Escola d'Enginyeria de Telecomunicació i Aeroespacial de Castelldefels
UNIVERSITAT POLITÈCNICA DE CATALUNYA

TRABAJO FINAL DE GRADO

TÍTULO DEL TFG: REMODELACIÓN DE LA RED LAN DE IEAISA A TRAVÉS DE SOLUCIÓN NAC

TITULACIÓN: Grado en Ingeniería de Sistemas de Telecomunicación

AUTOR: Víctor Giménez Porcell

DIRECTOR: Héctor Rodríguez Carro

SUPERVISOR: Enrica Valeria Zola

FECHA: 17 de junio del 2019

Título: Remodelación de la red LAN de IEAISA a través de la solución NAC

Autor: Víctor Giménez Porcell

Director: Héctor Rodríguez Carro

Fecha: 17 de junio del 2019

Resumen

Cada año que pasa la seguridad en las empresas está más presente en la sociedad. Eso se ve reflejado en los recursos que invierten para prevenir los posibles ataques e infecciones.

Este proyecto mostrará como la empresa IEAISA modifica toda su red LAN dándole una mayor seguridad y proporcionándole un funcionamiento mucho más eficiente.

La modificación ha sido iniciada por la proposición de una solución NAC (Network Access Control) que permita controlar el acceso de todos los dispositivos que estén en la empresa. Esta tecnología permite analizar y separar los dispositivos mediante diferentes políticas y procedimientos internos permitiendo así que un usuario que no tenga permisos para ver ciertos recursos no sea capaz de verlos independientemente de dónde o cómo realice su conexión.

Junto a esta solución se realizará una modificación de todos los dispositivos que ya existían antes de este proyecto adaptándose al nuevo funcionamiento que tendrá la red.

Se ha realizado una investigación sobre el funcionamiento de la solución NAC y tecnologías asociadas a ésta, seguido de una elección del mejor NAC que se adapte a las características de la empresa y documentando todo el proceso de cambio que ha sufrido toda la red de IEAISA, acabando con la configuración de todos los dispositivos y de la solución NAC elegida para poder llegar a los objetivos establecidos.

Title: Remodelación de la red LAN de IEAISA a través de la solución NAC

Author: Víctor Giménez Porcell

Director: Héctor Rodríguez Carro

Date: June 17, 2019

Overview

Information systems, security and networks are the main asset of organizations today. This is reflected in the resources they are investing in order to prevent further attacks and vulnerabilities.

This project shows how the IEAISA company has to restructure its local area network (LAN) in order to improve the security and to increase the efficiency in their daily operation.

In order to carry out the remodeling a Network Access Control (NAC) solution has been proposed allowing to control the access of all devices among the company. This technology enables the possibility to analyze and separate organization devices throughout the use of internal policies and procedures that restric the access according to specific control policies. Furthermore, it is capable to restrict the access to the resources of the company for those users who do not have a permission, regardless from where they try to access (i.e., inside the company or remotely).

Additionally, this solution requires that many devices must be reconfigured, by adapting them to the new operation and behavior of the network.

An investigation has been carried out on the operation of the NAC solution and associated technologies, followed by a choice of the NAC that best fits the characteristics of the company. The entire process has been documented, including the whole change process followed by IEAISA network and summing up with the configuration of all the devices and the NAC solution chosen in order to achieve the established objectives.

AGRADECIMIENTOS

Antes de todo agradecer a Enrica Valeria Zola por aceptar llevar mi Trabajo Final de Grado, por el perfecto seguimiento que ha hecho y todas las correcciones que han permitido mejorar el proyecto.

Agradecer con especial cariño a mi jefe y director de TFG Héctor Rodríguez Carro que fue el que me introdujo en el mundo de las redes y me dio la oportunidad de trabajar en este sector. Además, le doy las gracias por ayudarme a aprender cada día algo nuevo y por darme la oportunidad de certificarme en muchos cursos para poder adquirir nuevos conocimientos.

Por otro lado, agradecer a los compañeros y amigos de trabajo Álex, Óscar, Dani y Sergi que me han ayudado en los problemas que me han ido surgiendo y a la vez también me han enseñado muchos conocimientos del sector.

Por último, agradecer a mi familia y pareja Laura por animarme cada día y apretar cuando era necesario para que pudiera ya no solo realizar este trabajo sino poder optar a sacarme este Grado.

ÍNDICE

ÍNDICE DE FIGURAS

ACRÓNIMOS

- AD → Active Directory
- BYOD → Bring Your Own Device
- DG → Default Gateway
- DHCP → Dynamic Host Configuration Protocol
- DNS → Domain Name System
- EAP → Extensible Authentication Protocol
- EAPOL → Extensible Authentication Protocol Over LAN
- IP → Internet Protocol
- IPS → Intrusion Prevention System
- IT → Information Technology
- LAN → Local Area Network
- LDAP → LightWeight Directory Access Protocol
- MAC → Media Access Control
- NAC → Network Access Control
- PDP → Policy Decision Point
- PEP → Policy Enforcement Point
- RADIUS → Remote Authentication Dial-In User Service
- SSID → Service Set Identifier
- VID → VLAN ID
- VLAN → Virtual Local Area Network
- VPN → Virtual Private Network
- WAN → Wide Area Network

- WiFi → Wireless Fidelity

CAPÍTULO 1. INTRODUCCIÓN

1.1. LA SEGURIDAD EN EMPRESAS

La seguridad a nivel de IT en las empresas en los últimos años ha experimentado un crecimiento disparado debido al constante avance de la tecnología y al aumento de ataques e infecciones cibernéticas que se han ido produciendo en muchas de las empresas actuales. Según un estudio de Norton (el Cyber Security Insigh Report, [1, 2]), uno de cada tres españoles fue víctima de un ataque cibernético durante el 2018, situando a España en el tercer puesto de países que más ataques de este tipo reciben, detrás de E.E.U.U y el Reino Unido.

