UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Escuela Técnica Superior de Ingeniería Informática

Problemática de la gestión del acceso local a redes corporativas y su resolución en base a sistemas NAC.

Trabajo Fin de Grado

Grado en Ingeniería Informática

AUTOR/A: Torregrosa Navarrete, Carlos

Tutor/a: Serrat Olmos, Manuel David

CURSO ACADÉMICO: 2024/2025

Resum

La gestió de l'accés a les xarxes corporatives afronta reptes creixents a causa de la proliferació de dispositius, la mobilitat dels usuaris i l'augment de les amenaces cibernètiques. Aquest treball explora la implementació d'un sistema NAC (Network Access Control), com FortiNAC, per millorar la seguretat i el control d'accés en una xarxa empresarial fictícia. S'analitzen les limitacions de les arquitectures tradicionals, com el filtrat MAC i la segmentació estàtica, i es proposa una solució alineada amb el paradigma Zero Trust, que elimina la confiança implícita i exigeix autenticació contínua.

El projecte es desenvolupa en tres fases: primer, s'implementa un sistema NAC bàsic per gestionar l'accés per cable i VPN, integrant FortiNAC amb un Directori Actiu i el protocol 802.1X; segon, s'amplia el sistema per a suportar dispositius personals (BYOD) mitjançant un portal cautiu; i tercer, es planteja la integració de l'avaluació de la postura de seguretat. Els resultats demostren que els sistemes NAC permeten una segmentació dinàmica de la xarxa, autenticació robusta i visibilitat centralitzada dels dispositius connectats, reforçant la seguretat i l'adaptabilitat de la infraestructura.

Paraules clau: Gestió d'accés local, Xarxes corporatives, Polítiques d'accés, Autenticació de dispositius, Segmentació de xarxa, Control d'accés a la xarxa

Resumen

La gestión del acceso a redes corporativas enfrenta desafíos crecientes debido a la proliferación de dispositivos, la movilidad de los usuarios y el aumento de amenazas cibernéticas. Este trabajo explora la implementación de un sistema NAC (Network Access Control) como FortiNAC para mejorar la seguridad y el control de acceso en una red empresarial ficticia. Se analizan las limitaciones de las arquitecturas tradicionales, como el filtrado MAC y la segmentación estática, y se propone una solución alineada con el paradigma Zero Trust, que elimina la confianza implícita y exige autenticación continua.

El proyecto se desarrolla en tres fases: primero, se implementa un sistema NAC básico para gestionar el acceso por cable y VPN, integrando FortiNAC con un Directorio Activo y el protocolo 802.1X; segundo, se extiende el sistema para soportar dispositivos personales (BYOD) mediante un portal cautivo; y tercero, se plantea la integración de evaluación de postura de seguridad. Los resultados demuestran que los sistemas NAC permiten una segmentación dinámica de la red, autenticación robusta y visibilidad centralizada de los dispositivos conectados, reforzando la seguridad y adaptabilidad de la infraestructura.

Palabras clave: Gestión de acceso local, Redes corporativas, Políticas de acceso, Autenticación de dispositivos, Segmentación de red, Control de accesos a la red

Abstract

The management of access to corporate networks faces growing challenges due to the proliferation of devices, user mobility, and the increasing number of cyber threats. This work explores the implementation of a NAC (Network Access Control) system, such as FortiNAC, to enhance security and access control in a fictional enterprise network. The limitations of traditional architectures, such as MAC filtering and static segmentation, are analyzed, and a solution aligned with the Zero Trust paradigm is proposed, which eliminates implicit trust and requires continuous authentication.

The project is developed in three phases: first, a basic NAC system is implemented to manage wired and VPN access, integrating FortiNAC with an Active Directory and the 802.1X protocol; second, the system is extended to support personal devices (BYOD) through a captive portal; and third, the integration of security posture assessment is proposed. The results demonstrate that NAC systems enable dynamic network segmentation, robust authentication, and centralized visibility of connected devices, thereby strengthening the security and adaptability of the infrastructure.

Key words: Local access management, Corporate networks, Access policies, Device authentication, Network segmentation, Network access control

Índice general

Índice de figuras

Índice de tablas

Agradecimientos

Quiero expresar mi agradecimiento a Manuel David Serrat Olmos, tutor de este TFG, por su guía, sus aportaciones y sus correcciones a lo largo de todo el proceso.

A mis padres, por darme la oportunidad de llegar hasta aquí y por su apoyo constante durante estos años.

A Esther y a Elena, por estar siempre a mi lado y brindarme su respaldo incondicional.

Y a Quino y Christian, gracias por los momentos compartidos y la compañía en el camino de redactar nuestros TFG.

Glosario

802.1X La IEEE 802.1X es una norma del IEEE para el control de acceso a red (NAC) basada en puertos. Permite la autenticación de dispositivos conectados a un puerto LAN, estableciendo una conexión punto a punto o previniendo el acceso por ese puerto si la autenticación falla. Esta autenticación es realizada normalmente por un tercero, tal como un servidor de RADIUS.

perfil NAC Es la agrupación que se asigna a un dispositivo o usuario basándose en características y parámetros específicos que determinan su nivel de confiabilidad y adecuación para acceder a la red. Cada perfil puede tener diferentes niveles de acceso (y confiabilidad) dentro de la red.

RADIUS Es un protocolo de red que proporciona gestión centralizada de autenticación y autorización. Se compone de un servidor y de clientes compatibles que se conectan para autenticarse. Es un protocolo ampliamente utilizado, abierto, e integrado en multitud de soluciones y dispositivos.

sistema NAC Solución preparada para afrontar los principales objetivos del control de acceso a la red. Entre las funciones que puede tener se encuentran: prevenir la falta de antivirus o parches de seguridad en los equipos conectados, controlar y gestionar las políticas de acceso planteadas por los administradores y coordinarlas con el resto de dispositivos de seguridad de la red.

SNMP Es un protocolo de la capa de aplicación que permite intercambiar información entre dispositivos remotamente. Es utilizado por aplicaciones que necesitan obtener información de otros dispositivos, como *routers* o *switches* para comprobar el correcto funcionamiento de la red.

Acrónimos

BYOD *Bring Your Own Device*.

DMZ *Demilitarized Zone*.

EAPOL *EAP Over LAN*.

IoT *Internet of Things*.

NAC *Network Access Control*.

NTP *Network Time Protocol*.

RADIUS *Remote Authentication Dial-In User Service*.

SNMP *Simple Network Management Protocol*.

VPN *Virtual Private Network*.

CAPÍTULO 1
Introducción

1.1 Motivación

Desde su creación, las redes informáticas han revolucionado la forma en la que las organizaciones operan, permitiendo la consulta e intercambio de información de manera rápida y eficiente dentro y fuera de las mismas. Con el tiempo, el panorama de la seguridad corporativa ha evolucionado drásticamente, debido al aumento de dispositivos conectados y de usuarios a los que dar servicio, a la creciente importancia y dependencia de los recursos a los que ambos acceden, y a la expansión de las amenazas cibernéticas.

Dentro del entorno empresarial, es común proteger las redes locales del exterior empleando *firewalls* y otros elementos de seguridad. Sin embargo, en la mayoría de las ocasiones, los controles que se establecen en la red interna no son todo lo severos que deberían, y parten de la premisa de confianza implícita. Es decir, todo lo que ocurre del *firewall* hacia dentro, es seguro, y todo lo que ocurre fuera de este puede no serlo.

¿Realmente se puede confiar en todos los dispositivos conectados a la red interna?

Un principio más seguro que la confianza implícita es el de confianza cero o *Zero Trust*[1], que está ganando popularidad desde hace unos años. En este nuevo enfoque, se parte de la asunción de que un dispositivo conectado a la red local no es automáticamente seguro. En este enfoque, los sistemas de control de accesos a la red (NAC, de *Network Access Control*) han demostrado tener una gran capacidad a la hora de controlar el acceso a la red y sus recursos, obligando a que los dispositivos y/o sus usuarios cumplan ciertos requisitos antes de ser tratados como confiables.

1.2 Objetivos

Este trabajo explorará el uso de los sistemas NAC[2] y su utilidad a la hora de gestionar el acceso de los múltiples dispositivos que pueden conectarse a una red corporativa cada día.

Con el objetivo de ilustrar este problema de manera realista, se establecerá como escenario una empresa española ficticia, de tamaño medio, que busca tener un control más detallado sobre los dispositivos que se conectan a su red.

De esta forma, se presentan los siguientes objetivos, en orden creciente de requisitos funcionales:

- Implementación de un sistema NAC básico para el control de acceso por cable y VPN.

- Extensión del sistema NAC para dar soporte al *Bring your own device* (BYOD), permitiendo a los trabajadores utilizar sus propios dispositivos en la empresa para ciertas tareas.
- Integración de evaluación de postura de seguridad en el sistema NAC, asegurando que los dispositivos corporativos o personales de los trabajadores cumplen ciertos requisitos de seguridad, como tener instalado un antivirus o las últimas actualizaciones de su sistema operativo.

1.3 Estructura

1. Introducción

En este capítulo se presenta el proyecto, aportando contexto sobre el problema que se trata de solucionar y los objetivos que se alcanzarán en este trabajo.

2. Estado del arte

En este apartado se contextualiza el problema a abordar, aportando soluciones propuestas en el pasado y utilizadas en el presente. Además, se profundiza en los productos NAC que se encuentran en el mercado y sus características principales.

3. Diseño de la solución

En este capítulo se detallan los objetivos a alcanzar en el proyecto, presentando la estructura de red, junto a sus dispositivos y otros componentes.

4. Desarrollo de la solución

En este capítulo se documenta detalladamente el desarrollo de los objetivos, describiendo cómo se han llevado a cabo, las tecnologías utilizadas y los desafíos encontrados.

5. Conclusiones

El apartado de conclusiones contendrá una reflexión sobre los resultados obtenidos en el proyecto, evaluando si se han alcanzado los objetivos planteados.

1.4 Convenciones

Para garantizar cierta coherencia en el trabajo y una mejor lectura del mismo, se adoptan las siguientes convenciones:

- Las siglas se presentarán en mayúsculas y su significado completo se podrá comprobar en la lista de acrónimos.
- Los términos propios del campo de estudio que puedan ser necesarios para la comprensión del trabajo se podrán encontrar en el glosario.
- Las palabras extranjeras estarán escritas en *cursiva* para poder identificarlas fácilmente.

CAPÍTULO 2
Estado del arte

2.1 Introducción

La gestión del acceso a las redes locales ha sido un pilar fundamental de la seguridad en prácticamente cualquier entorno, cobrando una importancia creciente conforme las organizaciones han ido integrando más servicios, usuarios, información y dispositivos en sus redes empresariales. Las amenazas a las que están expuestas las redes empresariales han ido evolucionando conjuntamente con la tecnología, y han motivado la aparición y evolución de múltiples soluciones para alcanzar los requisitos de seguridad que se han ido estableciendo.

2.2 Arquitectura tradicional

El filtrado MAC y la segmentación de redes buscan limitar el acceso a la red, bien controlando los dispositivos que pueden acceder a la red, bien los destinos a los que pueden llegar. Por su naturaleza, ambas técnicas se encuentran limitadas a la hora de cumplir sus objetivos por las tecnologías utilizadas o los sistemas de los que dependen.

2.2.1. Filtrado MAC

El filtrado de direcciones MAC fue una de las primeras medidas diseñadas para gestionar el acceso a la red. Este sistema se basa en crear una lista de direcciones MAC permitidas (*whitelist*) o bloqueadas (*blocklist*), restringiendo el acceso a la red de ciertos dispositivos, o que solo los presentes en la lista blanca puedan conectar.

La realidad es más compleja. Aunque las direcciones MAC son únicas a nivel de fabricación (asignadas permanentemente a cada tarjeta de red) no funcionan como método de autenticación fiable. Su principal vulnerabilidad radica en la facilidad con la que pueden suplantarse (mediante la técnica conocida como *MAC spoofing*). Un usuario con conocimientos básicos en la materia no encontraría demasiadas dificultades para modificar su dirección MAC, lo que le permitiría impersonar dispositivos autorizados.

Otro golpe a su efectividad viene de las políticas de privacidad modernas. Sistemas como iOS, Android y Windows generan direcciones MAC aleatorias por defecto al conectarse a redes Wi-Fi, una medida para evitar el rastreo de dispositivos en lugares públicos. Esto no solo dificulta la gestión de listas predefinidas, sino que expone la naturaleza estática de este sistema en un entorno donde la identificación dinámica es clave.

Por tanto, debido a su complicada gestión, baja seguridad y recientes incompatibilidades con los dispositivos más nuevos, es una medida que, al menos hoy en día, en la mayoría de las ocasiones será descartada en favor de otras alternativas más robustas y modernas.

2.2.2. Segmentación de redes

Es una buena práctica en el entorno empresarial no tratar su red local como una única gran red, sino realizar una división en subredes. Esto es conocido como segmentación de redes[3]. Esta subdivisión se puede ejecutar en base a diferentes criterios, aunque una de las más extendidas es hacerlo de acuerdo a los departamentos físicos de la organización. Se puede ser todo lo específico que se requiera, llegando incluso a segmentar la red por tipología de equipos dentro de un mismo departamento.

Se pueden perseguir diferentes objetivos, como reducir el espacio de *broadcast* de la red local, reduciendo el tráfico de la red y mejorando la eficiencia, o el más interesante de cara a la seguridad de la red empresarial, el control de acceso. Gracias a dividir la red empresarial en varias redes locales, ahora se pueden gestionar los accesos entre ellas, permitiendo que los trabajadores de cada segmento de red accedan únicamente a los recursos que necesitan para desempeñar su función. Esto permite que, si es necesario, desde ningún segmento se tenga acceso a la red en su totalidad.

Sin embargo, pese a definir y configurar correctamente los segmentos de red, se siguen estableciendo límites algo laxos en ciertos aspectos. Por ejemplo, es posible que no todos los trabajadores de un segmento de red necesiten acceder a los mismos recursos y, aunque técnicamente se podría llegar a gestionar políticas de filtrado, el manejo de estas restricciones se hace prácticamente imposible conforme las excepciones aumentan en número. Además, se sigue asumiendo que todo dispositivo conectado a la red está autorizado a acceder a los recursos que establezcan las políticas. A día de hoy, estas medidas son insuficientes en la mayoría de ocasiones y las implementaciones modernas suelen acercarse todo lo posible al principio *ZeroTrust*.

2.3 Arquitectura Zero Trust

El paradigma *Zero Trust* se presenta como una solución robusta y adaptativa. Este nuevo enfoque mitiga el riesgo asociado a la confianza excesiva en los dispositivos y usuarios internos, una vulnerabilidad comúnmente explotada por las amenazas contemporáneas.

Sería extraño que algún dispositivo del departamento de administración de una empresa realizase un escaneo de puertos, o intentase acceder a recursos internos que no forman parte de su operativa habitual. Sin embargo, en una arquitectura tradicional, este tipo de comportamientos anómalos pueden pasar desapercibidos, permitiendo que amenazas internas o dispositivos comprometidos se muevan lateralmente sin demasiadas restricciones.

Este tipo de amenazas pueden provenir de actores malintencionados internos, de dispositivos comprometidos por *malware*, o incluso por dispositivos específicamente colocados para vulnerar la red. En un entorno tradicional, donde la confianza se otorga implícitamente a los dispositivos dentro del perímetro de la red, un atacante que logre infiltrarse en un punto de entrada tiene vía libre para explorar y comprometer otros sistemas sin demasiados obstáculos.

El paradigma *Zero Trust* busca mitigar estos riesgos eliminando la confianza implícita y adoptando un enfoque basado en la verificación continua y el acceso mínimo necesario. Cada solicitud de acceso se evalúa en función de múltiples factores, como la identidad, la ubicación, el estado del dispositivo y el contexto de la operación. De esta manera, incluso si un dispositivo de administración fuera comprometido, sus acciones dentro de la red estarían limitadas a los recursos estrictamente necesarios, reduciendo drásticamente las posibilidades de movimiento horizontal.

Dado el creciente interés en la arquitectura *Zero Trust*, multitud de empresas ofertan productos para tratar de cumplir con los objetivos de este paradigma. Estas soluciones suelen conocerse, de forma genérica, como soluciones NAC, siglas en inglés de ***N**etwork **A**ccess **C**ontrol*.

2.4 Soluciones NAC

La arquitectura *Zero Trust* establece principios de seguridad muy estrictos, pero aplicarlos puede representar ciertamente un desafío. Para desarrollar esta función, encontramos los anteriormente mencionados sistemas NAC.

2.4.1. Características

Estas soluciones basan su funcionamiento en tres pilares fundamentales:

Visibilidad

Para poder imponer las restricciones a los dispositivos, gestionar los accesos a los recursos y realizar otras tareas, es un requisito tener conocimiento de los clientes conectados a la red, y toda la información posible de estos: tipo de dispositivo, ubicación, función que desempeña, sistema operativo, etc. Además, será necesaria una vigilancia constante para asegurar que sus intenciones no varían en el tiempo.[4]

Esta visibilidad también es útil para los administradores, quienes pueden ver, etiquetar y administrar todos los dispositivos conectados a la red. Aunque es factible obtener funcionalidades parecidas con otras opciones, es interesante disponer de esa información de forma tan integrada y completa. En algunas soluciones específicas, y con el *hardware* adecuado, se puede llegar a saber en qué puerto de cada *switch* está conectado cierto dispositivo con solo mirar la interfaz de la solución NAC.

Segmentación

De forma análoga a la segmentación de redes en la arquitectura tradicional (sección 2.2.2), la idea es dividir la red según sea conveniente en base a criterios de seguridad y rendimiento, generalmente agrupando a los usuarios y dispositivos según los recursos a los que accedan o por departamentos. Habitualmente, esto se lleva a cabo utilizando las separaciones departamentales de la oficina (política basada en la ubicación física). Las tomas de red de cierta zona tienen acceso a ciertos recursos, mientras que las de otra ubicación permiten el acceso a otros distintos.

Este método es poco seguro, puesto que basa la seguridad de la red en las ubicaciones, no en identidades. Además, también es poco flexible, puesto que no permite la movilidad de los trabajadores por la oficina de forma sencilla. Si los empleados de cierto

departamento necesitan acceder a un recurso privado en una ubicación distinta a la suya habitual, no podrán hacerlo.

Las soluciones NAC permiten realizar una segmentación dinámica, que en lugar de estar basada en ubicaciones físicas, se trate de una política basada en identidades.[4] Esto supone que una misma persona, independientemente de su ubicación, siempre podrá acceder a los mismos recursos. No solo es más seguro, sino que además es mucho más conveniente, puesto que ahora los trabajadores pueden moverse libremente por la oficina y seguirán bajo el mismo control de acceso que en su mesa.

Respuesta

De la misma forma que se permite limitar el acceso a los empleados, también se puede limitar el acceso, o incluso aislar a los dispositivos malintencionados. Estas respuestas pueden darse gracias a la conexión con otro *hardware* específico, como *switches* o *firewalls* en respuesta a los eventos producidos por la monitorización de NAC.

Todo esto es posible gracias a la monitorización mencionada en el apartado de visibilidad, que comprueba cuándo un usuario o dispositivo está realizando accesos indebidos. En ciertas soluciones, pueden aplicarse restricciones según la postura de seguridad del equipo o, incluso, cuando se detecten infecciones de *malware* en los equipos de los empleados, para evitar la expansión de éstas.

2.4.2. Identificación

Los sistemas NAC suelen aprovechar el estándar IEEE 802.1X para controlar el acceso a la red. El protocolo EAPOL (***EAP Over LAN*** en inglés) implementa el estándar 802.1X y puede ser utilizado tanto en redes cableadas como inalámbricas. Generalmente, el flujo de autenticación de un usuario en un dispositivo sigue el patrón de la figura 2.1.

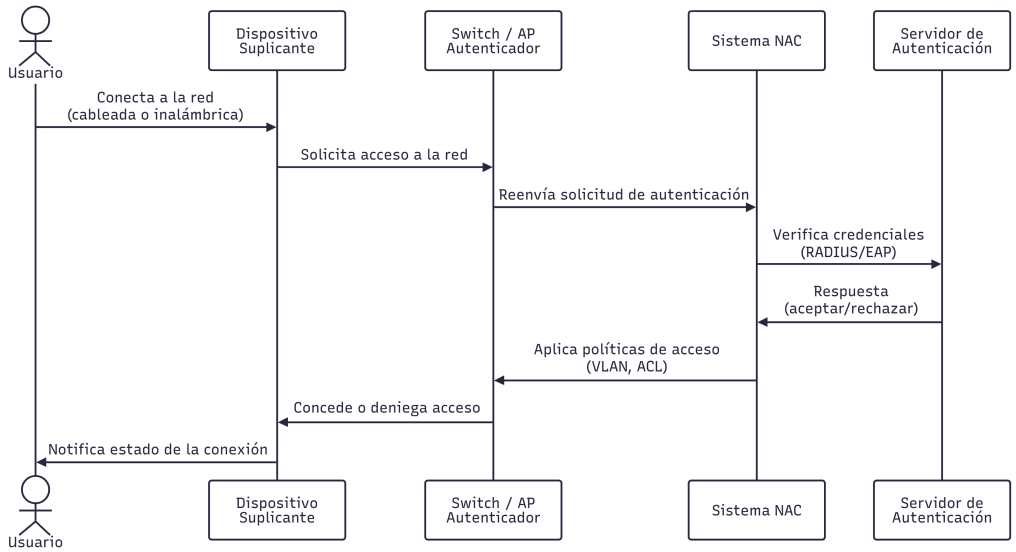


Figura 2.1: Proceso de identificación de un usuario por un sistema NAC.

El usuario (**suplicante**) conecta a la red su dispositivo. A través del intercambio de tramas EAPOL, el **autenticador** (switch o punto de acceso) pide al dispositivo que se autentique mediante usuario y contraseña o certificados (como haya sido configurado por los administradores). Existen diversos métodos EAP (como EAP-TLS, PEAP, EAP-MSCHAPv2) que definen el formato de este intercambio de credenciales. Esta petición

con los datos necesarios es transmitida hasta el NAC, el cual, gracias al **servidor de autenticación** (generalmente un RADIUS), verifica las credenciales. En caso de autenticación exitosa, el servidor RADIUS envía una respuesta de aceptación al NAC. En caso contrario, envía una respuesta de rechazo.

En caso de que se acepte la conexión, atendiendo a las políticas configuradas en la solución NAC, el switch colocará al usuario en la VLAN que corresponda de forma dinámica, y el puerto del switch pasará a un estado de .ªutorización", permitiendo el tráfico de datos del usuario. En caso de fallo en la autenticación, el acceso a la red puede ser bloqueado o el usuario podría ser redirigido a una VLAN de cuarentena para una posterior remediación.

2.4.3. Características a valorar en un sistema NAC

Al implantar una solución NAC en una organización, hay multitud de variables que deben tenerse en cuenta a la hora de escoger un producto que se adapte a las necesidades de la misma. Por ello, antes de evaluar y comparar algunas de las diferentes soluciones comerciales existentes, se va a realizar una pequeña descripción de las características que se han considerado más destacables.

- **Tipo de despliegue.** Los sistemas NAC generalmente pueden instalarse en la propia empresa o alojarse en la nube. La nube suele requerir un mantenimiento menor, pero también suele llevar consigo un aumento significativo de los costes y de la dependencia de servicios externos, lo que puede suponer un problema de disponibilidad de la solución en caso de caída de las comunicaciones.

- **Escalabilidad.** Generalmente, las limitaciones no suelen encontrarse tanto en la potencia del sistema, sino en las licencias de estos sistemas. Algunos modelos o suscripciones pueden no escalar bien con las necesidades de la organización, o no hacerlo a un coste razonable.

- **Usabilidad.** Como en todos los sistemas, se intentará buscar que el producto sea fácil de usar, tanto para los administradores (con un panel de administración fácil de usar y aprender) como para los trabajadores, quienes no estarán familiarizados con el uso de estos sistemas.

- **Integración.** Los productos NAC suelen poder conectarse con multitud de sistemas tanto *software* como *hardware* para completar su funcionalidad, aportarle visibilidad y permitirle reaccionar ante los eventos. Se pueden encontrar distintos niveles de integración, siendo los más extraños los productos que únicamente permiten la conexión con dispositivos de la misma marca y los más comunes aquellos que permiten ser integrados con multitud de dispositivos gracias al uso de protocolos genéricos (generalmente disfrutando de funciones especiales y una conexión más sencilla al utilizar dispositivos de la misma marca). En algunos casos, la integración de algunos protocolos o dispositivos puede estar detrás de licenciamiento.

