



UNIVERSITAT  
POLITÈCNICA  
DE VALÈNCIA

— **TELECOM** ESCUELA  
TÉCNICA **VLC** SUPERIOR  
DE INGENIERÍA DE  
TELECOMUNICACIÓN

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Escuela Técnica Superior de Ingeniería de  
Telecomunicación

Implementación de mecanismos de control y seguridad en  
una red corporativa basados en el software Fortinac

Trabajo Fin de Grado

Grado en Ingeniería de Tecnologías y Servicios de  
Telecomunicación

AUTOR/A: García Gallego, Juan

Tutor/a: León Fernández, Antonio

CURSO ACADÉMICO: 2022/2023



**PORTADA GENERADA AUTOMÁTICAMENTE EN EBRON**



## Resumen

Hoy en día los dispositivos inteligentes del famoso internet de las cosas han invadido nuestra casa, nuestra oficina y prácticamente todos los lugares que tengan una conexión de internet, lo cual sin duda alguna nos ha traído muchos beneficios para hacer nuestras vidas más fáciles. Pero hablando en términos de seguridad, nos quedan ciertos pasos que dar, ya que estos dispositivos se hicieron pensando en usabilidad más que en la seguridad, esto ha traído consigo muchos problemas en nuestras redes.

En este trabajo se expondrá la implantación de la herramienta FortiNAC en una red corporativa cuyo objetivo es el de cambiar la dinámica de registro de dispositivos hacia un modelo de confianza cero (ZTA), a partir del uso de herramientas de perfilado de dispositivos, instalación de agentes y certificados algo que nos proporcionará una visibilidad completa de la red.

Una vez identificados los dispositivos conectados en nuestra red y adquirida esa visibilidad, se podrá realizar un control dinámico basado en políticas de acceso, junto a la segmentación de nuestra red MPLS de Vodafone.

Esta visibilidad y control de nuestra red nos permitirá tener una respuesta continua y proporcionada a la criticidad del sistema basado en la importancia en el negocio.

## Resum

Hui dia els dispositius intel·ligents de la famosa internet de les coses han envaït la nostra casa la nostra oficina i pràcticament tots els llocs que tinguen una connexió d'internet la qual cosa sens dubte ens ha portat molts beneficis per a fer les nostres vides més fàcils, però parlant en termes de seguretat ens queden uns certs passos que donar ja que aquests dispositius es van fer pensant en usabilitat més que en la seguretat, això ha portat aconseguisc molts problemes en les nostres xarxes.

En aquest treball s'exposarà la implantació de l'eina FortiNAC en una xarxa corporativa l'objectiu de la qual és el de canviar la dinàmica de registre de dispositius cap a un model de confiança zero (ZTA) a partir de l'ús d'eines de perfilat de dispositius, instal·lació d'agents i certificats alguna cosa que ens proporcionara una visibilitat completa de la xarxa.

Una vegada identificats els dispositius connectats en la nostra xarxa i adquirida aqueixa visibilitat es podrà realitzar un control dinàmic basat en polítiques d'accés, al costat de la segmentació de la nostra xarxa MPLS de Vodafone.

Aquesta visibilitat i control de la nostra xarxa ens permetrà tindre una resposta contínua i proporcionada a la criticitat del sistema basat en la importància en el negoci.

## Abstract

Nowadays the smart dispositives of the internet of things (IOT) have invaded our home, our office and practically all places where there are internet connexion which have bring many benefits in order to ease our lives, but if we talk about security, this devices have been created thinking in usability more than security.

In this project will be exposed the implementation of the tool FortiNAC in our corporative network whose objective are change the dynamic of the device registration to a zero trust model using profiling tools, installation of agents and certificates that provide a complete visibiliy of the network.

When the devices have been identified and we have the visibility of the network, we can do a dinamic control based on access policies, together with a segmentation of our MPLS network of Vodafone.



## Índice

Capítulo 1.	Introducción .....	8
1.1	Contexto y justificación .....	8
1.2	Objetivos .....	8
1.3	Metodología .....	9
1.3.1	Distribución de las tareas. ....	9
1.3.2	Estructura de la memoria.....	10
Capítulo 2.	Herramientas software utilizadas .....	11
2.1	Funcionamiento y descripción del software utilizado. ....	11
2.1.1	Introducción a FortiNAC .....	11
2.1.2	¿Cómo aplica ZTA FortiNAC? .....	12
2.2	Uso y tipos de Agentes.....	13
2.2.1	Agente soluble.....	13
2.2.2	Agente Pasivo.....	14
2.2.3	Agente Movil.....	14
2.2.4	Agente Persistente. ....	14
Capítulo 3.	Desarrollo del trabajo fin de grado.....	15
3.1	Planificación.....	15
3.1.1	Arquitectura y topología de la red.....	15
	.....	15
3.1.2	Estudio de puntos de acceso y dispositivos que será necesario monitorear. ....	17
3.1.3	Recursos necesarios, hardware y licencias.....	17
3.2	Configuración del servidor de FortiNAC.....	18
3.2.1	Integración y configuración IP .....	18
3.2.2	Configuración de métodos de registro.....	19
3.3	Reglas de Perfilado.....	20
3.3.1	Implementación de Administradores.....	20
3.3.2	Creación de reglas de perfilado. ....	21
3.3.3	Asociación de perfiles a dispositivos. ....	24
3.3.4	Funcionamiento del perfilado.....	25
3.4	Agente Persistente y certificados SSL en ordenadores corporativos. ....	26
3.5	Políticas de acceso a la red.....	28
3.5.1	Agrupación de Perfiles. ....	28
3.5.2	Ámbitos de acceso a la red. ....	30
3.5.3	Creación de las políticas de acceso a la red.....	31
3.5.4	Creación de grupos.....	32



3.6	Configuración de los Switchs.....	37
3.7	Implantación de switches y puesta en marcha del sistema.....	38
3.7.1	Gestión y propagación de rutas por parte de Vodafone. ....	38
3.7.2	Creación de ámbitos servidor DHCP .....	39
3.7.3	Alta de switches en FortiNAC.....	40
Capítulo 4.	Conclusión.....	46



## Índice de figuras

- Ilustración 1: Estructura FortiNAC
- Ilustración 2: ZTA en FortiNAC
- Ilustración 3: Segmentación de la red
- Ilustración 4: Licencias
- Ilustración 5: CLI FortiNAC
- Ilustración 6: Instaurar FortiNAC en la red
- Ilustración 7: Conjunto de servidores
- Ilustración 8: Configuración de LDAP
- Ilustración 9: Servidor RADIUS
- Ilustración 10: Administradores
- Ilustración 11: Perfil Teléfono GrandStream
- Ilustración 12: Métodos de perfilado de dispositivos
- Ilustración 13: Perfiles creados
- Ilustración 14: Modificar clave de registro
- Ilustración 15: Agente Persistente
- Ilustración 16: Certificado SSL
- Ilustración 17: User/Host Profiles
- Ilustración 18: User/Host Profiles
- Ilustración 19: Filtros en base al Host
- Ilustración 20: Ámbitos de acceso a red
- Ilustración 21: Renombramiento de Métodos
- Ilustración 22: Políticas de acceso
- Ilustración 23: Grupos
- Ilustración 24: Grupo Administradores
- Ilustración 25: Grupo de gestión y administrador de interfaces
- Ilustración 26: Subgrupo PoC\_FortiNAC
- Ilustración 27: Grupo de asignación VLAN de Registro
- Ilustración 28: Subgrupo L2 Network Devices
- Ilustración 29: Grupo de dispositivos de capa 2
- Ilustración 30: Grupo de dispositivos de capa 3
- Ilustración 31: Grupo de dispositivos con Agente Persistente
- Ilustración 32: Grupo de dispositivos registrados
- Ilustración 33: Subgrupo PoC\_FortiNAC
- Ilustración 34: Grupo de Rogue Host.
- Ilustración 35: Inventario Vodafone



Ilustración 36: Dar de Alta VLAN

Ilustración 37: Modo Trunk

Ilustración 38: Búsqueda por IP

Ilustración 39: Publicación de rutas

Ilustración 40: Ámbitos direcciones IP DHCP

Ilustración 41: Inventory

Ilustración 42: Contenedor

Ilustración 43: Credenciales Switch.

Ilustración 44: Registro de switch

Ilustración 45: Registro switch como L2

Ilustración 46: L2 Polling

Ilustración 47: Habilitar aplicación agente persistente

Ilustración 48: Relacionamos las Network Access con su VLAN correspondiente

Ilustración 49: Actualizamos tabla ARP del switch

Ilustración 50: Selección de puertos

Ilustración 51: Añadir puertos a grupo

Ilustración 52: Añadimos los puertos al grupo PoC\_FortiNAC

## Índice de tablas

Tabla 1: Distribución de las tareas

Tabla 2: Direccionamiento IP

Tabla 3: Direccionamiento IP

Tabla 4: Already collected Data

Tabla 5: Needs to be read

Tabla 6: Must be received



## Listado de siglas y términos

**IP** Internet Protocol

**VLAN** Virtual local area network

**ZTA** Zero trust access

**OUI** Organizationally Unique Identifier

**HTTP** Hypertext Transfer Protocol

**HTTPS** Hypertext Transfer Protocol Secure

**SNMP** Simple Network Management Protocol

**SSH** Secure SHell

**TCP** Transmission Control Protocol

**Telnet** Teletype Network

**UDP** User Datagram Protocol

**WINRM** Windows Remote Management

**WMI** Windows Management Instrumentation

**Firewall** Cortafuegos que protege un sistema de ser atacado

**ONVIF** Open Network Video Interface Forum

**DHCP** Dynamic Host Configuration Protocol

**RADIUS** Remote Authentication Dial-In User Service

**FortiNAC** Network access control solution

**FortiNET** Cibersecurity components company



## Capítulo 1. Introducción

### 1.1 Contexto y justificación

Hoy en día, todas las empresas buscan la creación de un entorno corporativo a nivel de redes lo más seguro posible. El concepto de ciberseguridad está a la orden del día y se están realizando continuos pasos para hermetizar las redes frente a los ataques que buscan las vulnerabilidades de las mismas.

El primer paso para poder adoptar estas medidas de protección es poder tener una visibilidad [1] total de nuestra red, tras ello podremos ejercer un control dinámico y proporcionar una respuesta orquestada, adecuada y proporcionada a la criticidad del sistema, basado en la importancia que tenga cada uno de los elementos en el negocio.

Esta visibilidad la obtendremos a partir de herramientas de perfilado, FortiNAC ha creado hasta 20 mecanismos para ello que permiten realizar ese registro de dispositivos tanto con información estática (OUI) o información dinámica (Agente, WMI).

Tras identificar el usuario, el dispositivo y haber ejercido un control de riesgos, se lleva a cabo una computación de toda esta información con el fin de establecer un criterio de acceso. Para ello, se ha realizado una segmentación de nuestra red MPLS en 4 VLANs, Registro, Datos, VozIP y Servicios Externos.

A partir de la integración de FortiNAC con elementos de seguridad, se podrá llevar a cabo esa respuesta orquestada.

He optado por centrar la investigación del Trabajo Final de Grado en este ámbito debido a que la empresa en la que me encuentro actualmente me dio la posibilidad. Aunque se trata de un tema que dista de la rama de telecomunicaciones en la que me he especializado, pienso que me puede ayudar a poder ampliar mis conocimientos y descubrir nuevas vías de desarrollo laboral. Tras la exposición del proyecto, la idea de poder implementar una herramienta que pueda llevar un registro, control y respuesta totalmente dinámico me incitó a enfocar el trabajo en este tema.

### 1.2 Objetivos

A partir de la instauración de la herramienta de FortiNAC, se pretende aplicar una mentalidad ZTA o cero confianza en nuestra red, es decir, no se confía de ningún dispositivo conectado en nuestra red corporativa hasta que se aplique un perfilado y registro del mismo. Uno de sus objetivos es simplificar el acceso de múltiple factor y que la experiencia del usuario sea lo más sencilla posible [2].

Por otro lado, tener un control total sobre nuestra red y poder determinar el tipo de acceso en función del dispositivo conectado es otro de sus propósitos. Anteriormente, cualquier dispositivo que se conectaba tenía acceso a cualquier aplicación o web corporativa, ahora aplicando ciertas políticas, se le proporcionarán servicios en función del dispositivo y usuario.

Otro de los objetivos que nos proporciona este control y visibilidad de la red es la gestión del inventariado de los dispositivos conectados, saber en que sedes se encuentran y a quien pertenecen esos equipos.

Como objetivo final pretende automatizar las respuestas en función de los cambios que se puedan producir en los dispositivos conectados a partir de un control y monitorización continuo de los mismos.

### 1.3 Metodología

Como forma de gestión y control de los procesos de desarrollo del proyecto, se ha llevado una planificación de las tareas a realizar de forma temporal y periódica, no obstante, y debido a ciertos factores como puede ser pruebas en laboratorio o gestión de inconvenientes, estas tareas se han ido solapando.

#### 1.3.1 Distribución de las tareas.

- Tarea 1: Documentación sobre FortiNAC
- Tarea 2: Aprendizaje sobre el entorno de trabajo
- Tarea 3: Estructuración de la segmentación de la red
- Tarea 4: Creación de Perfiles dentro de la herramienta FortiNAC
- Tarea 5: Creación de Políticas dentro de la herramienta FortiNAC
- Tarea 6: Pruebas en el laboratorio
- Tarea 7: Planificación del despliegue de switch
- Tarea 8: Despliegue e instauración de los switches en cada una de las sedes
- Tarea 9: Resolución de problemas.

Tarea	Fecha inicio	Fecha Fin
Tarea 1	12/01/2023	25/01/2023
Tarea 2	26/01/2023	6/02/2023
Tarea 3	7/02/2023	15/02/2023
Tarea 4	16/02/2023	22/02/2023
Tarea 5	23/02/2023	28/02/2023
Tarea 6	1/03/2023	8/02/2023
Tarea 7	9/03/2023	12/03/2023
Tarea 8	15/03/2023	16/06/2023
Tarea 9	15/03/2023	Actualidad

Tabla 1. Distribución de las Tareas



### **1.3.2 Estructura de la memoria.**

La memoria se conforma de 4 apartados. En el primero de ellos describimos la importancia de la propuesta, los objetivos en los que se centra el proyecto descrito, al igual que la distribución y metodología empleadas para poder desarrollar el trabajo. En el segundo se describe el marco teórico y la herramienta implantada que proporcionará el servicio necesario. El tercer apartado y más extenso de la memoria se exponen y desarrollan todos los pasos seguidos durante la ejecución del trabajo. Para finalizar, se valoran los resultados obtenidos y se exponen las conclusiones extraídas durante el desempeño del trabajo.

## Capítulo 2. Herramientas software utilizadas

Antes de profundizar en el desarrollo de este TFG y con el fin de comprender el entorno en el que se produce este proyecto, vamos a realizar una breve explicación a nivel conceptual de las herramientas utilizadas.

### 2.1 Funcionamiento y descripción del software utilizado.

#### 2.1.1 Introducción a FortiNAC

FortiNAC es una herramienta perteneciente al ecosistema de dispositivos Fortinet que da una solución de confianza cero cuya finalidad es proteger y supervisar los activos digitales que se encuentren conectados a la red corporativa de la empresa. Esta herramienta proporciona visibilidad, control y respuesta automatizada para todos los dispositivos que se encuentran conectados a la red y ofrece protección contra amenazas de IoT [3].

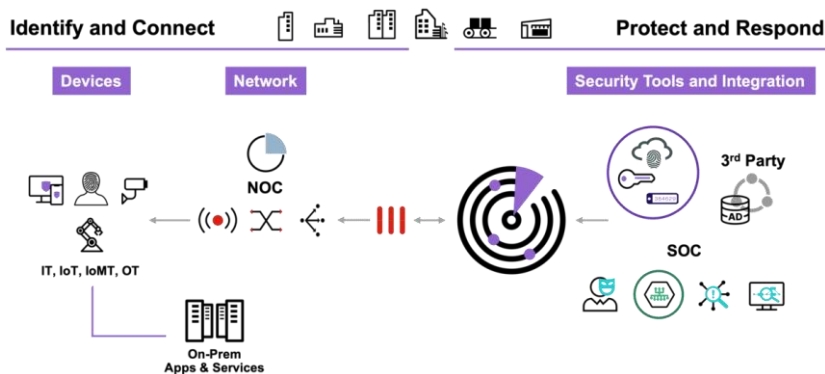


Ilustración 1: Estructura FortiNAC [Fuente: FortiNET control de acceso de red segura]

Las principales características que definen a FortiNAC son las siguientes.

- Permite controlar y gestionar el acceso de los usuarios y dispositivos a la red. Puede autenticar y autorizar a los usuarios antes de permitirles acceder a los recursos de red. Esto ayuda a garantizar que solo los dispositivos y usuarios autorizados puedan acceder a la red y los recursos correspondientes.
- Tiene la capacidad de detectar y descubrir dispositivos conectados a la red, aquellos que son nuevos o no autorizados. Proporciona información detallada sobre los dispositivos, como direcciones IP, fabricante, tipo de dispositivo, sistema operativo, historial de conexión, etc. Esto permite una mejor visibilidad y control sobre los dispositivos en la red.
- FortiNAC ayuda a garantizar el cumplimiento de las políticas de seguridad de la red. Pueden aplicar políticas de seguridad predefinidas o personalizadas para diferentes tipos de dispositivos y usuarios. Esto incluye la verificación de parches, la configuración del sistema operativo, la presencia de software antivirus, el cumplimiento de políticas de contraseña, entre otros criterios.
- También desempeña un papel en la seguridad de la red al proporcionar protección contra amenazas. Puede detectar y responder a amenazas en tiempo real, como dispositivos comprometidos, malware o actividades sospechosas en la red. Además, puede integrarse con otras soluciones de seguridad de Fortinet para una defensa más completa.

- Se puede integrar con otras soluciones de Fortinet, como firewalls y los sistemas de detección y prevención de intrusiones, para permitir la autorización y orquestación de acciones de seguridad. Esto permite una respuesta rápida y coordinada ante amenazas o eventos de seguridad.

### 2.1.2 ¿Cómo aplica ZTA FortiNAC?

Como hemos comentado anteriormente, al implantar la herramienta de FortiNAC se pretende habilitar una arquitectura basada en lo que se conoce como Zero Trust, es decir, se desconfía de todo dispositivo o usuario que tenga la intención de conectarse al perímetro interno de nuestra red corporativa [4].

