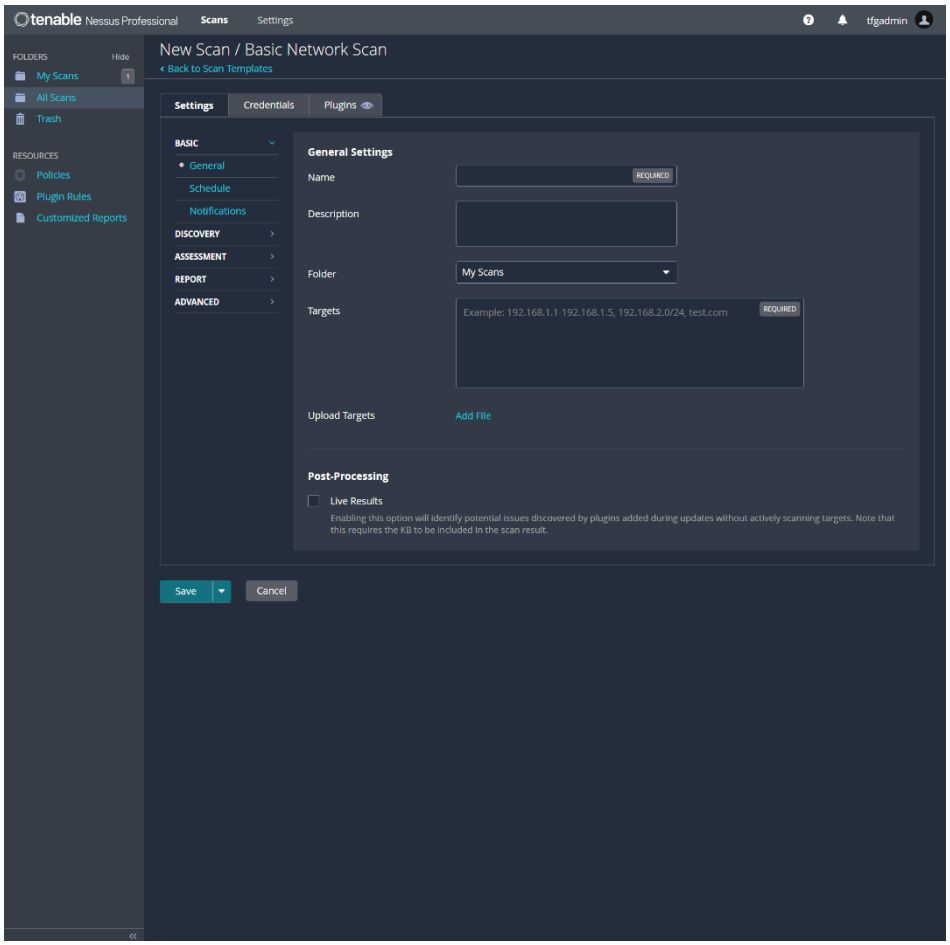


Figura 28 – Panel de lanzamiento de escaneos del Tenable Nessus

Enumeración de servicios: análisis de puertos TCP/UDP abiertos para determinar las diferentes formas de acceso a los sistemas.
Detección de vulnerabilidades: ejecución de plugins de Nessus para identificar software desactualizado, configuraciones inseguras y debilidades conocidas.
Diferentes tipos de escaneos: como se expuso anteriormente se han realizado escaneos con y sin autenticación para mostrar la diferencia en cuanto a visibilidad en el momento en el que se poseen credenciales.
Esta serie de pasos nos ha permitido entender de forma sencilla como realiza el sistema los escaneos hasta la detección de vulnerabilidades y su estudio final además de las mitigaciones necesarias.

4.2 Escaneos no autenticados

Los escaneos no autenticados realizan la simulación de un atacante que ha conseguido acceso a la LAN, pero no dispone de credenciales válidas para el sistema objetivo.
Este tipo de análisis se limita a la información que puede obtenerse únicamente a través de los servicios expuestos.

Alcance

- Metasploitable 3 – 172.16.1.10
- Kali Linux – 172.16.1.5

Resultados

En el caso de Metasploitable, el escaneo detectó un número significativo de servicios expuestos, entre ellos:

- Servicios FTP y MySQL accesibles desde la red.
- Versiones de software conocidas por contener vulnerabilidades críticas y altas.
- Un total de 3 vulnerabilidades críticas y 2 altas, detectables sin necesidad de credenciales.

Figura 29 – Resultado del Escaneo Básico de Tenable Nessus sin Autenticación

Comparándolo con la maquina Kali Linux, esta mostró una superficie de ataque mínima, con vulnerabilidades de carácter informativo o poco importantes, debido principalmente a la ausencia de servicios en escucha y a la actualización del sistema.
Con este análisis hemos podido ver como un sistema mal configurado incrementa su exposición aún frente a atacantes sin credenciales.

4.3 Escaneos autenticados

Con el objetivo de profundizar en la seguridad interna de los componentes del nodo y realizar el estudio más profundo posible, se realizaron escaneos autenticados proporcionando credenciales válidas a Nessus mediante acceso SSH.

Procedimiento

- Se procedió a habilitar el acceso remoto a las máquinas de la LAN.
- Nessus pudo analizar paquetes instalados, versiones de binarios y archivos de configuración locales.
- Se amplió significativamente la cobertura del análisis realizado respecto a los escaneos no autenticados.

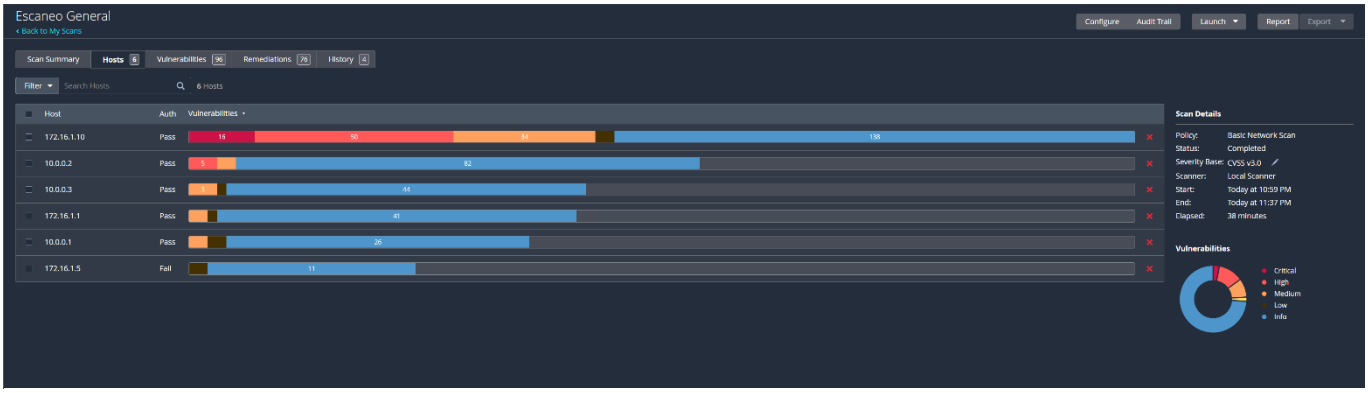


Figura 30 – Resultado del Escaneo Básico de Tenable Nessus con Autenticación

Valor añadido

Con este tipo de escaneo pudimos detectar vulnerabilidades que no eran viables solo desde la superficie como en el no autenticado:

- Fallos de escalada de privilegios local.
- Configuraciones inseguras del sistema operativo.
- Software vulnerable instalado, pero no expuesto.

Con este último análisis hemos podido ver un ejemplo de cómo se incrementan las vulnerabilidades cuando se ha realizado el escaneo con credenciales y el Nessus tiene mayor control y visibilidad sobre el sistema destino.

4.4 Resultados del análisis de vulnerabilidades

Los resultados obtenidos tras los escaneos autenticados muestran una clara diferencia entre las distintas maquinas del laboratorio:

Activo	IP	Críticas	Altas	Medias	Bajas	Informativas
Metasploitable	172.16.1.10	16	50	34	4	138
Servidor Nessus	10.0.0.2	0	5	2	0	82
FortiGate	10.0.0.3	0	0	3	1	44
Palo Alto	10.0.0.1	0	0	1	1	26
Kali Linux	172.16.1.5	0	0	0	1	11

Los datos ilustran una gran cantidad de vulnerabilidades graves en el sistema deliberadamente vulnerable (Metasploitable), mientras que los firewalls presentan únicamente hallazgos de impacto medio o bajo, en su mayoría relacionados con aspectos de configuración y certificados.

4.5 Comparativa entre equipos

Podemos ver diferencias claras si realizamos una comparación entre los diferentes equipos analizados:

- **Metasploitable** presenta un estado de inseguridad grande, diseñado para facilitar la explotación y el encadenamiento de vulnerabilidades.
- **Kali Linux** muestra muy pocas vulnerabilidades, análisis que es coherente con su rol como estación de pruebas y su mantenimiento de actualizaciones.
- **FortiGate y Palo Alto** presentan vulnerabilidades de bajo impacto, gracias también a la elección de máquinas en sus últimas versiones, además de porque son equipos sin hardening completo con solo una configuración inicial realizada.

Un aspecto especialmente relevante es el impacto del escaneo autenticado: en Metasploitable, el número de vulnerabilidades críticas aumentó de forma notable, lo que demuestra que gran parte del riesgo real permanece oculto hasta que se obtiene acceso interno.

4.6 Evaluación de la superficie de ataque

Dentro de los escaneos simples realizados con la herramienta de Nessus hemos podido encontrar tres riesgos reseñables en la red interna LAN:

Acceso remoto sin autenticación
Servicios como ProFTPD permiten la manipulación de archivos sin disponer de credenciales, permitiendo el acceso al sistema.

Servicios de datos vulnerables
MySQL como se ha podido ver tiene versiones susceptibles a ataques de denegación de servicio (DDOS), afectando a la disponibilidad.

Escalada de privilegios local
Una de las vulnerabilidades más comunes, las encontradas en el binario sudo permiten que un usuario sin privilegios obtenga escalando, acceso completo al sistema.

Los resultados obtenidos muestran la necesidad de aplicar una estrategia de **Defensa en Profundidad**, basada en la restricción del tráfico mediante firewalls, el uso de perfiles de seguridad y la mitigación de vulnerabilidades, aspectos que se desarrollan en los siguientes capítulos.

5. Análisis de Vulnerabilidades

Cuando ya se había procedido a la finalización de la fase de auditoria mediante el Tenable Nessus, realizamos una selección de las vulnerabilidades encontradas que ilustraran los escaneos realizados, para ello se seleccionó la máquina que tenía las más representativas que en este caso es Metasploitable.
Con las vulnerabilidades seleccionada cubrimos, ejecución remota de código sin autenticación, denegación de servicio sobre servicios críticos y escalada de privilegios local
Con este estudio podemos ver diferentes tipos de vulnerabilidades y como afectan a los sistemas además de como las medidas de mitigación reducen el riesgo de estas.

5.1 Introducción al CVSS

Con el objetivo de evaluar el impacto y la severidad de las vulnerabilidades estudiadas se ha utilizado el estándar abierto Common Vulnerability Scoring System (CVSS) [7] que asigna una puntuación numérica entre 0 y 10 tomando como base tres grupos de métricas:

- Base Score: describe las características intrínsecas de la vulnerabilidad, incluyendo el vector de ataque, la complejidad, los privilegios requeridos y el impacto sobre la confidencialidad, integridad y disponibilidad.
- Métricas Temporales: tienen en cuenta la madurez del exploit, la disponibilidad de parches y el estado actual de la vulnerabilidad.
- Métricas Ambientales: ajustan la puntuación según el contexto específico del entorno donde se encuentra el sistema afectado.

En este estudio de ha tomado como referencia CVSS V3.1, con las siguientes consideraciones:
Crítica: CVSS ≥ 9.0
Alta: CVSS entre 7.0 y 8.9
Media: CVSS entre 4.0 y 6.9
Las puntuaciones empleadas corresponden a las reportadas por Nessus y a la información oficial de cada CVE.