Además de los datos mostrados, INCIBE (Instituto Nacional de Ciberseguridad, [3]) dice que, a lo largo del primer trimestre de 2018, usuarios y empresas recibieron un total de 9.000 ataques.

Con esta información es lógico que cada vez más las empresas intenten permanecer protegidas contra estos ataques, contratando o haciendo ellos mismos una remodelación de su red que sea capaz de proporcionar la seguridad necesaria adaptándose a los avances que se vayan produciendo día a día.

Para llegar a un nivel de protección de la red óptimo, una empresa ha de ser capaz de proporcionar una seguridad tanto a nivel WAN (Wide Area Networks, zona que une varias zonas LANs y da la salida hacia internet) como LAN (Local Area Network, red interna que une diferentes dispositivos internos).

El error que se comete en muchas empresas es centrase únicamente en la parte WAN, es decir, invierten muchísimos recursos en adquirir un firewall de última generación que proteja contra ataques de intrusión (IPS, Intrusion Prevention System), Content Filter (control de acceso a las webs) y otros mil aspectos más relacionados con esa parte. En otras palabras, se protegen de los ataques que vienen desde el exterior. En cambio, no dedican recursos a proteger la zona LAN de la empresa, es decir, no se protege todo el tráfico interno que se genera en el interior.

Este proyecto se centrará en la parte que según la experiencia obtenida desde la incorporación a IEAISA es la más olvidada, la parte LAN de las empresas, donde es igual o más importante el uso de medidas de seguridad que en la zona WAN.

Según diversos estudios publicados, cada vez está más al día adoptar el termino BYOD (Bring Your Own Device) [4], este concepto significa que cada vez más empresas están permitiendo a sus trabajadores llevar sus dispositivos al trabajo y conectarse a su red. Esto puede provocar que la red sea vulnerada desde frentes donde antes no lo era. Cualquier empresa con un mínimo de seguridad, ya no puede tener un direccionamiento completamente plano, es

decir, una única LAN donde se sitúan trabajadores por red cableada, trabajadores que se conectan vía WiFi, servidores y todo el resto de recursos internos. Si la tiene, se expone a que todos los dispositivos sean capaces de acceder a recursos a los que no deberían tener acceso, y, además, si traen un malware o archivo infectado antes o una vez dentro de la red se propagará por toda ella sin siquiera pasar por el firewall de última generación debido a que el tráfico únicamente se propagaría por el interior de la LAN.

1.2. OBJETIVOS DEL PROYECTO

La empresa IEAISA se dedica a diseñar, evolucionar y mantener sistemas de IT, tanto para entidades privadas como para entidades públicas. Sus funciones básicas son prestar servicios de Consultoría, implantar y dar soporte y administración a sistemas IT (Networking , CiberSeguridad y Sistemas), tanto en formato on-premise (local) como en Cloud. Esto implica el diseño y planificación de muchos elementos de red interconectados entre ellos, consiguiendo un nivel de eficiencia y seguridad de red óptimo. Por ello, los clientes en muchas ocasiones piden un mínimo de confianza a la empresa para demostrar que es capaz de realizar dicha tarea con un procedimiento y un resultado muy alto.

Es por este motivo que IEAISA se propone obtener los certificados ISO 27001 y 27017 de Seguridad y Servicios en la nube, los cuales requieren un nivel de exigencia en la propia red excelente, tanto a nivel WAN como LAN. Además, consiguiendo estos certificados a la vez también se conseguiría proteger la red de cualquier tipo de ataque y dar la confianza necesaria a los clientes para que asignen la realización de sus proyectos con total seguridad de que los métodos utilizados serán los correctos.

Tal y como se ha explicado en la sección 1.1, IEAISA entra en el gran grupo de empresas que tienen una protección WAN muy buena, con un firewall de última generación configurado para bloquear todo tipo de ataques externos, pero una seguridad LAN muy baja con una red plana (es decir, con un direccionamiento único en el que todos los dispositivos de la red pertenecen al mismo rango IP) con acceso a todos los recursos.

La propuesta de este proyecto viene motivada por la necesidad de adaptar y mejorar toda la zona LAN con el propósito de mejorar su funcionamiento y la protección de la empresa.

Por ello IEAISA quiere instalar y configurar un dispositivo NAC que proporcione seguridad a la red y registre los dispositivos que se tienen conectados. Junto con esta propuesta y relacionada con la misma se requiere una mejora de todo el funcionamiento de la red en general que conllevará a una segmentación de la red a nivel cableado y wifi y que derivará en la modificación de muchos dispositivos para poder llegar al objetivo final.

Además de esto, IEAISA quiere que la red cableada sea auto gestionable, con lo que no se requiera de ningún técnico dedicado configurando puertos cada

vez que se tenga que asignar una dirección IP dependiendo del usuario que se conecte a cada toma.

Por tanto, este proyecto se ha centrado en la remodelación de la red LAN de la empresa IEAISA y en la instalación y configuración de la solución NAC con la finalidad de conseguir la seguridad en la autenticación y la red auto gestionable.

Visto de manera más clara los objetivos de este proyecto han sido:

- Remodelar el direccionamiento interno de la empresa
- Separar el acceso cableado de las diferentes zonas de trabajo como técnicos, comerciales o personas externas a la empresa
- Creación de nuevos Service Set Identifier (SSID) WiFis para la utilización del corporativo mediante autenticación LightWeight Directory Access Protocol (LDAP) y el de invitados sin acceso a los recursos internos de IEAISA
- Adaptar y crear configuraciones en los dispositivos existentes de la red
- Conseguir red auto gestionable
- Instalación y configuración de la solución NAC

1.3. METOLOGIA USADA

Para realizar todos los objetivos mencionados, durante el transcurso de este proyecto se ha seguido la siguiente metodología.