Con este nuevo método de acceso a la red corporativa de la empresa, lo que se pretende es que todo aquel que desee conectarse a ella deba estar identificado antes de poder acceder a ningún recurso interno [5].

Para ello, cada vez que se conecta un dispositivo, se llevan a cabo un procedimiento escalado hasta que se le concede acceso a los recursos correspondientes.

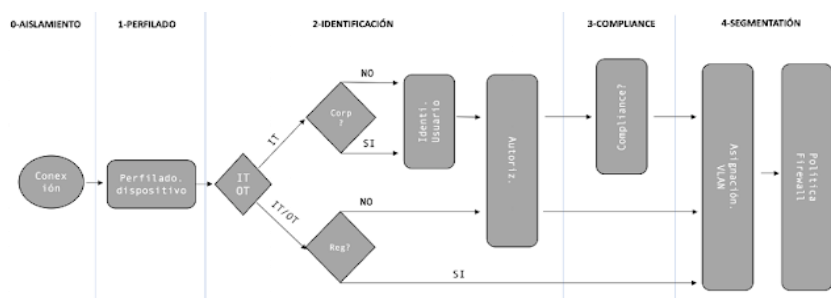


Ilustración 2: ZTA en FortiNAC [Fuente: Blog técnico FORTINET]

#### 0. Aislamiento:

En una primera instancia, todos los puertos de red en los que no hay ningún dispositivo conectado, se encuentran en una VLAN de contención que en FortiNAC recibe el nombre de registro, la cual proporcionan los servicios indispensables para poder ejecutar el resto de fases. Una vez se conecta un dispositivo se envía un trap SNMP o una petición de acceso 802.1x informando a FortiNAC que se ha producido una conexión [6].

#### 1. Perfilado del tipo de dispositivo:

En primer lugar, se tiene que llevar a cabo la identificación del tipo de dispositivo, para ello FortiNAC dispone de:

- Perfilado: Tiene hasta 21 opciones diferentes de perfilado, pasivas (fingerprint DHCP, OUI) como activas (escaneo de puertos, fingerprint nmap, WMI...).
- Integración con el directorio activo
- Integración con el gestor de Endpoints

FortiNAC ya conocerá el tipo de dispositivo conectado, si se trata de un elemento IOT/OT que no puede ejecutar políticas de autenticación (cámaras, impresoras...) o si por el otro lado se trata de un IT Corporativo o no corporativo.

#### 2. Identificación

Una vez los dispositivos perfilados, debemos verificar que usuario se está conectando a la red, para ello debemos diferenciar entre tipos de dispositivos.

- IT Corporativo: En nuestro caso se identifica a partir del uso de agente persistente
- IT No Corporativo: FortiNAC presenta un portal que permiten a usuarios no corporativos conectarse a la red.

Tras este proceso, el dispositivo ya estará perfilado, registrado y asociado a un usuario, en caso de que lo hubiera.

### 3. Verificación de Cumplimiento

Este proceso se lleva a cabo a partir del despliegue de agentes o la integración con el gestor de dispositivos

- Hosts Corporativos: Mediante el despliegue de agente persistente.
- Hosts No Corporativos: Mediante el uso de Agentes disoluble.

Utilizando perfilado mediante WMI, se realizan comprobaciones periódicas de los perfiles creados, si un equipo deja de cumplir las políticas de perfilado (antivirus, sistema operativo) sería reperfilado con casi total seguridad como dispositivo no válido.

### 4. Segmentación

En el momento en el que FortiNAC conoce el dispositivo conectado y el usuario que está registrado, tiene la opción de llevar a cabo ciertas acciones de control:

- Puede asignarle al dispositivo en cuestión a una determinada VLAN, algo que limitara la conectividad horizontal.
- Ejecutar comandos en el puerto
- Enviar un tag al firewall FortiGate, asociando el dispositivo a un grupo de usuarios que puede utilizarse en las políticas de seguridad, habilitando la segmentación vertical de dispositivos, incluso cuando varios equipos estén en la misma VLAN.

## 2.2 Uso y tipos de Agentes.

La implementación de agentes en los end point tiene la finalidad de escanear hosts y determinar si estos cumplen las políticas asignadas a ese tipo de dispositivos. Existen varios tipos de agentes disponibles con FortiNAC, Agente Disoluble, Agente Pasivo, Agente Movil y Agente Persistente, el cual es el que tenemos instalado en todos nuestros ordenadores y portátiles corporativos.

Si la respuesta tras un escaneo por parte del agente es fallida, existen diversas formas de actuación.

- El administrador recibe una advertencia en el que se indica que el escaneo por parte del agente ha sido erróneo junto a una lista de los fallos, pero el terminal sigue teniendo acceso a la red.
- El propio usuario puede recibir una advertencia indicando el fallo en el escaneo por parte del agente, pero sigue manteniendo acceso a la red.
- Se puede configurar para que en el momento en el que se detecta un error por parte del agente, este lo traslada a una VLAN de cuarentena. En el momento en el que se solventa el error y se vuelve a llevar a cabo el escaneo por parte del agente, se devuelve a la VLAN correspondiente.

### 2.2.1 Agente soluble

El usuario descarga el agente en su computadora, este lleva a cabo un escaneo, en caso de cumplir todas las políticas se le permitirá acceder a la red y el agente se eliminará del ordenador, en el caso de detectar algún fallo, se mantendrá instalado hasta solventarlo.



### **2.2.2 *Agente Pasivo***

Este agente no está instalado, emplea el inicio de sesión por parte de los usuarios de red contenidos en su LDAP o Active Directory para llevar a cabo el escaneo y determinar si cumple con las políticas que le acreditan como un usuario válido para acceder a la red.

### **2.2.3 *Agente Móvil.***

Este funciona en dispositivos Android, ayuda con la autenticación y registro al igual que proporciona un inventariado de las aplicaciones instaladas [7].

### **2.2.4 *Agente Persistente.***

El agente persistente permanece instalado en el host en todo momento, Una vez instalado se ejecuta en segundo plano y establece una conexión permanente con el servidor de agentes de FortiNAC. Su función principal es completar tareas de registro, autenticación y escaneo junto a la aportación de información adicional a FortiNAC sobre el host.

## Capítulo 3. Desarrollo del trabajo fin de grado

Una vez contextualizados y explicados los motivos por los que se tomó la decisión de implantar una herramienta que permita proteger las redes corporativas a partir de un control y autorización de acceso de dispositivos, pasamos a desarrollar punto por punto los pasos seguidos para poder insertar FortiNAC en nuestra red.

### 3.1 Planificación

En primer lugar y a fin de estructurar los procedimientos a llevar a cabo a lo largo de la implantación de esta nueva herramienta en la red de nuestra empresa, se procedió elaborando una planificación jerárquica de los puntos a seguir.

- Definir los objetivos y requisitos de implementación que ya han sido expuestos anteriormente
- Evaluar la arquitectura y topología de la red
- Determinar los puntos de acceso y los dispositivos que necesitan ser monitorizados y controlados por FortiNAC
- Asegurarnos de tener los recursos adecuados, como hardware y licencias, para implementar FortiNAC.

Una vez definidos, esclarecidos y resueltos todos los puntos a tratar, podemos pasar con el desarrollo del proyecto.

#### 3.1.1 Arquitectura y topología de la red.

El primer paso de este proyecto fue la esquematización y estructuración de la red MPLS de Vodafone.

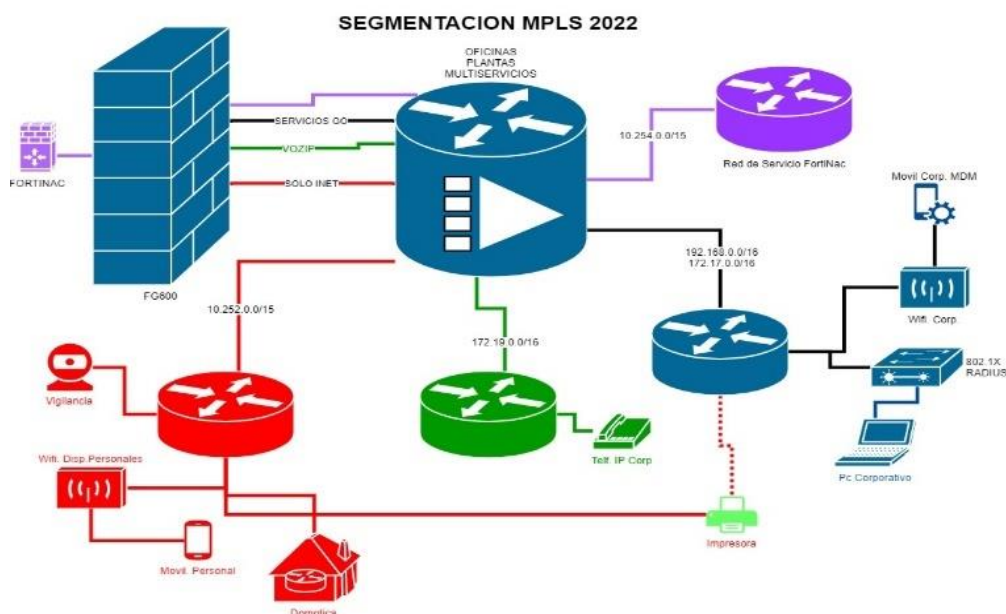


Ilustración 3: Segmentación de la red [Fuente Propia]

Como sabemos la segmentación crea diversos segmentos aislados dentro de una red más grande, cada uno de estos segmentos puede tener diferentes requisitos y políticas de seguridad.



Los dos objetivos principales de la segmentación son:

- Mejora del rendimiento, ya que elimina el tráfico innecesario en un segmento particular y así evitar la congestión de la propia red.
- Mejora de la seguridad, una red plana implica una gran área de ataque, al dividir la red, aísla el tráfico de la red en estas subredes, reduciendo la superficie de ataque e impide el desplazamiento lateral, es decir, los segmentos de red aíslan un ataque en una única porción de la red evitando que se propague por el resto.

Este nuevo esquema de red ha sido implementado en cada una de las sedes de nuestra empresa, la reestructuración de la red se basa en la inserción de 4 VLANs.

- Red de registro FortiNAC que pretende descubrir los nuevos dispositivos y usuarios conectados a la red, aplicar un perfilado de ellos y ejecutar ciertas políticas que determinarán el tipo de acceso a red correspondiente para cada uno de los dispositivos. Además, será empleada para aislar a todos los dispositivos que hayan sido infectados.
- Definimos una VLAN descrita como datos de delegación que se asocia a todos los usuarios que tengan instalado en sus computadoras un tipo de agente denominado persistente, junto a otros dispositivos corporativos como impresoras o elementos de control de acceso, todos estos dispositivos tendrán acceso a la red interna de la empresa.
- Para todo el tráfico generado por la telefonía IP, se ha instaurado una VLAN que recibe el nombre de VozIP.
- Por último, precisamos una VLAN denominada servicios externos, que autoriza únicamente el acceso a los usuarios a internet y a las aplicaciones que no se encuentran en nuestra red, dispositivos como cámaras u ordenadores que no poseen agente persistente serán asignados con esta VLAN.

Empleamos 2 rangos distintos de direcciones IP debido al gran número de sedes que se encuentran operativas actualmente en la empresa.

VLANs	Descripción	Direccionamiento IP	DHCP Relay
33	Datos delegación	192.168.0.0/16	192.168.3.33 192.168.3.27
69	VozIP	172.19.0.0/16	192.168.3.33 192.168.3.27
252	Servicios Externos Delegació	10.252.0.0/15	192.168.3.33 192.168.3.27
251	Red de registro FortiNAC	10.250.0.0/15	192.168.3.33 192.168.3.27

**Tabla 2: Direccionamiento IP**

VLANs	Descripción	Direccionamiento IP	DHCP Relay
33	Datos delegación	172.17.0.0/16	192.168.3.33 192.168.3.27
69	VozIP	10.19.0.0/16	192.168.3.33 192.168.3.27
252	Servicios Externos Delegació	10.253.0.0/15	192.168.3.33 192.168.3.27
251	Red de registro FortiNAC	10.251.0.0/15	192.168.3.33 192.168.3.27

**Tabla 3: Direccionamiento IP**

### 3.1.2 Estudio de puntos de acceso y dispositivos que será necesario monitorear.

Se recopila información de cada una de las sedes, es posible hacer una aproximación a partir de la herramienta de inventariado disponible, pero se precisó del contacto con las mismas para que elaboraran un informe con el conjunto de dispositivos que serán necesarios conectar en la sede, en un principio únicamente se tuvieron en cuenta Ordenadores, TelefoníaIP, Impresoras, etc.... sin tener en cuenta todos los dispositivos de IOT. De esta forma poder realizar un listado con los switches y las dimensiones de los mismos que serán necesarios implantar en cada una de las sedes de la empresa.

### 3.1.3 Recursos necesarios, hardware y licencias.

Debido a que en la mayoría de las sedes disponíamos de switches Linksys no gestionables de forma remota, fue necesario sustituir estos por otros que sí que lo fueran. Tras un exhaustivo estudio de mercado en el que se barajaron opciones como switches cisco descartado por su alto costo y FortiSwitch igualmente descartado por falta de stock, nos decantamos por la adquisición de switches HUAWEI (S5735-L8P4S-A1)(S5735-L8P4S-A1) que nos cuadraba tanto a nivel económico como técnico. Estos swichs se caracterizan por disponer de 8 y 24 interfaces respectivamente, ampliamente inteligente (iStack), redes Ethernet flexibles y control de seguridad diversificado, además admite múltiples protocolos de enrutamiento de capa 3 y proporcionan alto rendimiento y capacidades de procesamiento de servicios [8].

A nivel de adquisición de licencias, FortiNAC dispone de 3 niveles de licenciamiento.

- **BASE:** Adecuado para organizaciones cuya necesidad el proteger únicamente dispositivos IoT o dispositivos que no se encuentran asociados a personas. Habilita el bloqueo de la red sin más controles de red o proporcionando una respuesta automatizada a las amenazas [9].
- **PLUS:** Preciso para organizaciones que desean una visibilidad completa del endpoint. Se trata de una solución NAC flexible que aporta un control granular, pero que no dispone de respuestas automatizadas a amenazas [9].
- **PRO:** Se desea visibilidad completa de los endpoints. Al igual que la PLUS proporciona un control granular a lo que se añade una clasificación de eventos precisa y respuestas automatizadas en tiempo real [9].

FortiNAC LICENSE TYPES		BASE	PLUS	PRO
Network	Network Discovery	•	•	•
	Persistent Agent		•	•
User	Authentication		•	•
	Captive Portal		•	•
Visibility	Rogue Identification	•	•	•
	Device Profiling & Classification	•	•	•
Endpoint	Enhanced Visibility		•	•
	Anomaly Detection		•	•
	MDM Integration	•	•	•
	Network Access Policies	•	•	•
	BYOD / Onboarding		•	•
	Guest Management		•	•
Automation / Control	IoT Onboarding with Sponsor	•	•	•
	Endpoint Compliance		•	•
	Rogue Device Detection & Restriction	•	•	•
	Web & Firewall Single Sign On		•	•
	Firewall Segmentation	•	•	•
Incident Response	Event Correlation			•
	Extensible Actions & Audit Trail			•
	Alert Criticality & Routing			•
	Guided Triage Workflows			•
Integrations	Inbound Security Events			•
	Outbound Security Events		•	•
	REST API		•	•
	Live Reporting		•	•

Ilustración 4: Licencias [Fuente: <https://fortixpert.blogspot.com>]

En primera instancia, se adquirieron 2500 licencias de tipo PRO, pero tras un replanteamiento del proyecto, se está debatiendo el caso de introducir 4000 más para abarcar todos los dispositivos IoT conectados en la red.

## 3.2 Configuración del servidor de FortiNAC.

Una vez presentados los objetivos y planificación del proyecto, podemos comenzar con la integración y configuración del servidor FortiNAC dentro de nuestra red.