5.2 Vulnerabilidad crítica – ProFTPD mod_copy

- Puntuación CVSS: 9.8 (Crítica)
- CVE: CVE-2015-3306

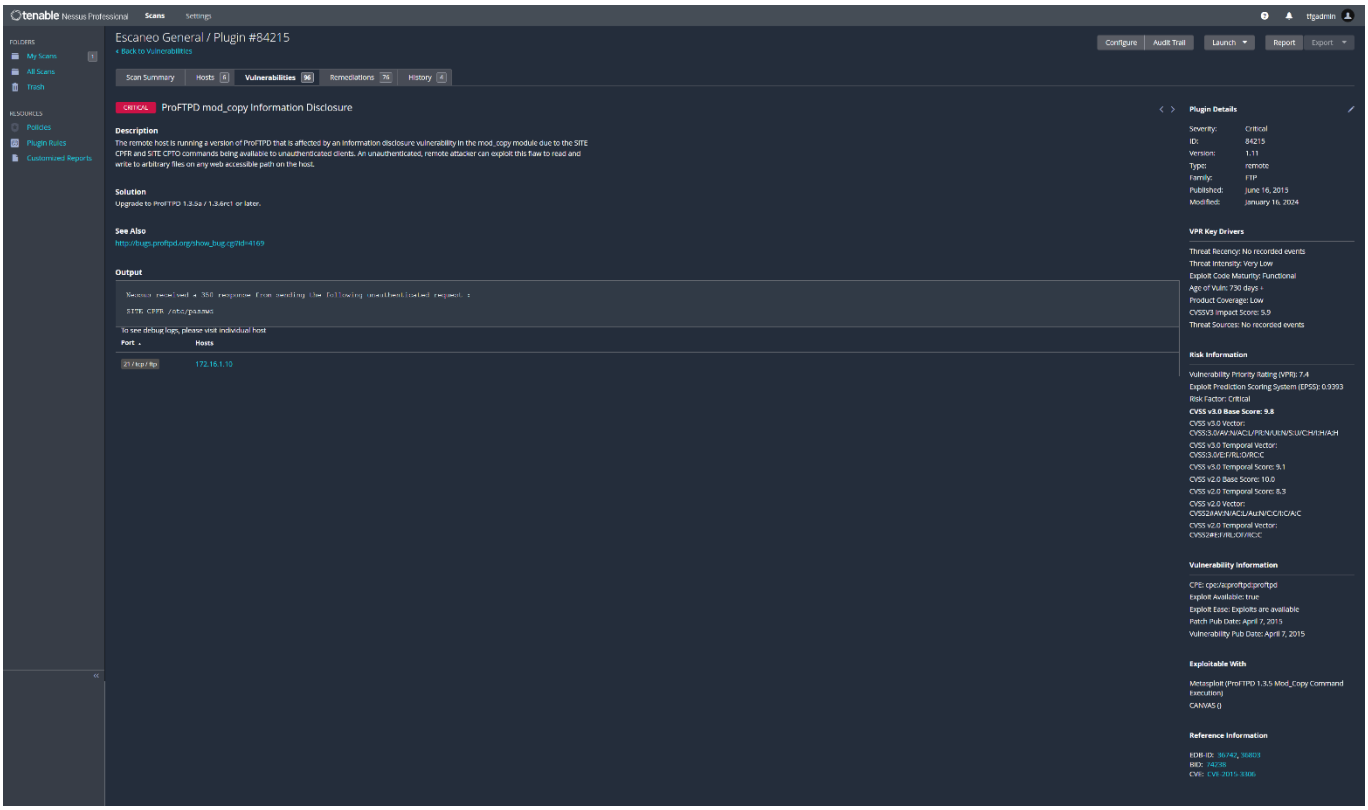


Figura 31 – Panel de Información de Tenable Nessus sobre la vulnerabilidad

- Descripción técnica

Vulnerabilidad que afecta al módulo mod_copy del servicio ProFTPD, este módulo permite copiar archivos en el sistema remoto utilizando comandos FTP extendidos como
SITE CPFR (Copy From) y SITE CPTO (Copy To), pudiéndose ejecutar sin necesidad de autenticación siendo el resultado que se habilita la lectura y escritura de archivos arbitrarios en el sistema de ficheros destino.

```
┌──(mirakenic㉿kali)-[~]
└─$ ftp 172.16.1.10
Connected to 172.16.1.10.
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [172.16.1.10]
Name (172.16.1.10:mirakenic): anonymous
331 Anonymous login ok, send your complete email address as your password
Password:
530 Login incorrect.
ftp: Login failed
ftp> quote SITE CPFR /etc/passwd
350 File or directory exists, ready for destination name
ftp>
```

Figura 32 – Comandos y resultado de la validación de la vulnerabilidad

- Vector de ataque en el laboratorio

El servicio FTP en la máquina de Metasploitable se encuentra accesible desde la red LAN sin restricciones iniciales, pudiéndose desde el Kali Linux identificar el servicio mediante herramientas de enumeración como nmap -p- -sVC 172.16.1.10 y confirmar el uso del módulo vulnerable.

```
┌──(mirakenic㉿kali)-[~]
└─$ nmap -p- -sVC 172.16.1.10

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-12-29 11:59 EST
Nmap scan report for 172.16.1.10
Host is up (0.00052s latency).
Not shown: 65524 filtered tcp ports (no-response)
PORT     STATE  SERVICE     VERSION
21/tcp   open   ftp         ProFTPD 1.3.5
22/tcp   open   ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 2b:2e:1f:a4:54:26:87:76:12:26:59:58:0d:da:3b:04 (DSA)
|   2048 c9:ac:70:ef:f8:de:8b:a3:a3:44:ab:3d:32:0a:5c:6a (RSA)
|   256 c0:49:cc:18:7b:27:a4:07:0d:2a:0d:bb:42:4c:36:17 (ECDSA)
|_  256 a0:76:f3:76:f8:f0:70:4d:09:ca:e1:10:fd:a9:cc:0a (ED25519)
80/tcp   open   http        Apache httpd 2.4.7
| http-ls: Volume /
| SIZE  TIME              FILENAME
| -     2020-10-29 19:37  chat/
| -     2011-07-27 20:17  drupal/
| 1.7K  2020-10-29 19:37  payroll_app.php
| -     2013-04-08 12:06  phpmyadmin/
|_
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Index of /
445/tcp  open   netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
631/tcp  open   ipp         CUPS 1.7
|_http-server-header: CUPS/1.7 IPP/2.1
|_http-title: Home - CUPS 1.7.2
| http-robots.txt: 1 disallowed entry
|_/
| http-methods:
|_  Potentially risky methods: PUT
3000/tcp closed ppp
3306/tcp open   mysql       MySQL (unauthorized)
3500/tcp open   http        WEBrick httpd 1.3.1 (Ruby 2.3.8 (2018-10-18))
|_http-title: Ruby on Rails: Welcome aboard
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: WEBrick/1.3.1 (Ruby/2.3.8/2018-10-18)
6697/tcp open   irc         UnrealIRCd
8080/tcp open   http        Jetty 8.1.7.v20120910
|_http-title: Error 404 - Not Found
|_http-server-header: Jetty(8.1.7.v20120910)
8181/tcp closed intermapper
MAC Address: 00:0C:29:25:16:E6 (VMware)
Service Info: Hosts: 127.0.0.1, METASPLOITABLE3-UB1404, irc.TestIRC.net; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 0s, deviation: 2s, median: 0s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: metasploitable3-ub1404
|   NetBIOS computer name: METASPLOITABLE3-UB1404\x00
|   Domain name: \x00
|   FQDN: metasploitable3-ub1404
|_  System time: 2025-12-29T17:01:56+00:00
| smb2-time:
|   date: 2025-12-29T17:01:58
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 170.10 seconds
```

Figura 33 – Resultado por consola del nmap propuesto

Tomando eso en cuenta, es posible:
Leer archivos sensibles como /etc/passwd
Escribir archivos en directorios accesibles por el sistema
Inyectar shells o binarios maliciosos
Encadenar la vulnerabilidad para obtener ejecución remota de comandos
Esta vulnerabilidad permite que sin credenciales sea posible vulnerar el sistema destino, por ello su clasificación como critica.

- Impacto

Pérdida total de confidencialidad
Modificación arbitraria de archivos
Ejecución remota de código
Punto de entrada inicial para ataques más complejos

5.3 Vulnerabilidad media – MySQL Denial of Service

- Puntuación CVSS: 6.5 (Media)
- CVE: CVE-2020-14567

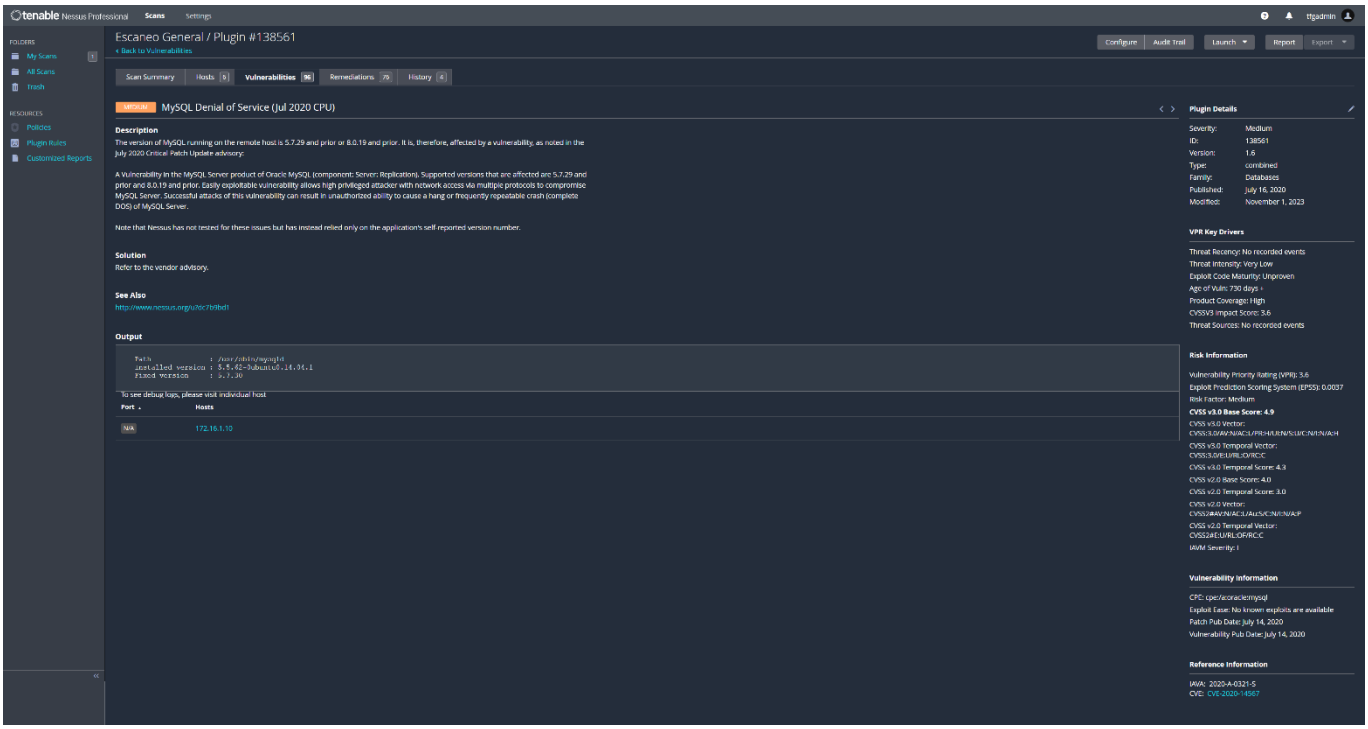


Figura 34 – Panel de Información de Tenable Nessus sobre la vulnerabilidad

- Descripción técnica

Vulnerabilidad que afecta a versiones antiguas de MySQL, como la que se ha podido encontrar en Metasploitable (5.7.29), este fallo permite provocar una denegación de servicio (por saturación de conexiones) mediante el envío de múltiples peticiones malformadas o la saturación de conexiones concurrentes, en este caso no permite la ejecución directa de código ni la obtención de

privilegios, pero si impacta sobre la disponibilidad.

- Vector de ataque en el laboratorio

Se ha podido ver que el puerto 3306/TCP se encontraba accesible desde la LAN sin restricciones, esto permite que sea posible:
Abrir múltiples conexiones simultáneas
Forzar errores internos del servicio
Agotar los recursos del proceso MySQL
Los problemas anteriormente expuestos pueden provocar la caída del servicio lo que conlleva la imposibilidad de atender peticiones, lo que afectaría a aplicaciones dependientes de la base de datos (BBDD).