- **Aplicación de políticas.** Poder definir directivas en muchas ocasiones es una de las características más buscadas de las soluciones NAC. Estas políticas generalmente pueden aplicarse atendiendo a usuarios, a dispositivos, o incluso a otros criterios.

- **Monitorización y respuesta.** Como en los anteriores apartados, se pueden encontrar soluciones y licencias con diversas opciones de cobertura. Algunas opciones únicamente controlarán algunos dispositivos, y otras monitorizarán todos los clientes de la red. También los hay que responden o no de forma automatizada a los

eventos de la red. Debe ajustarse a los requisitos actuales de la empresa, intentando dejar la puerta abierta a futuras necesidades. En el aspecto de la monitorización de las estaciones de trabajo de los empleados se pueden encontrar dos opciones principalmente:

- Con agente. Se instala un programa en los equipos finales para poder extraer más información de los equipos: actualizaciones, infecciones, aplicaciones utilizadas e instaladas, procesos, ...
- Sin agente. Se basan en la información que se puede obtener a través de la red, sin tener que instalar un programa en los equipos.

2.5 Comparativa de las soluciones comerciales

Existen soluciones NAC de diversos fabricantes para cumplir con los puntos anteriores. Se pueden encontrar incluso algunos sistemas de código abierto mantenidos por la propia comunidad. A continuación, se repasarán las principales alternativas disponibles.

2.5.1. FortiNAC[1]

FortiNAC es la solución ofertada por Fortinet[2] dentro de su familia de productos de seguridad. Por ello, tiene una especial conexión con *routers*, *switches*, *firewalls* y otros dispositivos de Fortinet.

Tipo de despliegue

Fortinet permite que FortiNAC se ejecute tanto en dispositivos específicos creados y pensados para ello, como en máquinas virtuales. Estas máquinas virtuales pueden ejecutarse en local o en la nube, en proveedores como AWS o Azure. Ofrece desplegar distintas máquinas para tener alta disponibilidad, con cambio automático al detectar que la principal no está disponible. [5]

Escalabilidad

Las licencias de FortiNAC son sencillas y pueden ser de por vida o en formato suscripción. Existen dos niveles de licencias, con el primer nivel para empresas que no necesiten la reacción automática a eventos, y el segundo para las organizaciones que sí la necesiten. El resto de características están incluidas en ambas, como se puede observar en la figura 2.2. Como suele ser común en estos productos, es necesario adquirir un número de licencias igual o superior al número de dispositivos que van a estar conectados simultáneamente.

Usabilidad

FortiNAC presenta una interfaz bien estructurada y ordenada, aunque llena de opciones por todos los menús. Puede ser algo complicado encontrar algunas opciones, aunque tiene un buscador en la parte superior de la pantalla.

[1] https://www.fortinet.com/lat/products/network-access-control/
[2] https://www.fortinet.com/products/network-access-control

		FORTINAC LICENSE TYPES	PLUS	PRO
Visibility	Network	Network Discovery	✓	✓
		Rogue Identification	✓	✓
		Device Profiling and Classification	✓	✓
	Endpoint	Enhanced Visibility	✓	✓
		Anomaly Detection	✓	✓
		MDM Integration	✓	✓
		Persistent Agent	✓	✓
	User	Authentication	✓	✓
		Captive Portal	✓	✓
Automation / Control		Network Access Policies	✓	✓
		IoT Onboarding with Sponsor	✓	✓
		Rogue Device Detection and Restriction	✓	✓
		Firewall Segmentation	✓	✓
		MAC Address Bypass (MAB)	✓	✓
		Full RADIUS (EAP)	✓	✓
		BYOD / Onboarding	✓	✓
		Guest Management	✓	✓
		Endpoint Compliance	✓	✓
		Web and Firewall Single Sign-on	✓	✓
Incident Response		Event Correlation		✓
		Extensible Actions and Audit Trail		✓
		Alert Criticality and Routing		✓
		Guided Triage Workflows		✓
Integrations		Inbound Security Events		✓
		Outbound Security Events	✓	✓
		REST API	✓	✓
Reporting		Customizable Reports	✓	✓

Figura 2.2: Tabla de características y licencias de FortiNAC.

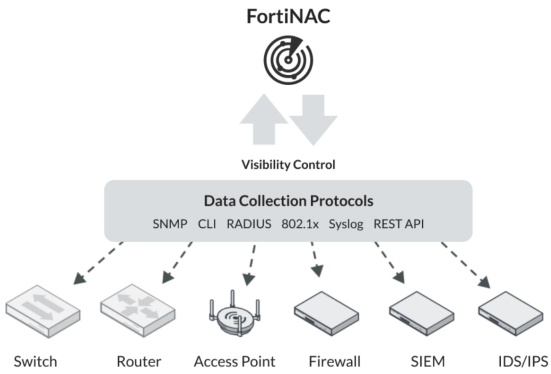


Figura 2.3: Conexión de dispositivos de red con FortiNAC.

Integración

El producto permite la conexión con multitud de marcas y soluciones *software* y *hardware* que probablemente ya se estén utilizando en la organización, como IDS, *firewalls*, *switches*, *routers*, etc. Además, no es necesario que sean de marca Fortinet, puesto que FortiNAC soporta protocolos estándar como SNMP, RADIUS o su propia API REST para integrarse con otros dispositivos (como se puede ver en la figura 2.3).

Aplicación de políticas

En el panel de administración se pueden crear perfiles en base a multitud de métodos (tabla 2.1), permitiendo la detección de usuarios en equipos de trabajo (gracias a RADIUS o *Windows Profile*) o la inclusión de dispositivos IoT que no tienen prácticamente posibilidad de configuración (analizando su tráfico, probando el acceso mediante SSH, o comprobando el estado de ciertos puertos). A cada uno de estos perfiles se les puede asociar una VLAN diferente, permitiendo una integración cómoda y sencilla con la red

Active	DHCP	FortiGate	FortiGuard
HTTP	IP Range	Location	Network Traffic
ONVIF	Passive	Persistent Agent	RADIUS
Script	SNMP	SSH	TCP
Telnet	UDP	Vendor OUI	WinRM
Windows Profile			

Tabla 2.1: Métodos de perfilado de FortiNAC.

de la oficina y dando acceso únicamente a los recursos a los que la propia VLAN tenga acceso.

Monitorización y respuesta

FortiNAC tiene soporte de monitorización con y sin agente. Cuando se escoja la instalación del agente, permitirá conectarse con antivirus (Norton, Panda, Avast, ...) para monitorizar el estado del dispositivo, o con los propios sistemas operativos, como Windows, para conocer el estado de las actualizaciones del equipo. En caso de no conectarse, la información que se obtendrá del dispositivo será menor. FortiNAC únicamente reaccionará automáticamente a los eventos ocurridos en la red con la licencia correspondiente.

2.5.2. Cisco Identity Services Engine[3]

Este producto se conoce también como Cisco ISE, y es la apuesta de Cisco por el *Zero Trust*. Tiene muchas similitudes con el entorno de Fortinet, aunque en este caso tiene especial conexión con productos que soporten su protocolo. [6]

Tipo de despliegue

Cisco ISE está disponible como dispositivo físico y máquina virtual. En ambos casos se puede crear un *cluster* que permita crear un entorno de alta disponibilidad o dotar de mayor escalabilidad al despliegue. Se puede desplegar en los principales hipervisores y proveedores de nube en línea, como AWS o Azure.

Escalabilidad

Por un lado, como se ha comentado en el apartado anterior, se puede formar un *cluster* de varias máquinas. Se necesita comprar un número de licencias igual o superior al número de dispositivos que van a estar conectados simultáneamente. Se trata de licencias algo limitadas en características en los primeros niveles (como se puede observar en la figura 2.4). Las licencias de Cisco ISE pueden ser de por vida y en formato suscripción, aunque algunos de sus niveles solo están disponibles en formato suscripción.

- ***Essentials***. Proporciona funcionalidades básicas como autenticación 802.1X, servicios para invitados y visibilidad de dispositivos en el panel de control del producto.
- ***Advantage***. Incluye todas las funcionalidades del nivel anterior y añade capacidades como control de acceso basado en políticas, perfilado, funcionalidad BYOD y la capacidad de integrar el dispositivo con otro *hardware* y *software*.

[3]https://www.cisco.com/site/us/en/products/security/identity-services-engine/index.html
[3]https://www.cisco.com/c/es_es/index.html

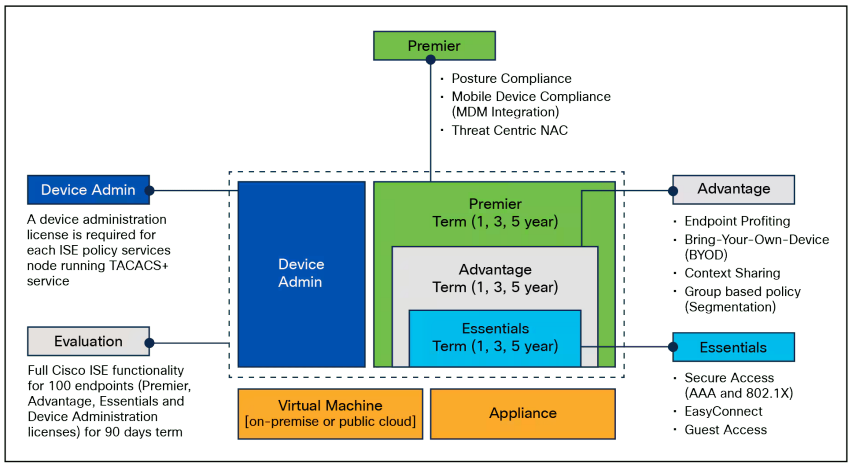


Figura 2.4: Gráfico de licencias de Cisco ISE.

RADIUS	SNMP	DHCP	DNS
HTTP	NetFlow	Ports	Active Directory
pxGrid			

Tabla 2.2: Métodos de perfilado de Cisco ISE.

- ***Premier***. Incluye las funcionalidades de los niveles anteriores y añade características avanzadas como la funcionalidad MDM o el aislamiento automático de los dispositivos que son detectados como amenazas.

Usabilidad

Como ocurre frecuentemente en este tipo de soluciones, el panel de administración de Cisco ISE concentra una gran cantidad de opciones y funcionalidades, lo que puede dificultar la navegación. Para paliar este inconveniente, cuenta con un buscador que facilita el acceso directo a las secciones deseadas. Además, la interfaz ha sido rediseñada recientemente, ya que presentaba un aspecto anticuado en comparación con otras alternativas del mercado.

Integración

Cisco ISE tiene un abanico similar a otras alternativas, contando con soporte para tecnologías como RADIUS, syslog o API REST, aunque tiene su foco en pxGrid, un protocolo propietario de comunicación entre dispositivos de red cuya adopción está siendo tímida pero continuada en los últimos años. Por tanto, la conexión con este protocolo es especialmente sencilla, aunque su mayor desventaja es que no está presente en todos los dispositivos de otros fabricantes.

Aplicación de políticas

Cisco ISE permite crear perfiles con multitud de métodos de perfilado, aunque siendo igualmente algo más limitada que otras alternativas, como se puede ver en la tabla 2.2. Una vez creados los perfiles, se pueden asignar políticas o VLANs a los mismos de forma dinámica.

Monitorización y respuesta

Cisco ISE permite el uso de su agente (conocido como Anyconnect Agent) para obtener más información acerca de los dispositivos y así poder establecer restricciones en base a su estado. En caso de no disponer del agente instalado, la información con la que contará Cisco ISE será menor.

2.5.3. Aruba ClearPass[4]

HPE Aruba ClearPass es la solución propuesta por Hewlett Packard Enterprise, una división de HP especializada en ofrecer soluciones para el entorno empresarial. Dentro de su catálogo, que incluye servidores, sistemas de almacenamiento y diversos dispositivos de red, destaca ClearPass, la plataforma que se analizará en este trabajo por su enfoque en el control de acceso a la red. [7]

Tipo de despliegue

Aruba ClearPass está disponible como un dispositivo físico o como un sistema virtual. Este último puede desplegarse tanto en local como en la nube, dando soporte a servicios como Azure o AWS, y a conocidos hipervisores como VMware ESXi o Hyper-V.

Escalabilidad

Es posible crear un clúster combinando máquinas virtuales y dispositivos físicos para conseguir alta disponibilidad en el servicio. Por otro lado, el sistema de licencias , además de limitar mucho las características en sus primeros niveles, puede resultar algo complicado de entender.

- ***Platform License***. Licencia ligada al producto. Viene incluida en caso de utilizar el dispositivo físico, y se debe comprar para utilizar Aruba ClearPass virtualizado.
- ***Base Application License***. Incluye las funcionalidades básicas del sistema NAC. Se debe contar con una licencia por cada dispositivo que vaya a conectarse a la red, pudiendo comprarse estas licencias en diferentes paquetes.
  - ***Entry License***. Esta licencia incluye las características más básicas de los sistemas NAC, no permitiendo, por ejemplo, que ClearPass se comunique con dispositivos externos (como *firewalls*, *routers*, IDS, ...). Tampoco estarían incluidas todas las opciones de perfilado de red, no obteniendo información de las tramas DHCP y otros protocolos.
  - ***Access License***. Este nivel sí que incluye todas las características base de la mayoría de los sistemas NAC, incluyendo las ausentes en el nivel anterior.
- ***Add-on Application Licenses***. Licencias que expanden la funcionalidad de Aruba ClearPass. Ahora mismo existen dos:
  - ***Onboard***. Una solución pensada para ocasiones en las que se requiere el uso de certificados. En ese caso, Aruba ClearPass actuará como unidad certificadora y mediante un portal cautivo, facilitará la instalación del mismo en los dispositivos. De nuevo, la licencia se realiza en función de los dispositivos necesarios.

[4] https://www.hpe.com/es/es/aruba-clearpass-policy-manager.html

MAC	DHCP	TCP	NetFlow
IPFIX	sFlow	Active Directory	HTTP User-Agent
IF-MAP	SNP	Ports (nmap)	SSH

Tabla 2.3: Métodos de perfilado de Aruba ClearPass.

- ***OnGuard.*** Permite añadir la funcionalidad de requerir la instalación de un agente en los dispositivos para obtener información que no se puede obtener de otra forma.

Usabilidad

El panel de administración de Aruba ClearPass está estructurado en categorías, intentando organizar las opciones para facilitar su navegación. En el caso de esta herramienta, su interfaz web se siente especialmente desactualizada. Como ocurre en otras soluciones, esta herramienta es transparente para los trabajadores. Además, tras una licencia adicional, ofrece soluciones para que los propios usuarios puedan configurar la conexión en sus dispositivos teniendo unas credenciales de acceso.

Integración

Teniendo la licencia requerida, se pueden conectar a Aruba ClearPass multitud de dispositivos mediante protocolos estándar, como TACACS+, RADIUS CoA, APIs o syslog.

Aplicación de políticas

Atendiendo a los perfilados, se pueden establecer las políticas necesarias para cada perfil, como la VLAN en la que se encontrará, o los recursos a los que tendrá acceso. Se puede utilizar información del tráfico de red, DHCP, *Active Directory* o *hardware* de red, entre otros. En la herramienta de perfilado se encuentran disponibles las herramientas mencionadas en la tabla 2.3.

Monitorización y respuesta

Con la licencia *OnGuard*, Aruba ClearPass permite utilizar un agente en los dispositivos para obtener más información acerca de ellos e imponer otras restricciones más específicas, como la necesidad de mantener actualizado el equipo. Además, Aruba ClearPass puede reaccionar a eventos de red y modificar el estado de autorización de un dispositivo en tiempo real y sin necesidad de intervención, por ejemplo, moviendo el dispositivo a una red de cuarentena.

2.5.4. OpenNAC[5]

OpenNAC es una solución con origen en 2012 en una empresa española de Barakaldo (Vizcaya), conocida como *Open Cloud Factory*. A finales de 2024 fue adquirida por el grupo Oesía, quien integró al equipo de 30 trabajadores de *Open Cloud Factory* dentro de la marca Cipherbit-Grupo Oesía para añadir este producto a su oferta de herramientas de ciberseguridad.[8]

[5]https://www.opencloudfactory.com/opennac/

La solución destaca por su modularidad e integración con multitud de dispositivos de diversas marcas. Además, OpenNAC cuenta con el apoyo del Centro Criptológico Nacional[6], incluyéndolo en su catálogo de productos supervisados en 2018[7] y garantizando así que el software cumple los estándares necesarios para ser utilizado en las empresas del sector público afectadas por el ENS. Un año más tarde, fue certificado[8] de nuevo por el CCN.

Tipo de solución

OpenNAC no está disponible como dispositivo físico, sino que puede desplegarse en máquinas virtuales tanto dentro como fuera de la empresa (nube).

La arquitectura de OpenNAC es diferente a las propuestas por el resto de soluciones, puesto que en lugar de tratarse de una instalación "monolítica", el *core* se instala en una máquina virtual y, a partir de ahí, cada módulo que se añada irá en su propia máquina virtual separada de la aplicación principal. .

Tanto la aplicación principal como los módulos se encuentran disponibles en dos formatos:

- **Archivo OVA.** Una imagen lista para importarse en la mayoría de hipervisores.
- **Playbooks de Ansible.** Permiten desplegar de forma sencilla los componentes necesarios de OpenNAC en una máquina Linux.

Escalabilidad

Se pueden crear clústers activo-activo y activo-pasivo sincronizando estados entre instancias y habilitando el cambio automático entre ellas, así como balanceo de carga de peticiones RADIUS y servicios web.

En cuanto a las licencias, OpenNAC permite pagar únicamente por los módulos que se van a utilizar, medido en número de dispositivos o usuarios autenticados. En el caso de los clúster, no es necesario que todos los nodos cuenten con las licencias, sino que las heredan del principal. Las licencias se pagan anualmente.

Los módulos que se encuentran disponibles actualmente son los siguientes:

- ***ON Core.*** Es el núcleo de la solución: aloja el motor de políticas, el motor de cumplimiento, plugins de perfilado, la consola de administración web, los repositorios de paquetes y actualizaciones, la gestión de logs, y almacena los parámetros de redes, *hosts* y autenticación.
- ***ON Analytics.*** Recibe logs y metadatos de todos los componentes de OpenNAC para almacenarlos y permitir su consulta de forma inmediata.
- ***ON Sensor.*** Actúa como un IDS: captura tráfico y decodifica protocolos de capa 2 a 7. Proporciona información sobre el comportamiento de red, habilitando visibilidad avanzada y detección de anomalías.

[6]https://www.ccn-cert.cni.es/es/

[7]https://oc.ccn.cni.es/component/djcatalog2/item?id=400:opennac-enterprise-v1-2&cid=56:control-de-acceso

[8]https://oc.ccn.cni.es/productos-certificados/productos-certificados/categoria-de-producto/10-dispositivos-de-control-de-acceso-a-red/445-opennac-enterprise-v1-2

Banner	DHCP Fingerprint	HTTP	MAC Vendor
Ports	Service Information	SNMP	OS
Network Protocol	DNS	Agent	

Tabla 2.4: Métodos de perfilado de OpenNAC.

- ***ON Agent.*** Es un cliente ligero que se instala en endpoints y servidores. Recopila información del sistema, estado de los parches, aplicaciones, salud del sistema, y otras opciones.

- ***VPN Gateway.*** Proporciona acceso remoto seguro a los usuarios: gestiona túneles VPN, aplica políticas de segmentación en función del perfil de usuario y registra logs de tráfico. Se recomienda desplegarlo en alta disponibilidad si se requiere continuidad de servicio.

Usabilidad

La gestión de OpenNAC se realiza mediante su completo panel web. Actualmente, esta interfaz web cuenta con dos versiones: un panel clásico y otro con un diseño y funcionalidad actualizados que va obteniendo nuevas funcionalidades progresivamente para equipararse al panel clásico. Esta interfaz de administración se despliega sobre el nodo **ON Core**.

Integración

OpenNAC ofrece integración con multitud de *hardware* y *software* de seguridad e infraestructura empresarial.

En cuanto a autenticación, soporta 802.1X, *Active Directory*, RADIUS, RADIUS-Proxy, certificados y doble factor de autenticación. Además, es agnóstico de fabricante, por lo que puede conectarse a multitud de dispositivos de Cisco, Juniper, Aruba, HP, Fortinet, etc. Se puede integrar a *firewalls* de multitud de fabricantes gracias al uso de protocolos estándar.

Aplicación de políticas

El motor de políticas de OpenNAC es muy flexible y detallado. Las políticas definen condiciones (atributos del usuario, del dispositivo, horario, etc.) y acciones en la red.

Las políticas se agrupan en *Business Profiles* (perfiles de negocio) configurables por el administrador. Se pueden filtrar por usuario, grupos AD, tipo de dispositivo, etiquetas, MAC, ubicación, hora del día, e incluso atributos de autenticación (802.1X, MAB, portal web). Cuando se cumple una política, puede realizarse multitud de acciones: asignar dinámicamente una VLAN o ACL en el *switch*, aplicar reenvío a VLAN de cuarentena, etiquetar el dispositivo con estados personalizados, o pasar parámetros adicionales al autenticador.

En los casos donde la autenticación no es posible, se pueden utilizar los métodos de perfilado disponibles en la solución (figura 2.4) para asignar los dispositivos al perfil adecuado.

Monitorización y respuesta

OpenNAC cuenta con dos tipos de agente disponibles en la mayoría de sistemas operativos que le permiten obtener información adicional para utilizar a la hora de aplicar políticas de acceso. Entre la información que se reporta al servidor OpenNAC, destaca: estado del dispositivo (antivirus, actualizaciones, rendimiento, ...), usuario conectado o telemetría.

- ***Multiplatform Agent***. La versión principal del agente, instalable en el dispositivo y que se ejecuta constantemente reportando información a OpenNAC.
- ***Soluble Agent***. Un agente más liviano que no reporta información de forma constante, sino que se ejecuta mediante línea de comandos cuando se requiere.

2.5.5. PacketFence[9]

PacketFence es un sistema NAC diferente, puesto que está soportado por Inverse, una empresa canadiense especializada en soluciones para controlar el acceso a la red y recursos. Es un proyecto de código abierto bajo la licencia *GNU General Public License v2* (GPL-2.0)[10], y aunque es principalmente desarrollado y guiado por Inverse, recibe un gran apoyo de su comunidad, encontrando errores o contribuyendo a su desarrollo.[9]

Debido a su naturaleza radicalmente distinta, se apoya en el uso de tecnologías ya existentes y ampliamente utilizadas como base para su funcionamiento, como se puede observar en la figura 2.5 y se detalla en los siguientes puntos.

- **FreeRADIUS.** Como método de autenticación para todas sus opciones.
- **Apache.** Como servidor web para el panel web y otras utilidades.
- **netdata.** Para monitorización en tiempo real de métricas del sistema (CPU, RAM, disco, red…).
- **MariaDB.** Como base de datos para almacenar toda la información que se necesita conservar (redes, políticas, ...).
- **Redis.** Para almacenar información en memoria principal, y como sistema gestión de trabajos asíncronos.

Tipo de solución

PacketFence no está disponible como un dispositivo físico, sino que debe ser instalado en nuestro propio *hardware* o en la nube. PacketFence puede encontrarse en varios formatos:

- **PacketFence Estándar.** Instalación pensada para entornos de producción y escenarios en los que se prefiere realizar una configuración manual muy granular. Se puede descargar en dos formatos:
  - Paquetes Debian / RedHat.
  - Imagen ISO.

[9] https://www.packetfence.org/
[10] https://www.gnu.org/licenses/old-licenses/gpl-2.0.html#SEC1

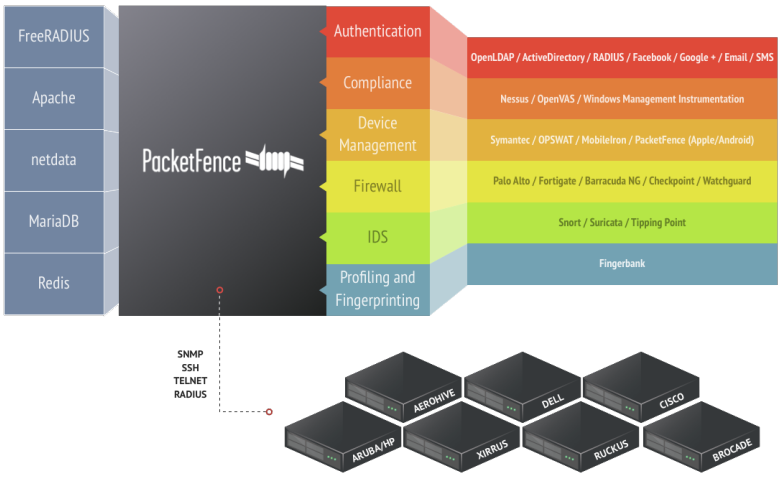


Figura 2.5: Arquitectura de PacketFence.