En primer lugar, se ha tenido que conversar con la empresa para ver cuál era el propósito final al que querían llegar. Tras informarse sobre qué era la tecnología NAC y cuál era su funcionamiento, se ha tenido que realizar un estudio exhaustivo de las soluciones NAC existentes para poder compararlas entre sí y poder finalmente elegir la solución que mejor se adaptará a las necesidades de la empresa.

Una vez elegida la tecnología a implementar, se ha tenido que estudiar con detalle la configuración actual de la LAN de IEAISA, evidenciar los puntos débiles de cara a posibles ataques internos y estudiar qué solución proponer para evitarlos.

Tras haber identificado los cambios necesarios para ofrecer una solución más segura a la LAN de IEAISA, se ha tenido que plantear un nuevo diseño de red y configurar todos los dispositivos implicados.

1.4. ESTRUCTURA DEL PROYECTO

En este punto se explicará de una forma un poco más extendida como se estructura todo el proyecto.

Tal y como se ha podido ver en la sección 1.3, el proyecto se ha divido en 5 capítulos principales.

El capítulo 1 es la introducción del trabajo, en ella se puede ver cuál es el escenario global que se plantea en el trabajo y de donde surge.

En el capítulo 2 se introducen conceptos teóricos generales que se han creído esenciales para entender el proyecto, en él se habla de lo que es una VLAN, la solución NAC y la normativa 802.1x.

El capítulo 3 ya se centra en la elección de la solución NAC que se ha llevado a cabo, compara soluciones tanto Opensource como de pago y en el tramo final explica cual se ha elegido y los motivos de su elección.

En el capítulo 4 se explica detalladamente el funcionamiento que tiene actualmente la red de IEAISA y se introducen los detalles de las mejoras que se tendrán que implementar.

En el último capítulo se ve el funcionamiento de la nueva red de IEAISA y se explica en detalle las mejoras en los dispositivos que ya existían y la implementación de la nueva solución NAC.

Tal y como puede deducirse viendo el avance del proyecto, los capítulos 4 y 5 serán los más largos debido a que serán los apartados donde realmente veremos el funcionamiento que tiene la empresa en la actualidad y los cambios que realizaremos para llegar al objetivo final. Además de las configuraciones vistas en el capítulo 5, habrá otros dispositivos de red que por temas de espacio estarán explicados en la sección de Anexos.

CAPÍTULO 2. BACKGROUND/NAC

2.1 CONCEPTOS GENERALES

A lo largo del proyecto se hablará sobre diferentes aspectos relacionados con el mundo de las redes de los cuales habrá que conocer su significado. Los conceptos más importantes que hay que conocer son:

- VLAN
- NAC → Dentro de este apartado también se explicará la normativa 802.1x

2.1.1 VLAN

Todo el mundo que tenga algún tipo de formación en el mundo de redes ha escuchado alguna vez la palabra VLAN, el problema es que muchas veces solo se coge el concepto inicial de la palabra (Virtual LAN), es decir, creación de una LAN virtual dentro de una red, pero no se indaga en entender bien el su significado. Diferentes certificaciones dicen que para empezar a entrar en el mundo de las redes se ha de tener muy claro el significado de esta palabra, por ello, en este apartado se intentará explicar de manera resumida porqué se crea, qué beneficios tiene y cómo usarla en una red.

Lo primero que se ha de entender es que dos VLANs son dos redes lógicas completamente independientes funcionando dentro de una misma red física. Su origen viene dentro del protocolo IEE 802.1Q, este surgió con la necesidad de crear múltiples redes interconectadas que compartiendo el mismo medio físico no se provocaran interferencias entre ellas.

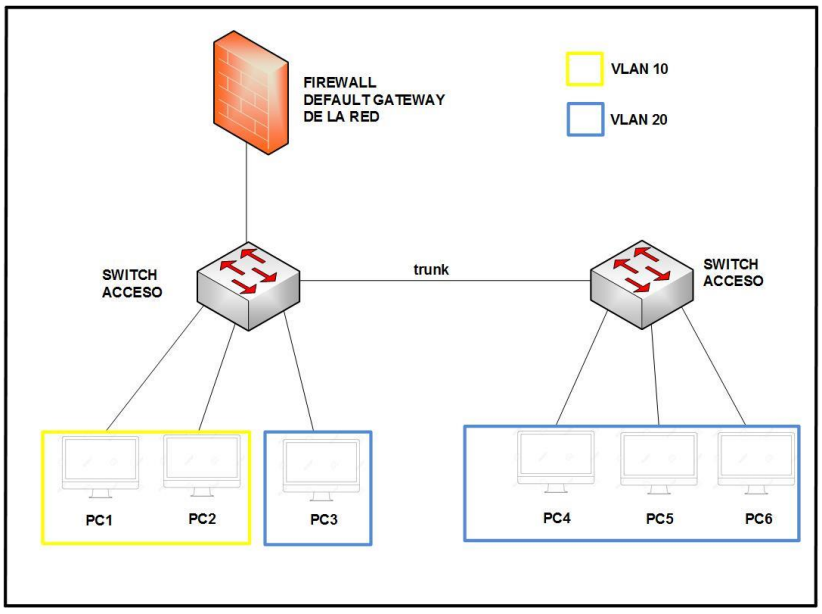


Figura 2.1 Esquema de funcionamiento de las VLANs

Lo mejor para entenderlo es viéndolo con un ejemplo práctico que podría darse en cualquier empresa o incluso vivienda. En la Figura 2.1 tenemos este ejemplo donde existen dos VLANs en la red, la 10 y la 20 que tienen salida a internet por su DG (Default Gateway, es decir, es donde va todo el tráfico de red que quiere salir a internet o comunicarse a otra subred. En el caso del ejemplo, es el Firewall). Este último es el que contiene las VLANs a nivel 3 (IP) creadas. Los PCs se conectan directamente a dos switches donde existen las dos VLANs creadas a nivel 2 (MAC).