- Impacto

Interrupción del servicio MySQL
Degradación del rendimiento
Posible parada de aplicaciones dependientes

5.4 Vulnerabilidad alta – Sudo Privilege Escalation

- Puntuación CVSS: 7.8 (Alta)
- CVE: CVE-2021-3156

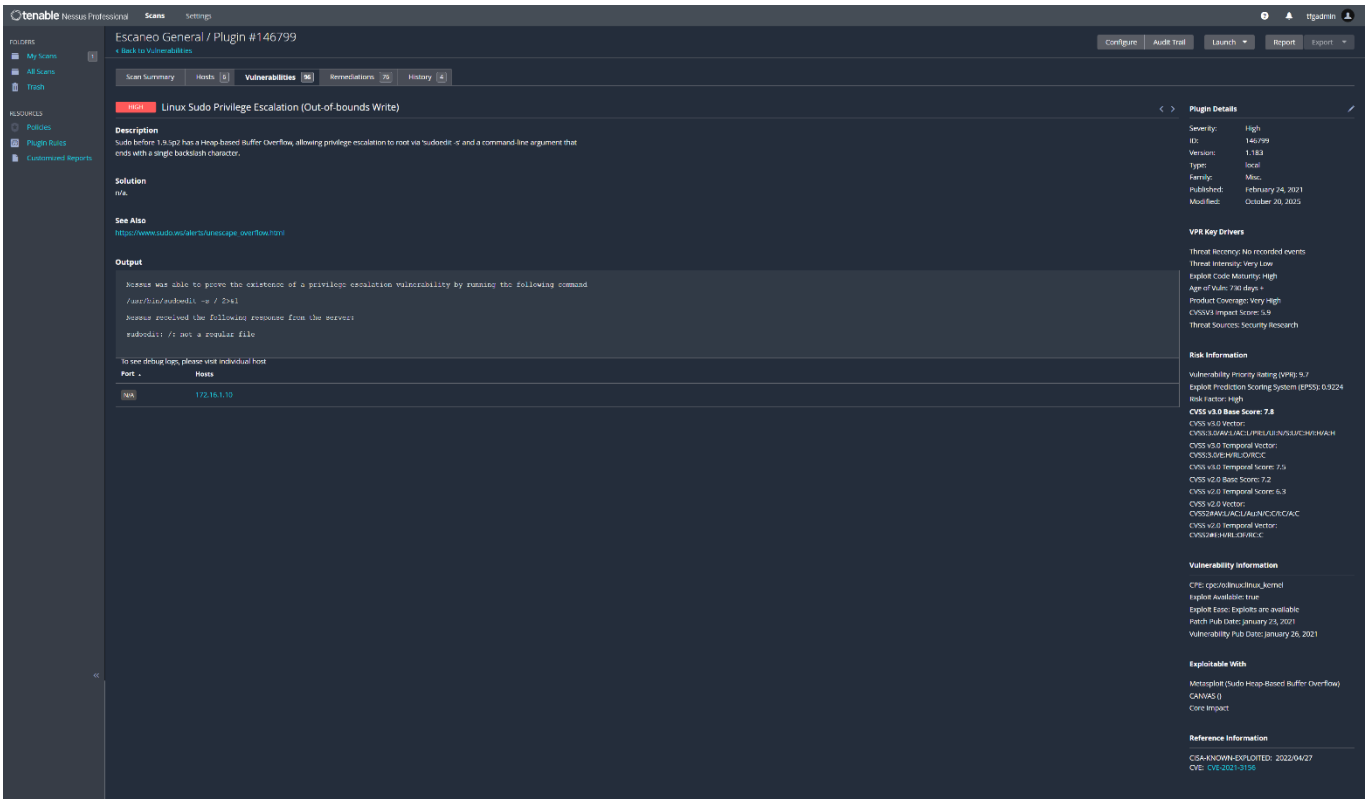


Figura 35 – Panel de Información de Tenable Nessus sobre la vulnerabilidad

- Descripción técnica

Esta vulnerabilidad es un desbordamiento de memoria en el binario sudo que permite a cualquier usuario local escalar privilegios hasta root sin necesidad de conocer la contraseña de administrador, siendo posible su ubicación durante el manejo incorrecto de argumentos en determinadas ejecuciones de sudoedit.

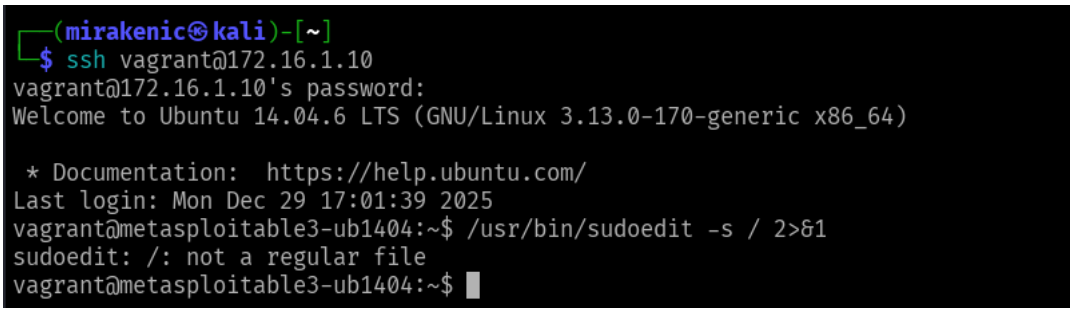


Figura 36 - Comandos y resultado de la validación de la vulnerabilidad

- Vector de ataque en el laboratorio

Esta vulnerabilidad fue detectada gracias a los escaneos autenticados realizados con Nessus, una vez obtenido el acceso inicial al sistema puede ser explotada para:
Obtener acceso root
Modificar configuraciones del sistema
Instalar backdoors
Eliminar evidencias del ataque

- Impacto

Compromiso total del sistema
Anulación de controles de seguridad locales
Persistencia del atacante
Movimiento lateral hacia otros sistemas

5.5 Impacto potencial en un entorno real

Este estudio demuestra cómo estas vulnerabilidades pueden incidir en los sistemas y combinarse para producir un gran impacto.
La implicación de los firewalls dentro del nodo (FortiGate como firewall de segmentación interna y Palo Alto como firewall perimetral), junto con perfiles de seguridad como IPS, control de aplicaciones y filtrado de servicios son muy importante para impedir su explotación antes de que el tráfico malicioso alcance las maquinas destino.
Usando toda la base de las vulnerabilidades comentadas y con la necesidad de mitigar este tipo de debilidades en los sistemas, en próximos capítulos se va a proceder a explicar la estrategia de Defensa en Profundidad, cuya utilización y desarrollo nos ayudara en este tipo de escenarios.

6. Mitigación y Endurecimiento

6.1 Estrategia de defensa en profundidad

La forma de mitigación empleada en el estudio de la infraestructura desarrollada es una que se aplica en gran cantidad de entornos reales (siguiendo buenas prácticas en entornos de seguridad perimetral y auditoria defensiva [11]) como es la defensa en profundidad, donde la seguridad no depende de un único control, si no de superponer diferentes capas; como ejemplo tenemos el entorno desplegado donde se debe de atravesar dos firewalls de distintos fabricantes antes de entrar en la red interna LAN.
Esta forma de estructurar la defensa de los activos nos permite reducir riesgos , ya que un fallo en un fabricante nos permite compensarlo con otro, permitiendo además aplicar controles diferenciados por zonas, lo que nos da la facilidad de separar la seguridad de manera específica, aplicando diferentes medidas de seguridad si así fuese requerido a cada una.

6.2 Mitigación en FortiGate

6.2.1 Políticas de firewall

En el Firewall de FortiGate se ha aplicado una política basada en el principio de mínimo privilegio, restringiendo el tráfico únicamente a los servicios necesarios para las pruebas y conectividad requeridas.

- Las principales medidas adoptadas han sido:

Separación de tráfico LAN → DMZ y DMZ → LAN.
Eliminación de referencias a any (cualquiera) y definición correcta de las reglas siempre que ha sido posible.
Limitación explícita de servicios permitidos (HTTP, HTTPS, SSH y PING según la casuística de cada regla).
Habilitación logtraffic all (loguear todo el tráfico) para ver correctamente los logs al realizar las pruebas y no solo con UTM que solo sacaría los registros de perfiles de seguridad.
Esta segmentación impide que un compromiso en la LAN permita el acceso libre a los sistemas de la DMZ o viceversa.

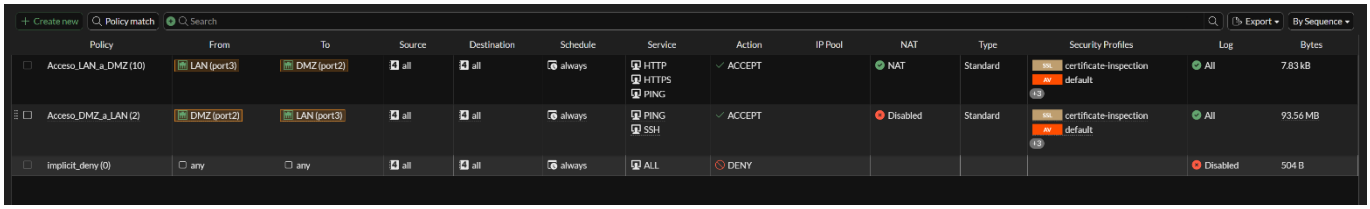


Figura 37 – Reglas configuradas en el Firewall de Fortinet.

En las políticas creadas, para aplicar el principio de mínimo privilegio se ha aplicado una regla por defecto que es la implicit_deny (Cleanup Rule), esta política (situada al final de la lista) deniega todo el tráfico y la aplicación de las

políticas superiores permitiendo el tráfico explícitamente nos habilita a poder gestionar de forma detallada que es lo que queremos que pase o no por el mismo.

6.2.2 Perfiles de seguridad

Fortigate se encarga de la inspección del tráfico interno, para ello usa los perfiles de seguridad, estos han sido configurados por defecto por su validez académica , seleccionando (tomando en cuenta la experiencia laboral adquirida) para su activación los siguientes:
IPS (Intrusion Prevention System): detección y bloqueo de firmas asociadas a vulnerabilidades conocidas, como ProFTPD mod_copy y fallos en MySQL.
Application Control: identificación de aplicaciones independientemente del puerto utilizado.
Antivirus: detección de malware conocido en tráfico permitido.
Web Filtering: control de accesos web a categorías maliciosas o no deseadas.
Certificate Inspection: inspección básica de certificados TLS para detectar anomalías sin entorpecer la navegación.
En un entorno productivo estos perfiles no tendrían su configuración por defecto, se ajustarían de forma específica según los requisitos necesarios (por ejemplo, en el caso que nos ocupa bloqueando las firmas IPS de las vulnerabilidades encontradas).
Como ejemplo aquí vienen reflejadas las firmas relacionadas para cada una de las vulnerabilidades antes estudiadas, se pueden buscar por nombre o por CVE (que proporciona Nessus) y así ver su estado o bloquearlas si fuera necesario.

Figura 38 – Firmas relacionadas con la vulnerabilidad en el IPS de Fortigate

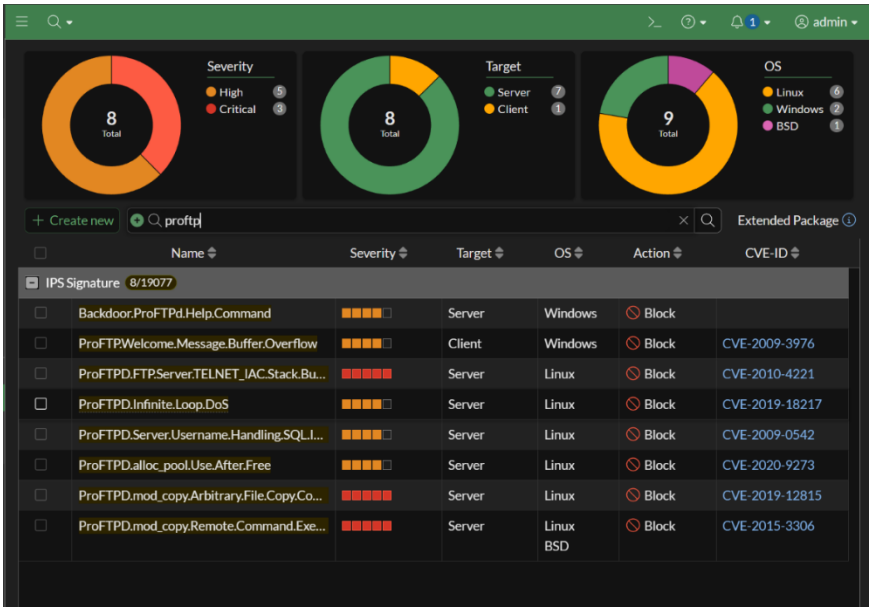


Figura 39 – Firmas relacionadas con la vulnerabilidad en el IPS de Fortigate

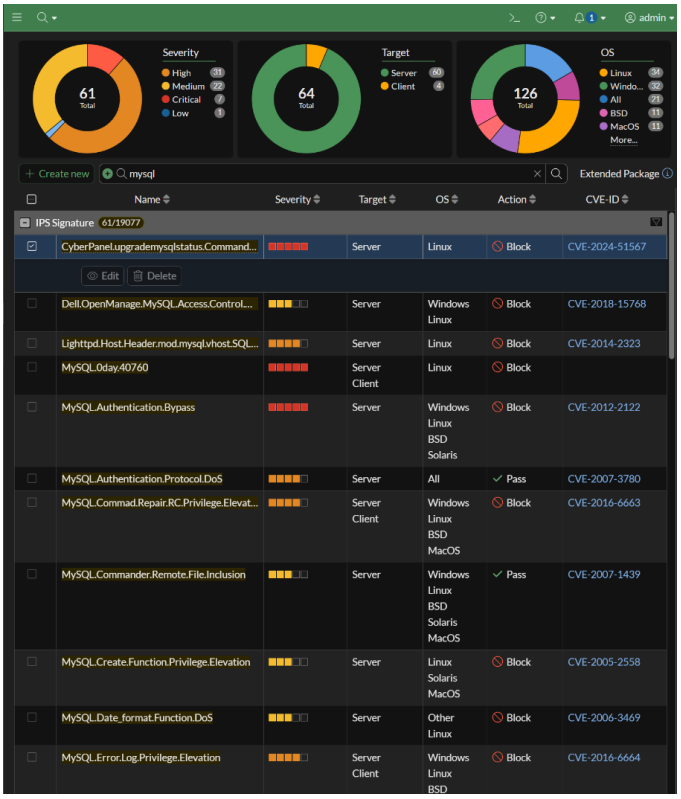


Figura 40 – Firmas relacionadas con la vulnerabilidad en el IPS de Fortigate

6.2.3 NAT y control de tráfico

Se procedido a configurar (como ya se explicó anteriormente) un SNAT en el FortiGate para permitir que los equipos de la LAN accedan a Internet a través del Firewall de Palo Alto, con ello permitiendo que el tráfico originado en 172.16.1.0/24 (LAN) se traduzca al salir por la interfaz DMZ (10.0.0.3) del Fortigate.
Esto nos permite ocultar el direccionamiento interno real y organizar la

estructura del nodo de tal forma que el control de salida a Internet se concentre en el firewall perimetral, manteniendo el FortiGate como firewall de segmentación.