- **PacketFence ZEN.** La edición ZEN (*Zero Effort NAC* en inglés) permite desplegar de forma muy sencilla un NAC funcional, con gran parte de sus componentes preconfigurados. Al iniciar, se guiará al usuario por la configuración inicial. Esta edición solo puede obtenerse en formato ISO, y está pensada para entornos de prueba o escenarios en los que no se necesita realizar una configuración especial.

Escalabilidad

PacketFence soporta el *clustering* activo-activo, con múltiples nodos coordinados entre sí gracias a MariaDB Galera. Además, es software completamente libre (GPL-2.0), así que no requiere de ningún tipo de licencia para su uso. Sin embargo, no se recibirá soporte más allá del prestado por la comunidad. Si se requiere, se puede adquirir una licencia de soporte (5000$ por año y por instalación) para recibir soporte oficial con los problemas que puedan encontrarse durante su uso y configuración.

Usabilidad

Aunque PacketFence cuenta con una buena interfaz web desde la cual es posible realizar la mayor parte de la gestión del sistema, puede que algunas funciones más avanzadas, como la definición de *clusters*, requieran configuración mediante terminal.

Integración

Puesto que está basado en protocolos abiertos y estándar, no es difícil integrar PacketFence siempre que contemos con dispositivos y *sofware* que soporten estos protocolos. Algunos de los protocolos utilizados son TACACS+, syslog, SNMP, RADIUS o 802.1X. En su página web[11] puede consultarse una tabla de compatibilidad con los dispositivos.

[11] https://www.packetfence.org/about.html#/material

HTTP	DHCP	Ports (nmap)	User-Agent
DNS	ARP	TCP	RADIUS

Tabla 2.5: Métodos de perfilado de PacketFence.

Aplicación de políticas

PacketFence ofrece un control de acceso basado en roles, permitiendo definir políticas por grupos de usuarios, tipos de *endpoint*, y otros valores. Como suele ser común en estas soluciones, incluye además un portal cautivo como método de autenticación.

Para aquellos dispositivos que no puedan autenticarse de forma automática, ofrece herramientas de perfilado (figura 2.5) para poder seguir identificando estos dispositivos y asignarles las políticas correspondientes. Para mejorar su perfilado, PacketFence puede utilizar Fingerbank[12], una herramienta de la misma empresa detrás de este proyecto, Inverse. Esta herramienta tiene una capa gratuita y puede tener un coste en caso de necesitar superarla.

Monitorización y respuesta

PacketFence realiza una monitorización continua de la red, en busca de cambios de estado, y respondiendo de forma automatizada si se requiere.

Aunque PacketFence tiene agentes para algunos sistemas operativos, no son tan sencillos de configurar como los de otras alternativas. Estos agentes permiten obtener información adicional de los dispositivos y conectarlos a las redes de la organización.

[12]https://www.fingerbank.org/

CAPÍTULO 3
Diseño de la solución

3.1 Arquitectura original

Como se detallaba en la introducción (apartado 1.2), este trabajo supone una estructura ya existente de una mediana empresa española que busca mejorar la seguridad de la red y tener un mayor control sobre los accesos a los recursos internos.

El esquema de red e infraestructura con el que cuenta dicha organización se puede observar en la figura 3.1. En los objetivos se utilizará como base desde la que partir.

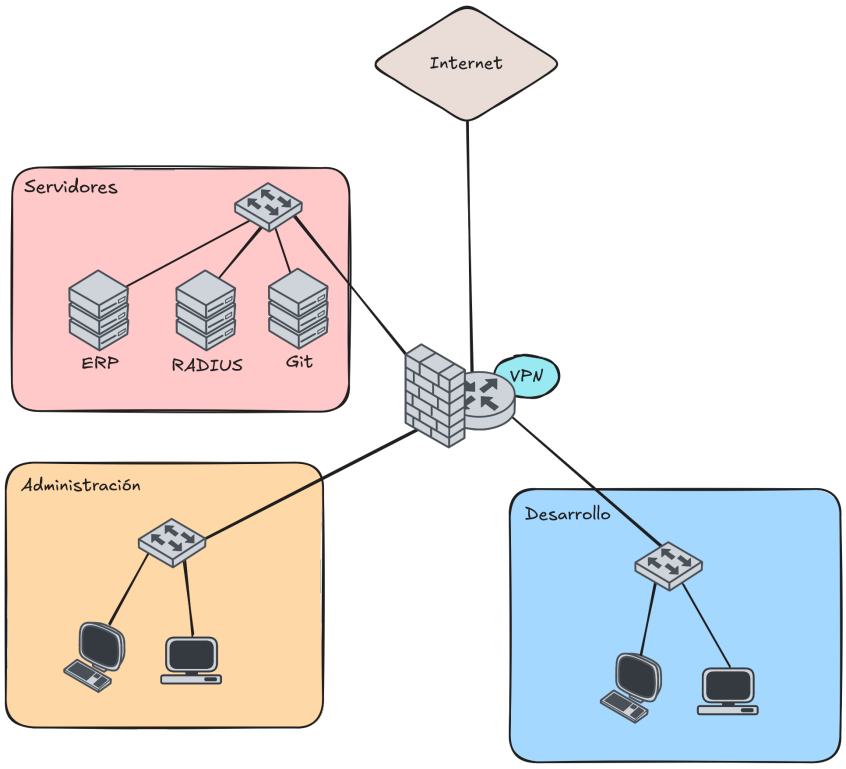


Figura 3.1: Esquema original de la infraestructura de la organización.

En el esquema de la organización (figura 3.1) se pueden distinguir dos departamentos (administración y desarrollo) junto a una red de servidores para albergar los recursos a los que accederán los trabajadores.

Los segmentos de red empleados se detallan en la tabla 3.1. Además de los segmentos para los departamentos y servidores, se han incorporado dos segmentos de VPN destina-

dos a la conexión remota de los empleados (tanto de administración como de desarrollo), así como un segmento adicional, la VLAN 30, que permite gestionar la red de manera segura desde el exterior.

VLAN	Información	Direccionamiento	Gateway
1	Red de Gestión	192.168.0.0/24	192.168.0.1
20	Red de Servidores	192.168.20.0/24	192.168.20.1
21	Red de Administración	192.168.21.0/24	192.168.21.1
22	Red de Desarrollo	192.168.22.0/24	192.168.22.1
30	Red de Administradores (VPN)	192.168.30.0/24	192.168.30.1
31	Red de Administración (VPN)	192.168.31.0/24	192.168.31.1
32	Red de Desarrollo (VPN)	192.168.32.0/24	192.168.32.1

Tabla 3.1: Segmentos de red utilizados por la organización.

3.2 Arquitectura final

La inclusión de FortiNAC en la red de la organización ha producido algunos cambios en la red local y en los dispositivos y servicios que esta tenía. El esquema de red final se puede observar en la figura 3.2. Se ha añadido un nuevo segmento de red para ubicar tanto el NAC como el Directorio Activo que se ha incluido.

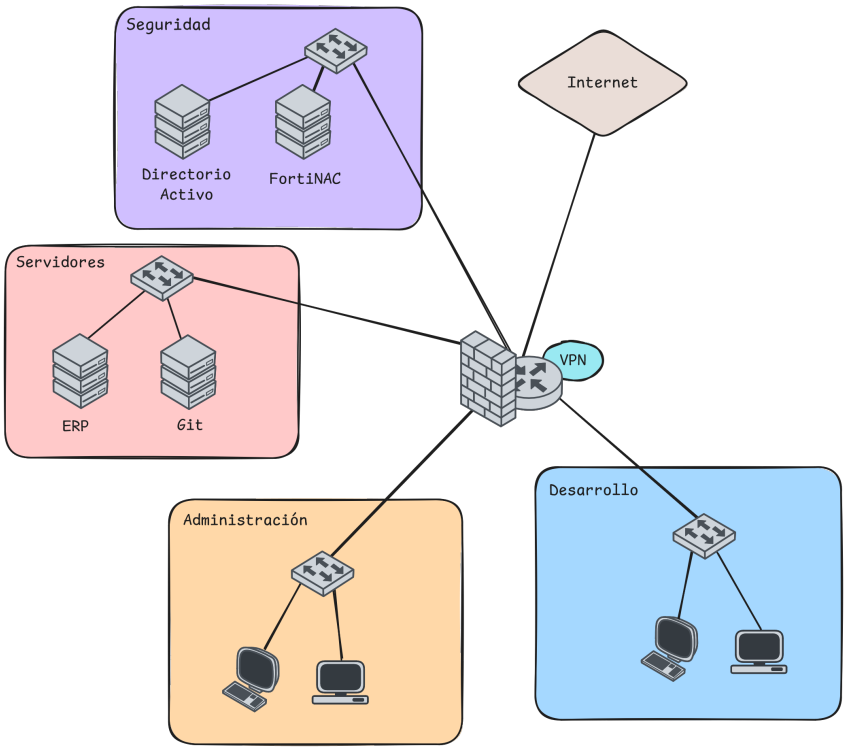


Figura 3.2: Esquema final de la infraestructura de la organización.

Se han integrado los servicios de freeRADIUS, anteriormente utilizado para autenticar a los usuarios en sus conexiones a la VPN, en el propio sistema NAC. Por esta razón, ha desaparecido de la red de servidores. Además, como puede observarse en la tabla 3.2, se han creado múltiples segmentos de red para dar soporte a las funcionalidades del NAC y cumplir los objetivos de este trabajo.

VLAN	Información	Direccionamiento	Gateway
1	Red de Gestión	192.168.0.0/24	192.168.0.1
20	Red de Servidores	192.168.20.0/24	192.168.20.1
21	Red de Administración	192.168.21.0/24	192.168.21.1
22	Red de Desarrollo	192.168.22.0/24	192.168.22.1
23	Red de Seguridad	192.168.23.0/24	192.168.23.1
24	Red de BYOD	192.168.24.0/24	192.168.24.1
30	Red de Administradores (VPN)	192.168.30.0/24	192.168.30.1
31	Red de VPN Administración (VPN)	192.168.31.0/24	192.168.31.1
32	Red de VPN Desarrollo (VPN)	192.168.32.0/24	192.168.32.1
40	Red de Autenticación	192.168.40.0/24	192.168.40.1
41	Red de Cuarentena	192.168.41.0/24	192.168.41.1
42	Red sin Salida	192.168.42.0/24	192.168.42.1
43	Red de Registro	192.168.43.0/24	192.168.43.1

Tabla 3.2: Segmentos de red utilizados tras la incorporación del NAC a la organización.

3.3 Tecnología utilizada

Los objetivos de este trabajo se llevarán a cabo en un entorno de virtualización que permite implementar las soluciones propuestas. En este caso se ha elegido GNS3[1] por sus capacidades y rendimiento. Permite realizar conexiones entre dispositivos, visibilizar y editar la red mediante una interfaz gráfica e instalar otros dispositivos con relativa facilidad.

Dentro de este laboratorio se utilizarán *routers* y *switches* de MikroTik[2]. Se han elegido por encima de otras alternativas como CISCO[3] por su capacidad y coste económico. En caso de querer utilizar infraestructura de CISCO se debe adquirir una licencia que permita la descarga de las imágenes virtualizables. En el caso de MikroTik, su uso es completamente gratuito (con sus puertos limitados a 1Mbps) y se puede contar con una prueba de dos meses que permite eliminar esa limitación.

Para la implementación de los servidores necesarios, se han empleado máquinas virtuales con Debian 12[4] como sistema operativo, debido a su amplia adopción, compatibilidad con las herramientas requeridas y su sencilla integración dentro del entorno de GNS3. Dado que la configuración completa de algunos servicios representados en el esquema de red excede el alcance de este trabajo, se ha optado por una simplificación de su funcionamiento. En estos casos, como ocurre con los servidores GIT y ERP, se ha simulado su presencia mediante páginas web informativas que identifican el servicio correspondiente (figura 3.3).

El servidor RADIUS original ha sido implementado utilizando FreeRADIUS[5], una de las implementaciones de RADIUS más reconocidas y ampliamente utilizadas. Esta solución ha sido seleccionada por su flexibilidad, su carácter de código abierto y su facilidad de configuración, lo que permite adaptarla perfectamente a las necesidades de este trabajo.

[1] https://gns3.com/
[2] https://mikrotik.com/
[3] https://www.cisco.com/
[4] https://www.debian.org
[5] https://www.freeradius.org/

Figura 3.3: Captura de las webs de los servidores ERP y GIT.

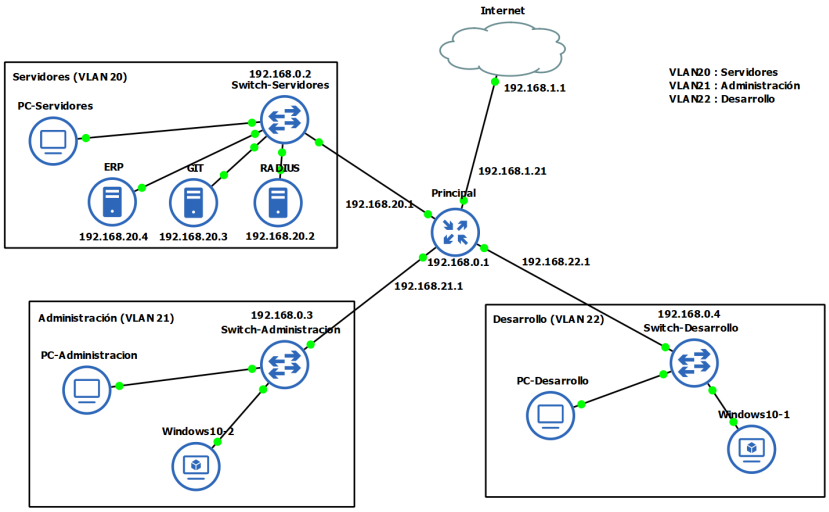


Figura 3.4: Esquema de red inicial de la organización implementado en GNS3.

Además, se cuenta con un servidor OpenVPN[6] en el router MikroTik para poder simular las conexiones externas de los trabajadores. Se ha escogido OpenVPN por ser un protocolo fiable, ampliamente utilizado y por contar con una implementación de su servidor en RouterOS, el sistema operativo utilizado por los dispositivos MikroTik.

El acceso a los distintos recursos está restringido únicamente a los usuarios autorizados. De este modo, el departamento de desarrollo podrá acceder al repositorio Git, mientras que el departamento de administración tendrá acceso al sistema ERP. Esta política de control de acceso se aplica tanto a las conexiones realizadas desde la red local en la oficina como a aquellas que se efectúan de forma remota a través de la VPN.

La solución de Control de Acceso a la Red (NAC) elegida para este proyecto es FortiNAC. Esta elección se fundamenta en su amplia compatibilidad con equipos de red de diferentes fabricantes, así como en su relativa facilidad de configuración en comparación con otras alternativas disponibles en el mercado. FortiNAC se destaca como uno de los principales productos NAC del sector y ofrece la posibilidad de obtener una licencia de prueba del producto.

En la figura 3.4 se puede ver el estado del laboratorio realizado en GNS3.

[6]https://openvpn.net/

CAPÍTULO 4
Desarrollo de las soluciones propuestas

4.1 Implementación de un sistema NAC básico para el control de acceso por cable y VPN

En este apartado se describirá el desarrollo del primer objetivo del trabajo, que comenzará con la instalación del sistema FortiNAC y la realización de las primeras modificaciones en la red de la organización para adaptarla a la solución NAC.

4.1.1. Instalación de FortiNAC

FortiNAC no puede virtualizarse en QEMU[1] (el hipervisor comúnmente utilizado por GNS3)[10], pero sí permite su ejecución en VMware[2]. Tras descargar la OVA de FortiNAC desde la página oficial, se importó en el hipervisor de VMware, para después incorporarlo dentro de GNS3 en el nuevo segmento de red creado para ese propósito (4.1). De esta forma, la interfaz de gestión del NAC queda aislada de otros servicios y usuarios.

VLAN	Información	Direccionamiento	Gateway
23	Red de Seguridad	192.168.23.0/24	192.168.23.1

Tabla 4.1: Red de seguridad añadida para ubicar FortiNAC.

Después de instalar FortiNAC, se debe conectar la interfaz de red al nuevo segmento de red de seguridad y configurarla con la dirección IP `192.168.23.5`. Además, es necesario especificar qué componentes de FortiNAC se utilizarán en esa interfaz. Todo esto se puede realizar accediendo a la consola con el usuario *admin* (sin contraseña) y ejecutando los comandos presentados en el fragmento 4.1.

[1] https://www.qemu.org/
[2] https://www.vmware.com/

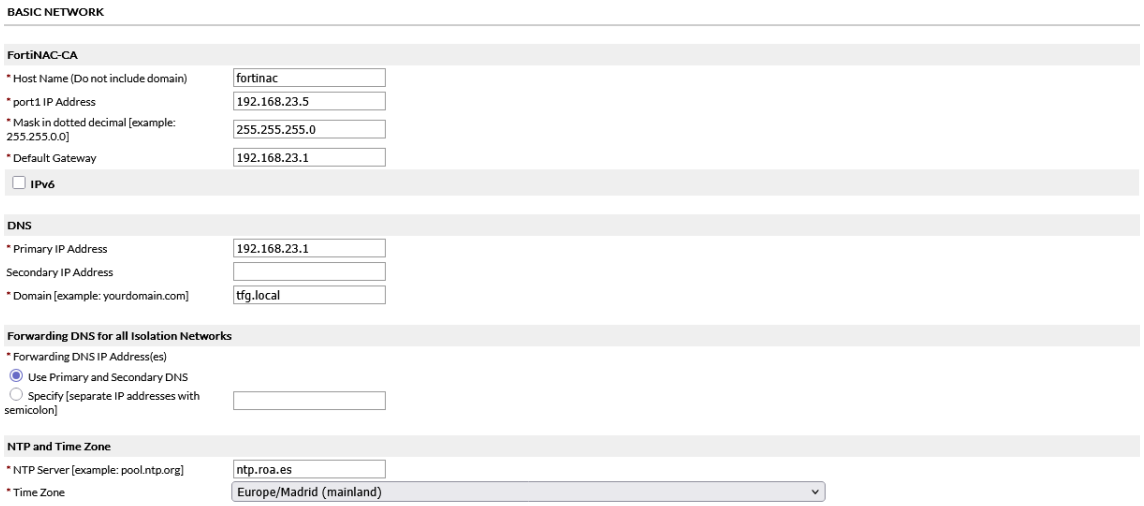


Figura 4.1: Configuración básica de FortiNAC en su panel web.

```
config system interface
edit port 1
set ip 192.168.23.5/24
set allowaccess https ping https-adminui radius-auth radius-acct snmp dns ssh
    http nac-agent netflow
next
end
config route static
edit 1
set device port1
set gateway 192.168.23.1
next
end
```

Fragmento 4.1: Configuración de la interfaz en FortiNAC.

Tras completar la configuración del fragmento 4.1 se habilitará el uso del panel web en esa interfaz, lo que permitirá acceder a la interfaz de administración para comenzar la configuración del NAC. Como se observa en la figura 4.1, es necesario definir el dominio que tendrá FortiNAC dentro de la organización (fortinac.tfg.local), así como la configuración de red y los parámetros para la sincronización de fecha y hora.

Para la sincronización de fecha y hora en todos los dispositivos, se ha decidido utilizar el servicio NTP proporcionado por el Observatorio de la Armada[3].

Se utilizará el servidor DNS integrado en el *router* MikroTik, centralizando así la configuración DNS en este equipo. Más detalles sobre cómo configurar el DNS se discutirán en la sección 4.1.4.

4.1.2. Configuración del servidor RADIUS de FortiNAC

Antes de la implementación de FortiNAC, se utilizaba un freeRADIUS en un servidor independiente para la autenticación de usuarios. No obstante, esta funcionalidad se ha integrado en FortiNAC, lo que reduce la complejidad de la solución global y la superficie de exposición a posibles ataques.

[3]https://armada.defensa.gob.es/ArmadaPortal/page/Portal/ArmadaEspannola/cienciaobservatorio/prefLang-es/06Hora–00Hora

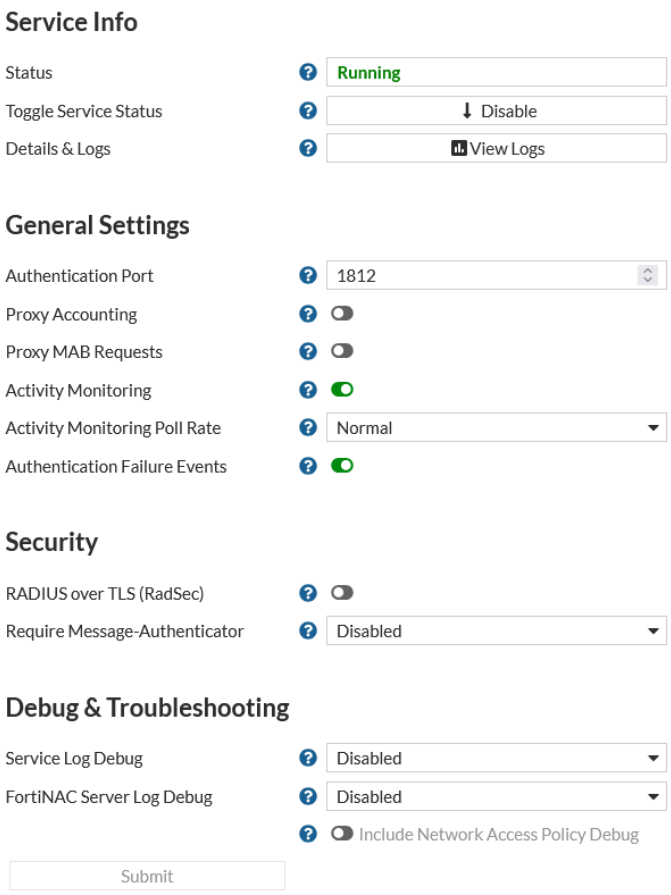


Figura 4.2: Página de estado y configuración del servicio de RADIUS.

Para activar el servicio RADIUS, se debe navegar al menú de Network → RADIUS, como se observa en la figura 4.2. No es necesario modificar la configuración predeterminada. FortiNAC ofrece la opción de configurar su propio servidor RADIUS (utilizando *FreeRADIUS*) o usarlo como *proxy* para un servidor RADIUS que ya esté presente en la infraestructura.

En esta situación, se optará por utilizar el servidor RADIUS local en lugar del servidor RADIUS dedicado, indicado en la figura 3.1 con la dirección IP `192.168.20.2`. Esto permite integrar el servidor dentro del propio NAC, con el objetivo de simplificar el proceso y optimizar los recursos del laboratorio. Además, se prevé la migración a un Directorio Activo para la gestión de usuarios. Los parámetros de configuración del servidor se muestran en la captura 4.3. Es importante habilitar los protocolos PEAP y MSCHAPV2, ya que son necesarios para la autenticación en equipos Windows.

Otro apartado de la configuración RADIUS son los atributos que enviará el servidor RADIUS a los clientes 802.1X en el caso de una autenticación exitosa (figura 4.4). El parámetro `%ACCESS_VALUE%` será sustituido por el número de VLAN que, de acuerdo con las políticas configuradas en el NAC, se asignará a la conexión de un usuario.

Para la mayoría de los dispositivos de red, así como en el caso de los *switches* MikroTik, el conjunto por defecto de `RFC_Vlan` es adecuado para permitir la asignación dinámica de VLAN en un puerto. Si fuera necesario, es posible agregar un conjunto de atributos personalizados.