Cuando cualquier PC envía una trama broadcast, ésta se queda únicamente dentro de la VLAN a la que pertenezca, es decir, no se propaga por toda la red como pasaría en el caso de que todos los PCs estuvieran en la misma VLAN.

A nivel 3, cada VLAN define un rango IP distinto; de este modo, si PC1 quiere comunicarse con PC4, necesariamente ha de enviar el tráfico al DG. Por lo contrario, si PC1 quiere enviar tráfico a PC2, puede enviar directamente el tráfico a PC2, sin tener que pasar por el DG (que es el encargado de enrutarlas), ya que pertenecen a la misma red IP (y a la misma VLAN).

Como último aspecto relacionado con la Figura 2.1, la conexión entre dispositivos está configurada como trunk, esto provoca que por esos puertos se permita el paso del tráfico de más de una VLAN, pero usando etiquetas explícitas para identificarlas. Si no estuviera configurado de esta manera, únicamente podrían transmitirse paquetes de la VLAN configurada en el puerto que los une.

Para poder saber cómo es posible que se realice todo este proceso, se ha de analizar a un nivel más bajo como el de la trama MAC. En ésta, lo que hizo el protocolo 802.1Q fue añadir 4 bytes más al encabezado.

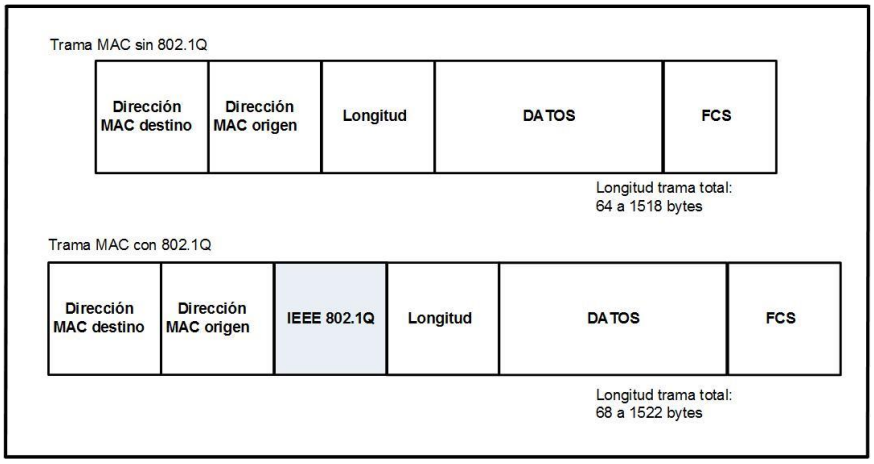


Figura 2.2 Trama MAC utilizando protocolo 802.1Q y trama MAC sin utilizar protocolo 802.1Q

Como puede apreciarse en la Figura 2.2, la segunda trama es la 802.1Q que añade esta cabecera que contiene diversos elementos. El único que se configurará a lo largo del proyecto es el siguiente.

- VID → Es el identificador que muestra la VLAN única a la que pertenece la trama Ethernet.

Una vez vista la información necesaria para entender el funcionamiento de una VLAN, puede deducirse que los beneficios pueden ser múltiples, entre los más destacados pueden estar los siguientes.

- Controlar el tráfico broadcast de la red.
- Conseguir una mayor seguridad en la red aislando los problemas solo dentro de la misma VLAN.
- Facilitar la localización y solución de incidencias.

2.1.2 Solución NAC

NAC hace referencia a las siglas Network Access Control y es una tecnología que proporciona un control en los accesos a la red de todos los endpoints (PC, móviles, impresoras, tablets…) de una organización.

Para hacerlo utiliza la propia infraestructura de red donde crea políticas y hace que cada dispositivo que se conecte sea analizado antes de poder tener acceso a cualquier recurso de la infraestructura.

Entrando en más detalle, sus funciones principales son las siguientes:

- Mitigar ataques de día cero → Como se ha dicho hace un momento, esto lo consigue haciendo que cada usuario sea analizado antes de poder entrar a cualquier recurso de la red, lo que consigue prevenir amenazas antes de que ocurran.
- Refuerzo de políticas → A través de la creación de políticas en esta solución se consigue controlar a qué recursos internos tienen acceso los usuarios, es decir, se puede distinguir entre ellos y darle más acceso a uno que a otro o colocarlos en diferentes redes según el usuario o SO (Sistema Operativo) que utilicen.
- Administración de acceso e identidad → La solución NAC refuerza las políticas de acceso mediante las identidades de los usuarios que se han autenticado.
- Encriptación del tráfico de la red usando los protocolos del 802.1X como EAP-TLS, EAP-PEAP…

Centrándose en su arquitectura, cualquier NAC funcionará utilizando los siguientes componentes básicos; además de éstos, dependiendo de la solución que se implemente podrán tener algunos extras.

- Solicitante → Dispositivo que quiere acceder a la red, puede ser desde un PC, móvil, tablet hasta una impresora o cámara de seguridad entre otros.
- PDP (Policy Decision Point) → Es el elemento que decide que política se ha de aplicar contra el dispositivo que intenta conectarse a la red.
- PEP (Policy Enforcement Point)→ Cuando se ha decidido que política aplicar al endpoint, PDP pasa la información a este dispositivo para que se lo comunique al usuario final.

Este proceso que sigue se basa en la normativa 802.1x. Esta normativa forma parte del IEEE 802, y su función es establecer una conexión punto a punto entre dispositivos para que haya una autenticación entre el endpoint y un dispositivo de una LAN, es decir, su función es maximizar la seguridad de las redes a través de la autenticación.