6.2.4 Hardenización del plano de gestión

Con la intención de proteger activamente el Fortigate se han aplicado una serie de medidas recomendadas:

- Bloqueo por intentos fallidos:

3 intentos fallidos → bloqueo de 300 segundos.

- Restricción de servicios de gestión:

Se han deshabilitado HTTP y Telnet.
Se ha establecido dentro de las buenas prácticas el uso de HTTPS y SSH.

- Configuración de NTP para mostrar una coherencia temporal en los logs:

Se ha configurado los servidores de Fortiguard (por simpleza técnica), siendo posible también configurar los mismos que en los DNS (8.8.8.8. 8.8.4.4) o en el caso de disponer de máquinas DNS las ips de esos servidores que tengan configurado el servicio NTP.

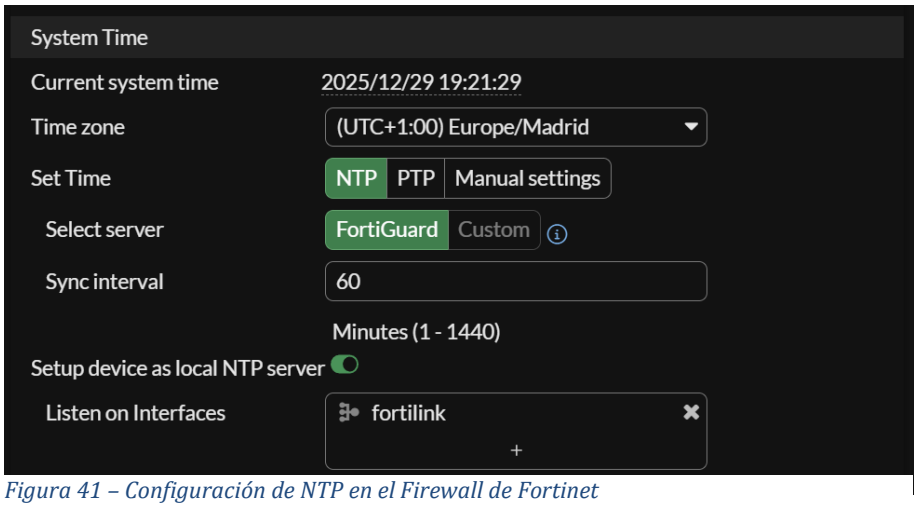


Figura 41 – Configuración de NTP en el Firewall de Fortinet

- Securización de servicios permitidos por interfaz:

Se han limitado los servicios permitidos en cada interfaz a los recomendados.

- Timeout de sesión:

Esta configuración evita tener la consola de administración abierta de forma constante aun sin estar presente la persona que está administrando el firewall.

6.3 Mitigación en Palo Alto

6.3.1 Políticas de seguridad

Se han definido políticas de seguridad en Palo Alto basadas en aplicación y no en puerto ya que permite un mayor control y definición de estas.
Por ejemplo:
Como necesidad para las pruebas de conectividad se habilitó la aplicación ping, evitando abrir ICMP de forma genérica.

El tráfico hacia Internet se abrió a aplicaciones estudiadas como necesarias, entre ellas *dns*, *ssl* y *web-browsing*.

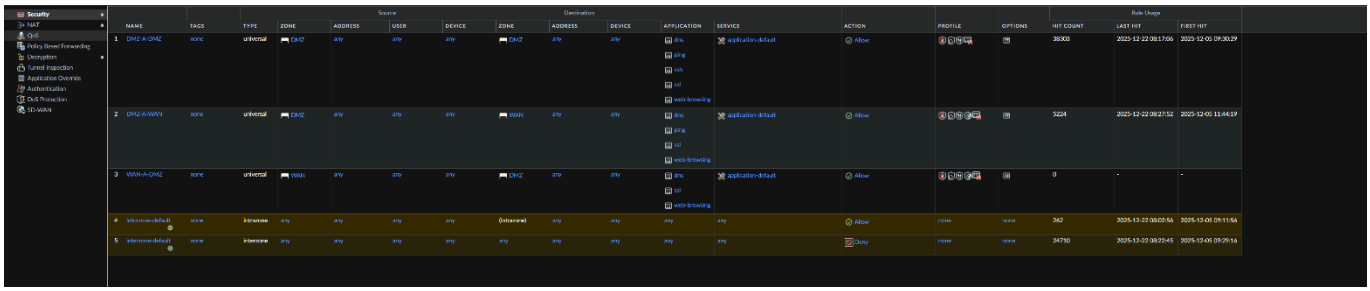
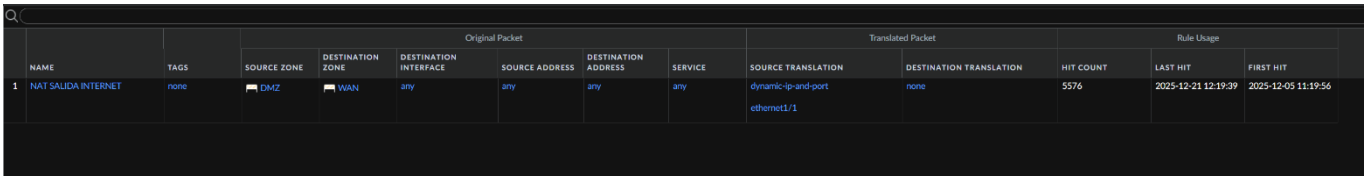


Figura 42 – Conjunto de reglas configuradas del Firewall de Palo Alto

En las políticas creadas, para aplicar el principio de mínimo privilegio se ha definido una regla por defecto que es la interzone_default (Cleanup Rule) con deny en la acción, esta política (situada al final de la lista) deniega todo el tráfico y la aplicación de las políticas superiores permitiendo el tráfico explícitamente nos habilita a poder gestionar de forma detallada que es lo que queremos que pase o no por el mismo.

6.3.2 NAT perimetral

El firewall Palo Alto es el único punto de salida a Internet de la infraestructura, realizando la traducción del tráfico de la DMZ hacia la WAN. Se configuró un dynamic IP and Port (DIPP) (Puerto y IP dinámicos) en la interfaz WAN, permitiendo que todo el tráfico saliente se traduzca a una única IP externa simulada (192.168.1.250).
Con esta configuración conseguimos:
Ocultar las redes internas.
Centraliza el control perimetral.



			Original Packet					Translated Packet		Rule Usage		
	NAME	TAGS	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION	HIT COUNT	LAST HIT	FIRST HIT
1	NAT SALIDA INTERNET	none	DMZ	WAN	any	any	any	any	dynamic-ip-and-port ethernet1/1	none	5576	2025-12-21 12:19:39	2025-12-05 11:19:56

Figura 43 – Regla de NAT de salida a internet del Firewall de Palo Alto

6.3.3 Certificate Inspection

Para poder estudiar las amenazas que se encuentren cifradas en el tráfico que pase por el firewall perimetral sin afectar a la navegación se ha configurado Certificate Inspection.
Durante su estudio y desarrollo fue necesario:
Crear un Forward Trust Certificate (utilizado para firmar dinámicamente los certificados presentados a los clientes cuando el certificado del servidor es

confiable)
Crear un Forward Untrust Certificate (empleado cuando el certificado original del servidor no es confiable)

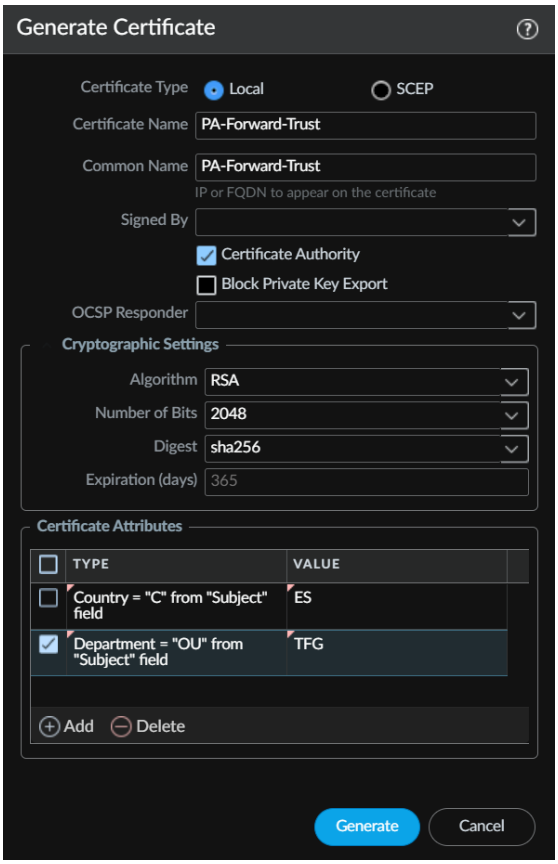


Figura 44 – Configuración del certificado de Forward Trust de Palo Alto (igual para el Untrust)

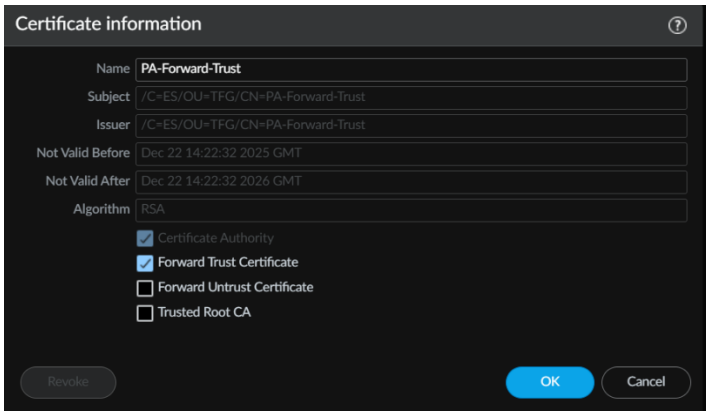


Figura 45 – Determinación del certificado creado como trust o untrust en el Palo Alto

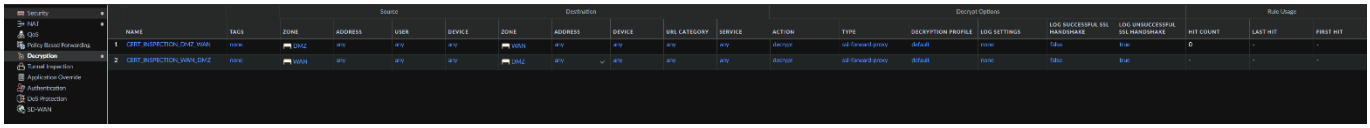


Figura 46 – Reglas de descifrado en el Palo Alto que permiten el análisis del tráfico DMZ – WAN y de forma teórica WAN - DMZ

Hemos procedido a asignarlos correctamente al motor de descifrado, designándolos como Forward Trust y Untrust Certificate en cada información del certificado.

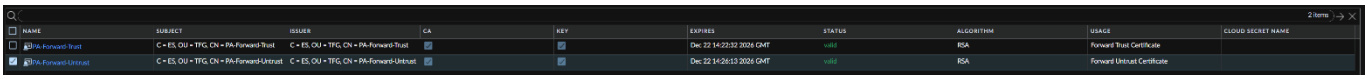


Figura 47 – Listado de certificados creados para el descifrado en el Palo Alto

Este método permite inspeccionar certificados TLS sin descifrar el contenido completo de la sesión, evitando problemas con certificados auto firmados y manteniendo el funcionamiento del tráfico estable sin añadir complejidad; en un entorno real sería posible su sustitución con SSL Deep Inspection con una CA Corporativa, con la idea de analizar todo el tráfico.
En la imagen podemos ver las reglas de descifrado creadas de DMZ a WAN y de WAN a DMZ para poder analizar el tráfico de entrada y de salida del firewall.