### 3.2.1 Integración y configuración IP

FortiNAC ha sido instaurado en una máquina virtual que se encuentra instalada en nuestra sede de Vara de Quart, en primera instancia deberemos asignarle una dirección IP estática.

```
FortiNAC FNMCA
root@fortinac:~
> ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.2.170 netmask 255.255.254.0 broadcast 192.168.3.255
inetc fe80::250:56ff:fe95:6d5a prefixlen 64 scopeid 0x20<link>
ether 00:50:56:95:6d:5a txqueuelen 1000 (Ethernet)
RX packets 31849696 bytes 8160801004 (7.6 GiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 21520692 bytes 2576671510 (2.3 GiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.250.0.10 netmask 255.255.255.0 broadcast 10.250.0.255
inetc fe80::250:56ff:fe95:113c prefixlen 64 scopeid 0x20<link>
ether 00:50:56:95:11:3c txqueuelen 1000 (Ethernet)
RX packets 53757 bytes 22577458 (21.5 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 28 bytes 1496 (1.4 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Ilustración 5: CLI FortiNAC [Fuente Propia]

Le fijamos la dirección IP 192.168.2.170/23 a una de sus interfaces correspondiente al rango de nuestra red de servidores y la cual está asociada a la VLAN 270, tras esto procedemos con la asociación de nuestros servidores DNS (192.168.3.26/23 y 192.168.3.50) junto con el dominio al que pertenecen corporativo.es.

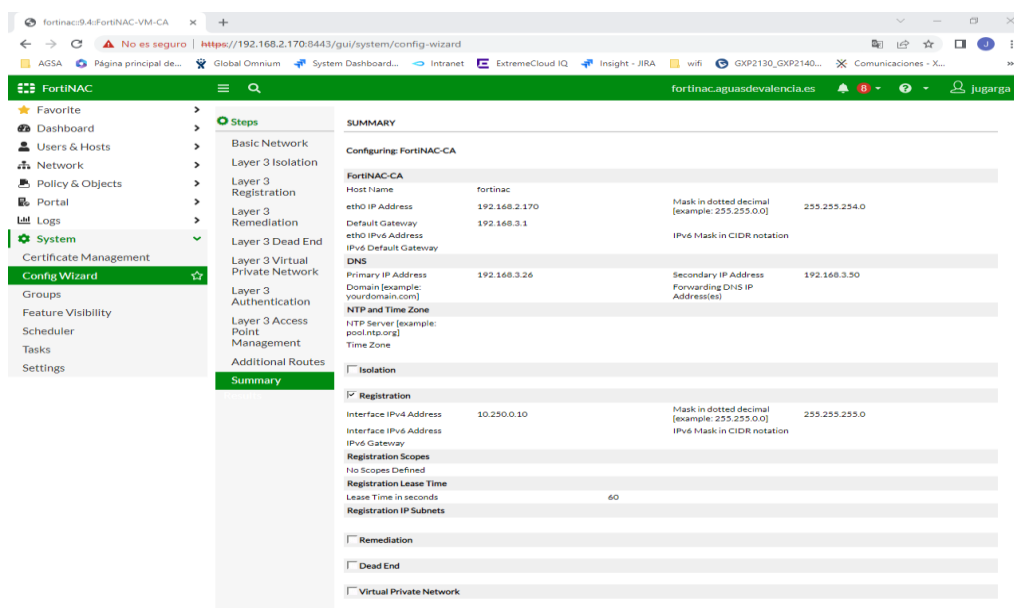


Ilustración 6: Instaurar FortiNAC en la red [Fuente Propia]

En un primer momento, se intentó implementar otra de sus interfaces a la que se le asignó la IP 10.250.0.10/24 para el registro de dispositivos, pero finalmente se descartó. Una vez se ha realizado este proceso ya tendremos acceso a FortiNAC vía web.

### 3.2.2 Configuración de métodos de registro.

Tras comprobar que tenemos acceso a la herramienta FortiNAC, comenzamos a configurarla. Primeramente, nos centraremos en conformar los métodos de registro y autenticación que empleará la herramienta, configuraremos 2 protocolos LDAP y RADIUS.

- LDAP: Protocolo de la capa de aplicación TCP/IP que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red [10].
- RADIUS: Protocolo de autenticación y automatización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1812 UDP para establecer sus conexiones [11].

Configuramos LDAP dentro de FortiNAC, para ello nos desplazamos por la interface Setting> Authentication>LDAP y seleccionamos la opción de Add.

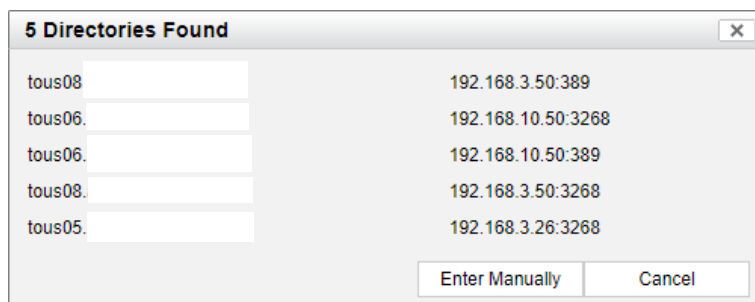


Ilustración 7: Conjunto de servidores [Fuente Propia]

Seleccionamos nuestra máquina con IP 192.168.3.26 donde se encuentra nuestro servidor LDAP junto con el puerto 389 empleado por dicho protocolo [12].

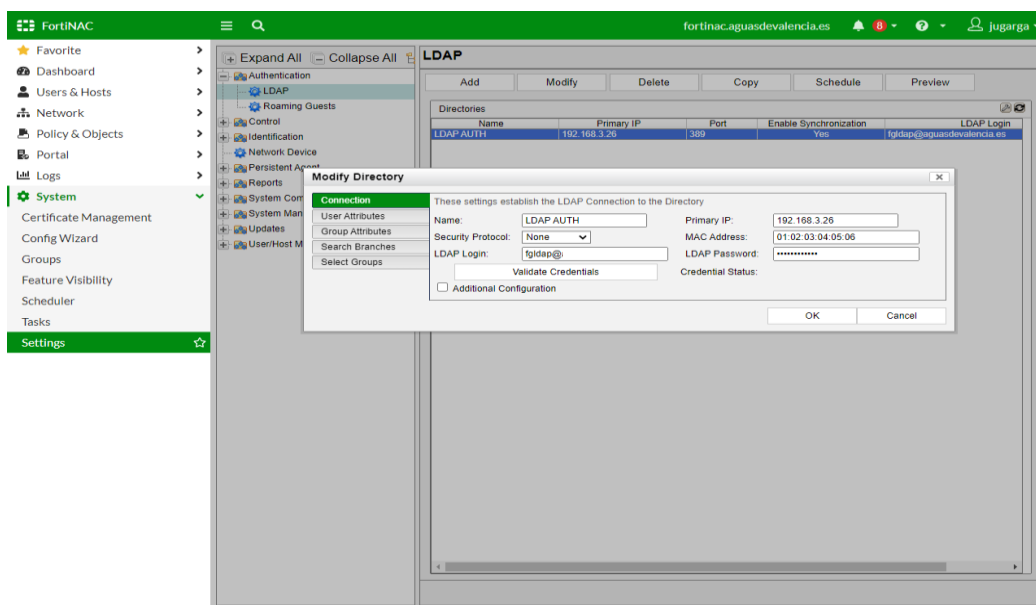
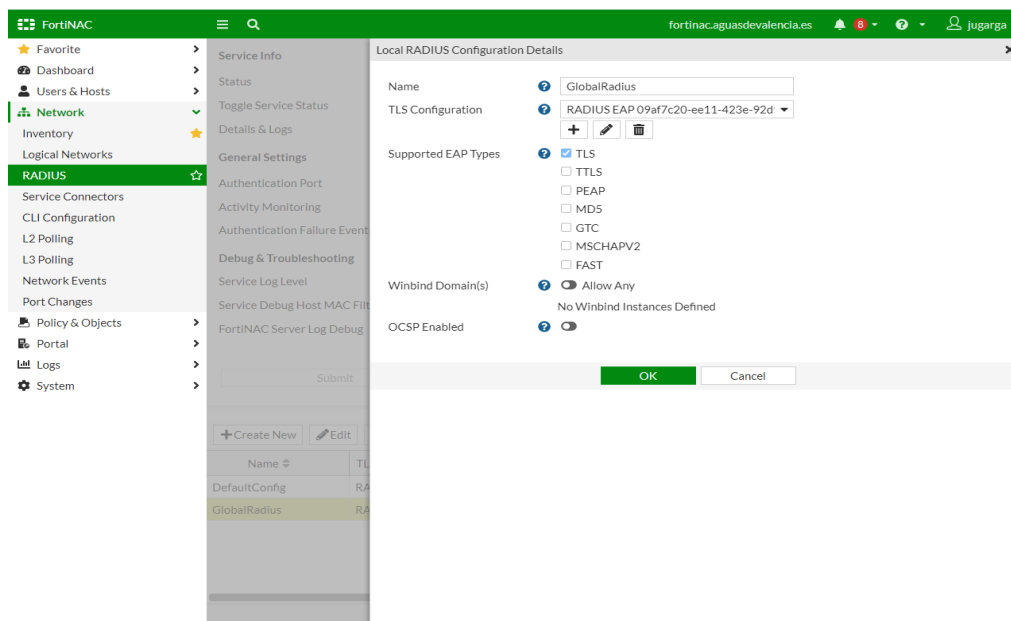


Ilustración 8: Configuración de LDAP [Fuente propia]

Introducimos las credenciales de registro en el servidor y le asignamos un nombre para identificarlo.

En este servidor están almacenados todos los datos asociados a nuestro Active Directory lo que permite asociar, comprobar y registrar quien está usando un determinado dispositivo a partir de la introducción de sus credenciales al iniciar sesión.

Además de LDAP, integramos nuestro servidor RADIUS con FortiNAC, este método es el que será empleado para el registro de switches. Nos desplazamos por la interfaz Network<RADIUS<Create New



**Ilustración 9: Servidor RADIUS [Fuente Propia]**

Configuramos TLS como método de conexión que proporcionará cifrado, autenticación e integridad de datos para el intercambio de mensajes RADIUS, se le asigna el puerto 1814 correspondiente al mismo protocolo de autenticación.

### 3.3 Reglas de Perfilado

La creación de perfiles dentro de la herramienta FortiNAC tiene como finalidad clasificar dispositivos no autorizados y crear un inventario de todos los dispositivos registrados de confianza.

Device Profiler es la solución que ofrece FortiNAC para la clasificación y evaluación de dispositivos, consiste en una serie de reglas ordenadas y personalizadas para definir todos aquellos dispositivos no autorizados que se conectan a la red, estas reglas evalúan los dispositivos a partir de su configuración y dan como respuesta un resultado de aprobación o rechazo.

#### 3.3.1 Implementación de Administradores.

El primer paso para poder crear perfiles es dar permiso de administrador a los usuarios permitidos. Los administradores poseen derechos completos sobre todas las partes del sistema FortiNAC y pueden implementar completamente el perfilado de dispositivos. Para poder acceder al apartado

de configuración de administradores nos debemos desplazar por la interface Users Host > Administrators.

Una vez tenemos los derechos de administrador, ya podremos comenzar con la creación de los perfiles de dispositivos.

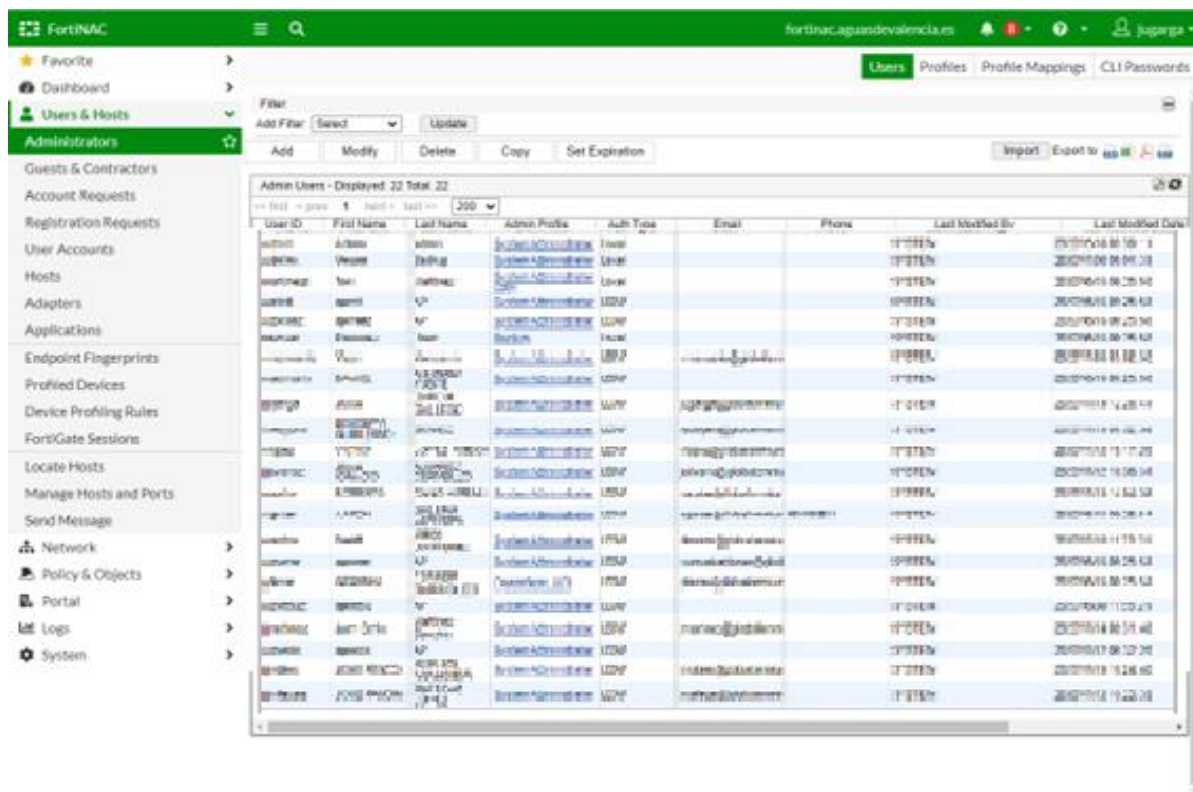


Ilustración 10: Administradores [Fuente Propia]

### 3.3.2 Creación de reglas de perfilado.

Se han definido 16 Reglas de perfilado. para la elaboración y configuración de estas accedemos a Users Hosts>Device Profiling Rules>Add. Utilizaremos de ejemplo una de las reglas ya creadas para dar una explicación de los parámetros a definir.

En primer lugar, le atribuimos un nombre, si deseamos que se nos notifique cada vez que se profile un dispositivo a partir de esta regla, activamos la opción Notify Sponsor, seguidamente y en fases iniciales se recomienda que se emplee un tipo de registro manual con el fin de comprobar que la regla ha sido correctamente creada. Una vez esté ciertamente definida podemos cambiarla a automático. A continuación, le atribuimos el tipo de dispositivo al que hará referencia esta regla y que en pasos posteriores nos ayudará a agrupar y simplificar la aplicación de las políticas de acceso a la red. En estos momentos el Rol que adquiere el dispositivo no lo tenemos definido. Finalmente, seleccionamos donde deseamos que el registro aparezca, en nuestro caso, en el visor de host, para ello, seleccionamos la opción Device in Host View, donde podremos descubrir de una forma sencilla la situación de un dispositivo a partir de su MAC o dirección IP.

**Modify Device Profiling Rule**

**General** | Methods

Enabled

Name: Telefono GrandStream

Description:

Note:

Notify Sponsor

Registration Settings

Registration:  Automatic  Manual

Type: IP Phone

Role: NAC-Default

Register as: Device in Host View

Add to Group: Forced Remediation Exceptions

Access Availability: Always

Rule Confirmation Settings

Confirm Device Rule on Connect

Confirm Device Rule on Interval: Minutes

Disable Device If Rule No Longer Matches Device

OK Cancel

**Ilustración 11: Perfil Teléfono GradStream [Fuente Propia]**

Una vez definidos los aspectos generales, seleccionamos el método o la forma por la cual la herramienta FortiNAC va a poder asociar un dispositivo con alguno de los perfiles creados. FortiNAC ha creado hasta 21 métodos de perfilado que serán tratados posteriormente

**Modify Device Profiling Rule**

General | **Methods**

Active

DHCP Fingerprinting

FortiGate

FortiGuard

HTTP/HTTPS

IP Range

Location

Network Traffic

ONVIF

Passive

Persistent Agent

RADIUS Request

Script

SNMP

SSH

TCP

Telnet

UDP

Vendor OUI

WinRM

Windows Profile

**Vendor OUI**

Matches if any of the following values equals the value in the field defined in the Vendor OUI database. [Vendor OUIs](#)

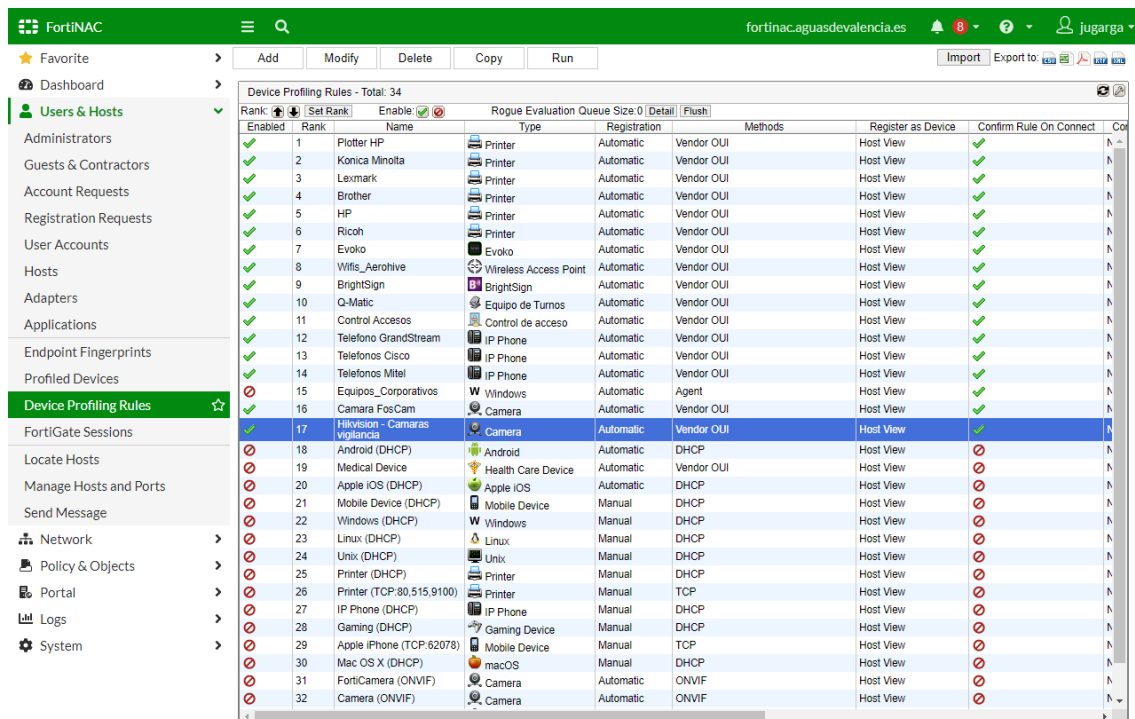
Add Modify Delete

Field	Value
Vendor Code	00:0B:82
Vendor Code	C0:74:AD

OK Cancel

**Ilustración 12: Métodos de perfilado de dispositivos.**

Para crear nuestros perfiles empleamos el OUI de Vendor con lo que se puede reconocer el tipo de dispositivo a partir de los 3 primeros octetos de la MAC del dispositivo, señal identificativa del fabricante al que pertenece dicho instrumento



Enabled	Rank	Name	Type	Registration	Methods	Register as Device	Confirm Rule On Connect	Co
✓	1	Plotter HP	Printer	Automatic	Vendor OUI	Host View	✓	N
✓	2	Konica Minolta	Printer	Automatic	Vendor OUI	Host View	✓	N
✓	3	Lexmark	Printer	Automatic	Vendor OUI	Host View	✓	N
✓	4	Brother	Printer	Automatic	Vendor OUI	Host View	✓	N
✓	5	HP	Printer	Automatic	Vendor OUI	Host View	✓	N
✓	6	Ricoh	Printer	Automatic	Vendor OUI	Host View	✓	N
✓	7	Evoko	Evoko	Automatic	Vendor OUI	Host View	✓	N
✓	8	Wifis_Aerohive	Wireless Access Point	Automatic	Vendor OUI	Host View	✓	N
✓	9	BrightSign	BrightSign	Automatic	Vendor OUI	Host View	✓	N
✓	10	Q-Matic	Equipo de Turnos	Automatic	Vendor OUI	Host View	✓	N
✓	11	Control Accesos	Control de acceso	Automatic	Vendor OUI	Host View	✓	N
✓	12	Telefono GrandStream	IP Phone	Automatic	Vendor OUI	Host View	✓	N
✓	13	Telefonos Cisco	IP Phone	Automatic	Vendor OUI	Host View	✓	N
✓	14	Telefonos Mitel	IP Phone	Automatic	Vendor OUI	Host View	✓	N
✓	15	Equipos Corporativos	Windows	Automatic	Agent	Host View	✓	N
✓	16	Camara FosCam	Camera	Automatic	Vendor OUI	Host View	✓	N
✓	17	Hikvision - Cámaras vigilancia	Camera	Automatic	Vendor OUI	Host View	✓	N