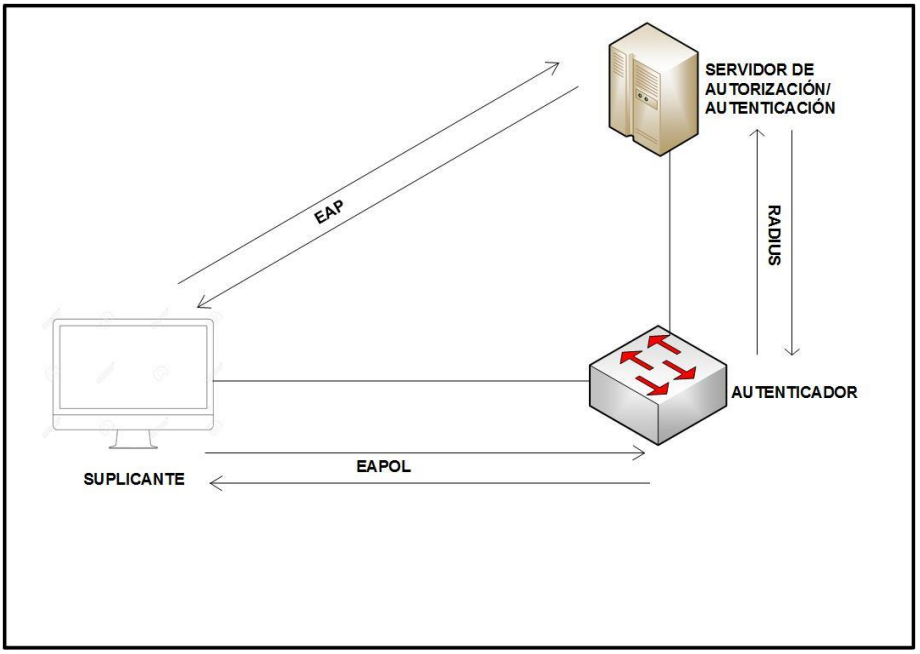


Figura 2.3 Esquema del funcionamiento de la normativa 802.1x

En la figura 2.3, se puede ver de manera más clara los elementos que participan en esta normativa y como utilizan los protocolos para comunicarse entre ellos.

- EAP (Extensible Authentication Protocol)→ Se utiliza en el intercambio de mensajes durante la autenticación. Establece la comunicación de mensajes entre el suplicante y el servidor de autorización.
- Radius (Remote Authentication Dial in User Service)→ Es el encargado de transportar los mensajes EAP entre el Autenticador y el Servidor de autorización.
- EAPOL (EAP Over LAN)→ Este protocolo transporta mensajes entre el suplicante y el Autenticador.

Siguiendo con la tecnología NAC, en la Figura 2.4 puede verse el funcionamiento que sigue esta solución cuando un endpoint se conecta a una red con la solución NAC implantada y en funcionamiento. Todo empieza en la parte de la Gestión de Identidad, donde el dispositivo aún no tiene acceso a los recursos de la red. Una vez analizado, si no tiene ninguna característica que el NAC detecte como dañina pasa a la fase de Seguridad del Endpoint, donde se decide si el dispositivo podrá acceder a la red o no. Una vez decidido, en la fase de Asignación de Políticas el NAC decidirá qué permisos darle al usuario, en qué VLAN situarlo, si se le asigna DHCP o no, cuáles son sus DNS...

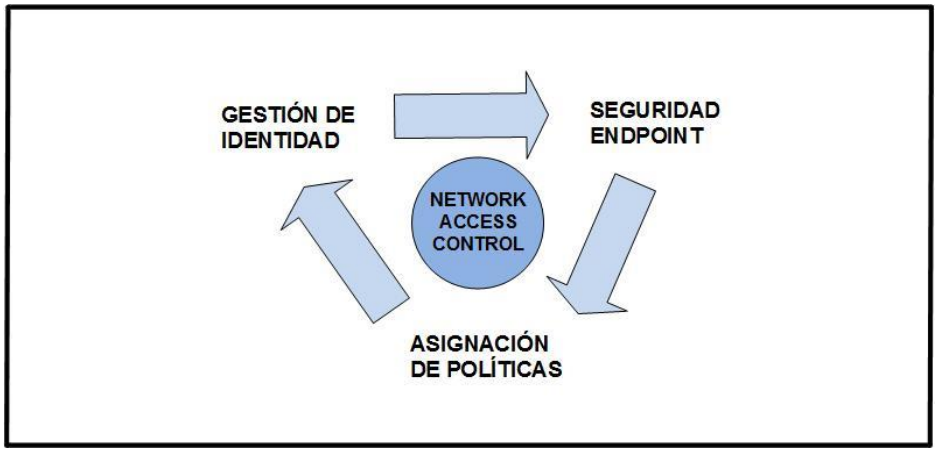


Figura 2.4 Esquema del funcionamiento de la solución NAC

Todo este proceso es cíclico, es decir, una vez el usuario ya ha pasado por las tres fases y está navegando, después de cierto tiempo vuelve a pasar por la fase de Gestión de Identidad para volver a examinarlo, ya que su situación puede haber cambiado mientras estaba conectado a la red. Por ello, la fase de seguridad del Endpoint podría dividirse en dos, una cuando se registra por primera vez el dispositivo, y el resto cada vez que repite el proceso una vez autenticado.

Existen diferentes maneras de controlar estos accesos a través de esta tecnología.

- Pre-admisión Post-admisión → Justo como se ha comentado en la explicación del proceso anterior, un endpoint puede ser analizado antes o después de su conexión, o en ambos casos.
- Agente - No Agente → Para poder llevar a cabo la toma de decisiones de acceso a la red, NAC necesita conocer las características de los dispositivos finales, para ello hay dos posibilidades. Una es la utilización de un agente que permita saber las características de estos equipos y la otra que mediante otras técnicas sean capaces también de saberlas sin la necesidad de usar el agente.
- Solución, cuarentena y portal cautivo → Es la manera de limitar el acceso a esos dispositivos que se encuentran infectados por algún

motivo y poder solventarlo para que finalmente puedan obtener los permisos necesarios. Para hacerlo es normal que se usen VLANs de cuarentena o portales cautivos donde se informa al usuario final los pasos que tendrá que seguir para poder llegar a tener acceso a la infraestructura de red de la empresa.