6.3.4 Hardenización del plano de gestión

Configuración de NTP para mostrar una coherencia temporal en los logs:
Se ha configurado los mismos servidores públicos que en los DNS 8.8.8.8 8.8.4.4 (por simpleza técnica) o en el caso de disponer de máquinas DNS las ips de esos servidores que tengan configurado el servicio NTP.

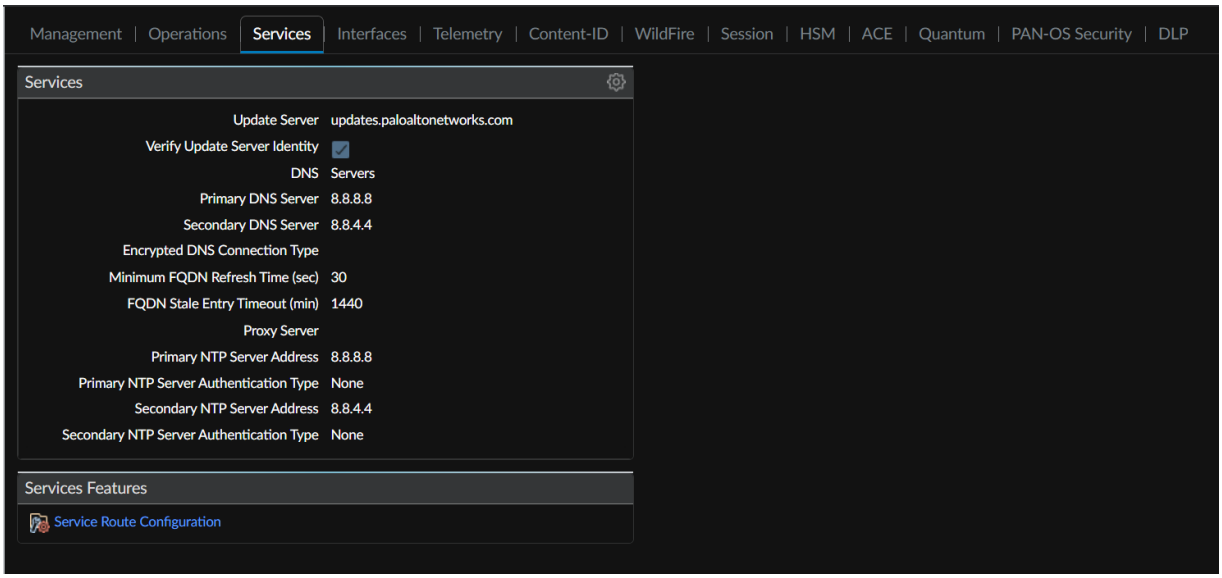


Figura 48 – Configuración de DNS y NTP en el Firewall de Palo Alto

Se configuro un idle timeout (tiempo de espera antes de que caduque la sesión) de 15 min lo que ayuda a proteger el plano de gestión y es una medida

recomendada de seguridad.

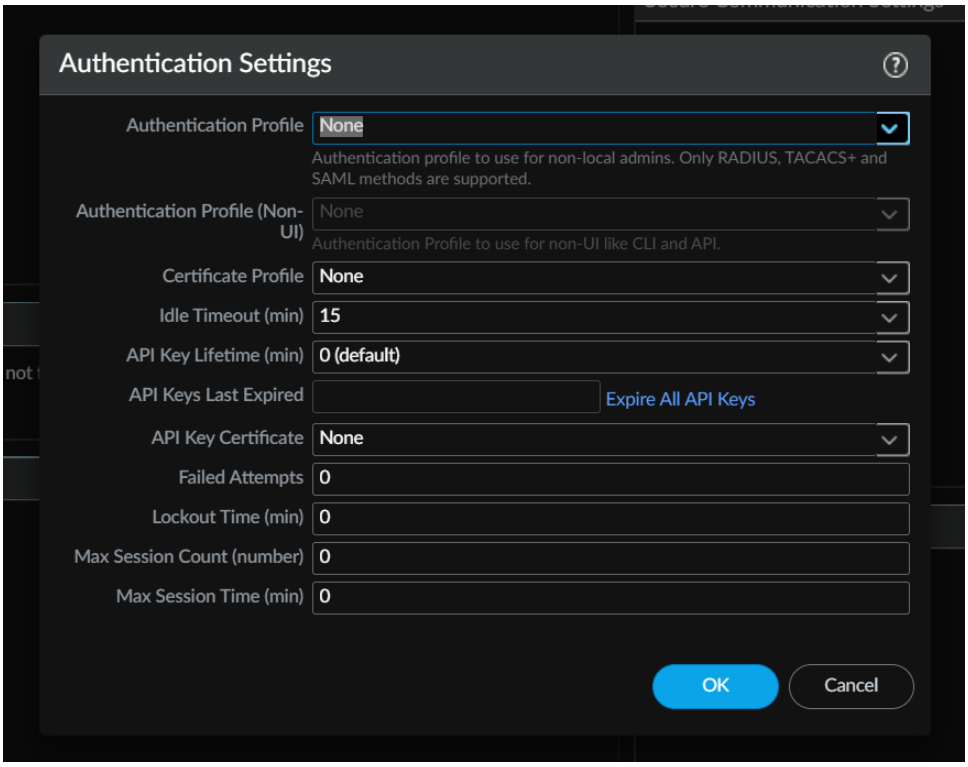


Figura 49 – Configuración de las opciones de autenticación del Palo Alto, entre ellas el idle timeout

No es posible la obtención de un device certificate para validar el acceso al Palo Alto porque lo chequea contra el customer portal donde se encuentre la licencia registrada del que no se posee acceso por haberla obtenido externamente.
No se configura microsegmentación extrema, perfiles complejos ni user-id por tratarse de un laboratorio académico y priorizarse claridad, reproducibilidad y alineación con escenarios reales básicos.

6.3.5 Perfiles de Seguridad

Palo Alto se encarga de la inspección del tráfico perimetral, para ello usa los perfiles de seguridad, estos han sido configurados por defecto por su validez académica , seleccionando (tomando en cuenta la experiencia laboral adquirida) para su activación los siguientes:

IPS (Intrusion Prevention System o Vulnerability Protection): detección y bloqueo de firmas asociadas a vulnerabilidades conocidas.

NAME	LOCATION	COUNT	RULE NAME	THREAT NAME	HOST TYPE	SEVERITY	ACTION	PACKET CAPTURE
strict	Predefined	Rules: 10	simple-client-critical	any	client	critical	reset-both	disable
			simple-client-high	any	client	high	reset-both	disable
			simple-client-medium	any	client	medium	reset-both	disable
			simple-client-informational	any	client	informational	default	disable
			simple-client-low	any	client	low	default	disable
			simple-server-critical	any	server	critical	reset-both	disable
			simple-server-high	any	server	high	reset-both	disable
			more...					
default	Predefined	Rules: 6	simple-client-critical	any	client	critical	default	disable
			simple-client-high	any	client	high	default	disable
			simple-client-medium	any	client	medium	default	disable
			simple-server-critical	any	server	critical	default	disable
			simple-server-high	any	server	high	default	disable
			simple-server-medium	any	server	medium	default	disable

Figura 50 – Captura del perfil de IPS del Firewall de Palo Alto

Antivirus: Detecta y bloquea virus, gusanos y troyanos en diferentes protocolos, utilizando firmas actualizadas constantemente.

Figura 51 – Captura del perfil de Antivirus del Firewall de Palo Alto

URL Filtering: Control de acceso a sitios web basándose en categorías.

NAME	LOCATION	SITE ACCESS	USER CREDENTIAL SUBMISSION	HTTP HEADER INSERTION
default	Predefined	Allow Categories (60)	Allow Categories (88)	
		Alert Categories (15)	Alert Categories (0)	
		Continue Categories (0)	Continue Categories (0)	
		Block Categories (13)	Block Categories (0)	
		Override Categories (0)		

Figura 52 – Captura del perfil de URL Filtering del Firewall de Palo Alto

File Blocking: Permite bloquear la carga o descarga de tipos de archivos específicos.

NAME	LOCATION	RULE NAME	APPLICATIONS	FILE TYPES	DIRECTION	ACTION
basic file blocking	Predefined	Block high risk file types	any	7z, bat, chm, class, cpl, dll, exe, hlp, hta, jar, ocx, PE, pif, rar, scr, torrent, vbe, wsf	both	block
		Continue prompt encrypted files	any	encrypted-rar, encrypted-zip	both	continue
		Log all other file types	any	any	both	alert
strict file blocking	Predefined	Block all risky file types	any	7z, bat, cab, chm, class, cpl, dll, exe, flash, hlp, hta, jar, msi, Multi-Level-Encoding, ocx, PE, pif, rar, scr, tar, torrent, vbe, wsf	both	block
		Block encrypted files	any	encrypted-rar, encrypted-zip	both	block
		Log all other file types	any	any	both	alert

Figura 53 – Captura del perfil de File Blocking del Firewall de Palo Alto

Anti-Spyware: Encargado de la identificación del tráfico de programas espía (spyware) y del de Comando y Control (C2).

NAME	LOCATION	COUNT	POLICY NAME	THREAT NAME	SEVERITY	ACTION	PACKET CAPTURE
default	Predefined	Policies: 4	simple-critical	any	critical	default	disable
			simple-high	any	high	default	disable
			simple-medium	any	medium	default	disable
			simple-low	any	low	default	disable
strict	Predefined	Policies: 5	simple-critical	any	critical	reset-both	disable
			simple-high	any	high	reset-both	disable
			simple-medium	any	medium	reset-both	disable
			simple-informational	any	informational	default	disable
			simple-low	any	low	default	disable

Figura 54 – Captura del perfil de Anti-Spyware del Firewall de Palo Alto

Wildfire Analysis: Se encarga del envío de archivos desconocidos a la nube de Palo Alto para ser analizados en un entorno seguro (sandbox).En el caso de que el fichero enviado resulte ser malicioso, se genera una firma en minutos para proteger a toda la comunidad pudiendo ser aplicada en equipos con las firmas actualizadas.

NAME	LOCATION	RULE NAME	APPLICATIONS	FILE TYPES	DIRECTION	ANALYSIS
default	Predefined	default	any	any	both	public-cloud

Figura 55 – Captura del perfil de Wildfire del Firewall de Palo Alto

Dos Protection: Se encarga de la protección contra ataques DDOS (por ejemplo, como los que usan técnicas de inundación SYN, UDP o ICMP) limitando el número de conexiones por segundo que un host o zona puede recibir o enviar.
El perfil de DDOS creado se ha realizado con la intención de proteger de una forma básica los activos del nodo, si tuviéramos más ips públicas (como en las ampliaciones futuras recomendadas con la introducción de un balanceador como A10) podríamos crear un perfil por cada ip publica en este caso lo hemos creado para proteger lo que venga de la zona WAN a la DMZ para que así genere logs y bloquee peticiones cuando supere unos umbrales en este caso los de por defecto dado el aspecto académico del desarrollo.
Hemos creado un DDOS Protection Profile donde hemos definido los umbrales (protegiendo contra SYN, UDP y ICMP Flood) y luego se ha aplicado a una DOS Protection Policy donde se protegerá lo que venga de la zona WAN a la zona DMZ poniendo el tipo de protección en aggregate para que los umbrales se apliquen a la suma de todo el tráfico que coincide con la regla.
Aquí podemos ver una captura del Dos Protection Profile (Lab-Default-Dos) y de la Dos Protection Policy (Protección-Servidores-Nodo) todo realizado de manera teórica y con los valores por defecto como forma ilustrativa de poder

explicar su funcionamiento en el escenario más lógico para proteger contra ataques desde internet a los activos del nodo.

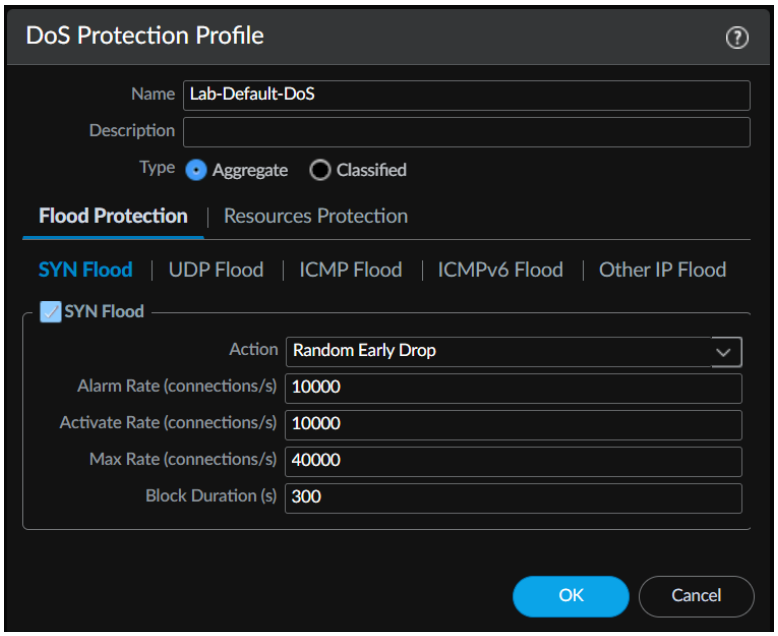


Figura 56 – Captura del perfil de DDOS Protection del Firewall de Palo Alto

Figura 57 – Regla de DDOS del Firewall de Palo Alto, protegiendo de las zonas WAN a DMZ

En un entorno productivo estos perfiles no tendrían su configuración por defecto, se ajustarían de forma específica según los requisitos necesarios (por ejemplo, en el caso que nos ocupa bloqueando las firmas IPS de las vulnerabilidades encontradas).