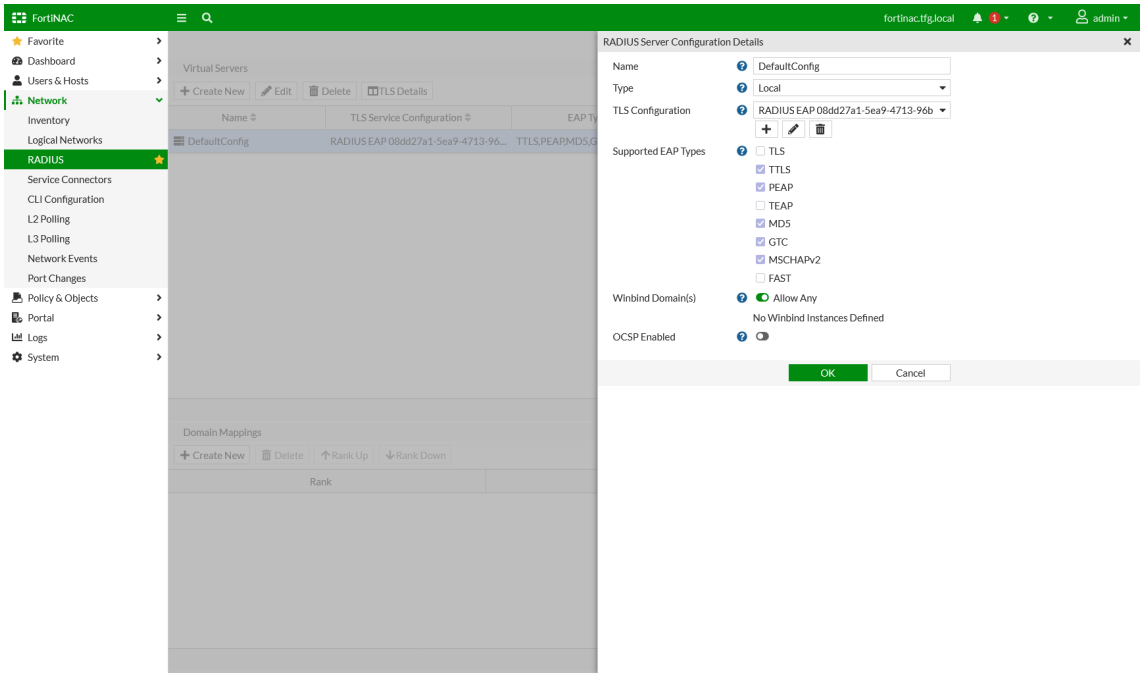


Figura 4.3: Página de configuración del servidor RADIUS.

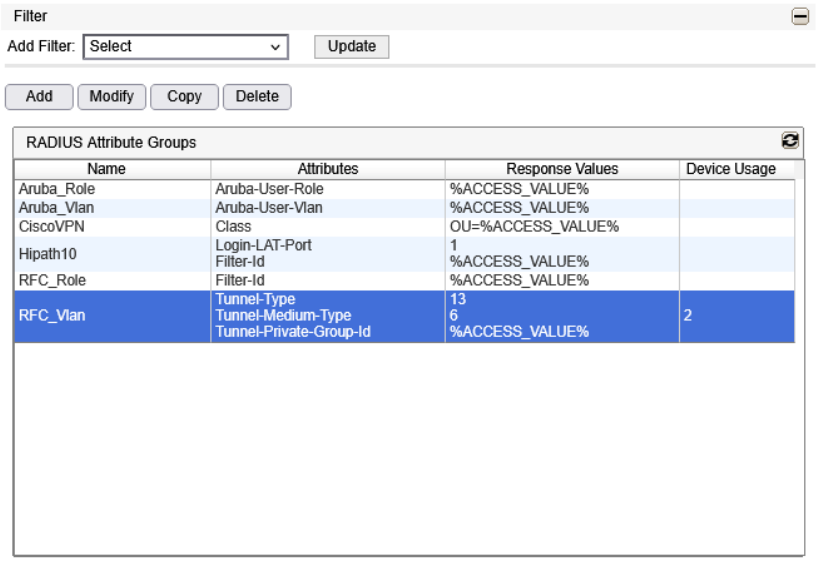


Figura 4.4: Menú de configuración de artributos RADIUS.

4.1.3. Inventario de red

FortiNAC opera únicamente como el orquestador y, por lo tanto, depende de los dispositivos de red para su funcionamiento. En la sección *Inventory* de su panel de configuración se mostrarán los equipos de red que se han añadido para garantizar la aplicación de políticas y el funcionamiento del NAC.

En FortiNAC, es posible añadir dispositivos mediante los protocolos SSH y SNMP, dos protocolos estándar para el control remoto de dispositivos. El protocolo SNMP (de *Simple Network Management Protocol*) permite a FortiNAC consultar el estado de los sistemas y realizar cambios de configuración en tiempo real.

Se pueden añadir dispositivos a través de la interfaz, en el apartado *Inventory*. Al agregar un nuevo equipo, deben proporcionarse las credenciales necesarias para su conexión. Para que la conexión se establezca, es necesario configurar cada dispositivo para aceptar el enlace. En el caso de los *routers* y *switches* MikroTik[4], estos ajustes se realizan conectando mediante SSH a estos dispositivos y añadiendo una entrada en la ruta `/snmp/community`.

```
1 name="seguridad"
2 addresses=192.168.23.5/32
3 security=Authorization
4 read-access=yes
5 write-access=yes
6 authentication-protocol=SHA1
7 encryption-protocol=AES
8 authentication-password="seguridad"
9 encryption-password="seguridad"
```

Fragmento 4.2: Configuración SNMP en los *switches* y el *router* MikroTik. Resultado de ejecutar `/snmp/community print detail`.

El fragmento 4.2 muestra la configuración aplicada a los dispositivos MikroTik para permitir la interacción de FortiNAC a través de SNMP, habilitando la lectura y escritura de la configuración del dispositivo. El acceso se ha limitado exclusivamente a la IP del FortiNAC, configurando un usuario y contraseña específicos para esta función. Asimismo, se han implementado los protocolos más seguros compatibles en ambos extremos de la conexión.

Los siguientes pasos deben llevarse a cabo en el panel de administración de FortiNAC, introduciendo los mismos datos que han sido configurados en los dispositivos de red. Esto se muestra en la figura 4.5 y se ha replicado para el resto de *switches* y el *router*. Además, FortiNAC permite utilizar credenciales SSH para conectar y realizar acciones avanzadas en el dispositivo. Al finalizar, se listan todos los dispositivos, como se observa en la figura 4.6.

Inventariar los equipos de red, además de habilitar la integración dentro de FortiNAC, permite monitorizarlos y administrarlos desde un panel centralizado, lo que facilita la gestión, sobre todo cuando se cuenta con una gran cantidad de equipos.

4.1.4. Instalación de Windows Server y configuración de un Directorio Activo

La instalación de un servidor con Windows Server y un Directorio Activo no fue considerada en un inicio. Principalmente por el ahorro de recursos en el sistema virtual y por no ser objeto de este trabajo.

[4] https://help.mikrotik.com/docs/spaces/ROS/pages/8978519/SNMP

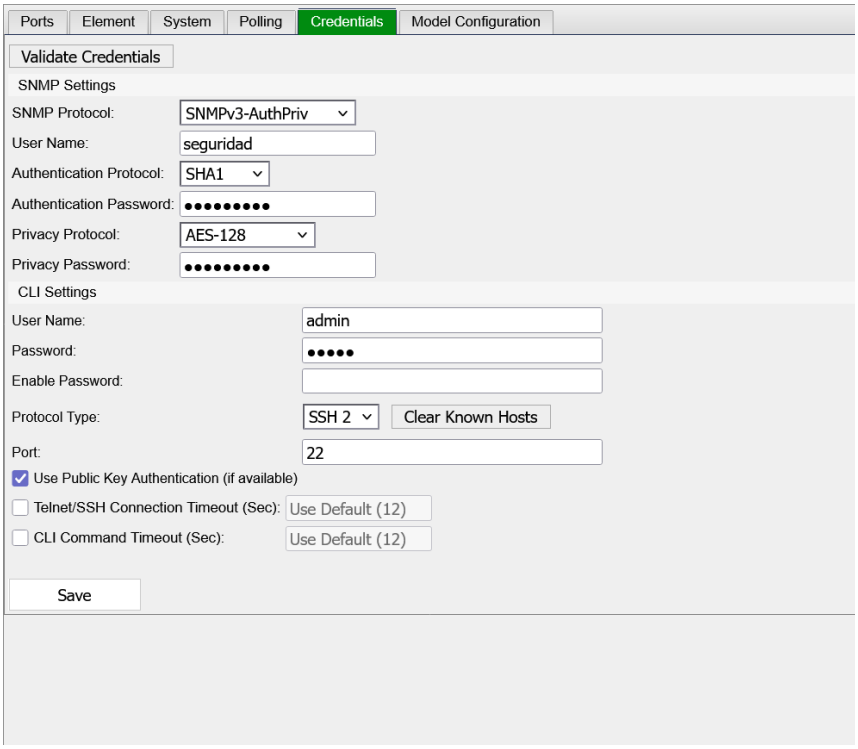


Figura 4.5: Configuración de las credenciales de conexión a uno de los *switches* MikroTik.

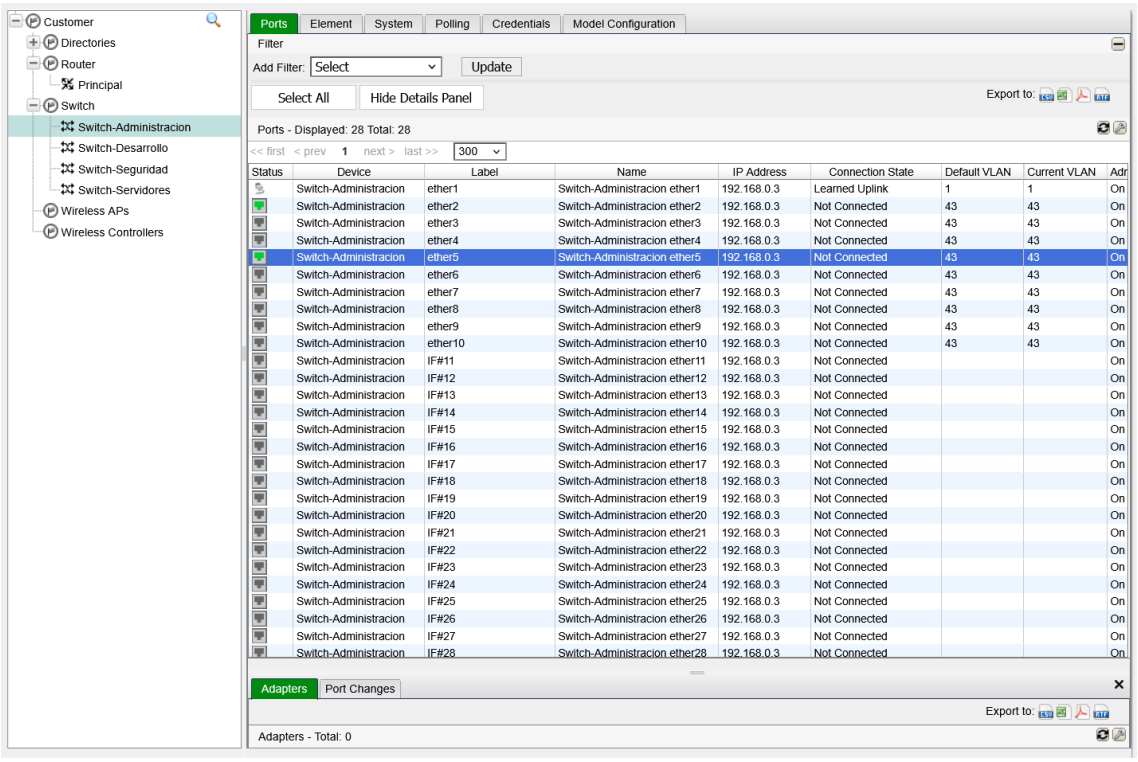


Figura 4.6: Inventario de FortiNAC, mostrando la organización de los elementos de red y la configuración de los puertos de un switch.

No obstante, al llevar a cabo este objetivo, se comprobó que la autenticación 802.1X en Windows exige el uso del protocolo MSCHAPv2 o, alternativamente, la aplicación de certificados en cada uno de los equipos. El uso de certificados resulta complicado y requiere un despliegue manual en cada equipo de la organización, lo cual, en un entorno real, no suele ser habitual. Sin embargo, es común contar con un Directorio Activo en organizaciones de todos los tamaños.

Llegado este punto, se consideró necesario desplegar un Directorio Activo para alcanzar el objetivo de manera realista.

Instalación de Windows Server

Tras la instalación de la nueva máquina virtual con Windows Server y la asignación de la IP `192.168.23.6` (ver figura 4.7), se promueve el servidor a controlador de dominio en el dominio `tfg.local`, convirtiéndose en `winserver.tfg.local`.

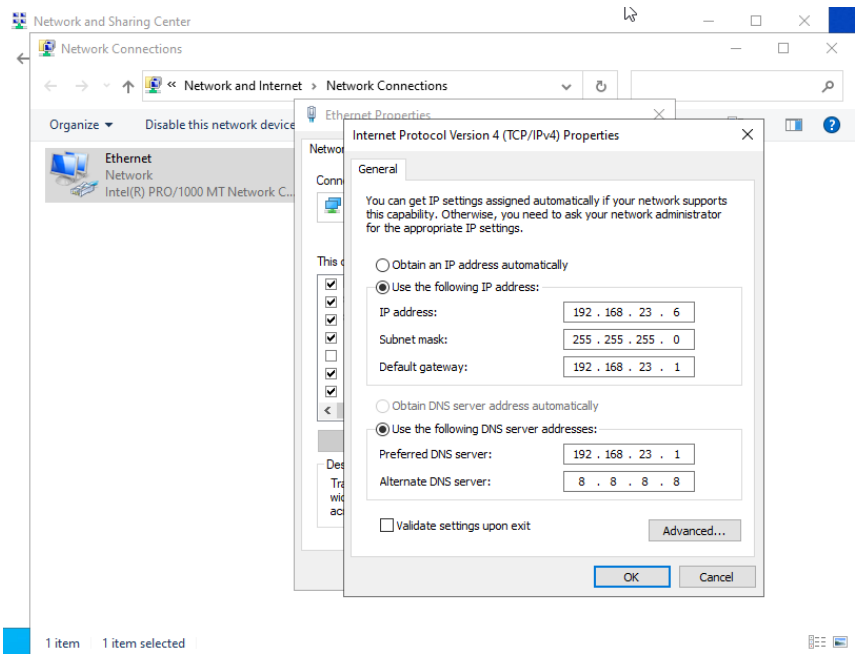


Figura 4.7: Configuración de red del servidor WINSERVER.

Para que los equipos puedan resolver el dominio `fortinac.tfg.local`, es necesario añadir una entrada en el gestor de DNS del servidor con la IP asignada a FortiNAC (figura 4.8). De este modo, todos los equipos podrán realizar la resolución correctamente.

Configuración de DNS en el router

Para permitir que los dispositivos resuelvan nombres de dominio de `*.local`, se ha configurado el router para redirigir las peticiones de dicho dominio al servidor DNS del controlador de dominio (figura 4.9). Como resultado, únicamente se envían al servidor las solicitudes locales, mientras que el router sigue actuando como servidor DNS para los dispositivos en la red local.

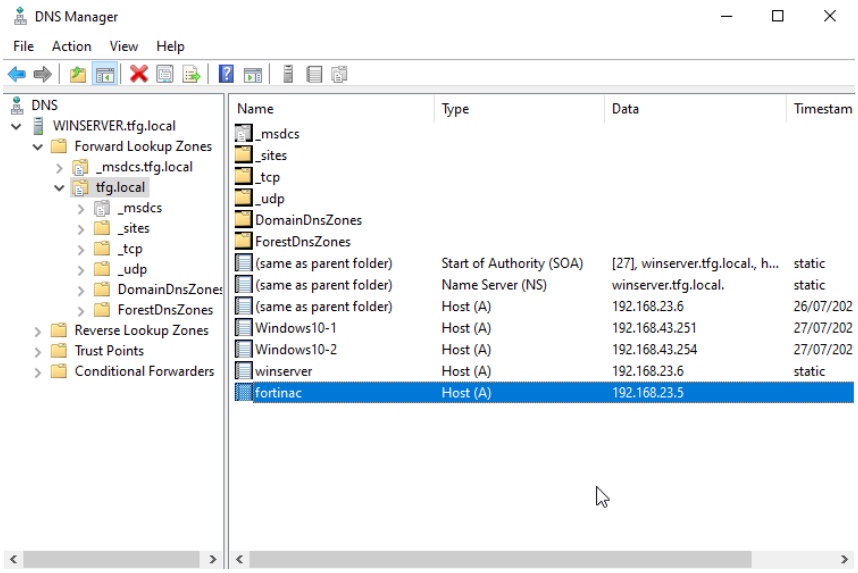


Figura 4.8: Entrada DNS para FortiNAC en Windows Server.

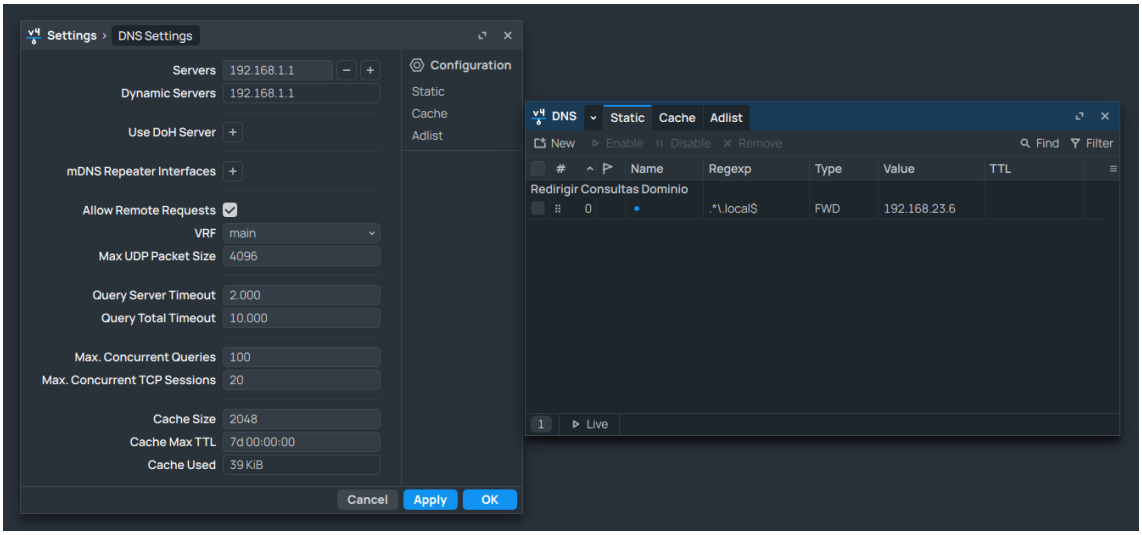


Figura 4.9: Configuración de DNS en el router MikroTik.

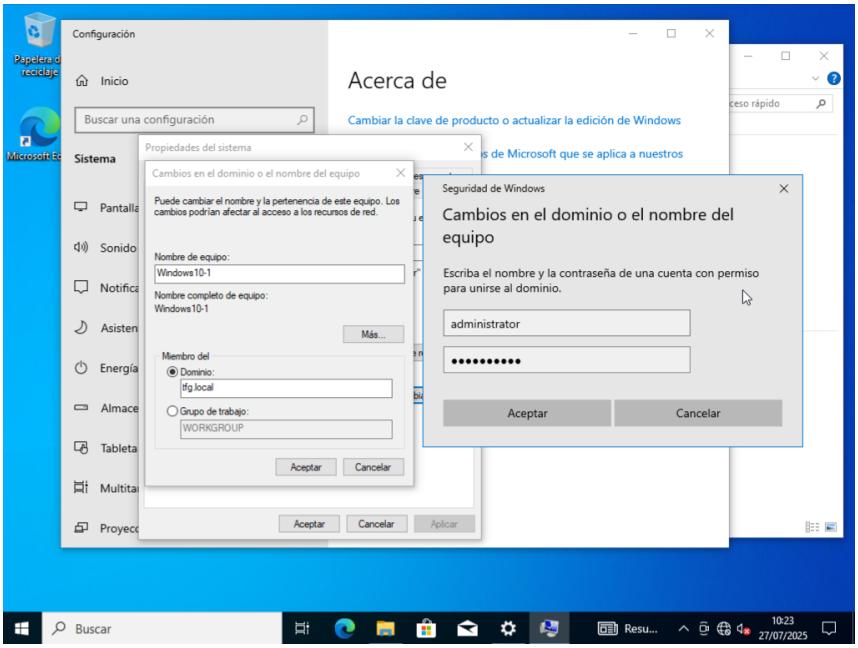


Figura 4.10: Añadiendo el equipo `Windows10-1` al dominio `tfg.local`.

Integrar los equipos de la oficina en el dominio

El proceso de integración de un equipo en el dominio debe realizarse en el propio dispositivo, accediendo al panel de configuración e introduciendo el dominio. Una vez validada la operación con una cuenta de administrador del dominio y reiniciado el equipo, este quedará correctamente integrado. Este proceso se muestra en la figura 4.10.

Gestión de usuarios y equipos en el Directorio Activo

Una vez que los equipos han sido añadidos al directorio, se pueden administrar y organizar mediante la herramienta `Usuarios y Equipos de Active Directory`.

Tras ingresar a esta consola, se deben reubicar los equipos en las unidades organizativas (figura 4.11) correspondientes a su ubicación en la oficina. Asimismo, se crearán dos usuarios de prueba para continuar con el proceso de implementación del NAC:

- **Administracion**. Usuario del departamento de administración y ubicado en la unidad organizativa correspondiente. Su campo **departamento** está configurado como `Administracion` (figura 4.12).
- **Desarrollo**. Usuario del departamento de desarrollo, ubicado en la unidad organizativa de desarrollo, siendo su campo **departamento** `Desarrollo` en este caso.

4.1.5. Configuración del Directorio Activo en FortiNAC

Con el propósito de permitir que FortiNAC utilice los usuarios registrados en el Directorio Activo y autentique a los empleados al iniciar sesión en sus equipos, es imperativo integrar FortiNAC con el dominio.

Este proceso consta de dos componentes. Por un lado, gracias a *Winbind* FortiNAC, se verifica que el usuario que intenta acceder a la red sea válido dentro del dominio de la empresa. Por otro lado, gracias al explorador LDAP integrado en FortiNAC, se examinan

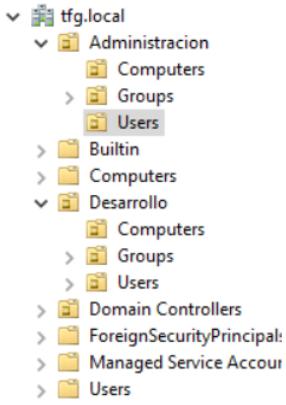


Figura 4.11: Organización de unidades organizativas en el Directorio Activo.

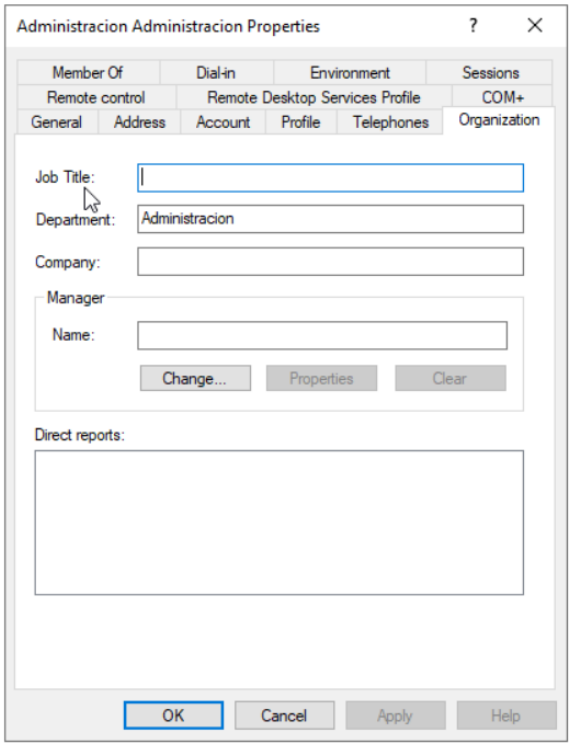


Figura 4.12: Propiedad departamento del usuario Administracion en el Directorio Activo.

todas las propiedades de cada objeto del dominio. Esto permite obtener el nombre, el usuario, el rol y el cargo, entre otros.

Winbind

El menú de configuración de *Winbind* se encuentra en la ruta `RADIUS → Winbind`. Una vez ingresados los datos de configuración (figura 4.13), FortiNAC se unirá al dominio y aparecerá dentro de la unidad organizativa "*Computers*".