Otro factor clave de esta tecnología que hay que tener presente en el momento que se decida su utilización es que podemos optar por diferentes maneras de instalarla.

- Basado en Hardware → Como el propio nombre indica, trata de instalar un dispositivo físico dentro de la infraestructura de red.
- Basado en Agente → Funciona a través de diferentes softwares instalados en los dispositivos finales, los cuales recopilan la información para enviársela al servidor.
- Sin Agente → Se instala un software en un servidor con la función de realizar un escaneo de la red.
- Dinámico → En vez de instalar el software en un solo servidor, se hace en diferentes de ellos consiguiendo de esta manera repartir el tráfico y provocar una congestión en la red menor.

CAPÍTULO 3. SOLUCIÓN NAC Y SU ELECCIÓN

Un primer paso importante en el desarrollo de este proyecto ha sido la elección de la tecnología NAC para luego implementarla en la red de la empresa. Para ello, se han tenido en cuenta diversos factores como:

- Solución Opensource o de pago
- Requisitos mínimos que requiere
- Potencial que ofrece
- Valoraciones externas del mismo
- Futura utilización en clientes
- Con agente o sin agente

Juntando todos estos puntos, se ha realizado una búsqueda que al final se ha filtrado a tres candidatos finales, dos de ellos opensource y el restante de pago.

3.1 SOLUCIONES OPENSOURCE

Dentro de esta categoría se ha buscado entre varias opciones disponibles en el mercado. En este caso, lo que más se valoró fue la capacidad de adaptación a la propuesta que la empresa quería llevar a cabo y la futura aplicación a clientes medianos. La empresa cree que una vez funcionando en nuestra propia sede será capaz de trasladarlo a clientes de índole mediana que son reticentes a pagar el dinero que vale esta tecnología dentro de las grandes marcas como Cisco, Fortinet, PaloAlto…

3.1.1 OpenNAC

Esta solución es la alternativa gratuita que aconseja Cisco si el cliente no puede adquirir un ISE (Identity Services Engine), es una herramienta de control de acceso a la red con código abierto que proporciona acceso LAN/WAN. A parte, cumple todas las funcionalidades que ha de ofrecer una tecnología de estas características tales como:

- Adaptabilidad → Es capaz de adaptarse a cada cliente sean cuales sean las características de su red.
- Flexibilidad → Funciona a través de plugins, lo que permite utilizar solamente los recursos necesarios para cada caso.
- Centralización → Dispone de una gestión centralizada que facilita la futura configuración o modificación de políticas.
- Multiplataforma → Capaz de convivir e integrarse con otras plataformas como SIEMS (Security Information and Event Management), MDMs (Mobile Device Management), NGFW (Next Generation Firewalls) …
- Escalable → Parecida a la primera característica, OpenNac es capaz de una vez instalado poder modificarlo según las necesidades y cambios que experimente la red del cliente.

- Monitorización → Ofrece un sistema de monitorización en tiempo real de los dispositivos que se están conectando a la red.
- Políticas de acceso → Capaz de segmentar la red a través de políticas de acceso para decidir en qué direccionamiento se sitúa cada dispositivo.

Los requerimientos mínimos para que esta solución pueda ejecutarse son:

- 2CPU 3GHz
- 80GB de RAM
- 50GB de espacio en disco
- 1 tarjeta de red

Si la red no cumple estas características, OpenNAC podría llegar a realizar cosas extrañas tales como la desconexión de los usuarios, no dejar añadir nuevas políticas, realizar la gestión de VLANs incorrectamente… Por ello, se ofrece una OVA (Open Virtualization Alliance) que se instala directamente por ejemplo en VMware o Proxmox con los mínimos necesarios para empezar la configuración sin incidencias (ver en [9]).

Por otro lado, IEASA funciona a nivel local con dos switches 2960 para gestionar la red a nivel de usuarios, por ello otro requisito básico es mirar con que dispositivos es compatible.

Device	802.1x Auth	802.1x Mac Auth	SNMP Traps	ONNetconf	ONNetBackup	ONNetDisco
Cisco 2950[2]	Yes	No	Yes	Yes	Yes	-
Cisco 2960[1]	Yes	Yes	Yes	Yes	Yes	-
Cisco 3500XL	No	No	Yes	Yes	Yes	-
Cisco 3560[1]	Yes	Yes	Yes	Yes	Yes	-
Cisco 3750[1]	Yes	Yes	Yes	Yes	Yes	-
Cisco 4500[1]	Yes	Yes	Yes	Yes	Yes	-
Cisco 6500[1]	Yes	Yes	Yes	Yes	Yes	-
Cisco WLC	Yes	No	-	Yes	Yes	-
Cisco AP 1242	Yes	No	-	Yes	Yes	-
Cisco AP 1600	Yes	No	-	Yes	Yes	-
Cisco AP 2800	Yes	No	-	Yes	Yes	-

Figura 3.1 Compatibilidad de la solución OpenNAC con fabricante Cisco

Como se puede apreciar en la tabla anterior, es compatible con las dos tecnologías que se requieren en el proyecto, 802.1x y 802.1x Mac authentication.

Además de éstas, como puede observarse en la Figura 3.2, OpenNAC también ofrece compatibilidades con muchos más proveedores.