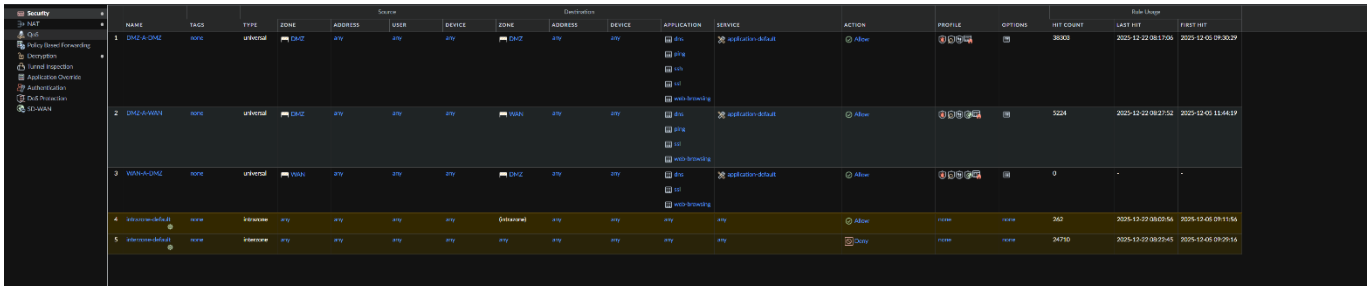


Figura 58 – Reglas del Firewall de Palo Alto con los perfiles de seguridad configurados

En las reglas creadas con la intención de dotar de protección a los activos desplegados se han puesto los perfiles de: Antivirus, Anti-Spyware,Vulnerability Protection,Url Filtering, Wildfire Analysis.

6.4 Hardening de sistemas

Procedemos a explicar el hardening realizado a los sistemas de la infraestructura, es importante comentar que no se ha realizado securización de Nessus nada más que la protección por el aislamiento por red y las políticas abiertas en el firewall de Fortinet, al tratarse de una ova cerrada y no querer entorpecer la labor del escaneo.

6.4.1 Kali Linux

Dentro del continuo avance por securizar todos los sistemas de la infraestructura, se han aplicado una serie de medidas en la máquina del cliente donde se realizan las pruebas para, aunque ya tiene una base de seguridad con el hardening inicial que trae ya que tiene características de máquina para pentesting, se han realizado algunas que ilustren como podríamos avanzar en su securización en un cliente real:

- Firewall local (UFW):

Política por defecto: *deny incoming* / *allow outgoing*.

```
└─$ sudo ufw status verbose
[sudo] password for mirakenic:
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
1234                       ALLOW IN    Anywhere
1234/tcp                   ALLOW IN    Anywhere
22/tcp                     ALLOW IN    Anywhere
Anywhere                   ALLOW IN    172.16.1.0/24
1234 (v6)                  ALLOW IN    Anywhere (v6)
1234/tcp (v6)              ALLOW IN    Anywhere (v6)
22/tcp (v6)                ALLOW IN    Anywhere (v6)
```

Figura 59 – Configuración de firewall de la maquina Kali Linux

- Reducción de superficie de ataque:

Con el comando ss -tuln, hemos podido verificar que no hay servicios en escucha.

```
┌──(mirakenic㉿kali)-[~]
└─$ ss -tuln
Netid    State     Recv-Q    Send-Q       Local Address:Port         Peer Address:Port
```

Figura 60 – Captura de los servicios a la escucha en la maquina Kali Linux

- Actualización del sistema:

Con este comando apt update && apt upgrade, se ha podido lanzar todas las actualizaciones disponibles para asegurarnos de cubrir gran cantidad de vulnerabilidades que pudieran estar pendientes de mitigar.

La protección realizada en esta máquina en cuanto a la infraestructura se basa principalmente en su aislamiento por red y en las políticas realizadas en

el firewall Fortinet.

6.4.2 Metasploitable

Metasploitable es una máquina que debe de permanecer por su naturaleza vulnerable, aun así, además de la aplicación de medidas de protección externas como las reglas en el firewall de Fortigate y no asignarle ip de MGMT, podríamos desde un punto de vista teórico realizar:

- Actualización de ProFTPD y MySQL a versiones seguras.
- Deshabilitación de módulos inseguros.
- Corrección de configuraciones del binario sudo y eliminación de permisos innecesarios.

Esto nos permitiría si la maquina estuviera en un entorno real (actualmente estas propuestas específicas son teóricas ya que es necesario que sea vulnerable a parte de las medidas externas de mitigación) reducir su superficie de ataque y darle una base propia de seguridad al margen de las medidas externas aplicadas.

7. Validación y Pruebas

7.1 Pruebas de conectividad final

Una vez planteadas las mitigaciones con la idea de asegurar la funcionalidad del nodo de interconexión, se procedió a realizar una validación sencilla de conectividad:
LAN → Internet: con las rutas y NAT en ambos firewalls el acceso fue correcto, se permitieron servicios lógicos para la navegación a internet como DNS, HTTPS, HTTP y se tuvo que permitir ping en las interfaces de los firewalls (aunque se había quitado por seguridad) para probar que la conectividad fuera correcta.
DMZ → Internet: tras configurar Service Routes para DNS y NTP en Palo Alto además de las reglas necesarias (permitiendo servicios básicos como HTTP, HTTPS, DNS) se comprobó que el acceso a internet era correcto para los dispositivos de la DMZ, en el caso de añadirse más maquinas tomando en cuenta las necesidades futuras habría que configurarlas para que si necesitan salir a internet tomen como gateway el Palo Alto.
DMZ->LAN: Acceso limitado a las máquinas de la LAN a servicios que requieran las maquinas corporativas (por ejemplo, los puertos del Nessus que sean necesarios en este caso se abrieron PING y SSH) para permitir la llegada desde equipos de la DMZ.

7.2 Validación de reglas y perfiles

Para poder probar los perfiles creados y documentar su funcionamiento realizamos una serie de pruebas desde la maquina base del cliente (Kali Linux) hacia el servidor con vulnerabilidades (Metasploitable).
Con la intención de que las prueban pasen por el Fortinet (actualmente el Kali y el Metasploitable se encuentran en la misma red por simpleza en la

construcción si fuera un entorno real habría que situarlos en diferentes VLANS) y capturar algunos resultados tuvimos que realizar un cambio en el Metasploitable poniéndolo en la DMZ dándole ip (10.0.0.10) y comprobando la conectividad desde el Kali.

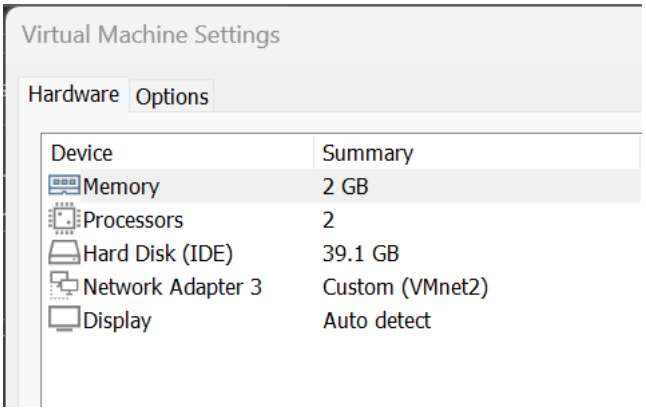


Figura 61 – Configuración provisional en VMware de la maquina Metasploitable

```
vagrant@metasploitable3-ub1404:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 100
0
    link/ether 00:0c:29:25:16:e6 brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.10/24 brd 10.0.0.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe25:16e6/64 scope link
       valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:b5:bf:3b:2d brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever
    inet6 fe80::42:b5ff:febf:3b2d/64 scope link
       valid_lft forever preferred_lft forever
vagrant@metasploitable3-ub1404:~$ ip route
default via 10.0.0.1 dev eth0
10.0.0.0/24 dev eth0  proto kernel  scope link  src 10.0.0.10
172.17.0.0/16 dev docker0  proto kernel  scope link  src 172.17.0.1
vagrant@metasploitable3-ub1404:~$ _
```

Figura 62 – Interfaces y Rutas provisionales de la maquina Metasploitable durante las pruebas

Se verificó la conectividad contra el Metasploitable en la 10.0.0.10 mediante ICMP correctamente.

En la figura siguiente mostramos el escaneo de puertos realizado mediante la herramienta nmap para ver el estado previo de los mismos sin pasar por el firewall de Fortinet.

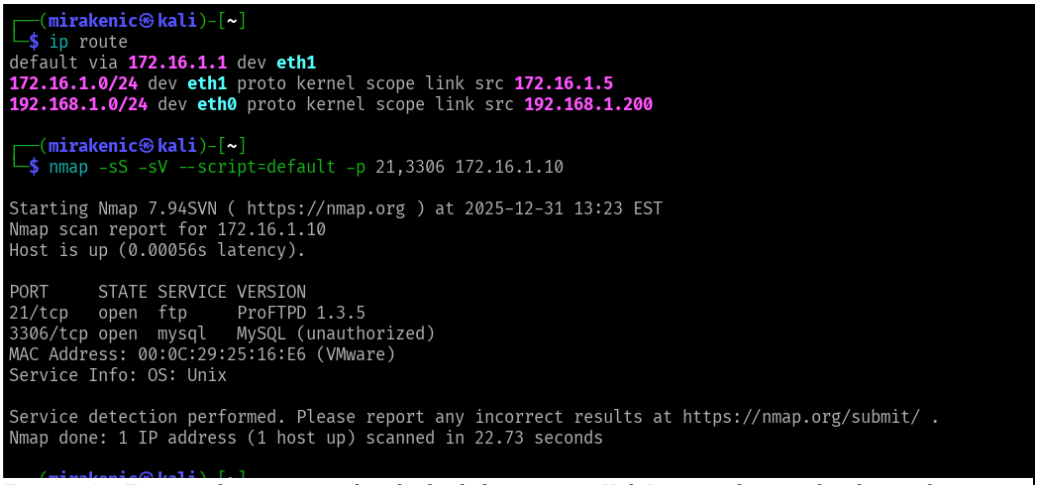


Figura 63 – Escaneo de puertos realizado desde la maquina Kali Linux en las pruebas hacia el Metasploitable antes del paso por el Firewall de Fortinet

Una vez que ya hemos comprobado que con la nueva localización del Metasploitable el tráfico pasaba por el Fortigate realizamos un nmap que ver los puertos abiertos y su estado además de que con la opción -sV nos identifique el servicio asociado y la versión:

```
┌──(mirakenic㉿kali)-[~]
└─$ nmap -sS -sV -p 21,22,80,3306 10.0.0.10

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-12-31 13:52 EST
Nmap scan report for 10.0.0.10
Host is up (0.0022s latency).

PORT     STATE    SERVICE VERSION
21/tcp   filtered ftp
22/tcp   filtered ssh
80/tcp   open     http    Apache httpd 2.4.7
3306/tcp filtered mysql
Service Info: Host: 127.0.0.1

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.84 seconds
```

Figura 64 – Escaneo de puertos realizado desde la maquina Kali Linux en las pruebas hacia el Metasploitable después del paso por el Firewall de Fortinet

Si no se encontrara el firewall monitorizando el tráfico saldría open en el state de cada puerto, recibir un filtered significa que el tráfico está controlado por un elemento intermedio como un firewall en este caso (En la captura más abajo podemos ver como el firewall lo permite).