Configuración LDAP

Dentro del apartado de `Settings → Authentication → LDAP` se pueden añadir configuraciones de conexión a sistemas LDAP. En la configuración, es necesario introducir algunos datos del controlador de dominio y del dominio, como se puede observar en la

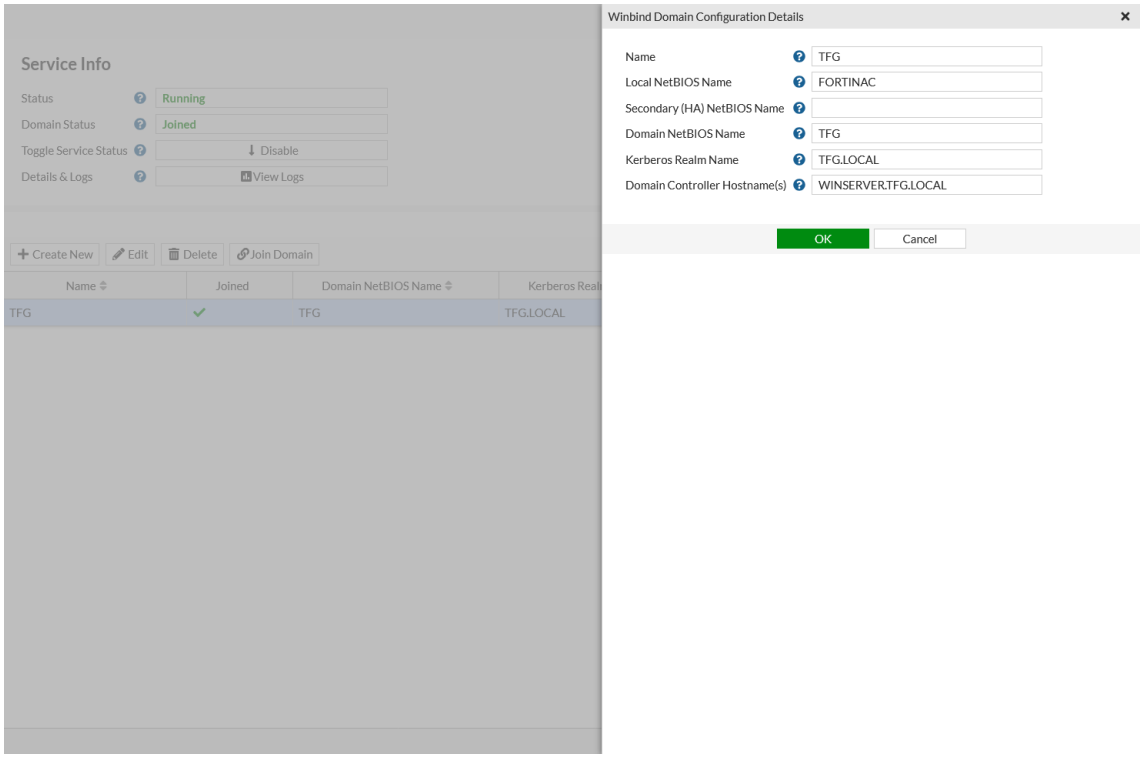


Figura 4.13: Configuración de Winbind en FortiNAC.

figura 4.14. En el apartado de `User Attributes` (figura 4.15) se ha asignado el atributo `Role` al parámetro del usuario `department`, en el que se había especificado previamente el departamento correspondiente a cada usuario.

De esta manera, en las políticas se podrá utilizar el rol del usuario para identificar el departamento al que pertenece cada empleado.

4.1.6. Configuración de 802.1X en los dispositivos

Como se indica en el apartado de Identificación (2.4.2), el protocolo 802.1X requiere compatibilidad y configuración en todos sus participantes.

Configuración de 802.1X en Windows (*Supplicant*)

La configuración de la interfaz de red de un equipo con Windows para aceptar 802.1X requiere habilitar un servicio y configurar el adaptador de red. Dado que los ordenadores están en un dominio, esta configuración puede realizarse una única vez mediante una GPO y distribuirse a todos los ordenadores del dominio. De este modo, no es necesario configurar cada equipo de forma individual. Si en el futuro se requiere modificar la configuración, este proceso se llevará a cabo de manera automática.

Esto puede llevarse a cabo desde la herramienta de *Group Policy Management*, añadiendo una nueva directiva (en este caso denominada `802.1X`), que almacenará la configuración de los equipos. Para localizar los ajustes de configuración de 802.1X, se debe acceder a la ruta:

```
1 Computer Configuration\Policies\Windows Settings\Security\Wired Network
    Authentication (802.3) Policies
```

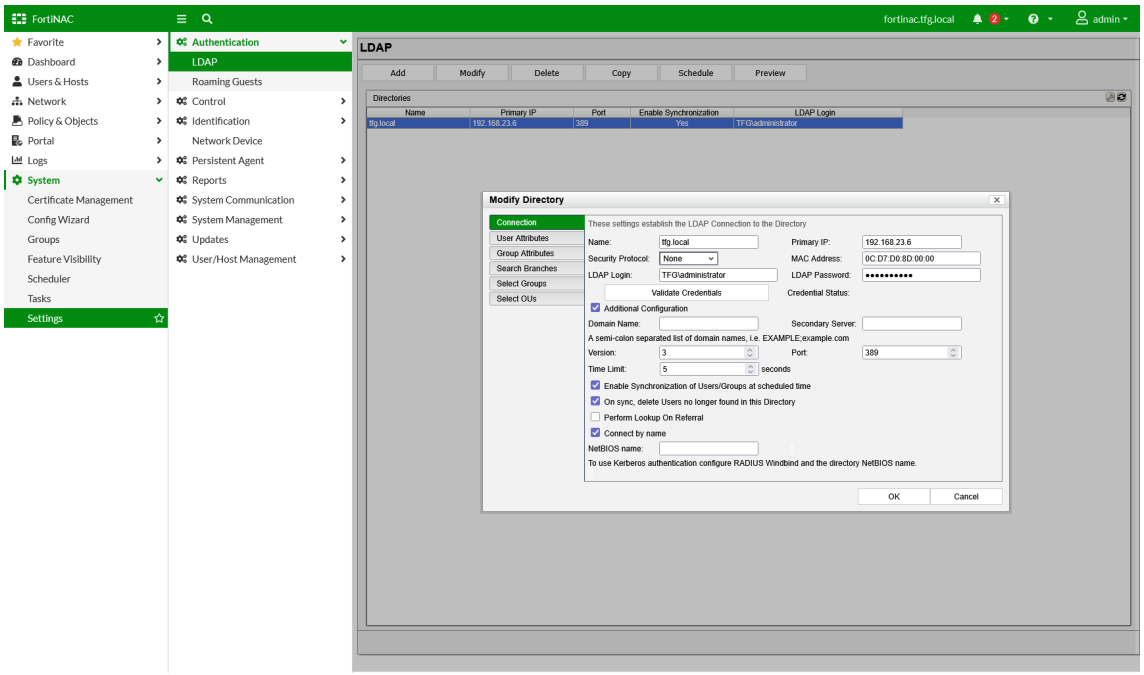


Figura 4.14: Configuración LDAP para obtener los objetos del Directorio Activo.

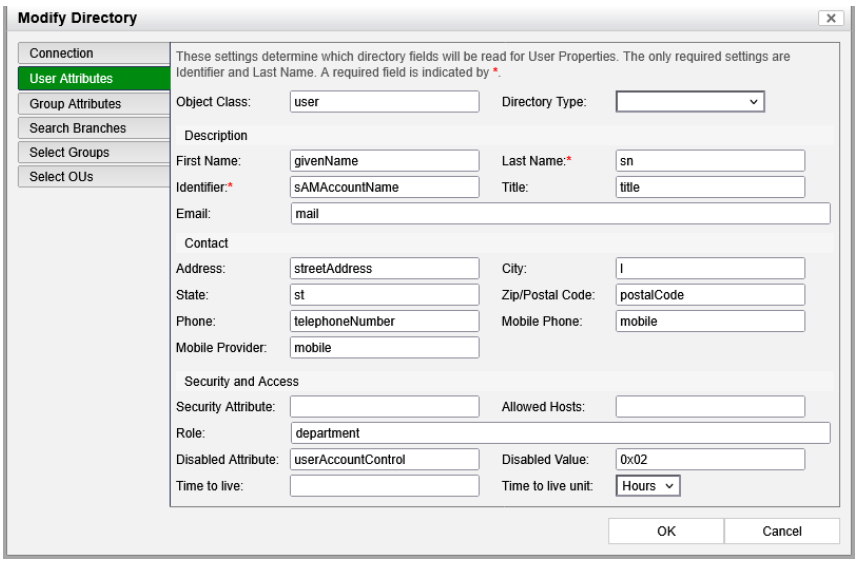


Figura 4.15: Apartado de usuario dentro de la configuración LDAP.

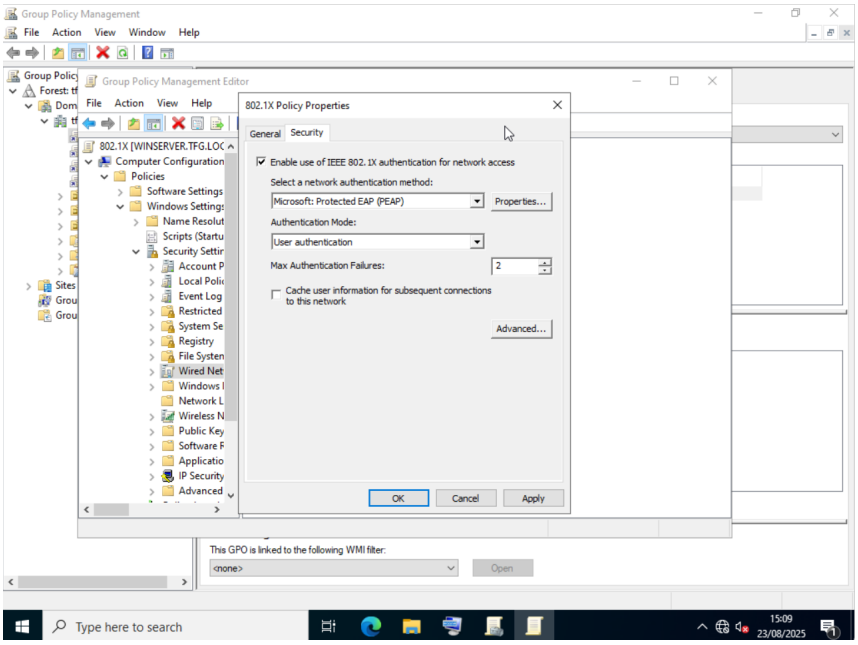


Figura 4.16: Pantalla de seguridad de la autenticación 802.1X.

En la pantalla de seguridad (figura 4.16), se elige `Microsoft: Protected EAP (PEAP)` como el protocolo de autenticación y `User Authentication` para que FortiNAC obtenga la información del usuario que ha iniciado sesión.

Dentro de la configuración del protocolo EAP (figura 4.17), se debe seleccionar `Secured Password (EAP-MSCHAP v2)` como método de autenticación y desactivar la opción de verificar la autenticidad del servidor RADIUS mediante un certificado, por cuestiones de simplicidad. Sin embargo, en un despliegue real, es muy recomendable configurar dichos certificados.

Se puede utilizar un certificado autofirmado al compartir la autoridad certificadora (CA) con los equipos del dominio mediante otra GPO, o se puede optar por un certificado firmado por una de las CAs confiables disponibles en el menú. En la configuración de `EAP MSCHAPv2` (figura 4.18) se puede lograr que el sistema envíe la información del usuario que ha iniciado sesión al servidor RADIUS, evitando así que se soliciten nuevamente el usuario y la contraseña al intentar autenticarse en la red. FortiNAC podrá validar al usuario del dominio gracias a la configuración de *Winbind* realizada previamente en el apartado 4.1.5. Además de la configuración de la autenticación 802.1X, es necesario habilitar el servicio de configuración de red cableada en Windows para que se inicie al arrancar el equipo y gestione el inicio de sesión en la red (figura 4.19). El servicio que se debe habilitar se denomina `Wired AutoConfig` y se puede configurar en la siguiente ruta:

```
1 Computer Configuration\Policies\Windows Settings\Security\System Services
```

Configuración de 802.1X en Switches (*Authenticator*)

Los switches tienen la función de solicitar las credenciales al dispositivo que se conecta a la red y de reenviar esta información a FortiNAC. Este último responderá indicando las acciones a seguir, según la validez de la información enviada.

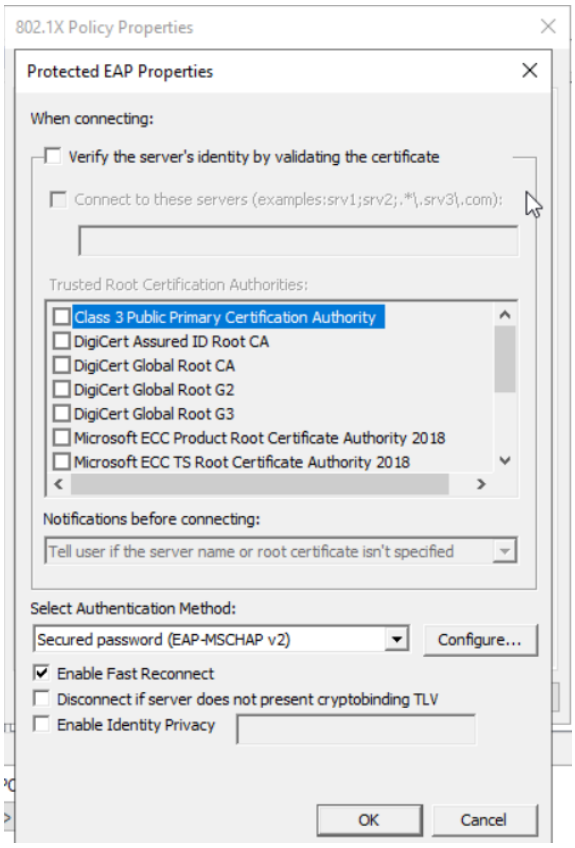


Figura 4.17: Pantalla de configuración del protocolo EAP.

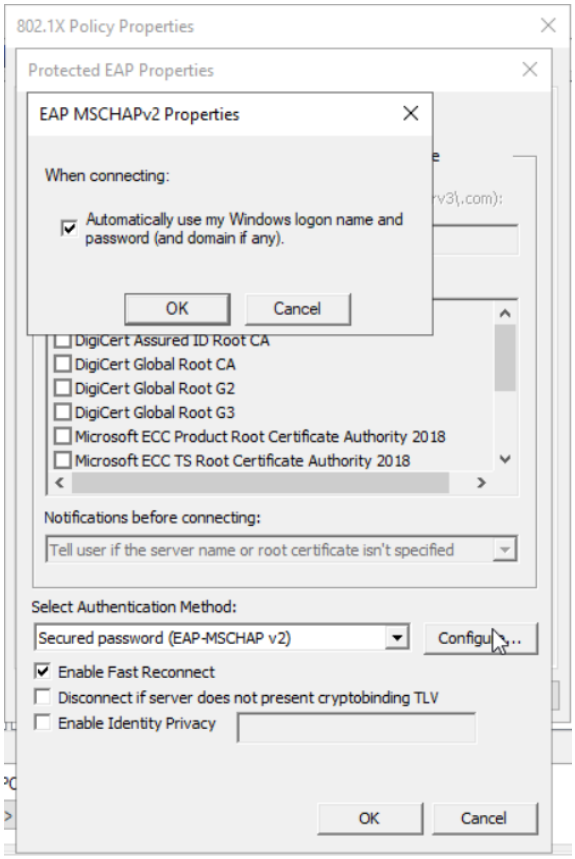


Figura 4.18: Captura de las propiedades de MSCHAPv2.

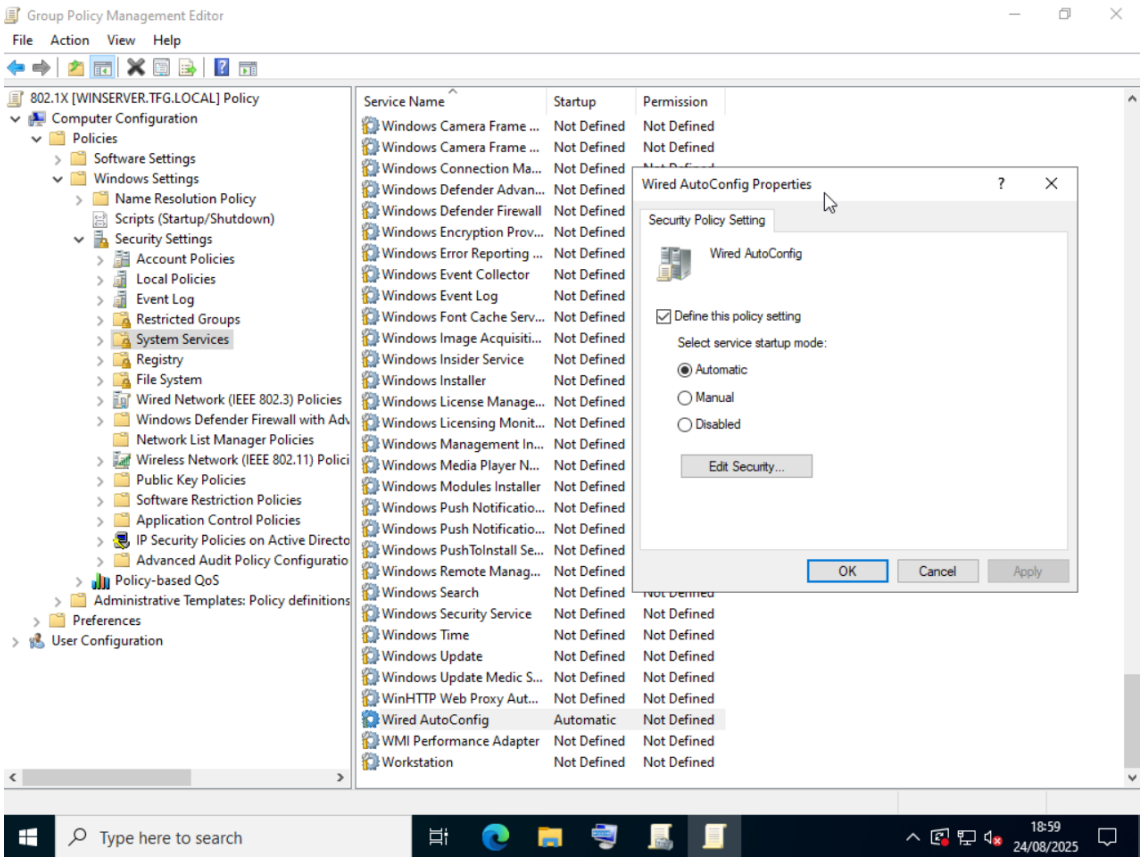


Figura 4.19: Configuración del servicio `Wired AutoConfig` en el GPO `802.1X`.

Para que estos dispositivos presenten este comportamiento, se requiere una configuración adecuada. En el caso de los *switches* MikroTik[11], es necesario especificar el servidor RADIUS que se utilizará para las solicitudes[5] (figura 4.20).

En el inventario de FortiNAC (figura 4.21) se ha definido previamente la clave `RADIUS` para ser utilizada por la administración de *switch* al realizar peticiones al RADIUS.

Además se ha especificado utilizar `RFC_Vlan` en el campo **Attribute Group**. Esto permitirá que FortiNAC envíe los atributos necesarios para configurar el *switch* tras la correcta autenticación de un usuario.

Posteriormente, se activa el protocolo 802.1X (representado como `Dot1X` en los menús de MikroTik) en todos los puertos donde se requiera autenticación, como se muestra en la figura 4.22.

Configuración de 802.1X en FortiNAC (*Authentication Server*)

Para activar el registro de dispositivos mediante 802.1X, es necesario acceder al inventario de FortiNAC y modificar las interfaces en las que se desea habilitar la autenticación. Los puertos seleccionados deben coincidir con aquellos que se habilitaron previamente en los *switches*, ya que, como se recordará, en el caso de usar NAC en redes Ethernet cableadas, la necesidad de autenticación se define en cada uno de los puertos de un *switch*.

En estas interfaces, se debe habilitar la opción `802.1X Authentication`. En el menú de *Group Membership* (como se observa en la figura 4.23) se deben seleccionar las siguientes opciones:

[5] https://help.mikrotik.com/docs/spaces/ROS/pages/328090/Dot1X

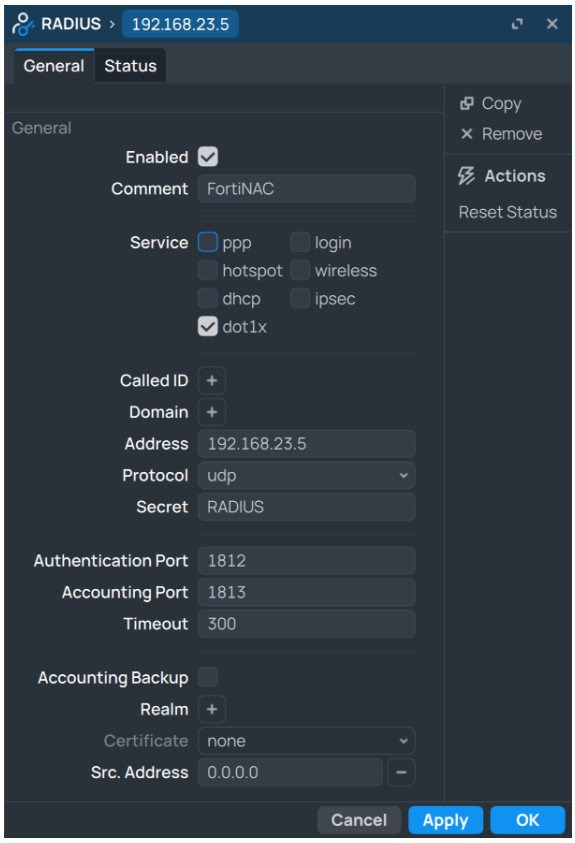


Figura 4.20: Configuración del cliente RADIUS del *switch* Administración.

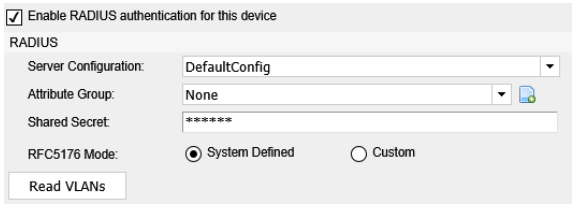


Figura 4.21: Captura de la configuración RADIUS para el *switch* Administración.

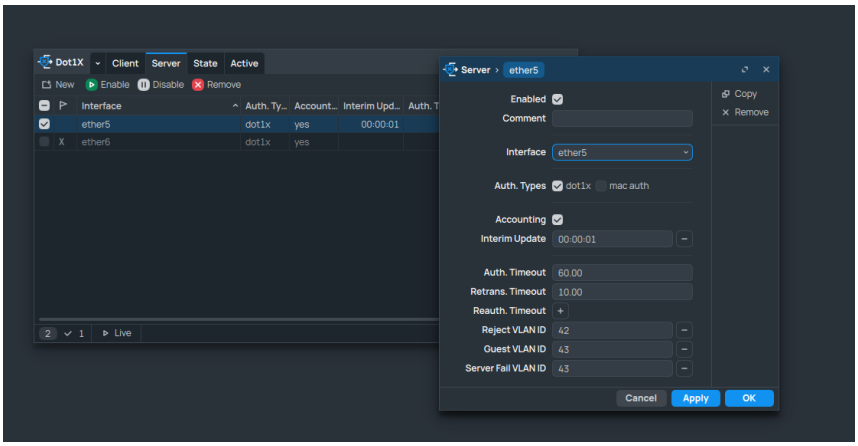


Figura 4.22: Configuración del protocolo 802.1X en el puerto `ether5` del *switch* Administración

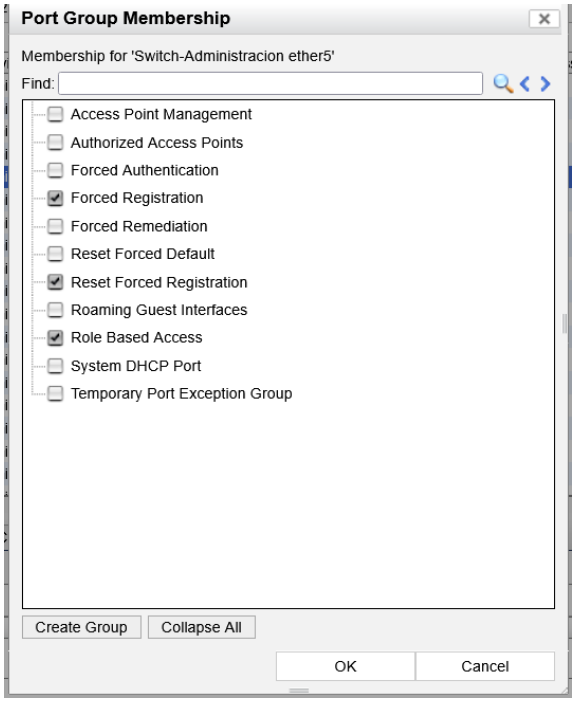


Figura 4.23: Grupos a los que debe pertenecer toda interfaz donde se quiera activar la autenticación 802.1X.