✗	18	Android (DHCP)	Android	Automatic	DHCP	Host View	✗	N
✗	19	Medical Device	Health Care Device	Automatic	Vendor OUI	Host View	✗	N
✗	20	Apple iOS (DHCP)	Apple iOS	Automatic	DHCP	Host View	✗	N
✗	21	Mobile Device (DHCP)	Mobile Device	Manual	DHCP	Host View	✗	N
✗	22	Windows (DHCP)	Windows	Manual	DHCP	Host View	✗	N
✗	23	Linux (DHCP)	Linux	Manual	DHCP	Host View	✗	N
✗	24	Unix (DHCP)	Unix	Manual	DHCP	Host View	✗	N
✗	25	Printer (DHCP)	Printer	Manual	DHCP	Host View	✗	N
✗	26	Printer (TCP.80,515,9100)	Printer	Manual	TCP	Host View	✗	N
✗	27	IP Phone (DHCP)	IP Phone	Manual	DHCP	Host View	✗	N
✗	28	Gaming (DHCP)	Gaming Device	Manual	DHCP	Host View	✗	N
✗	29	Apple iPhone (TCP.62078)	Mobile Device	Manual	TCP	Host View	✗	N
✗	30	Mac OS X (DHCP)	macOS	Manual	DHCP	Host View	✗	N
✗	31	FortiCamera (ONVIF)	Camera	Automatic	ONVIF	Host View	✗	N
✗	32	Camera (ONVIF)	Camera	Automatic	ONVIF	Host View	✗	N

Ilustración 13: Perfiles creados [Fuente Propia]

Como hemos mencionado, se han creado 16 perfiles de dispositivos, todos ellos identificados a partir de su OUI de Vendor.

- Plotter HP
- Konica Minolta
- Lexmark
- Brother
- HP
- Ricoh
- Evoko
- Wifis\_Aerohive
- BrightSign
- Q-Matic
- Control de Acceso
- Telefono GrandStream
- Telefonos Cisco
- Telefonos Mitel
- Camara FosCam
- Hikvision -Cámaras vigilancia



### 3.3.3 Asociación de perfiles a dispositivos.

En el momento que se conecta un dispositivo a la red, FortiNAC evalúa este frente a las reglas de perfilado creadas, esto requiere una clasificación eficiente y específica de las mismas.

- Cuando la validación resulta correcta y se da por aprobada, el dispositivo se clasifica según lo especificado en la regla.
- Si el resultado de la validación resulta en fallo, se pasará a la regla siguiente.
- Un resultado “No se puede evaluar” determina que un método dentro de una regla necesita cierta información no disponible o que no está actualizada.

Podemos agrupar los métodos que caracterizan cada una de las reglas de tres formas diferentes.

#### 1. Already collected Data

Method	Definition
Location	Compares device’s connected location to the specified location objects
Vendor OUI	Compares device’s OUI to FortiNAC’s OUI database

Tabla 4: Already collected Data [13]

#### 2. Needs to be read

Method	Definition
Active	OS evaluation using NMAP’s OS detection database
HTTP/HTTPS	URL query with or without authentication and the ability to match content within the result
IP Range	Compares device’s IP to the specified IP range(s)
SNMP	OID query with V1/V2/V3 authentication and the ability to match content within the result
SSH	Authenticated session with the ability to execute commands and match content within the result of the command
TCP	Open port scan using NMAP
Telnet	Authenticated session with the ability to execute commands and match content within the result of the command
UDP	Open port scan using NMAP
WinRM	Windows Remote Manager authenticated connection with the ability to execute commands and match content within the result of the command
WMI Profile	Authenticated WinRM or SSH connection with the ability to evaluate: <ul style="list-style-type: none"> <li>• OS, Windows Security Center, Serial Number and Asset Tag</li> <li>• Windows Services</li> <li>• Running processes</li> <li>• Installed Application</li> </ul>
Network Traffic/Network Flow	Device type evaluation based on FortiGate session information
FortiGate/Firewall	Device type evaluation based on matching a firewall policy
ONVIF	Determines whether or not an endpoint supports a specific ONVIF Profile

Tabla 5:Needs to be read [13]

### 3. Must be received

Method	Definition
DHCP Fingerprinting	Device type evaluation based on the DHCP fingerprint compared to FortiNAC's Device Type database. Provides Operating System (OS) and hostname information
Passive	OS evaluation through analyzing network traffic with POf database.
Persistent Agent	Device type evaluation based on the Persistent Agent reported OS compared to FortiNAC's Device Type database

Tabla 6: Must be received [13]

#### 3.3.4 Funcionamiento del perfilado.

- 1) Un dispositivo o host se conecta a la red o se mueve a un nuevo puerto
- 2) FortiNAC detecta que algo se ha conectado o movido a un puerto
- 3) En caso de que la dirección MAC del dispositivo esté disponible, Device Identity la compara con las direcciones MAC conocidas
- 4) En caso de no tener conocimientos a cerca de la dirección MAC del dispositivo, FortiNAC lo detecta como un rogue, se recopila toda la información disponible para iniciar el proceso de perfilado
- 5) En el caso de un dispositivo tenga una dirección IP, Device Profiler inicia una comparación con todas las reglas de perfilado creadas y que se encuentran habilitadas hasta que una de ellas concuerda con la información disponible del dispositivo.
- 6) Esta coincidencia determina el tipo de dispositivo a partir de los métodos presentes en esa regla.
- 7) Podemos configurar FortiNAC para que cada vez que se profile un nuevo dispositivo, nos llegue aviso a nuestro correo electrónico.
- 8) En caso de que el dispositivo no coincida con ninguna regla, se le asociara con la regla Catch All predeterminada, de esta forma, lo tendremos perfilado, pero seguirá siendo un rogue.
- 9) Dentro de la propia regla de perfilado, existe una opción que determina un tipo de rol al dispositivo perfilado, en caso de no estar configurado, se le asignará la función predeterminada de NAC
- 10) Los dispositivos se pueden registrar tanto de forma manual o automática, en función de como esté estipulado en la regla.
- 11) Si la opción Register As esta habilitada, el dispositivo puede ser añadido a la vista de Host, inventario o en ambas.

- 12) En caso de que la opción, Access Availability haya sido configurada en base a la opción Specify Time, el acceso a la red para dichos dispositivos se limita a un periodo de tiempo determinado.
- 13) En el momento que el dispositivo se haya registrado, ya no aparecerá como un rogue y se mostrará en Host View, Inventory o en ambas según haya sido configurado.
- 14) Los dispositivos registrados y asociados con un usuario se colocan en la Vista de host y se eliminan de la ventana Profiled Devices.

### 3.4 Agente Persistente y certificados SSL en ordenadores corporativos.

FortiNac permite desplegar un agente persistente en nuestros endpoints corporativos, con el fin de ayudar tanto en la fase de perfilado como para verificar el cumplimiento de la política de cumplimiento (antivirus, parches) [13]. Una vez instalado, cada vez que el dispositivo arranque intentará contactar con FortiNAC para establecer un canal seguro sobre el que transmitir la información del dispositivo.

Todos los agentes han sido instalados en ordenadores con sistema operativo Windows. Cuando FortiNAC detecte que el terminal presenta dicho agente, lo interpretará como que se trata de un dispositivo corporativo y le dará permisos para poder acceder a la red interna de la empresa, en caso de no percibir la existencia de este lo asociará a un dispositivo no corporativo y únicamente le proporcionará permisos para acceder a internet.

En adición a la instalación del agente, también debemos modificar la clave de registro para, de este modo, poder conectar nuestro agente al servidor de agentes de FortiNAC.

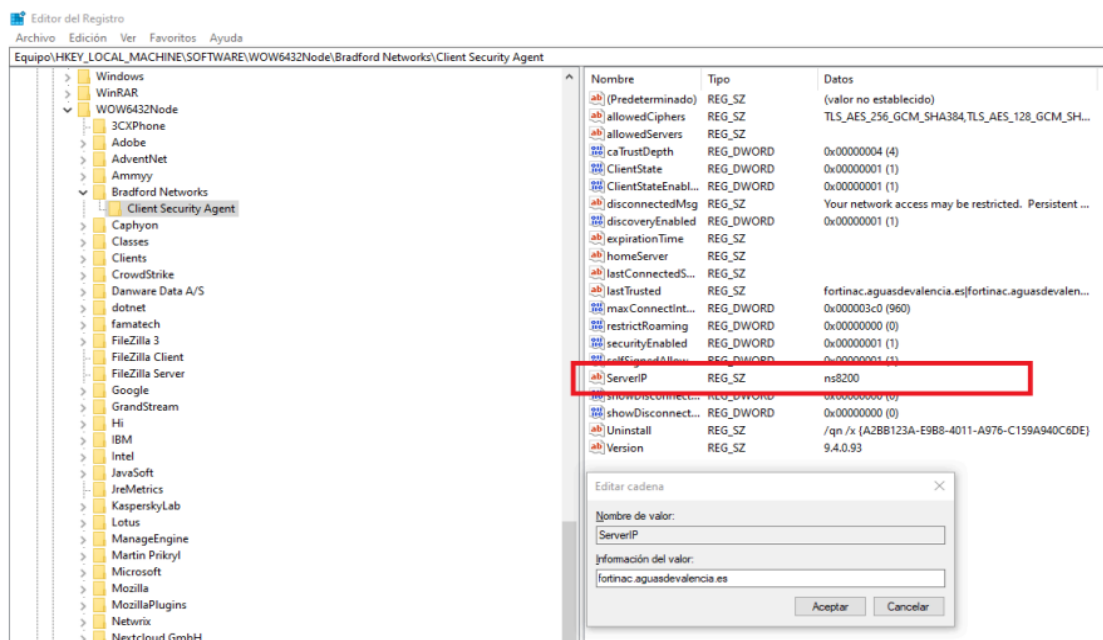


Ilustración 14: Modificar clave de registro [Fuente Propia]

Podemos identificar la presencia de este en nuestro terminal apreciando que aparece el siguiente símbolo en nuestra barra de tareas.

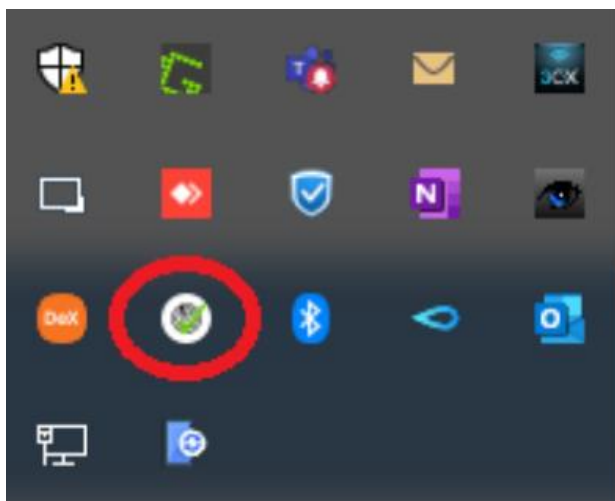


Ilustración 15: Agente persistente [Fuente Propia]

Con el fin de mantener una conexión SSL/TLS segura entre el Agente y el servidor de Agentes de FortiNAC, se precisará de la presencia e instalación de un certificado SSL en todos y cada uno de los dispositivos en los que se encuentre este agente.

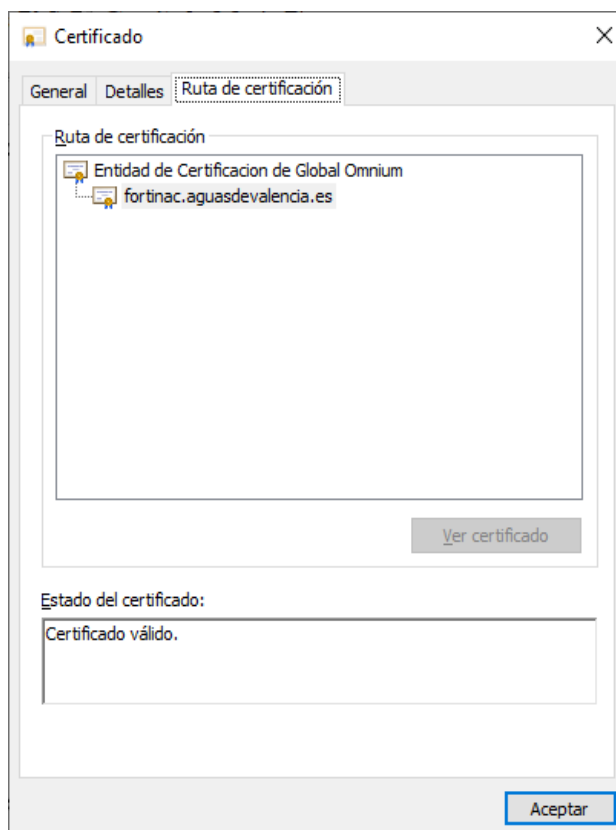


Ilustración 16: Certificado SSL

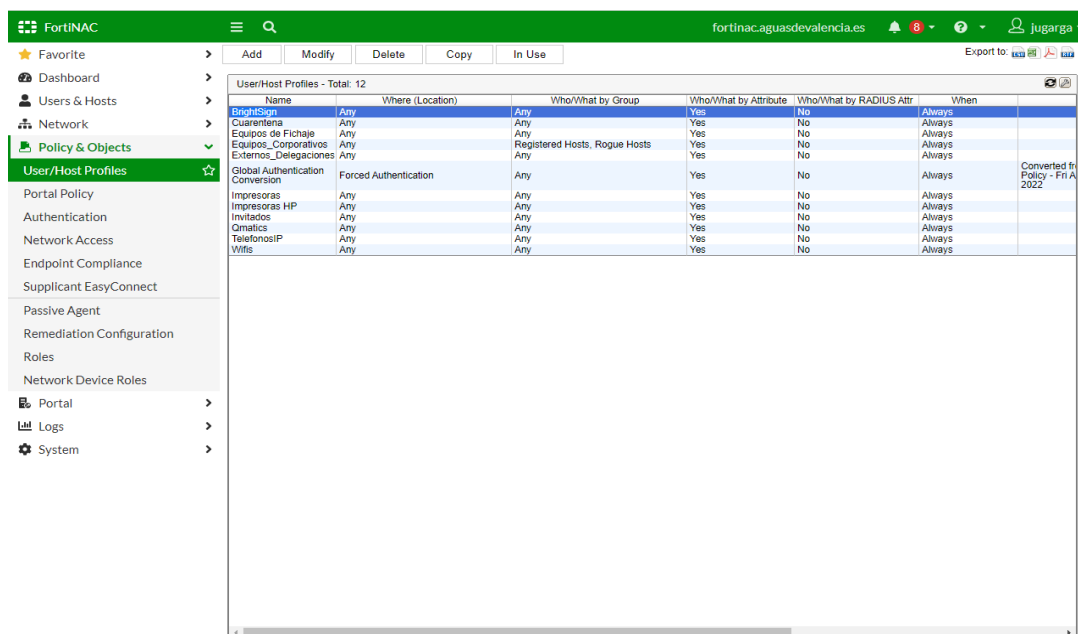
### 3.5 Políticas de acceso a la red.

Tras crear los perfiles de dispositivo e instalados los agentes persistentes en todos los ordenadores corporativos, procedemos a definir y relacionar los distintos dispositivos que se conecten a nuestra red con diversos métodos de acceso basándonos en la implantación de una serie de políticas. Para ello seguiremos una serie de directrices.

- Agrupación de perfiles.
- Definición de ámbitos de acceso a la red.
- Creación de las políticas de acceso a la red.

#### 3.5.1 Agrupación de Perfiles.

A modo de simplificar la aplicación de las políticas de acceso a la red, FortiNAC permite agrupar todos aquellos dispositivos que a precisar de una misma norma de acceso. Se han creado 12 grupos de dispositivos.

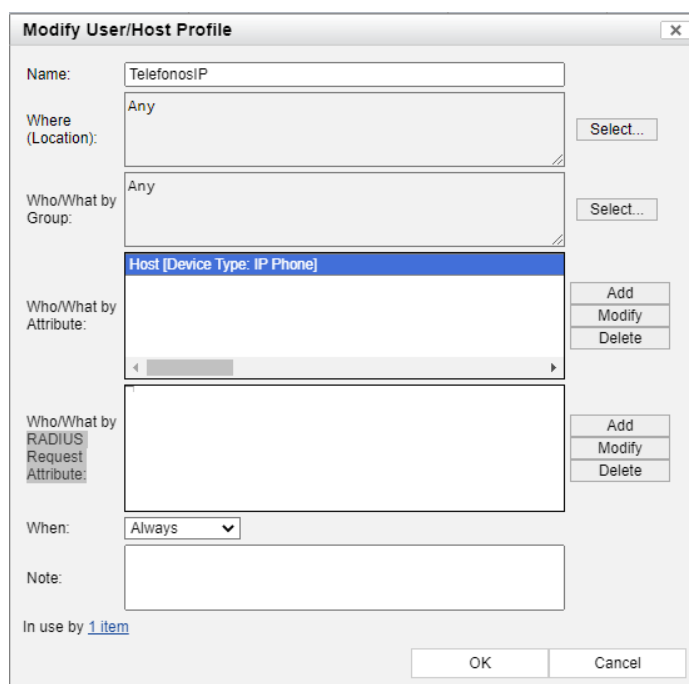


Name	Where (Location)	Who/What by Group	Who/What by Attribute	Who/What by RADIUS Attr	When
BrightSign	Any	Any	Yes	No	Always
Cuarentena	Any	Any	Yes	No	Always
Equipos de Fichaje	Any	Any	Yes	No	Always