2025/12/31 19:53:29	172.16.1.5	10.0.0.10	Ping	Accept (UTM Allowed)	Acceso_LAN_a_DMZ (10)
2025/12/31 19:52:54	172.16.1.5	10.0.0.10	HTTP.BROWSER	Accept (UTM Allowed)	Acceso_LAN_a_DMZ (10)
2025/12/31 19:52:54	172.16.1.5	10.0.0.10	HTTP.BROWSER	Accept (UTM Allowed)	Acceso_LAN_a_DMZ (10)
2025/12/31 19:52:54	172.16.1.5	10.0.0.10	HTTP.BROWSER	Accept (UTM Allowed)	Acceso_LAN_a_DMZ (10)
2025/12/31 19:52:54	172.16.1.5	10.0.0.10	HTTP.BROWSER	Accept (UTM Allowed)	Acceso_LAN_a_DMZ (10)
2025/12/31 19:52:54	172.16.1.5	10.0.0.10	HTTP.BROWSER	Accept (UTM Allowed)	Acceso_LAN_a_DMZ (10)
2025/12/31 19:52:54	172.16.1.5	10.0.0.10	HTTP.BROWSER	Accept (UTM Allowed)	Acceso_LAN_a_DMZ (10)
2025/12/31 19:52:54	172.16.1.5	10.0.0.10	HTTP.BROWSER	Accept (UTM Allowed)	Acceso_LAN_a_DMZ (10)
2025/12/31 19:52:54	172.16.1.5	10.0.0.10	HTTP.BROWSER	Accept (UTM Allowed)	Acceso_LAN_a_DMZ (10)
2025/12/31 19:52:50	172.16.1.5	10.0.0.10	HTTP	Accept (84 B / 44 B)	Acceso_LAN_a_DMZ (10)
2025/12/31 19:52:34	172.16.1.5	10.0.0.10	HTTPS	Accept (44 B / 40 B)	Acceso_LAN_a_DMZ (10)
2025/12/31 19:50:57	172.16.1.5	10.0.0.10	Ping	Accept (UTM Allowed)	Acceso_LAN_a_DMZ (10)

Figura 65 – Captura de los logs de tráfico del Firewall de Fortinet

Se han realizado dos intentos controlados de validación de vulnerabilidades registradas en la memoria, la de ProFTPD y la de MYSQL, aunque es importante destacar que no todas las vulnerabilidades son detectables ni explotables a nivel perimetral, algunas dependen de condiciones locales de la máquina destino o de patrones de tráfico específicos que no siempre generan firma IPS:

Para la vulnerabilidad de ProFTPD se habilitó en la regla del Fortinet de DMZ a LAN la aplicación FTP, después se realizó un acceso por ftp al Metasploitable [ftp 10.0.0.10](ftp://10.0.0.10) y los comandos que activan la vulnerabilidad mod_copy descrita:
SITE CPFR /etc/passwd
SITE CPTO /tmp/passwd.copy

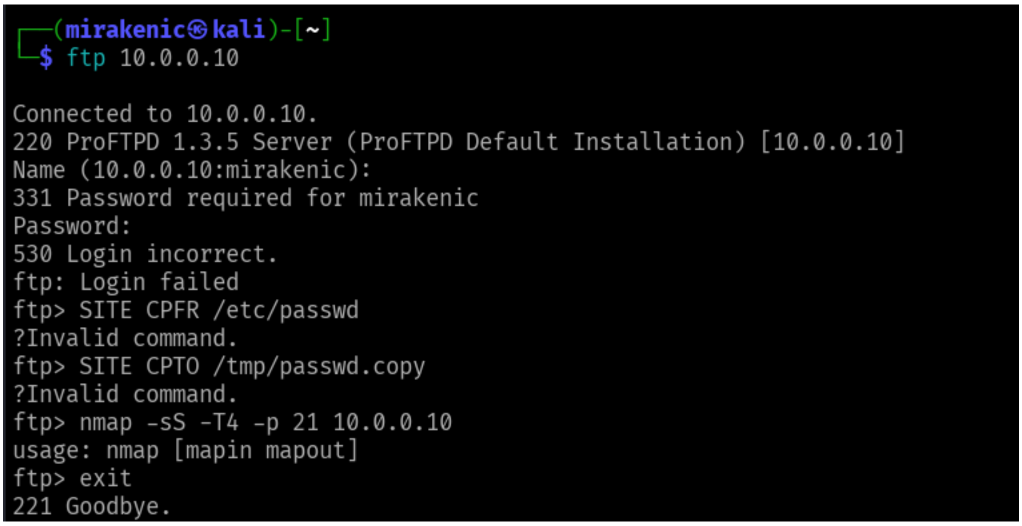


Figura 66 – Comandos realizados en la maquina Metasploitable a través de la maquina Kali Linux para intentar validar la vulnerabilidad descrita

Pero no vemos reflejo en los logs del IPS, se ha visto que es difícil su explotación y la obtención de valores dentro de los logs pudiéndose deber a varios factores.

Para la vulnerabilidad de MYSQL anteriormente descrita se ha intentado realizar un flood al puerto 3306 para ver si saltaban las firmas documentadas, pero no siempre ocurre ya sea por el tiempo que tarda en detectarla, por los umbrales de las firmas o la forma de lanzarlo, para realizar el intento hemos usado la herramienta hping aunque no ha tenido reflejo en la aparición de una firma en los logs del IPS.

```
┌──(mirakenic㉿kali)-[~]
└─$ sudo hping3 -S -p 3306 --flood 10.0.0.10

[sudo] password for mirakenic:
HPING 10.0.0.10 (eth1 10.0.0.10): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 10.0.0.10 hping statistic ---
1013520 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Figura 67 – Comando Hping realizado desde la maquina Kali Linux hacia la máquina Metasploitable para intentar validar la vulnerabilidad descrita

Como se vio que en el nmap se encontraba el puerto 80 abierto y con la idea de realizar un análisis de vulnerabilidades completo hemos probado con la herramienta nikto para realizar una validación activa de vulnerabilidades web, en este caso encontrando que lo bloqueaba el firewall de Fortinet mediante firma de IPS y sacaba logs de seguridad del mismo dando información sobre la protección realizada, lo que constituye un caso probado de securización aplicada al Metasploitable ya que podríamos en las reglas de la LAN a DMZ bloquear el puerto 80 por ejemplo además de la detección por firma (no realizable en este caso por ser necesario para la navegación web).

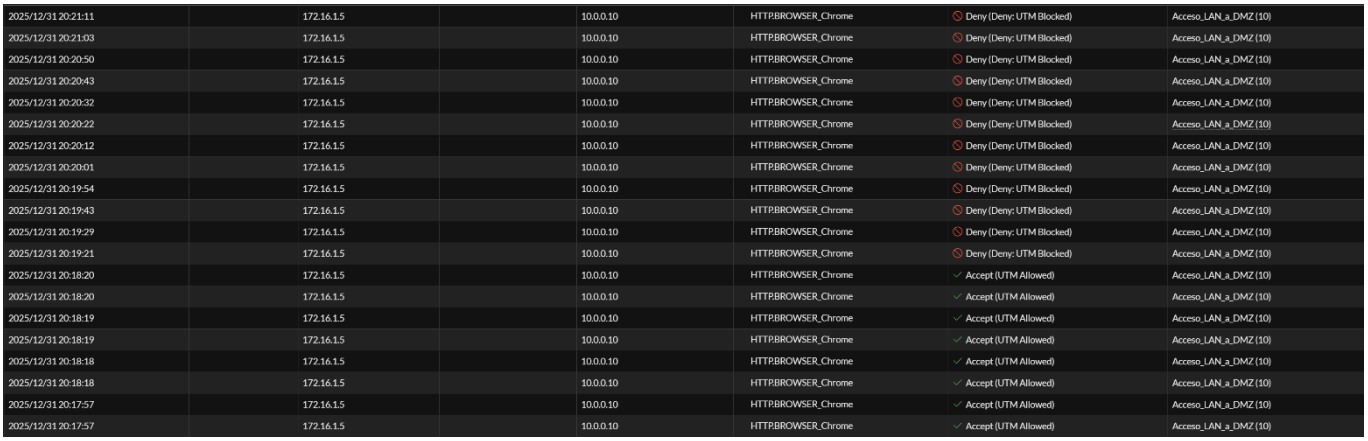
```
┌──(mirakenic㉿kali)-[~]
└─$ nikto -h http://10.0.0.10

- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.0.0.10
+ Target Hostname:    10.0.0.10
+ Target Port:        80
+ Start Time:         2025-12-31 14:17:55 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/
docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of
 the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanne
r/vulnerabilities/missing-content-type-header/
+ /: Directory indexing found.
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the
 2.x branch.
^C
```

Figura 68 – Comando nikto realizado desde la maquina Kali Linux hacia la máquina Metasploitable para realizar el análisis de vulnerabilidades descrito

Además, hemos podido ver con esta herramienta:

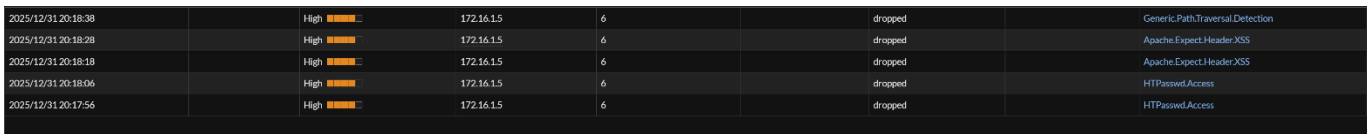
- Ausencia de cabeceras de seguridad (X-Frame-Options, X-Content-Type-Options)
- Indexación de directorios habilitada
- Uso de una versión obsoleta de Apache (2.4.7)

Aquí podemos ver capturas de los logs de firewall y de IPS mostrando las vulnerabilidades encontradas y denegadas durante los tests con la herramienta Nikto:



2025/12/31 20:21:11	172.16.1.5		10.0.0.10	HTTP.BROWSER_Chrome	Deny (Deny: UTM Blocked)	Acceso_LAN_a_DMZ (10)
2025/12/31 20:21:03	172.16.1.5		10.0.0.10	HTTP.BROWSER_Chrome	Deny (Deny: UTM Blocked)	Acceso_LAN_a_DMZ (10)
2025/12/31 20:20:50	172.16.1.5		10.0.0.10	HTTP.BROWSER_Chrome	Deny (Deny: UTM Blocked)	Acceso_LAN_a_DMZ (10)
2025/12/31 20:20:43	172.16.1.5		10.0.0.10	HTTP.BROWSER_Chrome	Deny (Deny: UTM Blocked)	Acceso_LAN_a_DMZ (10)
2025/12/31 20:20:32	172.16.1.5		10.0.0.10	HTTP.BROWSER_Chrome	Deny (Deny: UTM Blocked)	Acceso_LAN_a_DMZ (10)
2025/12/31 20:20:22	172.16.1.5		10.0.0.10	HTTP.BROWSER_Chrome	Deny (Deny: UTM Blocked)	Acceso_LAN_a_DMZ (10)
2025/12/31 20:20:12	172.16.1.5		10.0.0.10	HTTP.BROWSER_Chrome	Deny (Deny: UTM Blocked)	Acceso_LAN_a_DMZ (10)
2025/12/31 20:20:01	172.16.1.5		10.0.0.10	HTTP.BROWSER_Chrome	Deny (Deny: UTM Blocked)	Acceso_LAN_a_DMZ (10)
2025/12/31 20:19:54	172.16.1.5		10.0.0.10	HTTP.BROWSER_Chrome	Deny (Deny: UTM Blocked)	Acceso_LAN_a_DMZ (10)
2025/12/31 20:19:43	172.16.1.5		10.0.0.10	HTTP.BROWSER_Chrome	Deny (Deny: UTM Blocked)	Acceso_LAN_a_DMZ (10)
2025/12/31 20:19:29	172.16.1.5		10.0.0.10	HTTP.BROWSER_Chrome	Deny (Deny: UTM Blocked)	Acceso_LAN_a_DMZ (10)
2025/12/31 20:19:21	172.16.1.5		10.0.0.10	HTTP.BROWSER_Chrome	Deny (Deny: UTM Blocked)	Acceso_LAN_a_DMZ (10)
2025/12/31 20:18:20	172.16.1.5		10.0.0.10	HTTP.BROWSER_Chrome	Accept (UTM Allowed)	Acceso_LAN_a_DMZ (10)
2025/12/31 20:18:20	172.16.1.5		10.0.0.10	HTTP.BROWSER_Chrome	Accept (UTM Allowed)	Acceso_LAN_a_DMZ (10)
2025/12/31 20:18:19	172.16.1.5		10.0.0.10	HTTP.BROWSER_Chrome	Accept (UTM Allowed)	Acceso_LAN_a_DMZ (10)
2025/12/31 20:18:19	172.16.1.5		10.0.0.10	HTTP.BROWSER_Chrome	Accept (UTM Allowed)	Acceso_LAN_a_DMZ (10)
2025/12/31 20:18:18	172.16.1.5		10.0.0.10	HTTP.BROWSER_Chrome	Accept (UTM Allowed)	Acceso_LAN_a_DMZ (10)
2025/12/31 20:18:18	172.16.1.5		10.0.0.10	HTTP.BROWSER_Chrome	Accept (UTM Allowed)	Acceso_LAN_a_DMZ (10)
2025/12/31 20:17:57	172.16.1.5		10.0.0.10	HTTP.BROWSER_Chrome	Accept (UTM Allowed)	Acceso_LAN_a_DMZ (10)
2025/12/31 20:17:57	172.16.1.5		10.0.0.10	HTTP.BROWSER_Chrome	Accept (UTM Allowed)	Acceso_LAN_a_DMZ (10)

Figura 69 – Captura de logs de tráfico del Firewall de Fortinet



2025/12/31 20:18:38		High	172.16.1.5	6	dropped	Generic.Path.Traversal.Detection
2025/12/31 20:18:28		High	172.16.1.5	6	dropped	Apache.Expect.Header.XSS
2025/12/31 20:18:18		High	172.16.1.5	6	dropped	Apache.Expect.Header.XSS
2025/12/31 20:18:06		High	172.16.1.5	6	dropped	HTPasswd.Access
2025/12/31 20:17:56		High	172.16.1.5	6	dropped	HTPasswd.Access

Figura 70 – Captura de logs de IPS del Firewall de Fortinet

Con las pruebas realizadas, hemos podido realizar intentos de validación de las vulnerabilidades reseñadas anteriormente y la documentación de una no descrita extensivamente, pero encontrada con otra herramienta además de poder revisar el funcionamiento de los perfiles de seguridad y las reglas aplicadas, siendo importante reseñar que la ausencia de detección en algunas pruebas no implica la mala configuración de los sistemas de protección sino que algunas vulnerabilidades no generan patrones perimetrales claros o requieren umbrales muy específicos para que salte la firma IPS, lo cual se asemeja en su detección y análisis a un entorno real.

7.3 Comparativa antes / después

Antes del estudio realizado cuando se completó la configuración inicial en el primer escaneo autenticado del Nessus, encontramos una serie de vulnerabilidades, la mayoría de ellas en la maquina específicamente vulnerable como es el Metasploitable.
Durante el desarrollo del laboratorio después de su configuración inicial hemos aplicado una serie de medidas de mitigación, ya sea tanto en reglas y

perfiles de seguridad en los firewalls, como aplicando medidas dentro de las máquinas para securizarlas.
Con las acciones tomadas no hemos eliminado completamente el riesgo ya que si no se actualizan los sistemas o se parchean las vulnerabilidades siguen presentándose dentro de las maquinas, pero hemos reducido la superficie de ataque en gran manera, además de hacer que el tráfico sea inspeccionado y reducir el acceso por diferentes puertos a determinados elementos de la infraestructura.
Podríamos seguir avanzando en la mejora de la securización de los activos del nodo, pero con los cambios realizados nos hemos asegurado como en un entorno real que esas vulnerabilidades vean muy reducida su explotación que es con el estudio diario la base de cualquier grupo de trabajo real.

8. Conclusiones

8.1 Conclusiones técnicas

El desarrollo de la infraestructura y sus posteriores pruebas y documentación nos ha permitido probar y validar un laboratorio de seguridad donde se ha podido reproducir un entorno real corporativo tomando como base principios como la segmentación de red, defensa en profundidad y la funcionalidad más básica de las auditorias de seguridad.
Se ha desarrollado el nodo de interconexión propuesto en un sistema virtualizado conocido como es VMware Workstation integrando numerosos fabricantes y distintas tecnologías, asignando los recursos necesarios a los mismos para conseguir estabilidad y funcionalidad en la implantación de las configuraciones.
La decisión de integrar firewalls de dos fabricantes nos ha permitido trabajar con una estructura multicapa y aprender diferentes formas de realizar las implementaciones, el Palo Alto ha actuado de firewall perimetral, con control por aplicación, NAT, políticas de seguridad e inspección de tráfico, el Fortigate ha tenido el rol de firewall interno o de segmentación interna donde se ha configurado para controlar el tráfico interno y entre redes distintas (aunque en este caso el tráfico lateral no se ha controlado al no crear vlans en la LAN, mejora que se podría plantear para otros escenarios) además de controlar el tráfico en el segundo nivel junto a los perfiles de seguridad, esta forma de implementarlo nos da más seguridad ya que nos protege contra errores en uno de los firewalls ya sea de configuración o de firmas.
Con el análisis de vulnerabilidades realizado hemos podido ver la exposición real de los equipos, que no depende totalmente del número de vulnerabilidades presentes si no de la accesibilidad externa a las mismas, la aplicación de políticas, perfiles IPS y el control de tráfico han reducido la posibilidad de explotación poniendo en evidencia que es necesario implementar controles perimetrales y de segmentación.
Finalmente es importante destacar el trabajo de resolución de incidencias de conectividad documentado, que ha puesto de manifiesto la importancia del troubleshooting de bajo nivel en cualquier despliegue de seguridad y redes real.

8.2 Aprendizajes obtenidos

La realización de este TFG ha permitido con cierta paciencia y tranquilidad poder unir dos mundos que son el laboral y el académico, pudiendo aplicar los aprendizajes desarrollados en el ámbito laboral y otros de los que había necesidad en el montaje de este documento para poder dar forma a un nodo de interconexión sencillo pero que refleje un entorno real, entre ellos:

- Administración de firewalls de nueva generación (NGFW), incluyendo configuración de políticas, NAT, perfiles de seguridad, certificados, inspección de tráfico cifrado y endurecimiento del plano de gestión tanto en Fortinet como en Palo Alto, mejorando y ampliando el conocimiento actual adquirido en el entorno laboral (con la implementación de nuevas configuraciones) y aplicándolo a un documento académico.

- Desarrollo de auditoría realista, diferenciando entre escaneos no autenticados y autenticados, y comprendiendo cómo los sistemas de prevención (IPS, App-ID, filtrado de tráfico) modifican el resultado de las herramientas utilizadas.

- Diseño de arquitecturas de red seguras, entendiendo la importancia de la segmentación, el direccionamiento coherente y la correcta definición de rutas y zonas de seguridad.

- Capacidad de análisis y resolución de problemas de red o de sistemas, identificando fallos derivados de la virtualización, conflictos de direccionamiento, rutas erróneas, etc..

- Comprensión sobre la arquitectura de seguridad y el rol de cada dispositivo, por ejemplo, analizando una herramienta ofensiva como Kali Linux que también debe ser protegida para no convertirse en un vector de ataque adicional dentro de la red.

Poder desarrollar estas facetas muchas de ellas de las que no se había tenido oportunidad anteriormente, ha permitido tener una visión general de prácticamente todo lo que implica un entorno de seguridad actual, además de permitir profundizar en aspectos que no se habían configurado en otros escenarios para poder ilustrar como securizar el conjunto de dispositivos planteado.

8.3 Posibles mejoras futuras

La infraestructura creada presenta una base sólida y documentada para comprender el desarrollo inicial de un entorno de seguridad sencillo, pero a su vez permite evolucionar, debido a su construcción en base a modelos reales corporativos, a esquemas más avanzados con una serie de mejoras que plantean diferentes vías de actualización:

- Evolución de la DMZ con balanceo de carga (A10 Networks):

Una mejora importante (según la utilización del nodo, su inclusión aquí es solo conceptual) sería la integración de un Application Delivery Controller (ADC) A10 Thunder (también es realizable con un F5 siendo este un balanceador de tráfico a su vez) en la DMZ. Este componente permitiría evolucionar el diseño actual hacia un modelo en el que el firewall perimetral Palo Alto tenga un servicio es una IP pública que natee hacia un Virtual Server en el A10, el cual distribuiría el tráfico de forma balanceada entre varios servidores ubicados en la LAN o DMZ, permitiéndonos aplicar más medidas de seguridad y de control de peticiones mediante AFLEX (códigos donde podemos pedirle al ADC que haga diferentes acciones) o de protección de ataques DDOS. Esta implementación mejoraría la alta disponibilidad, el rendimiento y la seguridad de los servicios publicados.

- Implementación de un equipo DNS profesional (EfficientIP) en la DMZ:

La sustitución de la resolución DNS básica (o una implementación Linux) por una solución profesional de DNS, DHCP e IPAM (DDI) como EfficientIP permitiría una gestión centralizada y coherente del direccionamiento, así como una mayor visibilidad de los activos de red. Esto aportaría una mayor seguridad, gestión de los activos del nodo, mayor control de las resoluciones DNS y un acercamiento a un modelo más actualizado y claro de trabajar.

- Creación de usuarios personalizados y en base a una BBDD con la implementación de LDAP:

La incorporación de un servicio de directorio (LDAP o Active Directory) nos permitiría nutrir el nodo de interconexión con servicios de autenticación centralizada evitando los usuarios específicos dentro de cada equipo, permitiendo la aplicación de políticas basadas en la identidad del usuario (con un avance futuro de implementación de un proxy) y un mayor control de la infraestructura.

- Automatización y monitorización:

Para evitar depender al igual que con otras mejoras de los propios equipos y evitar por ejemplo problemas de espacio y de perdida de información, se podría integrar en la DMZ un servicio corporativo como sería un sistema de centralización de logs y monitorización (Elastic, Splunk u otros), lo que nos permitiría acceder a una herramienta donde se encuentra toda la información del tráfico del servicio, ayudando a la trazabilidad y detección de incidentes.

- Mejoras en la segmentación de red:

Como se ha comentado anteriormente, una mejora futura para dotar de mayor seguridad es la segmentación de la LAN en Vlans que permitan diferenciar diferentes utilizades de las maquinas desplegadas y poder analizar el tráfico entre ellas pasando por el Fortigate, además de permitir una mayor estructuración del nodo de interconexión.

9. Bibliografía y Referencias

La creación de este documento se ha fundamentado en una combinación de documentación oficial de fabricantes, herramientas de auditoría y marcos metodológicos de referencia en el campo de la seguridad de redes, utilizados

como guía y soporte en el desarrollo del diseño, la ejecución y la evaluación de la infraestructura creada.

- Documentación oficial de fabricantes

[1] Palo Alto Networks. *PAN-OS® Administrator's Guide*, Version 11.0, 2025.
Disponible en:
https://docs.paloaltonetworks.com/content/dam/techdocs/es_ES/pdf/pan-os/11-0/pan-os-admin-11-0-es-es.pdf
[2] Fortinet Inc. *FortiOS 7.x Administration Guide*, 2025.
Disponible en:
https://docs.fortinet.com/product/fortigate/7.4
[3] Tenable, Inc. *Nessus User Guide*, 2025.
Disponible en:
https://docs.tenable.com/nessus/
[4] VMware, Inc. *VMware Workstation Pro Documentation – Virtual Networking*, 2025.
Disponible en:
https://docs.vmware.com/en/VMware-Workstation-Pro/index.html
[5] A10 Networks, Application Delivery and Load Balancing – Product Documentation, 2025.
Disponible en: https://documentation.a10networks.com/

- Bases de datos de vulnerabilidades

[6] National Institute of Standards and Technology (NIST). *National Vulnerability Database (NVD).*
Disponible en:
https://nvd.nist.gov/
[7] CVE Program. *CVE Program Mission.*
Disponible en:
https://www.cve.org/
[8] Fortinet Inc. FortiGuard Security Services Documentation.
Disponible en:
https://www.fortiguard.com/threatintel-search

- Herramientas y entornos de laboratorio

[9] Kali Linux. *Kali Linux Documentation*, 2025.
Disponible en:
https://www.kali.org/docs/
[10] Rapid7. *Metasploitable 3 – Vulnerable by Design.* GitHub Repository, 2025.
Disponible en:
https://github.com/rapid7/metasploitable3
[11] Lyon, G. (Fyodor). *Nmap Network Scanning: The Official Nmap Project Guide*. Insecure.org, 2009.
Disponible en:
https://nmap.org/book/

- Metodologías, estándares y buenas prácticas

[12] National Institute of Standards and Technology (NIST). *Guide to Network*

Security Testing (SP 800-115), 2008.
Disponible en:
https://csrc.nist.gov/publications/detail/sp/800-115/final

- Seguridad perimetral y marco conceptual
[13] González, P. *The Art of Pentesting*, 2024.
Disponible en:
https://0xword.com/es/libros/236-the-art-of-pentesting.html
[14] The Penetration Testing Execution Standard (PTES). *PTES Technical Guidelines*.
Disponible en:
http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines

10. Anexos

Objetivos de Desarrollo Sostenible

ODS 9 – Industria, Innovación e Infraestructura
Incremento de la seguridad, resiliencia y fiabilidad de entornos digitales corporativos.

ODS 11 – Ciudades y comunidades sostenibles
Protección de servicios digitales críticos utilizados por organizaciones y entornos corporativos.

ODS 16 – Paz, justicia e instituciones sólidas
Refuerzo de buenas prácticas en organizaciones e instituciones de la ciberseguridad y la protección de la información.

Informe de Originalidad de Turnitín

Informe de originalidad (Turnitin) – Se incluye el informe de originalidad generado por la herramienta que corresponde a la versión final de la memoria entregada (Adjuntado a la entrega)

Memoria_TFG_Miguel_Garcia_Montero_t11

Este documento esta firmado por

	**Firmante**	CN=tfgm.fi.upm.es, OU=CCFI, O=ETS Ingenieros Informaticos - UPM, C=ES
	Fecha/Hora	Mon Jan 12 17:41:32 CET 2026
	Emisor del Certificado	EMAILADDRESS=camanager@etsiinf.upm.es, CN=CA ETS Ingenieros Informaticos, O=ETS Ingenieros Informaticos - UPM, C=ES
	Numero de Serie	561
	Metodo	urn:adobe.com:Adobe.PPKLite:adbe.pkcs7.sha1 (Adobe Signature)