- ***Forced Registration***: Para especificar que todo dispositivo debe autenticarse para acceder a la red.
- ***Reset Forced Registration***: Permitiendo que FortiNAC vuelva a establecer ese puerto a la `VLAN 43` (registro) cuando detecte que el dispositivo se ha desconectado. El puerto queda así preparado para autenticar otra conexión.
- ***Role Based Access***: Con esta opción FortiNAC asignará la VLAN basándose en las políticas que se definan.

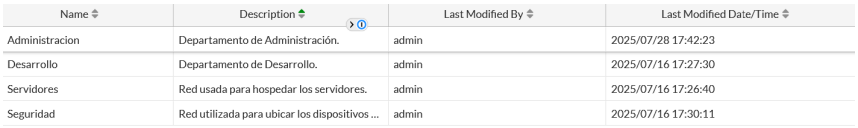
De esta manera, esta interfaz requerirá un registro para permitir la conexión de un equipo (modificar la VLAN del *switch* a una productiva o con salida a internet), regresará a la VLAN de registro al desconectarse dicho equipo, y se aplicará una red de producción diferente según las políticas establecidas para el usuario.

FortiNAC requiere especificar la VLAN asociada a cada red en cada uno de los dispositivos de red. Este mecanismo permite que una misma red lógica pueda vincularse a diferentes VLAN en distintos *switches* o *routers*. En la figura 4.24 se ilustran algunos ejemplos de redes definidas en el NAC, las cuales se representan únicamente mediante un nombre y una descripción.

Por su parte, la figura 4.25 muestra la relación entre las redes lógicas y las VLAN correspondientes. Para añadir una red al listado, es necesario seleccionar en el desplegable *Logical Network* una red previamente creada y asignarle un identificador de VLAN en el campo *Access Value*. Dicho valor será el que FortiNAC aplicará al establecer la conexión de esa red lógica en el *switch*.

4.1.7. Definición de políticas en FortiNAC

Habiendo configurado FortiNAC para autenticar usuarios en las interfaces pertinentes, es necesario definir las políticas que se aplicarán al detectar una conexión.



Name	Description	Last Modified By	Last Modified Date/Time
Administracion	Departamento de Administración.	admin	2025/07/28 17:42:23
Desarrollo	Departamento de Desarrollo.	admin	2025/07/16 17:27:30
Servidores	Red usada para hospedar los servidores.	admin	2025/07/16 17:26:40
Seguridad	Red utilizada para ubicar los dispositivos ...	admin	2025/07/16 17:30:11

Figura 4.24: Configuración de Redes Lógicas en FortiNAC.

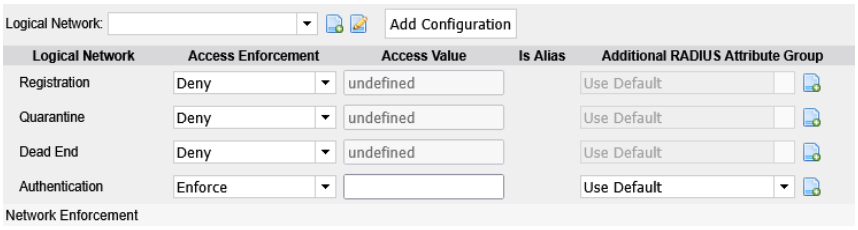


Figura 4.25: Relación de *VLANs* y Redes Lógicas en un dispositivo de red.

Se ha establecido una política que verificará que la conexión se realice desde un equipo registrado en el dominio y por un usuario autorizado. Si estas condiciones no se cumplen, se negará la conexión, dejando al equipo aislado en la `VLAN 43`.

La figura 4.26 muestra una captura de la política implementada a los usuarios del departamento de administración. La descripción de la política se puede observar en el fragmento 4.3.

```
1  Name: RADIUS_802.1X_ETH - Red Administracion
2  Configuration: RED Administracion - Config
3
4  Who/What: Where -> Adapter -> RADIUS Auth Type = 802.1X
5                EAP Type = PEAP
6                Inner EAP Type = MSCHAPv2
7       AND User -> Role = Administracion
8  Groups: Any
9  Where: AnyOf = L2 Wired Devices
10 When: Always
```

Fragmento 4.3: Definición de la política de acceso a la red de administración.

La primera parte de la condición verifica que el evento de conexión sea una solicitud RADIUS mediante `PEAP` y `MSCHAPv2`. En la segunda parte, se valida que el usuario pertenezca al rol `Administración` (obtenido del Directorio Activo). Además, en el apartado *Where* se confirma que la solicitud se origina desde un dispositivo de capa 2 (grupo asignado automáticamente a los *switches*).

En la descripción de la política (fragmento 4.3) se puede comprobar que se ha establecido `RED Administración - Config` como la configuración a aplicar en caso de cumplirse la política. Esta configuración especifica utilizar la *Logical Network* `Administracion`, asignada a la `VLAN 21` en los *switches*.

4.1.8. Aplicación del NAC al servidor OpenVPN

Con el objetivo de mantener un sistema único de autenticación, es necesario configurar el servidor RADIUS de FortiNAC para habilitar la autenticación de usuarios de VPN.

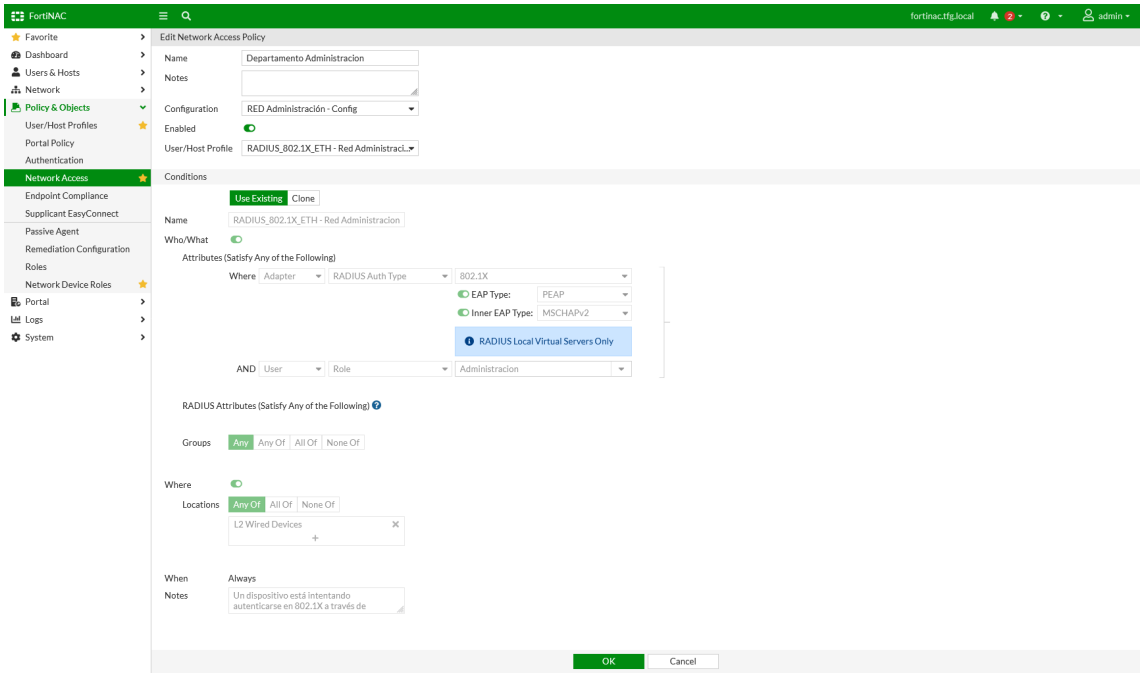


Figura 4.26: Captura de la política de acceso para los usuarios de Administración.

Configuración del cliente y servidor RADIUS

El primer aspecto a configurar es el servidor RADIUS. Esto ya se había realizado en los *switches*, pero ahora debe llevarse a cabo en el propio *router*. En este caso, se selecciona ppp como el servicio que podrá utilizar esta configuración, como se observa en la figura 4.27. De manera similar a la figura 4.21, se debe habilitar la conexión del cliente RADIUS del *router* principal y establecer la misma contraseña. En esta ocasión se utilizará `RADIUS` como contraseña y `None` como grupo de atributos que se enviarán en las respuestas RADIUS (*Attribute Group*).

Diseño de los perfiles de VPN de los departamentos

Con el objetivo de ubicar a los usuarios, se han creado varios perfiles de VPN en el servidor (figura 4.28), uno para cada departamento que requiere utilizar la VPN. Cada perfil lleva asignado el *pool* de IPs correspondiente, lo que permite aplicar reglas de firewall atendiendo al usuario tras la conexión.

Para que el servidor VPN identifique en qué perfil ubicar a cada usuario, se utilizará el parámetro RADIUS `Mikrotik-Group`[6], que permite indicar al servidor OpenVPN de MikroTik el **nombre** de un perfil de VPN al iniciar una conexión. Por lo tanto, es necesario crear un nuevo grupo de atributos en el menú mostrado en la figura 4.4, esta vez con el atributo `Mikrotik-Group` y `%ACCESS_VALUE%` como valor. Se denominará `MikroTik VPN` a este grupo.

Configuración de las redes lógicas en FortiNAC

Primero, se deben añadir las redes de VPN en FortiNAC (menú de la figura 4.24). Se les designará como `VPN Administracion` y `VPN Desarrollo`. A continuación, se debe asignar el identificador de VPN en el inventario a las nuevas redes lógicas de VPN. De

[6]https://help.mikrotik.com/docs/spaces/ROS/pages/328097/RADIUS

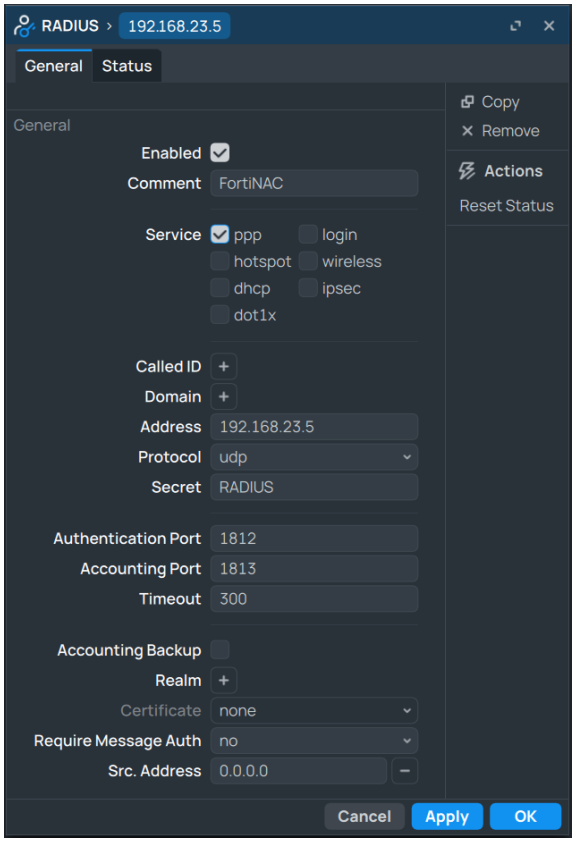


Figura 4.27: Configuración del cliente RADIUS en el *router* MikroTik.

manera similar a la configuración para la conexión por cable (figura 4.25), se asignarán en este caso los valores `31` y `32` respectivamente. Además, se seleccionará el nuevo grupo de parámetros `MikroTik VPN` en las redes lógicas de VPN. De este modo, se enviará el atributo necesario para seleccionar el perfil de VPN del usuario al router cuando las solicitudes de autenticación sean aceptadas.

Configuración de la Política de Acceso en FortiNAC

Al igual que en la conexión por cable, es necesario que FortiNAC asigne el perfil de VPN correspondiente a cada conexión. Para ello, se ha diseñado una nueva política de acceso, tomando como referencia la presentada en la figura 4.26.

```
1 Name: VPN - Red Administracion
```

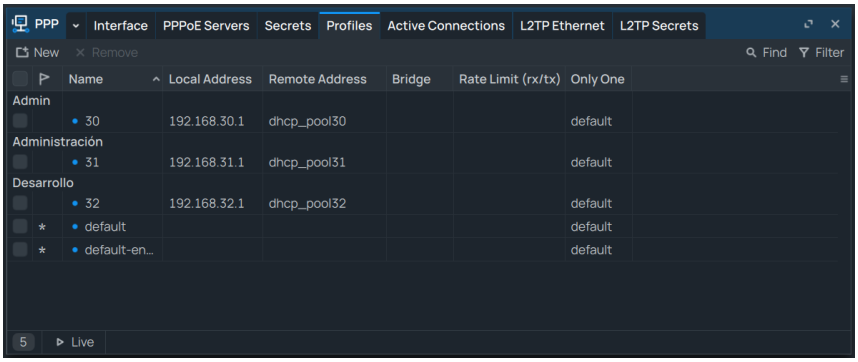


Figura 4.28: Perfiles de VPN creados en el servidor OpenVPN integrado en MikroTik.

```
Configuration: RED VPN Administracion - Config

Who/What: User -> Role = Administracion
Groups: Any
Where: AnyOf = L3 Wired Devices
When: Always
```

Fragmento 4.4: Definición de la política de acceso la red de VPN de administración.

```
Name: VPN - Red Desarrollo
Configuration: RED VPN Desarrollo - Config

Who/What: User -> Role = Desarrollo
Groups: Any
Where: AnyOf = L3 Wired Devices
When: Always
```

Fragmento 4.5: Definición de la política de acceso la red de VPN de desarrollo.

Como se puede apreciar en los fragmentos 4.4 y 4.5, la condición *Where* emplea `L3 Wired Devices` en lugar de `L2 Wired Devices`.

El *router* principal se encuentra en el grupo de dispositivos de capa tres, mientras que los *switches* están en el de capa dos. Esto permite que estas políticas únicamente se comprueben para conexiones de VPN, cuando las solicitudes RADIUS provienen del *router*.

Configuración adicional en el servidor OpenVPN

Tras la configuración anterior, FortiNAC enviará el atributo `Mikrotik-Group` junto al identificador de VLAN al router. RouterOS espera que este atributo sea el **nombre** del perfil de VPN, por lo que es necesario modificar el nombre de los perfiles para que coincidan con los identificadores de VLAN. Además, se recomienda agregar comentarios a los perfiles para poder identificarlos correctamente, como se puede observar en la figura 4.28.

4.1.9. Funcionamiento

Cuando un empleado de la organización, por ejemplo, un miembro del departamento de Administración, llega a su puesto de trabajo, su equipo corporativo ya está conectado físicamente al puerto de red Ethernet habilitado en su mesa. Este puerto, configurado en el *switch* MikroTik, requiere autenticación 802.1X antes de permitir cualquier comunicación en la red.

Al encender el equipo, el proceso de arranque de Windows inicia automáticamente. El usuario introduce sus credenciales corporativas (nombre de usuario y contraseña del dominio `tfg.local`) en la pantalla de inicio de sesión. Dado que el equipo ya está unido al dominio, el sistema valida las credenciales contra el controlador de dominio, el servidor `WINSERVER`.

El servicio *Wired AutoConfig* de Windows, habilitado mediante una una política de grupo (GPO), detecta que el puerto de red requiere autenticación 802.1X. Automáticamente, envía las credenciales del usuario que ha iniciado sesión al *switch*, que actúa como autenticador. El *switch* reenvía la solicitud de autenticación al servidor RADIUS de FortiNAC y verifica que el equipo esté registrado y que el usuario es válido.

FortiNAC aplica la política de acceso configurada para el departamento de administración. Esta política especifica que los usuarios con el rol `Administracion` deben ser

asignados a la red lógica `Administracion`, que está vinculada a la `VLAN 21` en el *switch*. El NAC envía al *switch* el atributo RADIUS correspondiente (`RFC_Vlan`) con el identificador de la `VLAN 21`. El *switch* recibe esta instrucción y configura el puerto para que el tráfico del equipo del trabajador pase exclusivamente por la `VLAN 21`.

Una vez asignada la VLAN, el equipo del trabajador obtiene acceso a los recursos de la red del departamento de administración, como el ERP. Las restricciones de acceso a estos servicios se gestionan desde el *router* Principal, que actúa también como *firewall* y controla a qué recursos puede acceder cada segmento de red. El trabajador puede utilizar ahora las aplicaciones y servicios necesarios para llevar a cabo sus tareas diarias, con la certeza de que su tráfico está aislado y protegido conforme a las políticas de la organización.

FortiNAC registra el evento de autenticación, la asignación de VLAN y cualquier cambio en el estado del dispositivo. Esta información está disponible en los *logs* del sistema, lo que permite a los administradores auditar el acceso y detectar cualquier actividad sospechosa. Si el trabajador desconecta su equipo o cierra sesión, FortiNAC detecta el evento y restablece el puerto del *switch* a la VLAN de registro (`VLAN 43`), dejando la interfaz lista y segura para la próxima conexión.

Este flujo garantiza que únicamente los empleados autorizados, utilizando equipos corporativos registrados, accedan a los recursos de la red de manera segura y controlada. Asimismo, la integración con el Directorio Activo y FortiNAC simplifica la gestión de usuarios y políticas, mejorando la eficiencia y la seguridad de la red corporativa.

4.2 Extensión del sistema NAC con soporte para dispositivos personales (BYOD)

Otro caso de uso comúnmente buscado en estos sistemas es el conocido como BYOD (*Bring Your Own Device*), que permite a los usuarios conectar sus dispositivos personales a la red. Esto puede representar un riesgo significativo si no se controla adecuadamente, ya que la seguridad de estos equipos no está garantizada. Por esta razón, los productos NAC ofrecen soluciones adaptadas a este propósito, que garantizan el cumplimiento de los requisitos de seguridad que desde la organización se hayan impuesto en los dispositivos finales antes de que puedan conectarse a la red.

Desde la organización se busca permitir la conexión de dispositivos personales a la red de la oficina. Sin embargo, estos equipos no tendrán acceso a los mismos recursos que los equipos corporativos. Asimismo, esta opción está contemplada únicamente para el personal del departamento de administración.

Aunque es posible en FortiNAC, GNS3 no soporta la simulación de redes WiFi, por lo que solo se considerará la conexión de equipos de trabajadores a través de cable Ethernet. Si se desea soportar la conexión de dispositivos móviles, también es factible mediante los agentes que FortiNAC proporciona para este fin.

Cuando un equipo personal de un usuario se conecte mediante cable a la red, no se asignará automáticamente a la VLAN que le corresponda. En su lugar, se requerirá seguir manualmente los pasos indicados en el portal de FortiNAC, procedimiento que no es necesario en los equipos de la organización.

De este modo, el portal de FortiNAC funcionará como un portal cautivo, filtrando el acceso de los dispositivos y usuarios autorizados y no autorizados.

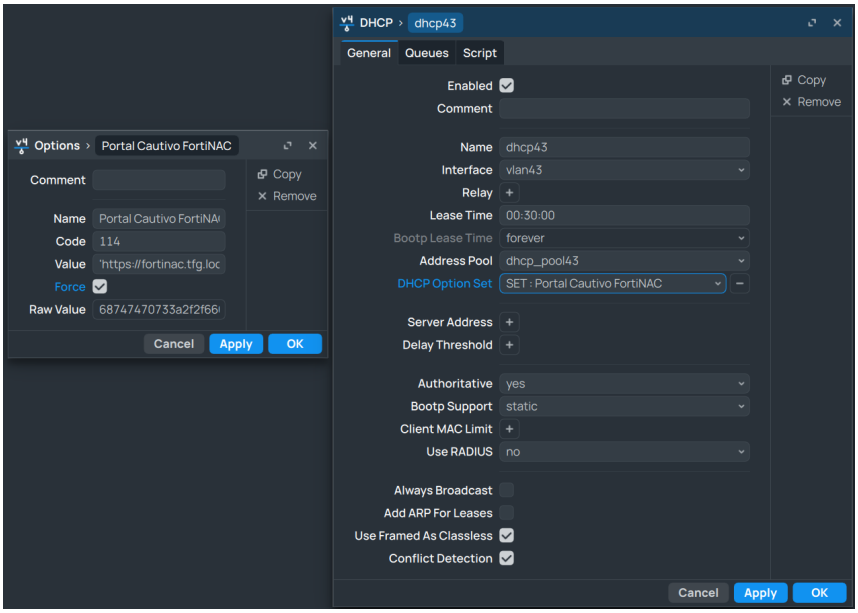


Figura 4.29: Configuración del servidor DHCP en el router MikroTik para la VLAN 43.

4.2.1. Configuración del Portal Cautivo de FortiNAC

De acuerdo con el estándar `RFC 8910`[7], se incluye el portal de FortiNAC como la dirección del portal cautivo (figura 4.29) en los *DHCP Options* que se asignarán a los equipos que soliciten una dirección IP en la red `192.168.43.0/24` (Registro).

Los dispositivos, al conectarse a una red, comprueban el acceso a internet mediante varios métodos. Generalmente hacen alguna peticion a una página externa dedicada a este propósito, como `captive.apple.com` o `www.msftconnecttest.com`. Cuando no tienen conexión a internet suelen asumir que están detrás de un portal cautivo, y habitualmente verifican los atributos DHCP que recibieron al solicitar la IP. Para los equipos virtuales Windows utilizados en este trabajo, con esta configuración eran correctamente redirigidos al portal cautivo de FortiNAC.

Gracias a las configuraciones realizadas para el objetivo 1 (apartado 4.1) el portal de ejemplo que incluye FortiNAC con su instalación no requiere grandes modificaciones para permitir que los usuarios puedan utilizar sus propios dispositivo. Con la instalación de FortiNAC se incluyen por defecto tres portales que pueden distingirse en la figura 4.30:

- ***Portal***. El principal, que incluye todos los pasos que pueden ser necesarios para una conexión. Es útil a modo de ejemplo para crear otros portales.
- ***Registration Portal***. Un pequeño portal centrado en el registro de usuarios y la autenticación de usuarios. Es el que se ha utilizado para conseguir el BYOD.
- ***Restricted Portal***. Un pequeño portal utilizado para los equipos que se han registrado pero ha fallado una política. Incluye pasos de resolución de problemas.

En el caso de un portal de este tipo, es imprescindible utilizar HTTPS para garantizar que el envío de usuarios y contraseñas al FortiNAC se realice de manera segura. Para simplificar el proceso, se ha empleado el certificado autofirmado de FortiNAC, lo que provocará que el navegador muestre una alerta al acceder al portal en los equipos.

[7] https://www.rfc-editor.org/rfc/rfc8910.html

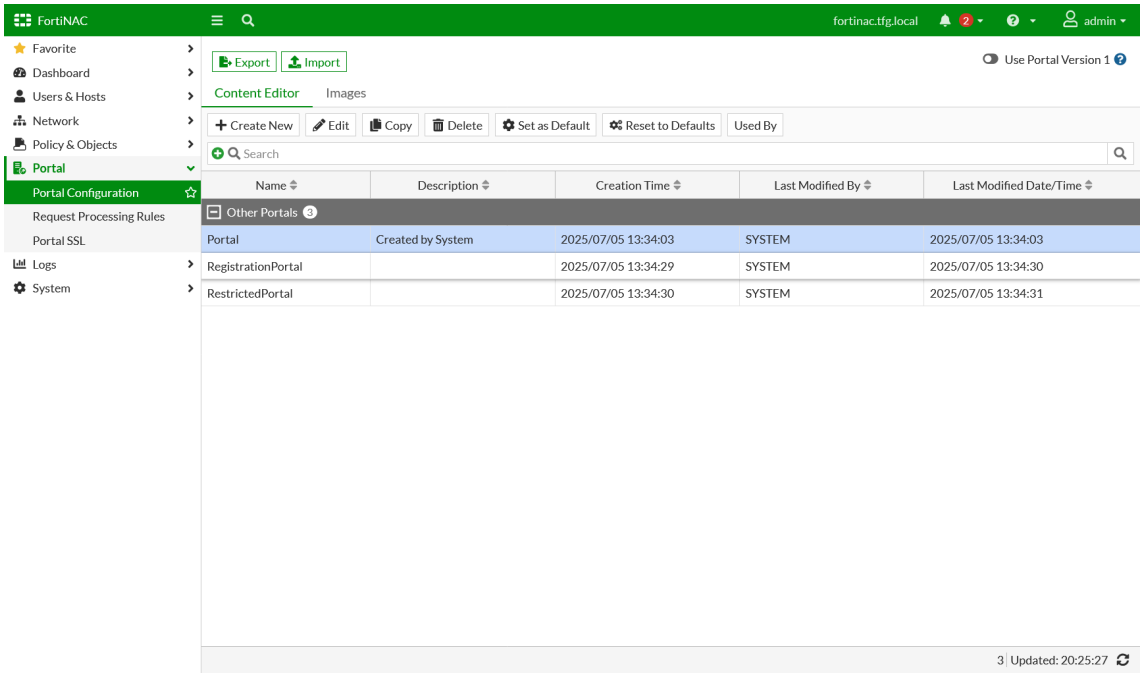


Figura 4.30: Apartado de gestión de todos los portales web de FortiNAC.