Equipos_Corporativos	Any	Registered Hosts, Rogue Hosts	Yes	No	Always
Externos_Delegaciones	Any	Any	Yes	No	Always
Global Authentication Conversion	Forced Authentication	Any	Yes	No	Always
Impresoras	Any	Any	Yes	No	Always
Impresoras HP	Any	Any	Yes	No	Always
Invitados	Any	Any	Yes	No	Always
Qmatics	Any	Any	Yes	No	Always
TelefonosIP	Any	Any	Yes	No	Always
Wifis	Any	Any	Yes	No	Always

Ilustración 17: User/Host Profiles [Fuente Propia]

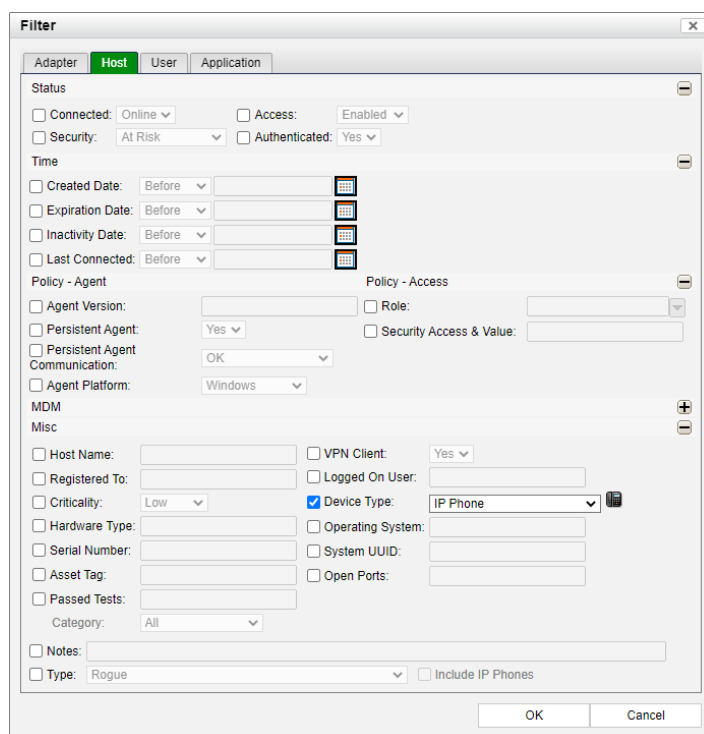
- BrightSign: Correspondiente a todos los dispositivos de cartelera.
- Cuarentena: Asociado a dispositivos que tienen algún error en el cumplimiento
- Equipos de Fichaje: Agrupa todos los dispositivos o perfiles de dispositivos empleados para registro de entrada y salida.
- Equipos\_Corporativos: Hace referencia a todos los dispositivos que tienen agente persistente instalado.
- Externos\_Delegación: Dispone de las cámaras de vigilancia, solo se le permitirá acceso a internet.
- Global Authentication Conversion:
- Impresoras: Incluye a todos los tipos de impresoras perfiladas.
- Invitados: Dispositivos no corporativos que se conecten a la red
- Qmatics: Agrupación de todos los dispositivos de pedida de turno.
- TelefonosIP: Hace referencia a todos los dispositivos de Telefonía IP.
- Wifis: Se encuentran reunidos todos los AP wifi

Tenemos diversas formas de poder generar estas agrupaciones, por localización, grupo al que pertenece, atributo al que hace referencia o solicitud de radius.



**Ilustración 18: User/Host Profile [Fuente Propia]**

Para llevar a cabo las agrupaciones, nos decantamos por el tipo de atributo, en la que nos permiten relacionarlos a nivel de adaptador, host, usuario o aplicación.



**Ilustración 19: Filtro en base al Host [Fuente Propia]**

### 3.5.2 Ámbitos de acceso a la red.

Debemos formalizar los distintos ámbitos de acceso a red que van a ser relacionados con las VLANs creadas y expuestas con anterioridad. La relación de estas mismas se efectuará en el momento en el que se de alta el switch de la sede en cuestión.

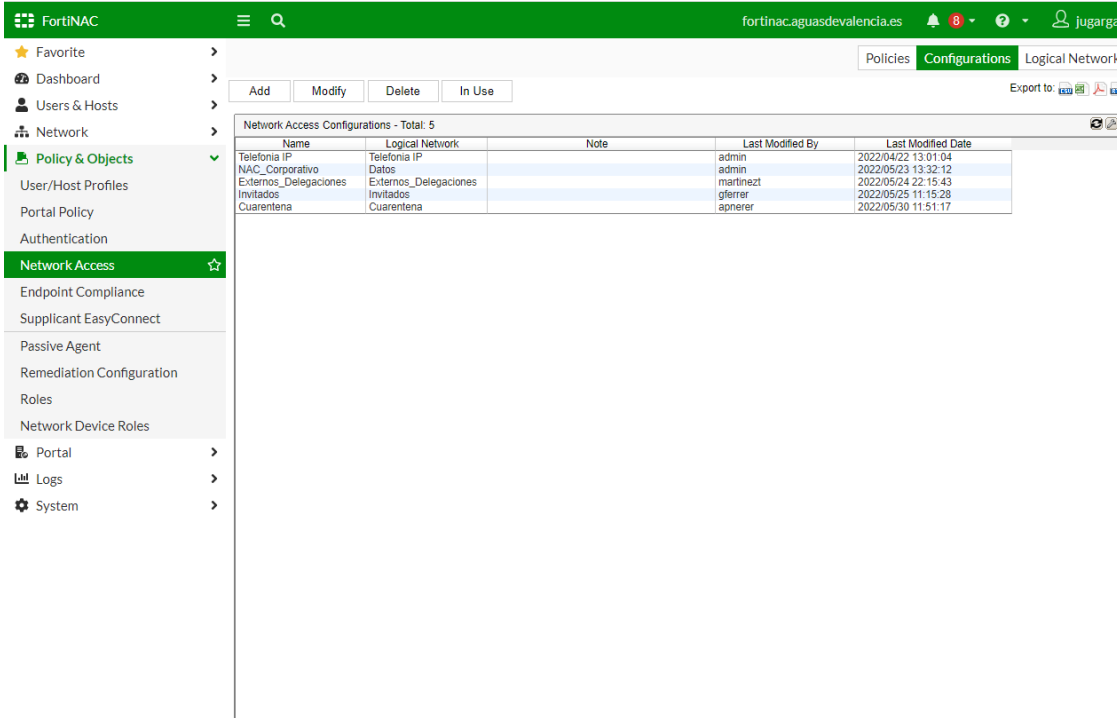
Name	Description	Last Modified By	Last Modified Date
Telefonia IP		admin	2022/04/22 13:01:02
Datos	VLAN para usuarios corporativos	admin	2022/04/28 12:28:10
Externos_Delegaciones		realinact	2022/05/24 22:14:28
Invitados		plernie	2022/05/25 11:15:27
Cuarentena		apnerer	2022/05/30 11:51:16

**Ilustración 20: Ámbitos de acceso a red [Fuente Propia]**

Se han creado cinco ámbitos de acceso que serán relacionados en función del dispositivo y el tipo de acceso que se requiera.

- TelefoníaIP: Asociado a la VLAN 69, este ámbito engloba a toda la Telefonía fija de la empresa.
- Datos: Asociada a la VLAN 33, se asociará a todos los dispositivos que tengan instalado agente persistente, Impresoras, equipos de fichaje y carteleras. A estos dispositivos se le dará acceso a la red interna de la empresa.
- Externos\_Delegación: Asociada a la VLAN 252, actualmente se le asigna a todos los dispositivos de vigilancia, como pueden ser cámaras, etc. Solo se da acceso a internet.
- Invitados: Asociada a la VLAN 252, todo ordenador que no tenga instalado agente persistente, es decir, sea detectado como un dispositivo no corporativo, se le asignará dicha VLAN con la que únicamente tendrá acceso a internet sin la posibilidad de acceder a la red interna de la empresa
- Cuarentena: Asociado a la VLAN 251, todo dispositivo que, durante el proceso de cumplimiento, sea detectado como un dispositivo no apto, falta de alguna actualización, detección de virus, será aislado en dicha VLAN hasta que el problema se haya subsanado.

Tras haber definido los distintos ámbitos de acceso a la red, los renombramos. Se tratan de cambios sutiles pero que serán necesarios para poder comprender la relación de estos con las distintas políticas de acceso a la red



The screenshot shows the FortiNAC web interface. The left sidebar contains navigation options like Dashboard, Users & Hosts, Network, Policy & Objects, and Network Access. The main content area displays a table of Network Access Configurations with 5 entries.

Name	Logical Network	Note	Last Modified By	Last Modified Date
Telefonia IP	Telefonia IP		admin	2022/04/22 13:01:04
NAC_Corporativo	Datos		admin	2022/05/23 13:32:12
Externos_Delegaciones	Externos_Delegaciones		martinez	2022/05/24 22:15:43
Invitados	Invitados		gferre	2022/05/25 11:15:28
Cuarentena	Cuarentena		agnerer	2022/05/20 11:51:17

**Ilustración 21: Renombramiento de Métodos [Fuente Propia]**

### 3.5.3 Creación de las políticas de acceso a la red.

Una vez han sido agrupados los perfiles de dispositivos en función de sus características y desempeño dentro de la red, creados los métodos de acceso a la misma y renombrados, debemos definir las políticas que relacionarán dichos métodos con las agrupaciones de dispositivos que hemos definido con anterioridad

Se han instaurado 10 políticas:

- Cuarentena
- Impresoras
- Acceso Telefono IP
- User\_Corp\_Acces
- Externos\_Delegación
- Invitados
- BrightSign
- Wifis Aerohive
- Qmatics
- Equipos de fichaje.



Rank	Enabled	Name	Network Access Configuration	User/Host Profile	Note	Last Modified By
1	✓	Cuarentena	Cuarentena	Cuarentena		apnerer
2	✓	Impresoras	NAC_Corporativo	Impresoras		apnerer
3	✓	Acceso Telefono IP	Telefono IP	TelefonosIP		apnerer
4	✓	User_Corp_Access	NAC_Corporativo	Equipos_Corporativos		jmartinez
5	✓	Externos_Delegaciones	Externos_Delegaciones	Externos_Delegaciones		jmartinez
6	✓	Invitados	Invitados	Invitados		jmartinez
7	✓	BrnchSign	NAC_Corporativo	BrnchSign		jmartinez
8	✓	Wifi Alerchive	NAC_Corporativo	Wifi		jmartinez
9	✓	Omatics	NAC_Corporativo	Omatics		jmartinez
10	✓	Impresoras HP	NAC_Corporativo	Impresoras HP		jmartinez
11	✓	Equipos de fichaje	NAC_Corporativo	Equipos de Fichaje	Equipos de fichaje	jmartinez

Ilustración 22: Políticas de acceso [Fuente Propia]

De esta forma, tendremos configurado los principales parámetros de nuestra herramienta de control de acceso.

### 3.5.4 Creación de grupos.

La funcionalidad de los grupos en FortiNAC tiene como objetivo organizar y administrar usuarios y dispositivos según ciertos criterios compartidos. Estos grupos se utilizan principalmente para facilitar la aplicación de políticas de seguridad, gestión y segmentación de la red.

Name	Type	Owner	Members	Days Valid	Days Inactive	Description	Last Modified By	Last Modified Date
Access Point Management	Port	System	0			Ports that have authorized access ports connected and the System is serving DHCP. Exceptions would be dumb hubs or wireless units.	SYSTEM	2020/07/22 05:01:36
Administrative Group	Administrator	System	25			Administrative users with all management access rights.	SYSTEM	2020/07/22 05:01:42
Authorized Access Ports	Port	System	2			Ports that have authorized access ports connected. Exceptions would be dumb hubs or wireless units.	SYSTEM	2020/07/22 05:01:37
Authorized DHCP Servers	Device	System	0			Authorized DHCP servers.	SYSTEM	2020/07/22 05:01:36
Device Interface Status	Device	System	211			Devices that participate in the updating of device interface status.	SYSTEM	2020/07/22 05:01:37
Forced Authentication	Port	System	0			Ports that participate in forced authentication LAN switching when hosts connect.	SYSTEM	2020/07/22 05:01:36
Forced Remediation	Port	User	1887			Ports that participate in forced remediation LAN switching when hosts connect.	jmartinez	2020/07/24 09:28:28
Forced Remediation Exceptions	Port	System	0			Ports that participate in forced remediation LAN switching when hosts connect. Hosts that do not participate in forced remediation.	SYSTEM	2020/07/22 05:01:37
Forced Scan Exceptions	Host	System	0			User machines that do not participate in forced scans.	SYSTEM	2020/07/22 05:01:36
Forced User Authentication Exceptions	Host	System	0			User machines that do not participate in forced user authentication.	SYSTEM	2020/07/22 05:01:36
GRP_FortNAC_OEM	Administrator	User	8			Host machines that all not have their agents updated through a global agent update.	SYSTEM	2020/07/23 13:50:12
GRP_FortNAC_READ	Administrator	User	2			Host machines that all not have their agents updated through a global agent update.	SYSTEM	2020/07/23 13:50:12
Global Agent Update Exceptions	Host	System	0			Host machines that all not have their agents updated through a global agent update.	SYSTEM	2020/07/23 13:50:12
INFORMATIONAL	Host	User	0			Informational hosts.	SYSTEM	2020/07/22 05:01:37
IP Phones	Host	User	0			IP phones that support the SNMP v3 protocol.	jmartinez	2020/07/22 05:01:37
L2 Network Devices	Device	System	214			Devices that support the SNMP v3 protocol.	SYSTEM	2020/07/22 05:01:37
L2 Wireless Devices	Device	System	211			Wireless devices that support the SNMP v3 protocol.	SYSTEM	2020/07/22 05:01:37
L3 (IP-NAC)	Device	System	5			Devices that participate in missing IP addresses to physical addresses.	SYSTEM	2020/07/22 05:01:37
Physical Agent Bridge	Host	User	1888			Physical agent bridge.	SYSTEM	2020/07/24 09:40:47
Physical Address Filtering	Device	System	0			Devices that participate in the enabling and disabling of physical addresses.	SYSTEM	2020/07/22 05:01:37
Port_FortNAC	Port	User	1887			Ports that participate in the enabling and disabling of physical addresses.	jmartinez	2020/07/24 09:28:28
Registration	Host	User	0			Group of all registered hosts.	SYSTEM	2020/05/28 11:58:29
Registration Hosts	Host	System	3727			Group of all registered hosts.	SYSTEM	2020/07/24 09:40:44
Reset Forced Default	Port	System	0			Ports that will return to the default VLAN when hosts disconnect.	SYSTEM	2020/07/22 05:01:36
Reset Forced Registration	Port	System	1887			Ports that will return to Registration when hosts disconnect.	SYSTEM	2020/07/22 05:01:37
Roaming Guest Hosts	Host	System	0			Roaming guest hosts (advertisers).	SYSTEM	2020/07/22 05:01:37
Roaming Quiet/Workbooks	Port	System	0			Hosts that participate in the Roaming quiet feature (advertisers).	SYSTEM	2020/07/22 05:01:37
Roaming Quiet Users	User	System	1			Roaming quiet users (advertisers).	SYSTEM	2020/07/22 05:01:37
Roque Hosts	Host	System	1128			Group of all roque hosts.	SYSTEM	2020/07/24 12:30:16
Role Based Access	Port	System	1887			Ports that participate in role based access when registered hosts with a Role connect.	SYSTEM	2020/07/22 05:01:36
Role Based Access	Port	User	1887			Ports that will be used to discover unauthorized DHCP servers and unauthorized DHCP servers.	jmartinez	2020/07/24 09:28:28
System DHCP Port	Port	System	0			System DHCP port.	SYSTEM	2020/07/22 05:01:36
Unauthorized Access Points	Device	System	0			Wireless Access Points whose connected clients should not be managed.	SYSTEM	2020/07/22 05:01:36

Ilustración 23: Grupos [Fuente Propia]

Los grupos permiten juntar elementos similares. Al crear estos, eliminamos la necesidad de configurar y controlar elementos dentro del grupo individualmente. Por ejemplo, si se colocan un conjunto de puertos en un grupo, puede modificar la configuración del grupo y afectará a todos los puertos simultáneamente.

En nuestro caso, no ha sido necesario la creación de ningún nuevo grupo diferente a los predefinidos por la propia herramienta FortiNAC.

- All Management Group: Grupo al que pertenecen todos los usuarios con derechos de gestión y administración de la herramienta.

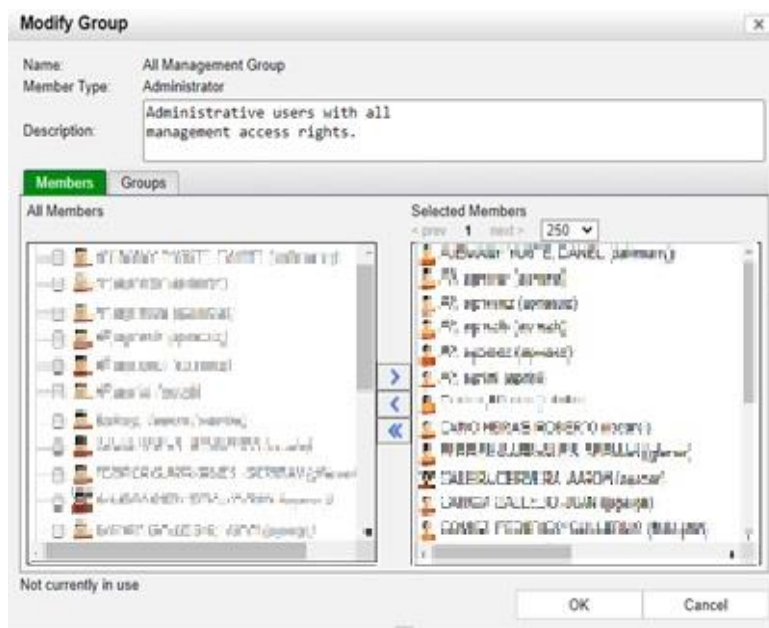


Ilustración 24: Grupo Administradores [Fuente Propia]

- Device Interface Status: Agrupación de dispositivos que participan en la actualización del estado de la interface de dispositivo.

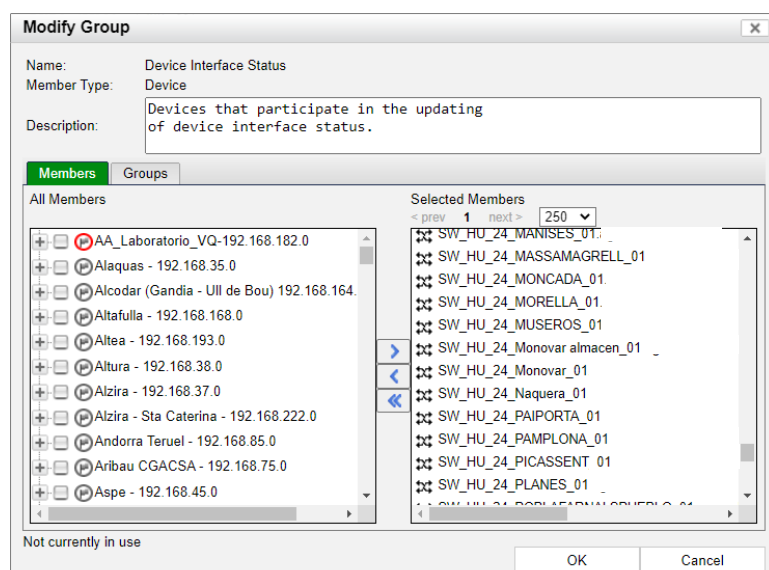


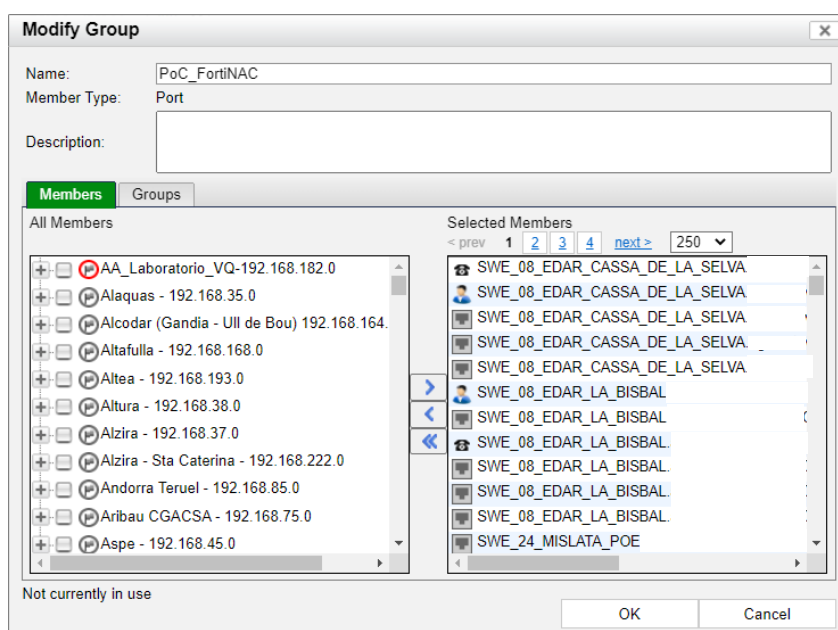
Ilustración 25: Grupo de gestión y administración de interfaces [Fuente Propia]

- Forced Registration: Grupo asignado a los puertos que participan en el registro forzado cuando se conectan dispositivos que anteriormente no han sido registrados. Dentro de este mismo grupo encontramos un subgrupo, PoC\_FortiNAC.

Forced Registration	Port	System	1666		Ports that participate in forced registration when unregistered hosts con
PoC_FortiNAC	Port	User	1666		

**Ilustración 26: Subgrupo PoC\_FortiNAC [Fuente Propia]**

PoC\_FortiNAC es asignado, como veremos posteriormente, a todas las interfaces de los nuevos switches instalados. El objetivo de este es asignar la VLAN 251 (Registro) a los dispositivos conectados para de esta forma poder aplicar el perfilado y asignación de las políticas de acceso a red.



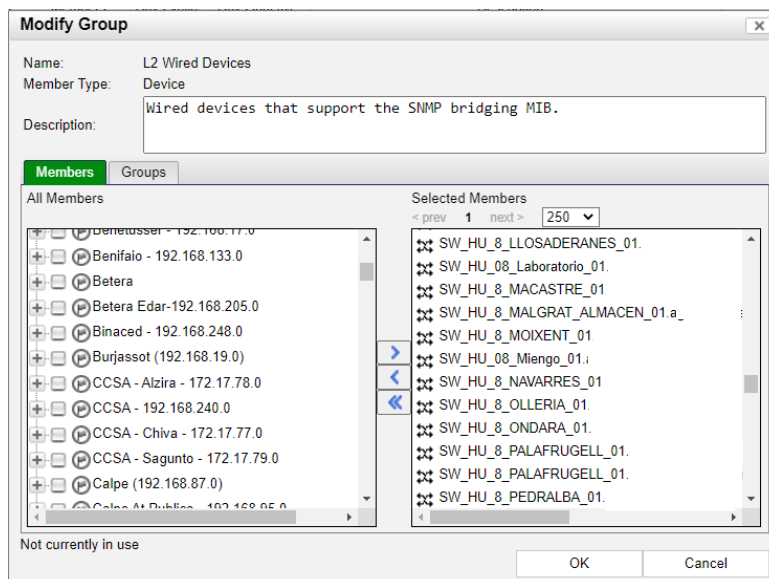
**Ilustración 27: Grupo de asignación VLAN de Registro [Fuente Propia]**

- L2 Wired Devices: FortiNAC lee la tabla de direcciones MAC del dispositivo de red (Switch). Esto le proporciona la dirección MAC del Host, el conmutador y la ubicación del puerto en la red. Los dispositivos L2 se colocan automáticamente en los grupos L2 Wired Devices o L2 Wireless.

L2 Network Devices	Device	System	214		Devices that support the SNMP bridging MIB.
L2 Wired Devices	Device	System	211		Wired devices that support the SNMP bridging MIB.
L2 Wireless Devices	Device	System	2		Wireless devices that support the SNMP bridging MIB.

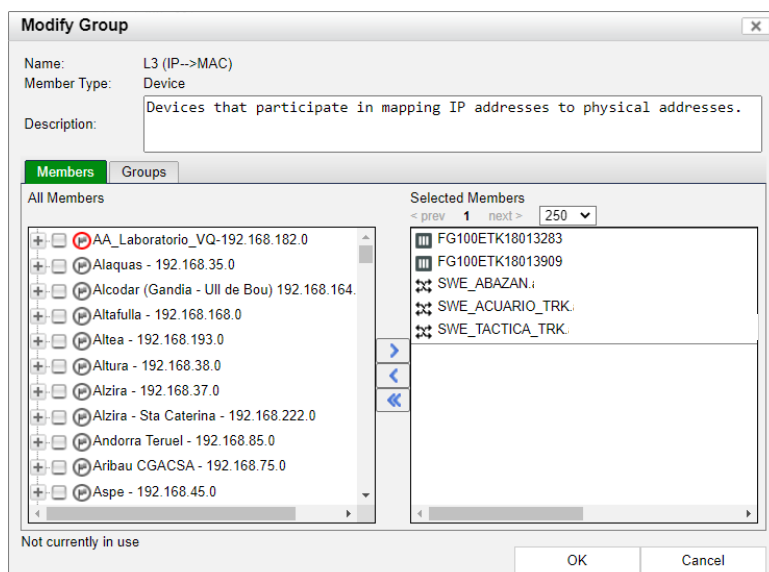
**Ilustración 28: Subgrupos L2 Network Devices [Fuente Propia]**

Podemos apreciar todos los dispositivos de capa 2 conectados a nuestra red, que están gestionados por FortiNAC.



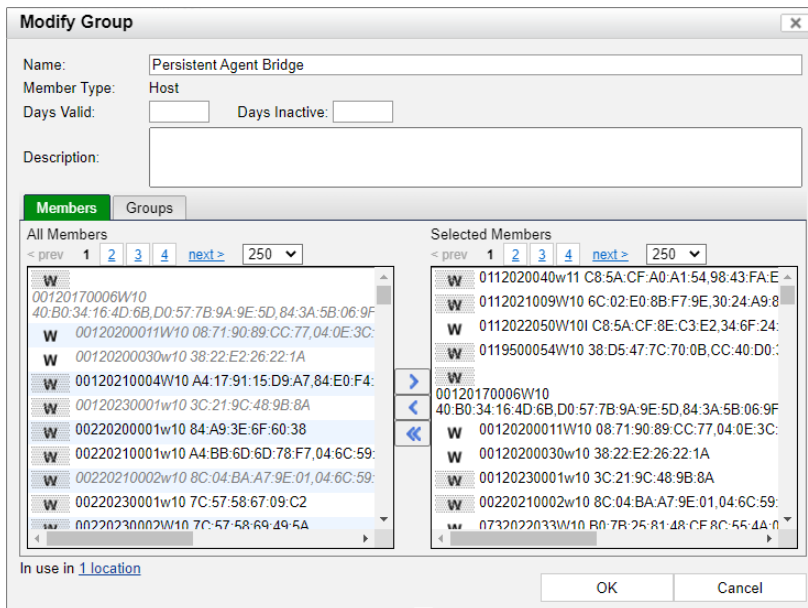
**Ilustración 29: Grupo de dispositivos de capa 2 [Fuente Propia]**

- L3 (IP→MAC): FortiNAC lee la tabla ARP del dispositivo de red, esto le proporciona la dirección IP correspondiente a la dirección MAC del host. Crea un grupo con todos estos dispositivos de capa 3 que se encuentran conectados a la red.



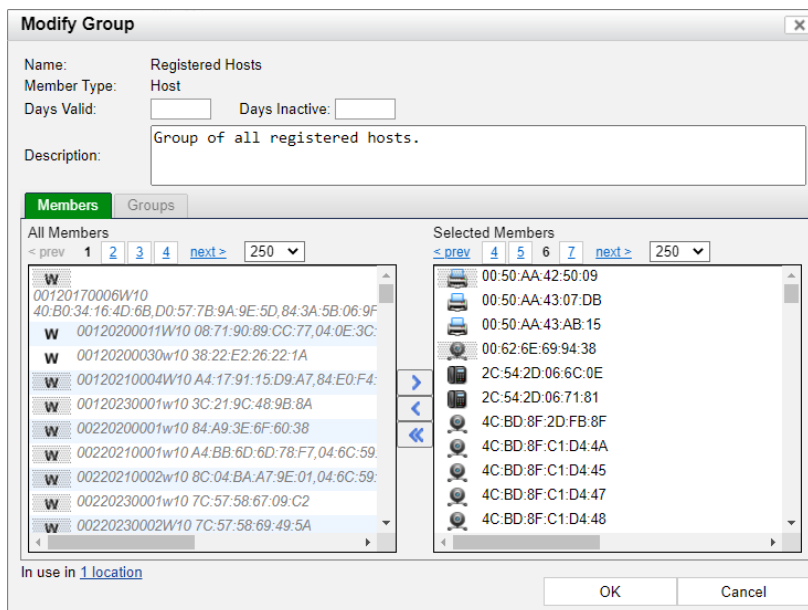
**Ilustración 30: Grupo de dispositivos de capa 3 [Fuente Propia]**

- Persistent Agent Bridge: En este grupo se encuentran todos los dispositivos finales (ordenadores) en los que tenemos instalado agente persistente.



**Ilustración 31: Grupo dispositivos con Agente Persistente [Fuente Propia]**

- Registered Hosts: Grupo en el que se incluyen todos los dispositivos que han sido registrados.



**Ilustración 32: Grupo de dispositivos registrados [Fuente Propia]**

- Reset Forced Registration: Puestos que deben volver a registrarse cuando el host se desconecta y se vuelve a conectar.

<input checked="" type="checkbox"/> Reset Forced Registration	Port	System	1666		Ports that will return to Registration when hosts disconnect.
PoC_FortiNAC	Port	User	1666		

**Ilustración 33: Subgrupo PoC\_FortiNAC [Fuente Propia]**

A los dispositivos que se encuentren conectados a ese puerto, se le asignará la VLAN de registro, es decir, este grupo, como podemos comprobar en la figura debe comprender el subgrupo PoC\_FortiNAC, una vez el dispositivo vuelva a ser detectado FortiNAC comprenderá que ese host ya ha sido perfilado y registrado y se le aplicarán las políticas correspondientes de acceso a la red, se trata de los mismos puertos comprendidos en la Ilustración 27.

- Rogue Host: Grupo al que pertenecen todos los dispositivos que han sido perfilados, pero actualmente no han podido ser registrados, el caso de aquellos que se han conectado alguna vez a la red, pero actualmente no se encuentran en ella.

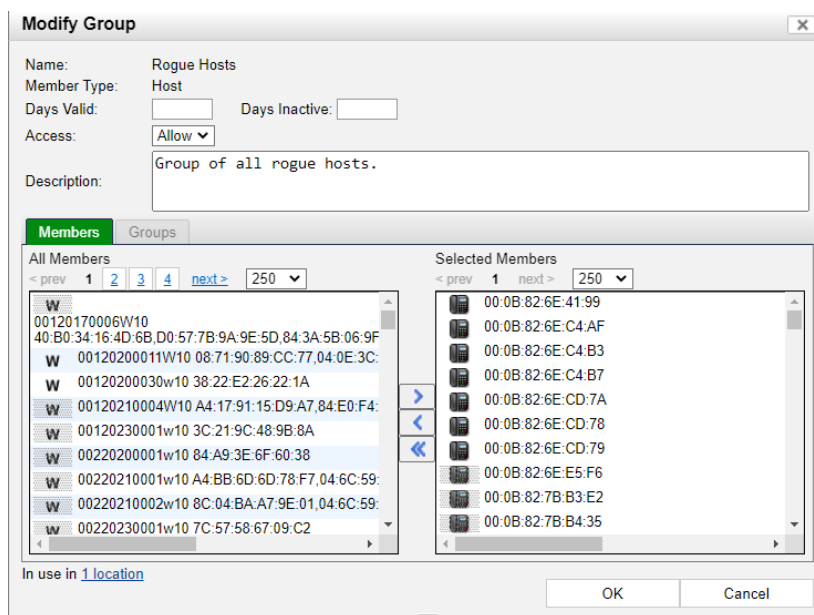


Ilustración 34: Grupo de Rogue Host [Fuente Propia]

### 3.6 Configuración de los Switchs

Ya tenemos configurada nuestra herramienta de control de acceso, una vez finalizada esta primera parte, comenzamos con la configuración de los switchs que van a ser instalados en cada una de las sedes.

Para configurar los switchs seguimos los siguientes pasos.

- Creamos la vlan de datos interface Vlanif33, le asignamos una IP al switch, ip address 192.168.x.5 255.255.255.0. La x la podemos interpretar por la subred correspondiente a cada una de las sedes [14].
- Creamos ruta estática entre cualquier dirección IP y la puerta de enlace (router) principal de cada sede ip route-static 0.0.0.0 0.0.0.0 192.168.x.1.
- Creamos el resto de interfaces virtuales, vlan de voz, vlan de registro y vlan de servicios externos.
- Añadimos las VLAN en modo hybrid en cada una de las interfaces del switch, en caso de los de 24 bocas en las 20 primera, dejando 3 de respaldo, en los de 8, se asignarán a las 7 primeras. Tanto la boca 24 como la 8 de cada uno de los switchs se configurarán en modo truck, estas interfaces serán las que se conecten con el router de la sede en cuestión.
- Configuramos los protocolos SNMP y SSH en cada uno de los switchs.

- Configuramos radius en todos los dispositivos como método de registro de los swichs en la herramienta FortiNAC.

Una vez configurados todos los switches, podemos comenzar con el despliegue de los mismos en cada una de las sedes de la empresa.

### 3.7 Implantación de switches y puesta en marcha del sistema.

En última instancia, debemos planificar el despliegue de switches en cada una de las sedes y coordinarnos con nuestros responsables de Vodafone para llevar a cabo la migración y reestructuración de la red. De forma inicial, en cada una de las sedes disponíamos de una única VLAN, para poder desplegar el nuevo servicio será necesario la propagación de 4 rutas correspondientes a cada una de las VLAN que se van a requerir.

#### 3.7.1 Gestión y propagación de rutas por parte de Vodafone.

En primer lugar, debemos contactar con nuestro CSV de Vodafone que en nuestro caso lo tenemos en la propia empresa indicándole la sede donde se va a hacer la migración, su direccionamiento IP y el DHCP Relay.

CLIENTE	SEDE	IP LAN	IP GESTION PPAL	TECNOLOGIA	IP GESTION BK	TECNOLOGIA BK	MODELO PPAL	Nº RO	MODELO BK
	vpn_laboratorio	192.168.182.0	172.18.111.90	4G	NA	NA	Huawei AR129	NA	NA

**Ilustración 35: Inventario Vodafone [Fuente Propia]**

Una vez tiene esta información, hace una búsqueda en su inventariado, asociando la IP de la sede a su IP de gestión del router, accede a el vía SSH.

Una vez dentro del router, se dan de alta las VLAN y se asocia el DHCP relay:

```
interface Vlanif33
description VLAN_DATOS
set flow-stat interval 30
ip address 192.168.182.1 255.255.255.0
clear ip df
dhcp select relay
dhcp relay server-ip 192.168.3.33
dhcp relay server-ip 192.168.3.27
```

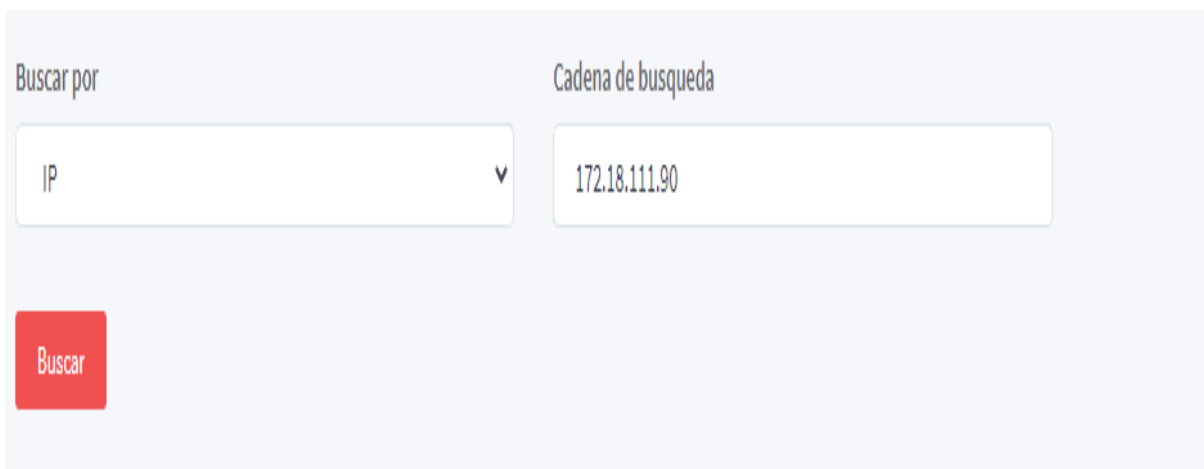
**Ilustración 36: Dar de alta VLAN [Fuente Propia]**

A nivel físico, la interface GigabitEthernet 0/0/0 se configura en modo trunk, esta interface es la que posteriormente se conectara a la boca 8 o 24 del switch.