Esta situación no es ideal en un entorno de producción, aunque resulta aceptable en un entorno de pruebas.

Además de crear o eliminar portales según los usos requeridos, también es posible editar aquellos que proporciona FortiNAC por defecto. En la figura 4.31 puede observarse la pestaña de estilos del portal *Default*. En esta página, es posible modificar los aspectos estéticos de cada portal, como los componentes que se mostrarán en caso de éxito, error, entre otros. Asimismo, se pueden editar las imágenes y los colores para que coincidan con la identidad visual de la organización.

Al hacer clic en la pestaña de *Configuration* en la figura 4.31 es redirigido al menú de la figura 4.32, donde es posible modificar los aspectos técnicos del portal. Es fundamental verificar que la fuente de datos esté configurada en LDAP, para poder aprovechar la conexión con el Directorio Activo establecida en el objetivo 1 de este proyecto y que FortiNAC pueda comprobar las credenciales de los usuarios. Esta verificación puede realizarse en el apartado de *Standard User Login Form* de la figura 4.32. Al seleccionar el portal que utilizarán los equipos para conectarse a la red, es fundamental definir la URL correcta en el *OptionSet* configurado en la figura 4.29. Para las pruebas de BYOD se ha establecido la siguiente URL: `https://fortinac.tfg.local/RegistrationPortal`, la cual redirigirá a los dispositivos al portal de registro mencionado anteriormente.

4.2.2. Constitución de la nueva red de BYOD

Se ha creado una nueva red (tabla 4.2) con el objetivo de ubicar los equipos personales de los trabajadores. En esta nueva red, los usuarios autorizados cuentan únicamente con acceso a internet y a la impresora de administración.

VLAN	Información	Direccionamiento	Gateway
24	Red de BYOD	192.168.24.0/24	192.168.24.1

Tabla 4.2: Red de BYOD añadida para ubicar los equipos personales de los trabajadores.

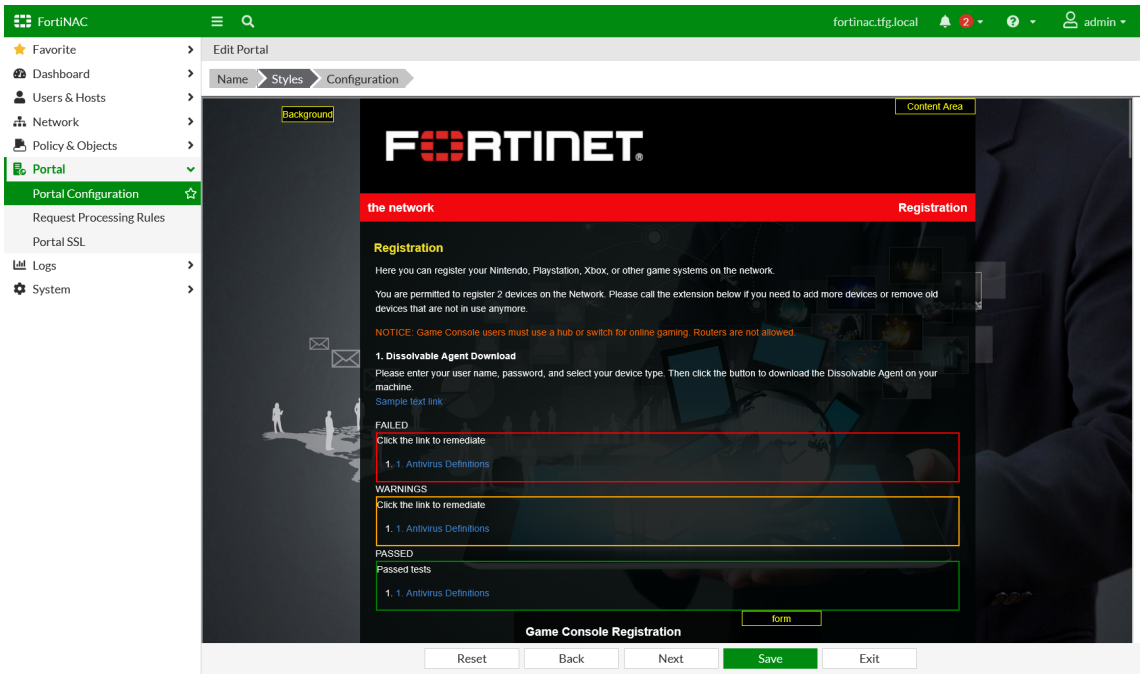


Figura 4.31: Pestaña de edición de estilos del portal *Default* de FortiNAC.

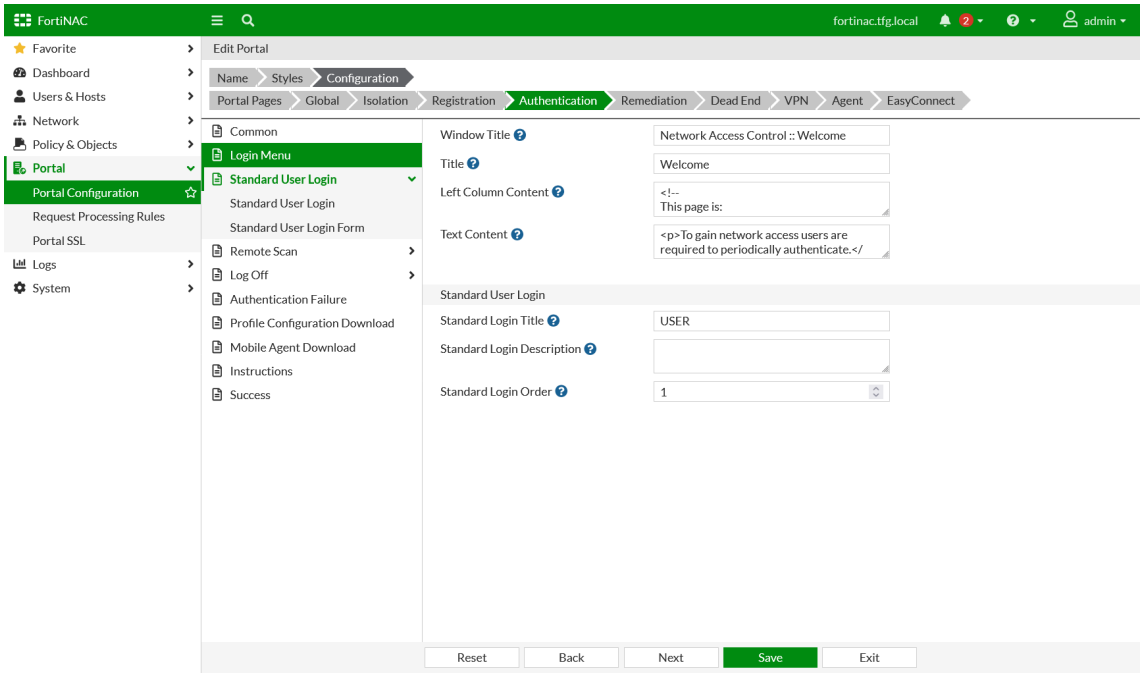


Figura 4.32: Edición de la pestaña de *Authentication* del portal *Default* de FortiNAC.

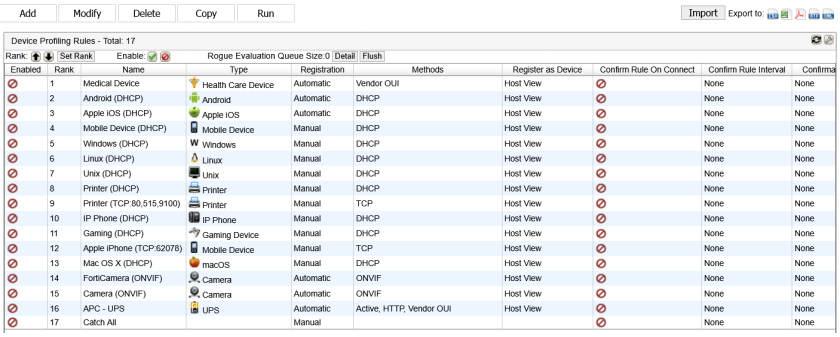


Figura 4.33: Lista de plantillas de perfilado de dispositivos de FortiNAC.

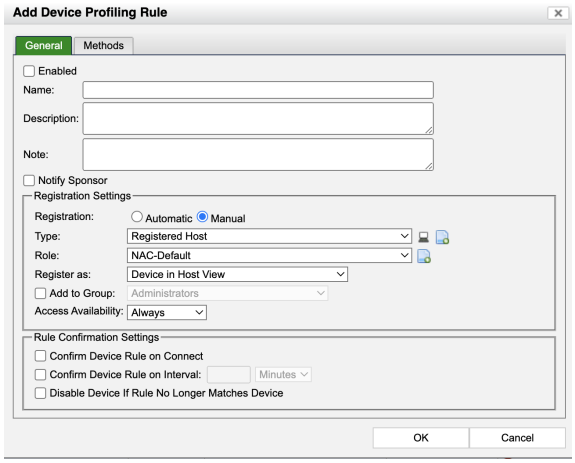


Figura 4.34: Menú de configuración de una nueva plantilla de perfilado en FortiNAC.

4.2.3. Configuración de la impresora de Administración

Para ilustrar el acceso limitado de esta política, se ha simulado una impresora en el departamento de Administración. La impresora se ha configurado en la dirección IP `192.168.21.2` y ha sido registrada en FortiNAC para garantizar una protección adecuada. De forma similar a lo expuesto en el apartado 3.3 (Tecnología Utilizada) sobre el servicio GIT y ERP, la impresora opera como un servidor Debian con una interfaz web.

Con el objetivo de asegurar el acceso de la impresora a la red, se ha utilizado la función de perfilado que integra FortiNAC, la cual permite reconocer dispositivos que no pueden registrarse en el NAC mediante otros métodos, como 802.1X y el portal web.

En el menú de *Device Profiling Rules* (figura 4.33) se ha añadido un nuevo perfil específico para la impresora, el cual permitirá añadir las impresoras al grupo *Printer* (definido en el atributo *Add to Group* de la figura 4.34). Los métodos de perfilado asignados al perfil son los siguientes:

- **TCP**. Comprueba que los puertos `22` y `80` sean accesibles.
- **SSH**. Se han introducido las credenciales SSH del servidor Debian para que FortiNAC trate de iniciar sesión mediante SSH.

De este modo, cuando FortiNAC detecte un dispositivo que cumpla con los requisitos anteriores, lo añadirá automáticamente al grupo *Printer*, lo que posibilita la creación de políticas específicas para dichos dispositivos. Es fundamental ser meticuloso al seleccionar los métodos de perfilado para dificultar la suplantación de estos dispositivos.

```
Name: BYOD_ETH_Administracion
Configuration: RED BYOD Administracion - Config

Who/What: Where -> Adapter -> Authentication Type = WebAuth
    AND User -> Role = Administracion
Groups: Any
Where: AnyOf = L2 Wired Devices
When: Always
```

Fragmento 4.6: Definición de la política de BYOD de los usuarios autenticados mediante el portal de registro de FortiNAC.

Para finalizar la configuración de la impresora, solo es necesario definir en una política la ubicación de los dispositivos del grupo *Printer* como la impresora. En un entorno real, se recomienda asignar una red específica para estos dispositivos. No obstante, en este caso, se ubicará en la red de Administración, ya que la organización solo dispone de una impresora.

4.2.4. Creación de la política en FortiNAC

Al igual que en la autenticación 802.1X, es necesario definir en una política las condiciones requeridas para el acceso a la red BYOD. Tomando nuevamente como ejemplo la figura 4.26, se puede derivar la política del fragmento 4.6, esta vez en el menú *Portal Policy*:

La configuración de `RED BYOD Administracion - Config` lleva asignada la *Logical Network* `BYOD`.

4.2.5. Funcionamiento

Cuando un usuario conecte su equipo personal a la toma de red, el equipo recibirá una dirección IP de la red de registro (`192.168.43.0/24`) sin conexión a Internet ni a la red interna. Al abrir un navegador de Internet, se cargará la página del portal de FortiNAC (figura 4.35). El portal guiará a los usuarios en la descarga del *Dissolvable Agent*, un ejecutable que permite a FortiNAC verificar el equipo. No se ha definido ninguna comprobación adicional hasta el momento, por lo que, tras ejecutarlo, el portal avanzará al siguiente paso: la autenticación. En esta fase, se deben introducir las credenciales de la empresa, que FortiNAC consultará en el Directorio Activo para su validación e intentará aplicar las políticas definidas (en este caso, solo la anterior).

Si el usuario pertenece al departamento de Administración, se aplicará la política (fragmento 4.6) y FortiNAC dará la orden al *switch* de colocar el equipo en la red de BYOD (`VLAN 24`). Si el usuario no pertenece al departamento de Administración, el equipo permanecerá en la red `Sin Salida` (`VLAN 42`).

4.3 Integración de evaluación de postura de seguridad en el sistema NAC

Lamentablemente, no se dispuso del tiempo necesario para completar este último objetivo, ya que la licencia de prueba de dos meses concedida por Fortinet había expirado para cuando se llegó a este punto. No obstante, se puede definir lo que se habría im-

Figura 4.35: Panel de bienvenida del portal de FortiNAC al iniciar el navegador de un equipo sin registrar.

plementado de haberse contado con la oportunidad, puesto que se planificó al inicio del proyecto y las características estaban adecuadamente especificadas.

La evaluación de la postura de seguridad es un componente crítico en los sistemas NAC, especialmente en entornos donde se permite el uso de dispositivos personales (BYOD). Este apartado busca garantizar que los dispositivos que acceden a la red corporativa cumplan con unos requisitos mínimos de seguridad, como la presencia de software antivirus actualizado, parches del sistema operativo, y configuraciones seguras. La integración de esta evaluación en el sistema NAC permite no solo autenticar y autorizar el acceso, sino también verificar el estado de seguridad de los dispositivos antes de concederles permisos en la red.

FortiNAC cuenta con diversos agentes para los diferentes escenarios y dispositivos a los que es posible enfrentarse:

- ***Dissolvable Agent.*** Se descarga desde el portal de registro de FortiNAC, se instala en el dispositivo para realizar las comprobaciones, y se elimina tras haber comprobado el cumplimiento de los requisitos. Para comprobar ciertos aspectos puede ser necesario ejecutarlo como administrador. Está disponible para Windows, MacOS y Linux.

- ***Persistent Agent.*** Este agente está pensado para permanecer instalado y en ejecución en los equipos donde se despliega. Las capacidades son las mismas que las del *Dissolvable Agent*, con la ventaja de permanecer instalado en el dispositivo y realizar escanéos contínuos. Permite el envío de mensajes a los usuarios por parte de los administradores y puede comunicar el estado del equipo al usuario mediante notificaciones. Normalmente se configura en los equipos de la empresa distribuyéndolo mediante una política de grupo. Está disponible para Windows, MacOS y Linux.

- ***Mobile Agent.*** Permite a FortiNAC obtener información acerca del estado del dispositivo móvil. Este agente permanece instalado en el dispositivo, y está disponible para Android e IOS.

- ***Passive Agent.*** Este agente permite registrar los equipos en FortiNAC y asociarlos al usuario que ha iniciado sesión. Lo que lo diferencia del resto es su forma de ejecutarse, pues no se instala en el ordenador, sino que es servido a través de la red por el propio FortiNAC al equipo cuando un usuario inicia sesión. Se ejecuta de forma temporal y transparente para el usuario, realizando un análisis del equipo y comprobando el cumplimiento de los requisitos de seguridad. Este agente únicamente puede utilizarse en Windows.

4.3.1. Requisitos a implementar y elección del agente

Este objetivo se ha formulado considerando los equipos de los empleados, permitiendo su uso mientras se garantiza la seguridad de la red interna. Por lo tanto, los requisitos que se contemplan imponer son los siguientes:

- El equipo cuenta con un sistema antivirus actualizado.
- El dispositivo utiliza un sistema operativo moderno.

Para garantizar que los equipos personales de los empleados cumplen con los requisitos establecidos, se utilizará el *Dissolvable Agent*, ya que es el que mejor se adapta a las necesidades de la organización para la política de BYOD. Este agente puede ser utilizado independientemente del sistema operativo del usuario, ya que es compatible con Linux, Windows y MacOS. Además, a diferencia de otros agentes, el *Dissolvable Agent* no requiere que el equipo esté unido al dominio.

4.3.2. Configuración de FortiNAC

Para que el *Dissolvable Agent* conozca los requisitos de seguridad que debe verificar, es necesario crear una política dentro de *Policy & Objects* → *Endpoint Compliance*. Esta interfaz permite crear tantas políticas como se necesiten, generalmente una para cada sistema operativo que se desee soportar.

Se ha diseñado la primera política, a la que se ha denominado `Rogue Host`, visible en el fragmento 4.7. Esta política será aplicada por el *Dissolvable Agent* a los equipos externos a la organización. En la línea 19 del fragmento 4.7 se ha especificado que solo se registre un dispositivo cuando este cumpla todos los requisitos de seguridad.

```
1  Name: Rogue Host - Endpoint Compliance
2  User/Host Profile:
3      Name: RogueHost - Profile
4      Where (Location): Network-Security
5      Who/What by Attribute:
6          Host:
7              Type: Rogue
8              Persistent Agent: No
9      Endpoint Compliance Configuration:
10         Name: RogueHost - Configuration
11         Scan:
12             Name: Scan
13             Scan:
14                 General:
15                     Name: RogueHost - Scan
16                     Remediation: On Failure
17                     Agent Order of Operations:
18                         Scan before Registering: Yes
19                         If the scan fails: Do not Register, Remediate
20                 Windows:
```

```
                Operating-System:
                    Windows-10: Yes
                    Windows-10-x64: Yes
                    Windows-11: Yes
                Anti-Virus:
                    AVG-2017: Yes
                    AVG-2018: Yes
                    Avast-Business-Security: Yes
                    Avast-Internet-Security: Yes
                    ...
            MacOS:
                Anti-Virus:
                    AVG-2017: Yes
                    AVG-2018: Yes
                    Avast-Business-Security: Yes
                    Avast-Internet-Security: Yes
                    ...
            Linux:
                Anti-Virus:
                    Clam-AV: Yes
                    BitDefender: Yes
                    Comodoro-Antivirus: Yes
                    Eset-NOD32: Yes
                    ...
        Agent:
            Windows: Latest Dissolvable Agent
            Mac-OS-X: Latest Dissolvable Agent
            Linux (x86_64): Latest Dissolvable Agent
            Android: Latest Mobile Agent
```

Fragmento 4.7: Definición de la política *Endpoint Compliance* para los dispositivos BYOD.

La política anterior (fragmento 4.7) funcionará en conjunto con la política de acceso del portal de registro establecida en la sección 4.2, de acuerdo con lo señalado en el fragmento 4.6. Esta última especifica al *Dissolvable Agent* los requisitos que debe cumplir el equipo, que anteriormente estaban vacíos.

A su vez, en el menú de *Inventory*, en la definición de las redes lógicas y sus *Access Value* (observado en la figura 4.25), se ha configurado la red *Quarantine* en *Enforce* con su *Access Value* en 41. Esto permitirá que FortiNAC traslade automáticamente a esta red los equipos que no cumplan con los requisitos, para que se realicen los cambios necesarios hasta satisfacerlos. Esta red cuenta únicamente con conexión a Internet, lo cual es suficiente para descargar las soluciones de antivirus necesarias o actualizar los sistemas operativos.

4.3.3. Funcionamiento

Cuando un usuario conecte su equipo personal a la red, el *switch* tendrá dicho puerto en la `VLAN 43`, que únicamente permite el contacto con el NAC. El sistema operativo verificará que se encuentra detrás de una red sin acceso a Internet, instando al usuario a seguir los pasos del panel de registro de FortiNAC.

El portal del NAC guiará al usuario a través del proceso de registro, solicitando la descarga del ejecutable del *Dissolvable Agent*. Este ejecutable tendrá la función de verificar el estado del equipo y el cumplimiento de los requisitos de seguridad. Una vez definidos cuáles son estos requisitos, se podrá determinar si se cumplen o no.

Si el equipo no cumple con los requisitos de seguridad, FortiNAC lo moverá a la `VLAN 41` (red de cuarentena) para corregirlo. El agente descargado permanecerá abierto mostrando los fallos, y se podrá repetir la comprobación pulsando el botón correspondiente.

Si el equipo cumple con los requisitos de seguridad, el agente se cerrará y el portal web avanzará al apartado de a autenticación, donde el usuario ingresará sus credenciales de la organización. Si son correctas, el proceso habrá finalizado finalizará y el equipo estará en la `VLAN 24`, destinada para los equipos BYOD del departamento de administración.

CAPÍTULO 5
Conclusiones

En conclusión, este Trabajo de Fin de Grado ha permitido analizar la problemática de la gestión del acceso en redes corporativas y comprobar la relevancia de los sistemas NAC como pieza clave dentro de las arquitecturas modernas de seguridad. El repaso realizado en el Estado del Arte mostró la evolución desde medidas tradicionales como el filtrado MAC o la segmentación estática, hasta enfoques más sólidos como Zero Trust o Network Access Control y las soluciones comerciales actuales, lo que aportó una base teórica fundamental para contextualizar el trabajo.

El funcionamiento de un NAC puede resumirse en tres pilares: visibilidad de los dispositivos conectados, segmentación dinámica de la red y respuesta ante comportamientos anómalos. Mediante protocolos como 802.1X y RADIUS, el servicio NAC autentica a usuarios y equipos y, según las políticas definidas, asigna de manera dinámica la VLAN correspondiente. Con ello, el acceso ya no depende de la ubicación física, sino de la identidad y el estado del dispositivo, reforzando la seguridad y la movilidad en el entorno corporativo.

A partir de aquí, se aprecia una clara relación colaborativa entre los sistemas NAC y los *firewall*: mientras el NAC determina a qué VLAN debe incorporarse un dispositivo, son *routers*, *switches* o cortafuegos los que implementan las restricciones entre segmentos y son los responsables de habilitar la autenticación. En este sentido, el NAC actúa como un coordinador del perímetro "físico" de la red, un perímetro que se vuelve cada vez más difuso por la movilidad, el teletrabajo y las políticas BYOD de las organizaciones modernas.

Durante el desarrollo del proyecto se presentaron diversos desafíos. Se había estimado que los dos meses de licencia de FortiNAC serían suficientes, pero los requisitos de instalación y la complejidad de algunas configuraciones consumieron más tiempo del previsto, lo que obligó a recurrir tanto a documentación extensa como al soporte oficial del producto. Además, aunque en la planificación inicial se descartó el uso de un Directorio Activo para simplificar el escenario, finalmente resultó imprescindible para continuar, lo que supuso replantear parte del diseño original.

A nivel de aprendizaje, este trabajo ha consolidado conocimientos adquiridos en asignaturas previas: en RCO, la configuración de routers y la comprensión práctica de protocolos de red, y en SRE, la visión global de lo que implica administrar una red y la importancia de la seguridad como eje central. Sobre esa base, el TFG ha permitido profundizar en nuevas tecnologías como FortiNAC, la gestión avanzada de VLANs, el uso de RADIUS como servicio de autenticación, la configuración de *routers*, *switches* y *firewalls*, la integración con un Directorio Activo y el control de accesos mediante 802.1X, logrando un resultado que intenta acercarse al ámbito profesional.

Si bien se alcanzaron los objetivos principales, no se pudo completar totalmente la integración de la evaluación de postura de seguridad. Asimismo, en un entorno más completo y sin las limitaciones temporales derivadas de la licencia, así como por la falta de soporte para la simulación de WiFi, el proyecto podría haberse ampliado con la gestión de eventos o con la simulación de escenarios de WiFi para BYOD.

En definitiva, este TFG pone de manifiesto que los sistemas NAC no solo incrementan la seguridad de la red, sino que también fortalecen la resiliencia organizativa, aportando flexibilidad en la gestión de accesos y visibilidad sobre los dispositivos conectados. Además, se integran de forma natural en arquitecturas Zero Trust y Network Access Control, donde la verificación continua de la identidad del equipo conectado y la segmentación dinámica son requisitos indispensables. Más allá de lo técnico, el proyecto demuestra cómo los NAC se han convertido en una herramienta estratégica que redefine el concepto de perímetro de red, adaptándose a un entorno en el que los usuarios tienen movilidad, los dispositivos personales conviven con los corporativos y las amenazas evolucionan constantemente. En este sentido, los NAC no son únicamente una capa de seguridad más, sino un componente esencial para garantizar la continuidad del negocio y la protección de los activos críticos en un mundo cada vez más interconectado.

Bibliografía

[1] «What is zero trust?», Red Hat. (2022), dirección: https://www.redhat.com/en/topics/security/what-is-zero-trust (visitado 01-02-2025).

[2] J. Flores, V. Ramos, R. Lozada y T. Flores, «Analysis of solutions of network access control to improve in and out securities on corporative networks», en *2017 CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON)*, 2017, págs. 1-5. DOI: 10.1109/CHILECON.2017.8229518.

[3] W. R. Simpson y K. E. Foltz, «Network segmentation and zero trust architectures», en *Lecture Notes in Engineering and Computer Science, Proceedings of the World Congress on Engineering (WCE)*, 2021, págs. 201-206.

[4] Fortinet, *Zero Trust Access For Dummies, 3rd Fortinet Special Edition*, 3rd. Fortinet Press, 2023.

[5] «FortiNAC Data Sheet», Fortinet Inc. (2024), dirección: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortinac.pdf (visitado 06-04-2025).

[6] «Cisco Identity Services Engine Data Sheet», Cisco Systems, Inc. (2024), dirección: https://www.cisco.com/c/en/us/products/security/identity-services-engine/ise-ds.html (visitado 08-04-2025).

[7] «Aruba ClearPass Policy Manager Data Sheet», Hewlett Packard Enterprise. (2025), dirección: https://www.hpe.com/psnow/doc/PSN1009432804ATEN (visitado 08-04-2025).

[8] «OpenNAC Data Sheet», Open Cloud Factory. (2025), dirección: https://doc-opennac.opencloudfactory.com/1.2.3/general/index.html (visitado 10-05-2025).

[9] «PacketFence Overview», Inverse Inc. (2025), dirección: https://packetfence.org/about.html (visitado 14-04-2025).

[10] «FortiNAC 7.6.0 Administration Guide», Fortinet Inc. (2025), dirección: https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/ (visitado 08-08-2025).

[11] «RouterOS Documentation», MikroTik. (2025), dirección: https://help.mikrotik.com/docs/spaces/ROS/pages/328059/RouterOS (visitado 02-08-2025).

APÉNDICE A

Registros de FortiNAC en una petición de autenticación 802.1X de un equipo Windows 10

En el fragmento A.1 se pueden comprobar los *logs* extraídos de FortiNAC al realizar una solicitud de inicio de sesión en un ordenador con Windows 10 unido al dominio. Estos *logs* abarcan desde la recepción de la solicitud hasta el cambio de VLAN del *switch*, incluyendo la autenticación del usuario en el Directorio Activo y la evaluación de políticas.

De las líneas 2 a 15 se pueden observar los atributos de la solicitud RADIUS realizada por el `Switch-Administracion`.

Entre las líneas 160 y 172, se pueden observar algunos de los atributos enviados por el servicio RADIUS de FortiNAC al `Switch-Administracion`. En la línea 170, se incluye el atributo que indica que se debe asignar la `VLAN 21` en el puerto donde se encuentra conectado el usuario.

```
1  (23) Received Access-Request Id 199 from 192.168.23.1:40750 to
       192.168.23.5:1812 length 230
2  (23)   Framed-MTU = 1400
3  (23)   NAS-Port-Type = Ethernet
4  (23)   Called-Station-Id = "0C-BB-3A-12-00-04"
5  (23)   Calling-Station-Id = "0C-36-98-C3-4A-7D"
6  (23)   Service-Type = Framed-User
7  (23)   EAP-Message = 0x0207002e1900170303002300000...
8  (23)   Message-Authenticator = 0x426eeb3c6a0159e61afa45d42ce819f7
9  (23)   User-Name = "TFG\\administracion"
10 (23)   Acct-Session-Id = "02005086"
11 (23)   NAS-Port-Id = "ether5"
12 (23)   State = 0x304f1a1d3648030e1e61187919fc783e
13 (23)   EAP-Key-Name = 0x00
14 (23)   NAS-Identifier = "Switch-Administracion"
15 (23)   NAS-IP-Address = 192.168.0.3
16 (23) Restoring &session-state
17 (23)   &session-state:Hint = "34587c7f-a986-46f0-9c5f-04b347133f54"
18 (23)   &session-state:Tmp-String-1 := "request"
19 (23)   &session-state:Framed-MTU = 1180
20 (23)   &session-state:TLS-Session-Information = "(TLS) PEAP - recv TLS 1.3
       Handshake, ClientHello"
21 (23)   &session-state:TLS-Session-Information = "(TLS) PEAP - send TLS 1.2
       Handshake, ServerHello"
22 (23)   &session-state:TLS-Session-Information = "(TLS) PEAP - send TLS 1.2
       Handshake, Certificate"
```

```
(23)   &session-state:TLS-Session-Information = "(TLS) PEAP - send TLS 1.2 Handshake, ServerKeyExchange"
(23)   &session-state:TLS-Session-Information = "(TLS) PEAP - send TLS 1.2 Handshake, ServerHelloDone"
(23)   &session-state:TLS-Session-Information = "(TLS) PEAP - recv TLS 1.2 Handshake, ClientKeyExchange"
(23)   &session-state:TLS-Session-Information = "(TLS) PEAP - recv TLS 1.2 Handshake, Finished"
(23)   &session-state:TLS-Session-Information = "(TLS) PEAP - send TLS 1.2 ChangeCipherSpec"
(23)   &session-state:TLS-Session-Information = "(TLS) PEAP - send TLS 1.2 Handshake, Finished"
(23)   &session-state:TLS-Session-Cipher-Suite = "ECDHE-RSA-AES128-GCM-SHA256"
(23)   &session-state:TLS-Session-Version = "TLS 1.2"
(23)   &session-state:User-Name := "TFG\\administracion"
(23)   &session-state:MS-MPPE-Send-Key += 0x3abee034f1b2c6909c657e31ca4d89c7
(23)   &session-state:MS-MPPE-Recv-Key += 0xf80ccf46aba68e51cdf010e9fdcb0aea
(23)   &session-state:REST-HTTP-Status-Code += 200
(23)   &session-state:Tunnel-Type += VLAN
(23)   &session-state:Tunnel-Private-Group-Id += "21"
(23)   &session-state:Tunnel-Medium-Type += IEEE-802
(23) # Executing section authorize from file /etc/raddb/radiusd.conf
(23)   authorize {
(23)     if (!EAP-Message) {
(23)     if (!EAP-Message)  -> FALSE
(23)     if (!&session-state:Hint && !&request:Fortinet-Tenant-Identification) {
(23)     if (!&session-state:Hint && !&request:Fortinet-Tenant-Identification)  -> FALSE
(23)     if (&session-state:Tmp-String-9) {
(23)     if (&session-state:Tmp-String-9)  -> FALSE
(23)     if ( &request:Fortinet-Tenant-Identification ) {
(23)     if ( &request:Fortinet-Tenant-Identification )  -> FALSE
(23)     if (!&session-state:Tmp-String-1) {
(23)     if (!&session-state:Tmp-String-1)  -> FALSE
(23)     policy filter_username {
(23)       if (&User-Name) {
(23)       if (&User-Name)  -> TRUE
(23)       if (&User-Name)  {
(23)         if (&User-Name =~ / /) {
(23)         if (&User-Name =~ / /)  -> FALSE
(23)         if (&User-Name =~ /@[^@]*@/ ) {
(23)         if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(23)         if (&User-Name =~ /\.\./ ) {
(23)         if (&User-Name =~ /\.\./ )  -> FALSE
(23)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))  {
(23)         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/))  -> FALSE
(23)         if (&User-Name =~ /\.$/)  {
(23)         if (&User-Name =~ /\.$/)  -> FALSE
(23)         if (&User-Name =~ /@\./)  {
(23)         if (&User-Name =~ /@\./)  -> FALSE
(23)       } # if (&User-Name) = notfound
(23)     } # policy filter_username = notfound
(23)     [preprocess] = ok
(23) suffix: Checking for suffix after "@"
(23) suffix: No '@' in User-Name = "TFG\administracion", looking up realm NULL
(23) suffix: No such realm "NULL"
(23)     [suffix] = noop
(23) ntdomain: Checking for prefix before "\"
(23) ntdomain: Looking up realm "TFG" for User-Name = "TFG\administracion"
(23) ntdomain: No such realm "TFG"
(23)     [ntdomain] = noop
(23)     update control {
```

```
78 (23)       &Proxy-To-Realm := LOCAL
79 (23)     } # update control = noop
80 (23)     [mschap] = noop
81 (23)     if (!EAP-Message) {
82 (23)     if (!EAP-Message)  -> FALSE
83 (23)     else {
84 (23)       if (User-Name && Calling-Station-Id && User-Name =~ /^([0-9a-fA-F
    ]{2}[:]?){5}[0-9a-fA-F]{2}$/ ) {
85 (23)       if (User-Name && Calling-Station-Id && User-Name =~ /^([0-9a-fA-F
    ]{2}[:]?){5}[0-9a-fA-F]{2}$/ )  -> FALSE
86 (23) eap-DefaultConfig: Peer sent EAP Response (code 2) ID 7 length 46
87 (23) eap-DefaultConfig: Continuing tunnel setup
88 (23)       [eap-DefaultConfig] = ok
89 (23)     } # else = ok
90 (23)     [chap] = noop
91 (23)     [logintime] = noop
92 (23)   } # authorize = ok
93 (23) Found Auth-Type = EAP-DEFAULTCONFIG
94 (23) # Executing group from file /etc/raddb/radiusd.conf
95 (23)   Auth-Type EAP-DEFAULTCONFIG {
96 (23) eap-DefaultConfig: Finished EAP session with state 0x304f1a1d3648030e
97 (23) eap-DefaultConfig: Previous EAP request found for state 0x304f1a1d3648030e
    , released from the list
98 (23) eap-DefaultConfig: Peer sent packet with method EAP PEAP (25)
99 (23) eap-DefaultConfig: Calling submodule eap_peap to process data
100 (23) eap_peap: (TLS) EAP Done initial handshake
101 (23) eap_peap: Session established.  Decoding tunneled attributes
102 (23) eap_peap: PEAP state send tlv success
103 (23) eap_peap: Received EAP-TLV response
104 (23) eap_peap: Success
105 (23) eap-DefaultConfig: Sending EAP Success (code 3) ID 7 length 4
106 (23) eap-DefaultConfig: Freeing handler
107 (23)     [eap-DefaultConfig] = ok
108 (23)   } # Auth-Type EAP-DEFAULTCONFIG = ok
109 (23) # Executing section post-auth from file /etc/raddb/radiusd.conf
110 (23)   post-auth {
111 (23)     if (&session-state:Tmp-String-8) {
112 (23)     if (&session-state:Tmp-String-8)  -> FALSE
113 (23)     if (!EAP-Type || (EAP-Type != "TTLS" && EAP-Type != "PEAP" && EAP-Type
     != "TEAP")) {
114 (23)     if (!EAP-Type || (EAP-Type != "TTLS" && EAP-Type != "PEAP" && EAP-Type
     != "TEAP"))  -> FALSE
115 (23)     [exec] = noop
116 (23)     policy remove_reply_message_if_eap {
117 (23)       if (&reply:EAP-Message && &reply:Reply-Message) {
118 (23)       if (&reply:EAP-Message && &reply:Reply-Message)  -> FALSE
119 (23)       else {
120 (23)         [noop] = noop
121 (23)       } # else = noop
122 (23)     } # policy remove_reply_message_if_eap = noop
123 (23)     update {
124 (23)       &reply::Hint += &session-state:Hint[*] -> '34587c7f-a986-46f0-9c5f
    -04b347133f54'
125 (23)       &reply::Tmp-String-1 += &session-state:Tmp-String-1[*] -> 'request'
126 (23)       &reply::Framed-MTU += &session-state:Framed-MTU[*] -> 1180
127 (23)       &reply::TLS-Session-Information += &session-state:TLS-Session-
    Information[*] -> '(TLS) PEAP - recv TLS 1.3 Handshake, ClientHello'
128 (23)       &reply::TLS-Session-Information += &session-state:TLS-Session-
    Information[*] -> '(TLS) PEAP - send TLS 1.2 Handshake, ServerHello'
129 (23)       &reply::TLS-Session-Information += &session-state:TLS-Session-
    Information[*] -> '(TLS) PEAP - send TLS 1.2 Handshake, Certificate'
130 (23)       &reply::TLS-Session-Information += &session-state:TLS-Session-
    Information[*] -> '(TLS) PEAP - send TLS 1.2 Handshake, ServerKeyExchange'
```

```
131 (23)        &reply::TLS-Session-Information += &session-state:TLS-Session-
    Information[*] -> '(TLS) PEAP - send TLS 1.2 Handshake, ServerHelloDone'
132 (23)        &reply::TLS-Session-Information += &session-state:TLS-Session-
    Information[*] -> '(TLS) PEAP - recv TLS 1.2 Handshake, ClientKeyExchange'
133 (23)        &reply::TLS-Session-Information += &session-state:TLS-Session-
    Information[*] -> '(TLS) PEAP - recv TLS 1.2 Handshake, Finished'
134 (23)        &reply::TLS-Session-Information += &session-state:TLS-Session-
    Information[*] -> '(TLS) PEAP - send TLS 1.2 ChangeCipherSpec'
135 (23)        &reply::TLS-Session-Information += &session-state:TLS-Session-
    Information[*] -> '(TLS) PEAP - send TLS 1.2 Handshake, Finished'
136 (23)        &reply::TLS-Session-Cipher-Suite += &session-state:TLS-Session-
    Cipher-Suite[*] -> 'ECDHE-RSA-AES128-GCM-SHA256'
137 (23)        &reply::TLS-Session-Version += &session-state:TLS-Session-Version[*]
     -> 'TLS 1.2'
138 (23)        &reply::User-Name += &session-state:User-Name[*] -> 'TFG\\
    administracion'
139 (23)        &reply::MS-MPPE-Send-Key += &session-state:MS-MPPE-Send-Key[*] -> 0
    x3abee034f1b2c6909c657e31ca4d89c7
140 (23)        &reply::MS-MPPE-Recv-Key += &session-state:MS-MPPE-Recv-Key[*] -> 0
    xf80ccf46aba68e51cdf010e9fdcb0aea
141 (23)        &reply::REST-HTTP-Status-Code += &session-state:REST-HTTP-Status-
    Code[*] -> 200
142 (23)        &reply::Tunnel-Type += &session-state:Tunnel-Type[*] -> VLAN
143 (23)        &reply::Tunnel-Private-Group-Id += &session-state:Tunnel-Private-
    Group-Id[*] -> '21'
144 (23)        &reply::Tunnel-Medium-Type += &session-state:Tunnel-Medium-Type[*]
    -> IEEE-802
145 (23)      } # update = noop
146 (23)      update reply {
147 (23)        &User-Name !* ANY
148 (23)      } # update reply = noop
149 (23)      update session-state {
150 (23)        &Tmp-String-1 := "accept"
151 (23)      } # update session-state = noop
152 (23) logNetworkAccess: EXPAND messages.%{session-state:Tmp-String-1}
153 (23) logNetworkAccess:     --> messages.accept
154 (23) logNetworkAccess: EXPAND %T [Access-Accept]  %{Calling-Station-Id} USER
    [%{User-Name} %{session-state:User-Name}] DEVICE [%{%{NAS-IP-Address}:-%{
    Packet-SRC-IP-Address}}] ATTRIBUTES [%{pairs:reply:}]
155 (23) logNetworkAccess:     --> 2025-08-21-18.50.39.210949 [Access-Accept]  0C
    -36-98-C3-4A-7D USER [TFG\administracion TFG\administracion] DEVICE
    [192.168.0.3] ATTRIBUTES [MS-MPPE-Recv-Key = 0
    xfc73563da23bcb3cce6f32e89a3d29a2d464484441f8ef99dd427d317c322943, MS-MPPE-
    Send-Key = 0x1e1278f57d08babe869..., EAP-MSK = 0xfc73563da23b..., EAP-EMSK
    = 0xafb504d0ef3f42db..., EAP-Session-Id = 0x1968a73249fb04..., EAP-Message
    = 0x03070004, Message-Authenticator = 0x00000000000000000000000000000000,
    Hint = "34587c7f-a986-46f0-9c5f-04b347133f54", Tmp-String-1 = "request",
    Framed-MTU = 1180, TLS-Session-Information = "(TLS) PEAP - recv TLS 1.3
    Handshake, ClientHello", TLS-Session-Information = "(TLS) PEAP - send TLS
    1.2 Handshake, ServerHello", TLS-Session-Information = "(TLS) PEAP - send
    TLS 1.2 Handshake, Certificate", TLS-Session-Information = "(TLS) PEAP -
    send TLS 1.2 Handshake, ServerKeyExchange", TLS-Session-Information = "(TLS
    ) PEAP - send TLS 1.2 Handshake, ServerHelloDone", TLS-Session-Information
    = "(TLS) PEAP - recv TLS 1.2 Handshake, ClientKeyExchange", TLS-Session-
    Information = "(TLS) PEAP - recv TLS 1.2 Handshake, Finished", TLS-Session-
    Information = "(TLS) PEAP - send TLS 1.2 ChangeCipherSpec", TLS-Session-
    Information = "(TLS) PEAP - send TLS 1.2 Handshake, Finished", TLS-Session-
    Cipher-Suite = "ECDHE-RSA-AES128-GCM-SHA256", TLS-Session-Version = "TLS
    1.2", MS-MPPE-Send-Key = 0x3abee034f1b2c6909c657e31ca4d89c7, MS-MPPE-Recv-
    Key = 0xf80ccf46aba68e51cdf010e9fdcb0aea, REST-HTTP-Status-Code = 200,
    Tunnel-Type = VLAN, Tunnel-Private-Group-Id = "21", Tunnel-Medium-Type =
    IEEE-802]
156 (23) logNetworkAccess: EXPAND /var/log/radius/networkAccess.log
157 (23) logNetworkAccess:     --> /var/log/radius/networkAccess.log
```

```
158 (23)       [logNetworkAccess] = ok
159 (23)     } # post-auth = ok
160 (23) Login OK: [TFG\administracion] (from client 192.168.23.1 port 0 cli 0C
    -36-98-C3-4A-7D)
161 (23) Sent Access-Accept Id 199 from 192.168.23.5:1812 to 192.168.23.1:40750
    length 266
162 (23)     MS-MPPE-Recv-Key = 0
    xfc73563da23bcb3cce6f32e89a3d29a2d464484441f8ef99dd427d317c322943
163 (23)     MS-MPPE-Send-Key = 0
    x1e1278f57d08babe869c83f490802e6ad38127385a7a351589fa2a4b3262be89
164 (23)     EAP-Message = 0x03070004
165 (23)     Message-Authenticator = 0x00000000000000000000000000000000
166 (23)     Framed-MTU += 1180
167 (23)     MS-MPPE-Send-Key += 0x3abee034f1b2c6909c657e31ca4d89c7
168 (23)     MS-MPPE-Recv-Key += 0xf80ccf46aba68e51cdf010e9fdcb0aea
169 (23)     Tunnel-Type += VLAN
170 (23)     Tunnel-Private-Group-Id += "21"
171 (23)     Tunnel-Medium-Type += IEEE-802
172 (23) Finished request
```

Fragmento A.1: Registros de FortiNAC del proceso de registro de un usuario en un equipo de la organización.

ANEXO

OBJETIVOS DE DESARROLLO SOSTENIBLE

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

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

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

ODS 8. Trabajo decente y crecimiento económico

META 8.2. Lograr niveles más elevados de productividad económica mediante la diversificación, la modernización tecnológica y la innovación, entre otras cosas centrándose en los sectores con gran valor añadido y un uso intensivo de la mano de obra.

La inversión en ciberseguridad y su aplicación en las organizaciones contribuyen a disminuir incidentes y tiempos de inactividad por accesos no autorizados, además de aumentar la disponibilidad de los servicios de TI, lo que impacta directamente en la productividad.

META 8.8. Proteger los derechos laborales y promover un entorno de trabajo seguro y sin riesgos para todos los trabajadores, incluidos los trabajadores migrantes, en particular las mujeres migrantes y las personas con empleos precarios.

La protección de los recursos digitales del personal es esencial para mantener un "entorno de trabajo seguro", ya que previene intrusiones, ransomware y fugas de datos en la red corporativa. La ciberseguridad y el desarrollo socioeconómico deben estar siempre interrelacionados.

ODS 9. Industria, innovación e infraestructuras

META 9.1. Desarrollar infraestructuras fiables, sostenibles, resilientes y de calidad, incluidas infraestructuras regionales y transfronterizas, para apoyar el desarrollo económico y el bienestar humano, haciendo especial hincapié en el acceso asequible y equitativo para todos.

Una solución NAC, como FortiNAC, contribuye a que la infraestructura TIC sea confiable y resistente, al impedir que dispositivos no conformes o no autorizados accedan a la red. Aportar seguridad a la red impacta de manera directa en la resiliencia de todos los recursos que alberga.

META 9.4. De aquí a 2030, modernizar la infraestructura y reconvertir las industrias para que sean sostenibles, utilizando los recursos con mayor eficacia y promoviendo la adopción de tecnologías y procesos industriales limpios y ambientalmente racionales.

La automatización del control de acceso y la segmentación dinámica modernizan la red con mayor eficiencia operativa y menor superficie de ataque.

META 9.C. Aumentar significativamente el acceso a la tecnología de la información y las comunicaciones y esforzarse por proporcionar acceso universal y asequible a Internet en los países menos adelantados de aquí a 2020.

Facilitar el acceso a tecnologías como es Internet y todas las redes que conecta puede ser vital, así como lo es garantizar que tanto los accesos como todo lo que se encuentra dentro de una red es seguro y confiable. Los dispositivos NAC son una herramienta importante para aportar seguridad.

ETS Enginyeria Informàtica
Camí de Vera, s/n, 46022, València
T +34 963 877 210
F +34 963 877 219
etsinf@upvnet.upv.es - www.inf.upv.es

ODS 16. Paz, justicia e instituciones sólidas

META 16.6. Crear a todos los niveles instituciones eficaces y transparentes que rindan cuentas.

Los controles de acceso y la trazabilidad mejoran la gobernanza y la rendición de cuentas. Los últimos estándares, como el Zero Trust, establecen el acceso autorizado y el principio de mínimo privilegio como base de la gestión pública/empresarial responsable.

META 16.10. Garantizar el acceso público a la información y proteger las libertades fundamentales, de conformidad con las leyes nacionales y los acuerdos internacionales.

Proteger la disponibilidad, integridad y confidencialidad de la información institucional, mediante la aplicación de medidas adecuadas de ciberseguridad, favorece el acceso confiable a la información de acuerdo con la legislación.

META 16.A. Fortalecer las instituciones nacionales pertinentes, incluso mediante la cooperación internacional, para crear a todos los niveles, particularmente en los países en desarrollo, la capacidad de prevenir la violencia y combatir el terrorismo y la delincuencia.

Elevar la ciberresiliencia de infraestructuras críticas y redes organizativas contribuye a prevenir y responder al cibercrimen que puede afectar a los servicios esenciales de una nación.

En conclusión, este Trabajo de Fin de Grado destaca las soluciones NAC como una gran herramienta para mejorar la seguridad de las redes informáticas. El proyecto, al alinearse con diferentes ODS, promueve un entorno digital más sólido y seguro, con un acceso a la red amplio y sin restricciones. Además, fomenta el desarrollo económico mediante la innovación tecnológica y refuerza las instituciones nacionales a través de la seguridad de sus infraestructuras.