```
interface GigabitEthernet0/0/0
description switch FortiNAC
port link-type trunk
port trunk allow-pass vlan 2 to 4094
```

**Ilustración 37: Modo trunk [Fuente Propia]**

Una vez se ha configurado correctamente el router y en caso de que en la sede haya instalado 4G, se publican las rutas a la red de MPLS de Vodafone.



**Ilustración 38: Búsqueda por IP [Fuente Propia]**

IP	Mascara	Next Hop	Etiquetas
192.168.182.0	255.255.255.0		Eliminar Ruta
172.19.182.0	255.255.255.0		Eliminar Ruta
10.252.182.0	255.255.255.0		Eliminar Ruta
10.250.182.0	255.255.255.0		Eliminar Ruta

**Ilustración 39: Publicación de rutas [Fuente Propia]**

### 3.7.2 Creación de ámbitos servidor DHCP

Damos de alta todos los ámbitos correspondientes a las distintas subredes de cada una de las sedes (Datos, Voz, Registro, Servicios Externos) en nuestro servidor `sil1.aguasdevalencia.es`, se configuran para que puedan entregar IPs del rango 192.168.x.220 a la 192.168.x.240 (Datos). En sedes más grandes el rango de direcciones se amplía para poder tener suficientes, pero por lo general, con disponer de 20 IPs en cada uno de los ámbitos es suficiente.



Dirreción IP del clic...	Nombre	Expiración de cesión	Tipo	Id. exclusivo	Descripción	Protección de acceso a redes	Expiración del...
192.168.190.26	0112019044a10...	Reserva (activa)	DHCP	443909123car		Acceso completo	ND
192.168.190.27	01120202523a7...	Reserva (activa)	Ninguno	a55c645d40	This address...	Acceso completo	ND
192.168.190.29	01120190697W15a...	Reserva (activa)	DHCP	3c4e16ff66a		Acceso completo	ND
192.168.190.30	01120190470a10...	Reserva (activa)	DHCP	186024a43ab		Acceso completo	ND
192.168.190.31	01120220230a7b10...	Reserva (activa)	DHCP	a8b17b3d59a	José Plaza M...	Acceso completo	ND
192.168.190.32	01120170250W15a...	Reserva (activa)	DHCP	1860247b0d1		Acceso completo	ND
192.168.190.33	01120170389W15a...	Reserva (activa)	DHCP	40b054a3eaf		Acceso completo	ND
192.168.190.34	01120190440a10...	Reserva (activa)	DHCP	443909123dar		Acceso completo	ND
192.168.190.35	01120202030a10...	Reserva (activa)	DHCP	e4d01e097f8	IRENE MOC...	Acceso completo	ND
192.168.190.36	0112017055W15a...	Reserva (activa)	DHCP	c4d8ff4b931		Acceso completo	ND
192.168.190.37	01120190370a10...	Reserva (activa)	DHCP	3c4e16f2751	Emilia Bonet	Acceso completo	ND
192.168.190.38	01120190537a10...	Reserva (activa)	DHCP	94b66e0e405		Acceso completo	ND
192.168.190.39	01120190445a10...	Reserva (activa)	DHCP	443909123a6		Acceso completo	ND
192.168.190.40	01120190537a10...	Reserva (activa)	DHCP	10e3a25a2b6		Acceso completo	ND
192.168.190.41	01120190370a10...	Reserva (activa)	DHCP	3c4e16f1e41		Acceso completo	ND
192.168.190.42	01120190441a10...	Reserva (activa)	DHCP	443909123d71		Acceso completo	ND
192.168.190.44	01120210430W15a...	Reserva (activa)	DHCP	6c0a08f817		Acceso completo	ND
192.168.190.45	01120190363a10...	Reserva (activa)	DHCP	10e3a25d118		Acceso completo	ND
192.168.190.46	01120190320a10...	Reserva (activa)	DHCP	1860247b2c3		Acceso completo	ND
192.168.190.47	01120170548W15a...	Reserva (activa)	DHCP	c4d8ff4b629		Acceso completo	ND
192.168.190.48	01120190100a10...	Reserva (activa)	DHCP	c4d8ff4b0421		Acceso completo	ND
192.168.190.49	01120210420W15a...	Reserva (activa)	DHCP	6c0a08f87b6	Ignacio Mor...	Acceso completo	ND
192.168.190.50	01120190711a10...	Reserva (activa)	DHCP	3c4e16f08a		Acceso completo	ND
192.168.190.51	01120190370a10...	Reserva (activa)	DHCP	a0c8374c31d		Acceso completo	ND
192.168.190.54	0112017050W15a...	Reserva (activa)	DHCP	c4d8ff4b099		Acceso completo	ND
192.168.190.55	01120170271a10...	Reserva (activa)	DHCP	c4d8ff4b286		Acceso completo	ND
192.168.190.57	01120190918a10...	Reserva (activa)	DHCP	96474d2f8f8		Acceso completo	ND
192.168.190.58	01120210007a10...	Reserva (activa)	DHCP	6c0a08f70ca		Acceso completo	ND
192.168.190.59	01120203098W15a...	Reserva (activa)	DHCP	74379330ca	Pascual Ra...	Acceso completo	ND
192.168.190.60	01120200118a10...	Reserva (activa)	DHCP	3822ba0ca0		Acceso completo	ND
192.168.190.61	01120160779W8...	Reserva (activa)	DHCP	10026c03302		Acceso completo	ND
192.168.190.62	0112017051W15a...	Reserva (activa)	DHCP	c4d8ff4b77a		Acceso completo	ND
192.168.190.63	01120170486W15a...	Reserva (activa)	DHCP	c4d8ff4b7b1		Acceso completo	ND
192.168.190.65	01120180317a10...	Reserva (activa)	DHCP	1860247b0af		Acceso completo	ND
192.168.190.66	01120190918a10...	Reserva (activa)	DHCP	96474d2f8f8		Acceso completo	ND
192.168.190.67	01120200234a10...	Reserva (activa)	DHCP	b05dad41985		Acceso completo	ND
192.168.190.68	01120202999W15a...	Reserva (activa)	DHCP	bce39b1d8c7		Acceso completo	ND
192.168.190.69	01120190918a10...	Reserva (activa)	DHCP	6c0a08f70ca		Acceso completo	ND
192.168.190.71	01120190404a10...	Reserva (activa)	DHCP	b05dad41975d4		Acceso completo	ND
192.168.190.72	01120200043a10...	Reserva (activa)	DHCP	3448e5da605	Antonio Pur...	Acceso completo	ND
192.168.190.74	01120190370a10...	Reserva (activa)	DHCP	a0c8374c3cc		Acceso completo	ND
192.168.190.75	01120170420W15a...	Reserva (activa)	DHCP	c4d8ff4b011		Acceso completo	ND
192.168.190.76	01120200200a10...	Reserva (activa)	DHCP	b05dad41949		Acceso completo	ND
192.168.190.78	01120190400a10...	Reserva (activa)	DHCP	443909123b180		Acceso completo	ND
192.168.190.80	01120203991a10...	Reserva (activa)	DHCP	7c73551c4d9	Marc Monc...	Acceso completo	ND
192.168.190.81	[Signat] Samsung...	Reserva (inactiva)	Ninguno	3077207cc	Vicente Villa...	Acceso completo	ND
192.168.190.82	01120200244a10...	Reserva (activa)	DHCP	b05dad42a2c		Acceso completo	ND

Ilustración 40: Conexiones direcciones IP DHCP [Fuente Propia]

### 3.7.3 Alta de switches en FortiNAC.

Tras tener preparado el ecosistema de FortiNAC, nos encontramos en disposición de comenzar con la implantación de los switches en cada una de las sedes de la empresa.

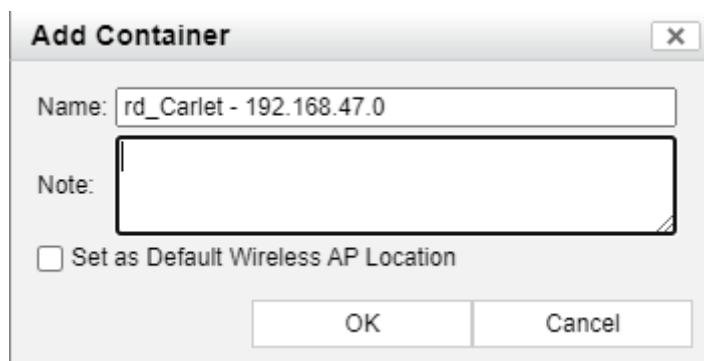
Una empresa externa, junto a nuestro CSV de Vodafone, se encargó de llevar a cabo la instalación en cada sede, una vez el switch se encontraba bien instalado y el CSV lo veía en la tabla ARP del router, podemos iniciar el proceso de registro en FortiNAC del nuevo switch.

Para ello en primer lugar vamos a la pestaña Inventory, hacemos clic derecho sobre Customer y seleccionamos Add container.

Customer	Name	Discovery Status	SNMP Devices	All Devices	Note
AA	Laboratorio_VQ-192.168.182.0	No discovery information available	3	3	
Alba	Albaquas - 192.168.35.0	No discovery information available	1	1	
Alca	Alcodor (Gandia - UI de Bou) 192.168.164.0	No discovery information available	2	2	
Alc	Alcudia Edar - 172.16.96.0	No discovery information available	0	0	
Alf	Alfaluja - 192.168.160.0	No discovery information available	1	1	
Alte	Altea - 192.168.193.0	No discovery information available	1	1	
Alt	Altura - 192.168.38.0	No discovery information available	1	1	
Alz	Alzira - 192.168.37.0	No discovery information available	1	1	
Alz	Alzira - Sta. Caterina - 192.168.2.0	No discovery information available	1	1	
And	Andorra Teruel - 192.168.85.0	No discovery information available	1	1	
Alt	Altura - 192.168.38.0	No discovery information available	1	1	
Anb	Anbau CGACSA - 192.168.75.0	No discovery information available	1	1	
Alz	Alzira - Sta. Caterina - 192.168.222.0	No discovery information available	1	1	
Asp	Aspe - 192.168.45.0	No discovery information available	1	1	
Beg	Begur - 192.168.145.0	No discovery information available	1	1	
Ben	Benetusser - 192.168.17.0	No discovery information available	2	2	
Ben	Benifaio - 192.168.133.0	No discovery information available	1	1	
Bet	Betera	No discovery information available	1	1	
Bet	Betera Edar-192.168.205.0	No discovery information available	1	1	
Bin	Binaced - 192.168.248.0	No discovery information available	1	1	
Bur	Burjassot (192.168.19.0)	No discovery information available	1	1	
CCS	CCSA - Alzira - 172.17.78.0	No discovery information available	1	1	
CCS	CCSA - 192.168.240.0	No discovery information available	5	5	
CCS	CCSA - Chiva - 172.17.77.0	No discovery information available	1	1	
CCS	CCSA - Sagunto - 172.17.79.0	No discovery information available	1	1	
Cal	Calpe (192.168.87.0)	No discovery information available	3	3	
Cal	Calpe At Publico - 192.168.95.0	No discovery information available	1	1	
Cal	Calpe Edar - 192.168.46.0	No discovery information available	1	1	
Cam	Campteluris - 192.168.122.0	No discovery information available	1	1	
Can	Canals - 192.168.39.0	No discovery information available	1	1	
Can	Canals Edar - 192.168.231.0	No discovery information available	1	1	
Can	Canals Edar - 192.168.231.0	No discovery information available	1	1	
Car	Carcaixent - 192.168.27.0	No discovery information available	1	1	
Cat	Catarroja - 192.168.29.0	No discovery information available	3	3	
Chi	Chiva - 192.168.216.0	No discovery information available	1	1	
Cor	Corbera del Ebre - 192.168.135.0	No discovery information available	1	1	
Den	Denia Edar - 172.17.16.0	No discovery information available	1	1	

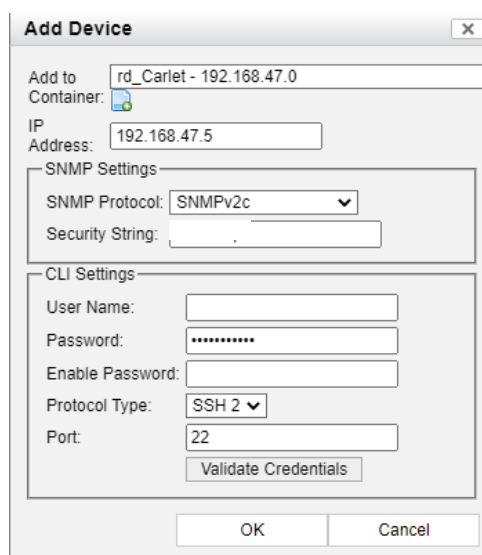
Ilustración 41: Inventory [Fuente Propia]

Creamos el contenedor con el nombre de la sede y la dirección IP de la subred correspondiente.



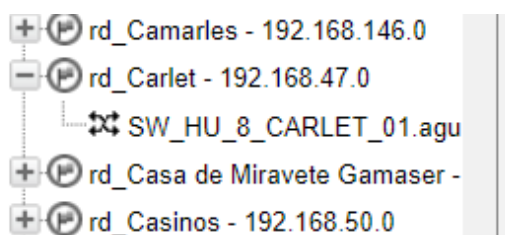
**Ilustración 42: Contenedor [Fuente Propia]**

Una vez creado el contenedor seguimos en la ventana Inventory hacemos clic derecho sobre el mismo y seleccionamos la opción Add device. Añadimos todos los parámetros de configuración para el switch en cuestión, emplea el protocolo SNMPv2c como método de control de red y se añaden las acreditaciones para poder acceder al switch via SSH.



**Ilustración 43: Credenciales switch [Fuente Propia]**

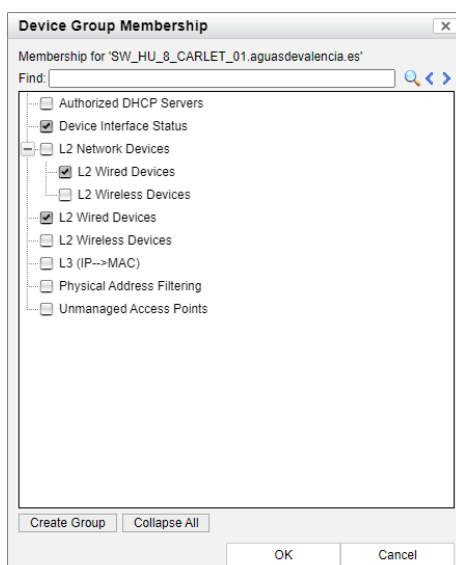
Una vez validadas las credenciales y en caso de no haber ningún problema con la configuración del switch o router, nos aparecerá un objeto dentro del contenedor creado.



**Ilustración 44: Registro del switch [Fuente Propia]**

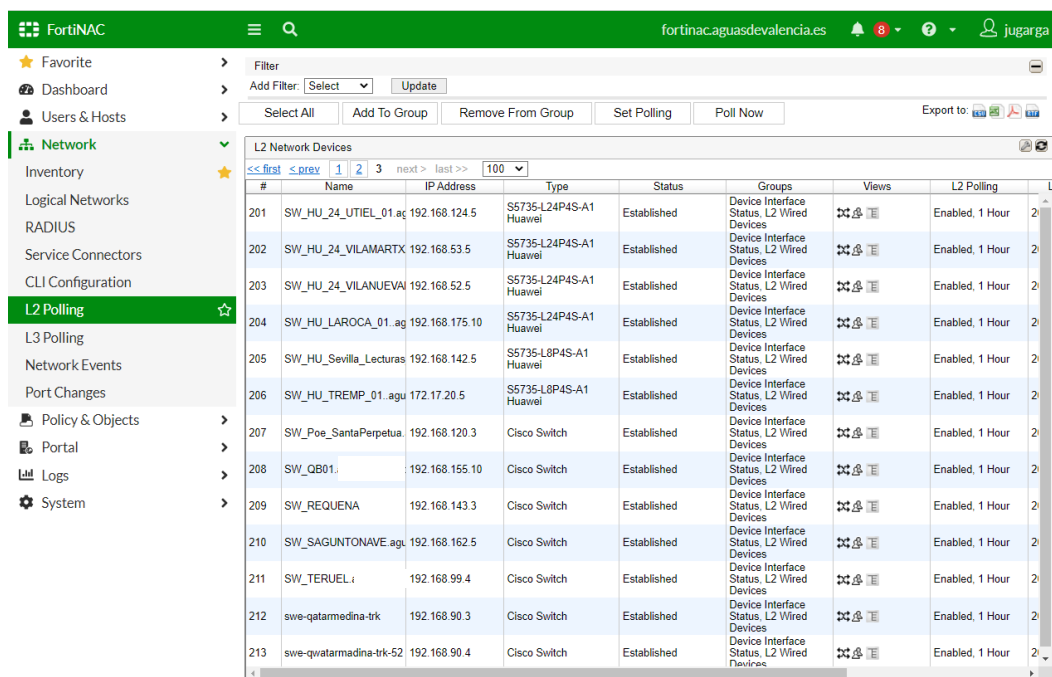
FortiNAC utiliza la función de sondeo L2 para saber dónde están conectados los hosts en la red según su dirección MAC. FortiNAC lee la tabla de direcciones MAC del dispositivo de red. La base de datos se actualiza con la dirección MAC, el conmutador correspondiente y la ubicación del puerto.

La ventana Sondeo L2 muestra los dispositivos que se agregaron manualmente. A medida que se agregan dispositivos, se evalúan. Cualquier dispositivo que sea capaz de sondear L2 (hosts de sondeo) se coloca inmediatamente en el subgrupo Dispositivos cableados L2 o Dispositivos inalámbricos L2



**Ilustración 45: Registro switches como L2 [Fuente Propia]**

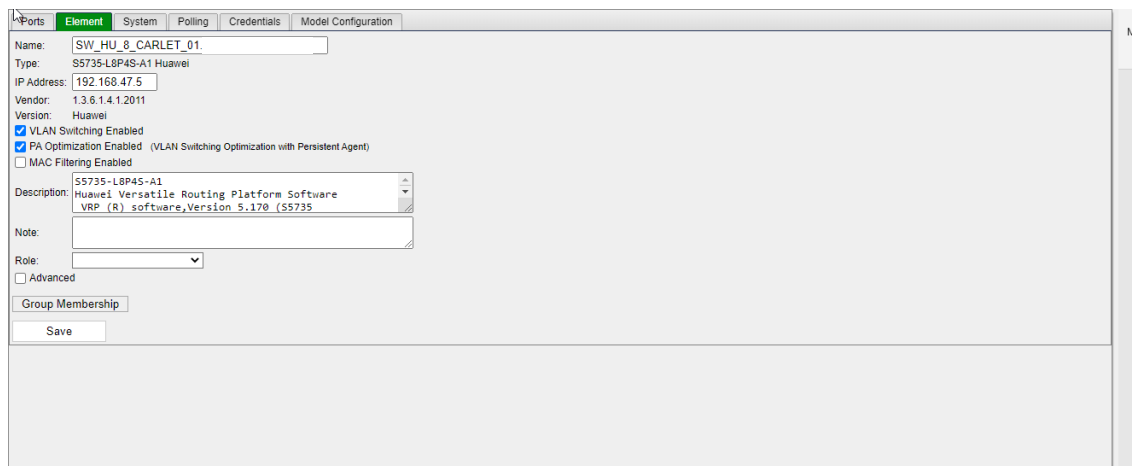
Si nos desplazamos por el menú hasta network L2 Polling, tendremos una vista de todos los dispositivos registrados manualmente y de capa 2.



#	Name	IP Address	Type	Status	Groups	Views	L2 Polling
201	SW_HU_24_UTIEL_01.ag	192.168.124.5	S5735-L24P4S-A1 Huawei	Established	Device Interface Status, L2 Wired Devices	🔍 📄 🗑️	Enabled, 1 Hour 2
202	SW_HU_24_VILAMARTX	192.168.53.5	S5735-L24P4S-A1 Huawei	Established	Device Interface Status, L2 Wired Devices	🔍 📄 🗑️	Enabled, 1 Hour 2
203	SW_HU_24_VILANJEVAI	192.168.52.5	S5735-L24P4S-A1 Huawei	Established	Device Interface Status, L2 Wired Devices	🔍 📄 🗑️	Enabled, 1 Hour 2
204	SW_HU_LAROCA_01.ag	192.168.175.10	S5735-L24P4S-A1 Huawei	Established	Device Interface Status, L2 Wired Devices	🔍 📄 🗑️	Enabled, 1 Hour 2
205	SW_HU_Sevilla_Lecturas	192.168.142.5	S5735-L8P4S-A1 Huawei	Established	Device Interface Status, L2 Wired Devices	🔍 📄 🗑️	Enabled, 1 Hour 2
206	SW_HU_TREMP_01.agu	172.17.20.5	S5735-L8P4S-A1 Huawei	Established	Device Interface Status, L2 Wired Devices	🔍 📄 🗑️	Enabled, 1 Hour 2
207	SW_Poe_SantaPerpetua	192.168.120.3	Cisco Switch	Established	Device Interface Status, L2 Wired Devices	🔍 📄 🗑️	Enabled, 1 Hour 2
208	SW_QB01.	192.168.155.10	Cisco Switch	Established	Device Interface Status, L2 Wired Devices	🔍 📄 🗑️	Enabled, 1 Hour 2
209	SW_REQUENA	192.168.143.3	Cisco Switch	Established	Device Interface Status, L2 Wired Devices	🔍 📄 🗑️	Enabled, 1 Hour 2
210	SW_SAGUNTONAVE.agu	192.168.162.5	Cisco Switch	Established	Device Interface Status, L2 Wired Devices	🔍 📄 🗑️	Enabled, 1 Hour 2
211	SW_TERUEL	192.168.99.4	Cisco Switch	Established	Device Interface Status, L2 Wired Devices	🔍 📄 🗑️	Enabled, 1 Hour 2
212	swe-qatarmadina-trk	192.168.90.3	Cisco Switch	Established	Device Interface Status, L2 Wired Devices	🔍 📄 🗑️	Enabled, 1 Hour 2
213	swe-qatarmadina-trk-52	192.168.90.4	Cisco Switch	Established	Device Interface Status, L2 Wired Devices	🔍 📄 🗑️	Enabled, 1 Hour 2

**Ilustración 46: L2 Polling [Fuente Propia]**

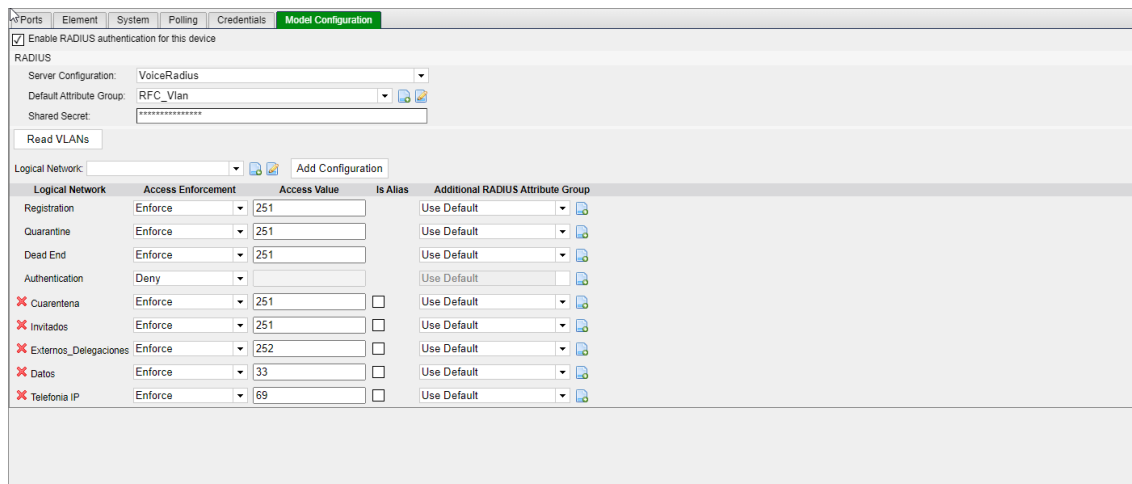
Seguindo con el registro del switch. En primer lugar, vamos a la pestaña Elements y seleccionamos la pestaña PA Optimization Enabled, opción cuya función es minimizar la cantidad de tiempo necesario para renovar la dirección IP del host cuando este se mueve a una nueva VLAN, esta opción se aplica únicamente a dispositivos que tengan instalado agente persistente.



**Ilustración 47: Habilitar aplicación agente persistente [Fuente Propia]**

En segundo lugar, vamos a la pestaña Model Configuration, seleccionamos la pestaña de Radius y aplicamos la configuración que se muestra en la Ilustración 48.

A continuación se muestra como mapeamos y asociamos la capa virtual creada en nuestro switch a nuestra herramienta de control FortiNAC. Appreciamos como la VLAN 69 se asocia a la telefonía IP, 33 a datos, 252 externos delegaciones e invitados y la 251 a Registro y Cuarentena



**Ilustración 48: Relacionamos las Network Access con su VLAN correspondiente. [Fuente Propia]**

Tras esto, hacemos un Polling para actualizar la tabla MAC del switch y ver los dispositivos que hay conectados a él, para ello pulsamos la opción L2 (Hosts) Polling → Poll Now

Ports | Element | System | **Polling** | Credentials | Model Configuration

Contact Status Polling: 10 (minutes) Poll Now  
Last Successful Poll: 2023/05/09 12:41:53  
Last Attempted Poll: 2023/05/09 12:41:53

L2 (Hosts) Polling: 60 (minutes) Poll Now  
Last Successful Poll: 2023/05/09 12:40:26  
Last Attempted Poll: 2023/05/09 12:40:26

Save

**Ilustración 49: Actualizamos tabla ARP del switch [Fuente Propia]**

Vamos a la pestaña de Ports y añadimos todos los puertos al grupo PoC\_FortiNAC, para ello seleccionamos todos los puertos, desde el 1 hasta el 7 o 23 en función del número de interfaces del switch, las interfaces 8 y 24 están conectadas al router de la sede

Ports | Element | System | Polling | Credentials | Model Configuration

Filter

Add Filter: Select Update

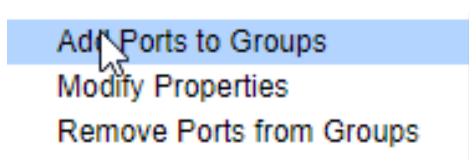
Select All Hide Details Panel Export to CSV PDF XLS

Ports - Displayed: 12 Total: 12

Status	Device	Label	Name	IP Address	Connection State	Default VLAN	Current VLAN	Admin Status	Operational State
	SW_HU_8_CARLET_01	IF#1	SW_HU_8_CARLET_01: GigabitEthernet0/0/1	192.168.47.5	Registered Host	251	33	On	Link Up
	SW_HU_8_CARLET_01	IF#2	SW_HU_8_CARLET_01: GigabitEthernet0/0/2	192.168.47.5	Phone	251	251	On	Link Up
	SW_HU_8_CARLET_01	IF#3	SW_HU_8_CARLET_01: GigabitEthernet0/0/3	192.168.47.5	Not Connected	251	251	Off	Link Down
	SW_HU_8_CARLET_01	IF#4	SW_HU_8_CARLET_01: GigabitEthernet0/0/4	192.168.47.5	User	251	33	On	Link Up
	SW_HU_8_CARLET_01	IF#5	SW_HU_8_CARLET_01: GigabitEthernet0/0/5	192.168.47.5	Not Connected	251	251	On	Link Down
	SW_HU_8_CARLET_01	IF#6	SW_HU_8_CARLET_01: GigabitEthernet0/0/6	192.168.47.5	Not Connected	251	251	On	Link Down
	SW_HU_8_CARLET_01	IF#7	SW_HU_8_CARLET_01: GigabitEthernet0/0/7	192.168.47.5	Not Connected	251	251	On	Link Up
	SW_HU_8_CARLET_01	IF#8	SW_HU_8_CARLET_01: GigabitEthernet0/0/8	192.168.47.5	Rogue Host	1	1	On	Link Up
	SW_HU_8_CARLET_01	IF#9	SW_HU_8_CARLET_01: GigabitEthernet0/0/9	192.168.47.5	Not Connected	1	1	On	Link Down
	SW_HU_8_CARLET_01	IF#10	SW_HU_8_CARLET_01: GigabitEthernet0/0/10	192.168.47.5	Not Connected	1	1	On	Link Down
	SW_HU_8_CARLET_01	IF#11	SW_HU_8_CARLET_01: GigabitEthernet0/0/11	192.168.47.5	Not Connected	1	1	On	Link Down
	SW_HU_8_CARLET_01	IF#12	SW_HU_8_CARLET_01: GigabitEthernet0/0/12	192.168.47.5	Not Connected	1	1	On	Link Down

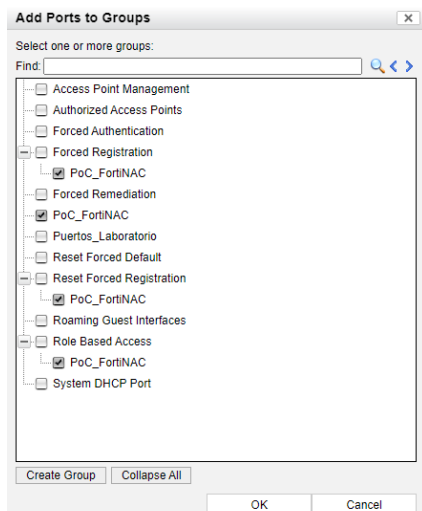
**Ilustración 50: Selección de puertos [Fuente Propia]**

Una vez los puertos han sido seleccionados, añadimos todos ellos a un grupo, para ello hacemos clic derecho y seleccionamos la opción Add Ports to Group.



**Ilustración 51: Add ports to group [Fuente Propia]**

Tras esto, nos aparecerá una tabla en la que se nos mostrarán todos los grupos comentados con anterioridad, en nuestro caso, seleccionaremos el correspondiente a PoC\_FortiNAC, el cual, como hemos explicado, apropiará a los dispositivos que se conecten a esa interface de la VLAN 251 (registro).



**Ilustración 52: Añadir puertos a grupo [Fuente Propia]**

Tras seguir todos estos pasos, registrados todos los componentes en la red y asignados a una de las VLAN's en función de sus características, tendremos una visión total de todo lo que se encuentra conectado al switch correspondiente.



## Capítulo 4. Conclusión

Para finalizar el Trabajo de Fin de Grado, se ha visto oportuno culminar con las ideas principales que se extraen tanto tras su realización como de su lectura.

A lo largo del desarrollo del proyecto he podido adquirir nuevos conocimientos y formándome en un área de las telecomunicaciones que no es en la que me he especializado, algo que ha supuesto un esfuerzo extra para poder entender y desarrollar el proyecto planeado.

Considero que haber podido trabajar en este proyecto ha supuesto un beneficio mutuo tanto para mí como para la empresa. Por un lado, a la empresa le ha servido para dar un primer paso para el control de acceso a la red, poder inventariar todos los dispositivos que hay conectados a ellas y poder responder a amenazas de una forma automatizada. Mis estudios a cerca de la herramienta han servido para la correcta estructuración e implantación de la misma en nuestra red, junto con la supervisión, gestión y migración de todas las sedes en las que se han instalado los nuevos switchs gestionados por FortiNAC, desde concordar entre las sedes y la empresa instaladora las fechas propicias para poder ir a realizar la instalación del nuevo switch, hasta el alta del mismo en la herramienta FortiNAC.

Refiriéndonos al aspecto económico, podríamos comentar que se trata de una inversión importante debido a la magnitud de la empresa, algo que supone un gran número de dispositivos conectados a la red y esto a su vez la necesidad de una gran cantidad de licencias. Hay que enfatizar en que el número de licencias consumidas no es en base a la cantidad de puertos disponibles sino al número de MACs descubiertas.

Por mi parte, el desarrollo del TFG me ha permitido formarme y adquirir conocimiento en base a la herramienta de control de acceso FortiNAC perteneciente a la rama de servicios que proporciona Fortinet, empresa que actualmente se considera puntera en desarrollo de softwares de ciberseguridad, junto a ello, tener el conocimiento del tipo de inconvenientes que pueden surgir a lo largo de su desarrollo e implantación y la manera de poder solventarlos de una forma rápida y eficiente ha sido otro de los aspectos en los que más puedo enfatizar.

Considero que he hecho un buen trabajo, he aportado y aprendido de mis compañeros, he tenido la oportunidad de formar parte de un grupo con el que he podido aprender y formarme y en el que se me ha proporcionado cierto grado de libertad para poder investigar y adquirir soltura con las herramientas empleadas.

## Bibliografía

1. Taniun, “Visibilidad, la pieza fundamental en las estrategias de ciberseguridad” [Citado el 25 de Mayo de 2023]; Disponible en; <https://cso.computerworld.es/tendencias/visibilidad-la-pieza-fundamental-en-las-estrategias-de-ciberseguridad> [Internet].
2. Jordi García (Arrow Español), “Expert’s View Webinar FortiNAC conoce todo en tu red” [Citado el 14 de Julio 2023]; <https://www.youtube.com/watch?v=DYtuO4WQ2mw&t=2702s> [Internet]
3. Fortinet, “Control de acceso a red segura” [Citado el 29 de Mayo de 2023]; [https://www.fortinet.com/lat/products/network-access-control\\_](https://www.fortinet.com/lat/products/network-access-control_), [Internet]
4. CIO Perú, “¿Qué es el NAC y por qué es importante para la seguridad de la red?” [Citado el 6 de Junio de 2023] <https://cioperu.pe/articulo/34067/que-es-el-nac-y-por-que-es-importante-para-la-seguridad-de-la-red/> [Internet]
5. NEURONET “FortiNAC, el Network Access Control de FORTINET” [Citado el 3 de Julio de 2023]; <https://neuronet.cl/fortinac-el-network-access-control-de-fortinet/> [Internet]
6. FotiXpert, “FortiNAC: Zero Trust con FortiNAC y FortiClient” [Citado el 26 de Mayo de 2023]; <https://fortixpert.blogspot.com/2020/04/fortinac-zero-trust-con-fortinac-y.html> [Internet]
7. FortiNAC Document Library, “Comunicaciones del servidor del agente” [Citado el 26 de Junio de 2023]; <https://docs.fortinet.com/document/fortinac/9.4.0/administration-guide/197526/mobile-agent> [Internet]
8. Snetic, “Switch Huawei S5735-L8P4S-A1 (S5735-L8P4S-A1)” [Citado el 3 de Julio de 2023] <https://www.snetic.es/product/S5735-L8P4S-A1> [Internet]
9. FortiXpert, “FortiNAC: Funcionalidades disponibles con la licencia Basic” [Citado el 3 de Julio de 2023]; <https://fortixpert.blogspot.com/2019/11/fortinac-funcionalidades-disponibles.html> [Internet]
10. Contribuyentes Wikipedia, “Protocolo ligero de acceso de directorios” [Citado el 12 de Julio de 2023]; [https://es.wikipedia.org/wiki/Protocolo\\_ligero\\_de\\_acceso\\_a\\_directorios](https://es.wikipedia.org/wiki/Protocolo_ligero_de_acceso_a_directorios) [Internet]
11. Contribuyentes Wikipedia, “RADIUS” [Citado el 14 de Julio de 2023]; <https://es.wikipedia.org/wiki/RADIUS> [Internet]
12. José Antonio Castillo, “LDAP: Qué es y para qué se utiliza este protocolo” [Citado el 12 de Julio de 2023]; <https://www.profesionalreview.com/2019/01/05/ldap/> [Internet]
13. FortiNAC, “Device Profiler Configuration” [Citado el 16 de Julio de 2023]; [https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/9529d49c-892c-11e9-81a4-00505692583a/FortiNAC\\_Device\\_Profiler\\_Configuration.pdf](https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/9529d49c-892c-11e9-81a4-00505692583a/FortiNAC_Device_Profiler_Configuration.pdf) [Internet]
14. FortiXpert, “Agente persistente FortiNAC” [Citado el 6 de Junio de 2023]; <https://fortixpert.blogspot.com/2019/03/agente-persistente-fortinac.html> [Internet]
15. FortiXpert, “FortiNAC: Gestión de puertos con múltiples hosts mediante 802.1x - MAB” [Citado el 5 de Julio de 2023]; <https://fortixpert.blogspot.com/2020/04/fortinac-gestion-de-puertos-con.html> [Internet]