Aerohive AP Series	Yes	Yes	-	Yes	Yes	-
Allied Telesis AT-8000S	Yes	Yes	Yes	Yes	Yes	-
Allied Telesis AT-8012M	Yes	No	Yes	Yes	Yes	-
Allied Telesis AT-9924T	Yes	Yes	Yes	Yes	Yes	-
Avaya P133 G2	-	-	-	-	-	-
3Com HUB PS40	-	-	-	-	-	-
3Com 4200	Yes	Yes	No	No	No	-
Cajun P120	No	No	No	No	No	-
Enterasys vh4802	-	-	-	-	-	-
Force10 S25	Yes	Yes	Yes	Yes	Yes	-
HP 5500	Yes	Yes	-	Yes	Yes	-
HP ProCurve 2500 Series	Yes	Yes	-	Yes	Yes	-
HP ProCurve 2600 Series	Yes	Yes	-	Yes	Yes	-
HP ProCurve 2910 Series	Yes	Yes	-	Yes	Yes	-
Linksys LGS528P	Yes	Yes	-	-	-	-
Ruckus WLC	Yes	Yes	-	-	-	-

Figura 3.2 Compatibilidad de la solución NAC con otros fabricantes

3.1.2 Packetfence

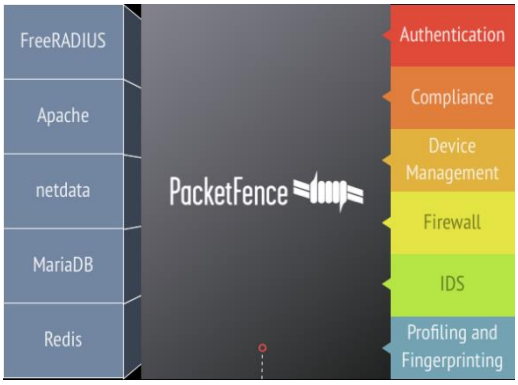


Figura 3.3 Solución Packetfence

Packetfence es una solución NAC gratuita de rasgos muy parecidos a OpenNac, su código es abierto y ofrece las siguientes características.

- Adaptabilidad → Como en el caso de OpenNac, es capaz de adaptarse a las diferentes redes que tenga cada escenario.
- Centralización → Toda su gestión se realiza mediante la web de gestión, además del acceso por ssh por si se quieren crear o modificar los archivos de configuración.
- Administración flexible de VLANs y control de acceso basado en roles.
- Registro automático de los dispositivos.
- Integración con Firewalls.
- Integración con Active Directory.
- Relación dispositivo-usuario → Packetfence es capaz de relacionar cada usuario (LDAP), con su dispositivo (MAC).

- Detección de problemas en capa 2.

Los requerimientos mínimos para el correcto funcionamiento de la solución son:

- CPU 3GHz Intel o AMD
- 8 GB RAM
- 100GB de espacio en disco
- 1 tarjeta de red

Como pasaba en el anterior caso, no cumplir estos mínimos significaría arriesgarse a sufrir incidencias de las cuales no sabríamos identificar el origen. También se ofrece una OVA para desplegarla en VMware y empezar la configuración sin inconvenientes (ver en [10]).

A nivel de compatibilidad con otras soluciones, Packetfence ofrece integración con los siguientes fabricantes.

TECNOLOGÍA	FABRICANTES
Autenticación	OpenLDAP, AD, Radius, Facebook, Google, Email, SMS
Compliance	Nessus,OpenVAS,WindowsManagementInstrumentation
Device Management	Symantec,OPSWAT,MobileIron,Packetfence (Apple/Android)
Firewall	Palo Alto, Fortigate, Barracuda, Checkpoint, Watchguard
IDS	Snort, Suricata, Tipping Point
Profiling	Fingerbank
Switch	Cisco, HP, DELL, Avaya, Brocade…

Tabla 3.1 Compatibilidad de la solución Packetfence con los fabricantes

Como se puede apreciar, Cisco aparece como una de las compatibilidades, en el apartado de switch, aunque no se vea en la tabla 3.1, ofrece compatibilidad con casi todas las soluciones Cisco, entre ellos los 2960.

3.2 SOLUCIONES DE PAGO

De todas las soluciones de pago analizadas, la única que llegó a convencer tanto a IEAISA como a los ingenieros fue la solución de Fortinet, FortiNAC. Esta elección se produjo debido a las características y precio que ofrecía y a la posible compra futura de un Firewall Fortinet para la red local de IEAISA.

3.2.1 FortiNAC

Para el análisis de esta solución se seleccionará el modelo 550C, el más barato que ofrece el fabricante pero que ya tiene las características más que necesarias para el propósito al que se quiere llegar. Sus especificaciones son las siguientes:

	FNC-M-550C	FNC-CA-600C	FNC-C/A-1000C	FNC-R-650C	FNC-CA-500C
System					
CPU	Intel Xeon Silver 4110 2.1 G, 8C/16T, 9.6 GT/s, 11M Cache, Turbo, HT (85W) DDR4-2400 (Qty 2)				Intel Xeon E3-1220 v5 3.0 GHz, 8M cache, 4C/4T, Turbo (Qty 1)
Memory	8 GB RDIMM, 2666 MT/s, Single Rank (Qty 4)				4 GB UDIMM, 2400 MT/s, ECC (Qty 3)
Hard Disk	1TB 7.2K RPM SATA 6 Gbps 2.5in Hot-plug Hard Drive (Qty 2)				1TB 7.2K RPM SATA 6 Gbps 3.5in Hot-plug Hard Drive RAID1 (Qty 2)
Optical Drive	None Required				DVD ROM SATA Internal (Qty 1)
BMC	iDRAC9 Express, integrated (Qty 1)				iDRAC8 Express (Qty 1)
Network Interface	Broadcom 5720 QuadPort 4x 1 GB Ethernet, RJ45				4x 10/100/1000 Ethernet, RJ45
RAID Card	PERC H330 Integrated RAID Controller (Qty 1)				PERC H330 Integrated RAID Controller (Qty 1)
RAID Configuration	RAID 1				RAID 1
Console Access	None				Front LCD Panel
Form Factor	1U Rack mountable				1U Rack mountable
Dimensions					
Height x Width x Length (inches)		1.68 x 18.9 x 29.73		1.68 x 17.08 x 24.60	1.68 x 17.08 x 24.60
Height x Width x Length (mm)		42.8 x 482.4 x 755.12		42.8 x 434.0 x 625.0	42.8 x 434.0 x 625.0
Weight		43.056 lbs (19.76 kg)		40.96 lbs (18.58 kg)	43.87 lbs (19.9 kg)
Environment					
Power Supply	Dual 550W Hot Plug Power Supply				Dual 350W Hot Plug Power Supplies
Input Power	100-240V AC Autoranging				100-240V AC Autoranging
Input Current	6.25 A				3.0 A
Cooling	7 fans				4 fans
Panel Display	No LCD				20 Char LCD
Heat Dissipation	2559 BTU/hr				1357.1 BTU/hr
Operation Temperature Range	50–95°F (10–35°C)				50–95°F (10–35°C)
Storage Temperature Range	-40–149°F (-40–65°C)				-40–149°F (-40–65°C)
Humidity (Operating)	10–80% non-condensing				10–80% non-condensing
Humidity (Non-operating)	5–95% non-condensing				5–95% non-condensing
Certification					
Safety	Certified as applicable by Product Safety authorities worldwide, including United States (NRTL), Canada (SCC), European Union (CE).				
Electromagnetic (EMC)	Certified as applicable by EMC authorities worldwide, including United States (FCC), Canada (ICES), European Union (CE).				
Materials	Certified as applicable by Materials authorities worldwide, including European Union (ROHS) and China (ROHS).				

Figura 3.4 Especificaciones de la solución FortiNAC

Las correspondientes al modelo previamente elegido son las marcadas en los recuadros negros en la Figura 3.4.

Como principales características de esta solución destacan:

- Visibilidad del dispositivo → FortiNAC es capaz de analizar todo tipo de redes sin necesidad de agentes a través de 13 técnicas diferentes. Haciendo esto, puede crear perfiles basados en los comportamientos y características observadas y aplicar políticas diferentes dependiendo de este perfil creado.
- Respuestas automáticas → Es capaz de retener un dispositivo en una VLAN de cuarentena cuando detecta un abanico de posibilidades tales como sistema operativo, usuario no permitido, actualizaciones pendientes…
- Control dinámico de la red → Se utiliza el control de acceso dinámico para segmentar la red a partir de roles creados.

Por otro lado, los fabricantes con los que se puede integrar esta solución son:

Network Infrastructure	Aerohive, Adtran, Alcatel-Lucent, Allied Telesis, Alteon, Apple, APC, Avaya, Brocade/Foundry Networks/ Ruckus, Cisco/Meraki, SonicWall, D-Link, Extreme/Enterasys/Siemens, H3C, HP/Colubris/3Com/Aruba, Huawei Technology, Intel, Juniper, Riverbed/Xirrus
Security Infrastructure	CheckPoint, Cyphort, Cisco/SourceFire, FireEye, Juniper/Netscreen, Qualys, Sonicwall, Tenable
Authentication & Directory Services	RADIUS — Microsoft IAS, Cisco ACS, Free RADIUS LDAP — Microsoft Active Directory, OpenLDAP, Google SSO
Operating Systems	Microsoft Windows, Apple MAC OSX and iOS, Linux, Android
Endpoint Security Applications	Authentium, Avast, AVG, Avira, Blink, Bullguard, CA, ClamAV, Dr. Web, Enigma, ESET, F-Prot, F-Secure, G Data, Intego, Javacool, Kaspersky, Lavasoft, Lightspeed, McAfee, Microsoft, MicroWorld, Norman, Norton, Panda, PC Tools, Rising, Softwin, Sophos, Spyware Bot, Sunbelt, Symantec, Trend Micro, Webroot SpySweeper, Vexira, Zone Alarm

Figura 3.5 Compatibilidad de la solución FortiNAC con otros fabricantes

Como puede apreciarse en la Figura 3.5, tanto Cisco como en el caso que se quisiera vincular con el firewall ASA Cisco actual estarían aceptados por el fabricante.

Por último, el precio de esta solución mezclaría dos cosas, lo primero sería el precio del hardware en sí con un contrato de mantenimiento de un año y, lo segundo, la licencia básica de un año para que funcionen las funcionalidades que se necesitan.

FORTINAC			
UNIT	**DIR PRICE**	**1 YEAR DIR PRICE**	**1 YEAR BASE LICENSE**
FortiNAC-CA-500C	7250 $	1712$	635$

Tabla 3.2 Precio de la solución FortiNAC

El hardware básico con un año de mantenimiento saldría por un total de 8962$, 7250$ por el hardware y 1712 por 1 año mantenimiento, añadido a esto, se tendría que sumar el precio de la licencia básica de un año por un total de 635$, con lo que quedaría por un precio final de 9597$.

3.3 ELECCIÓN

En la tabla 3.3. se han comparado las funcionalidades más importantes que consideraba el equipo técnico de IEAISA en el momento de adquirir una solución de este tipo. Como se puede ver, las tres soluciones son muy parecidas si únicamente nos centramos en esas funciones.

FUNCIONES	FORTINAC	PACKETFENCE	OPENNAC
Gestión de VLANs	Sí	Sí	Sí
Red cableada y Wireless	Sí	Sí	Sí
Soporte de la comunidad	Sí	Sí	Sí
Gestión de ancho de banda	Sí	Sí	No
Agente	Sí	No	No
Detección de dispositivos	Sí	Sí	Sí
Integración con Active Directory	Sí	Sí	Sí
Función de reportes	Sí	Sí	Sí
Soporte de técnicos	Sí	No	No

Tabla 3.3 Requisitos que se requieren por parte de IEAISA para la solución NAC

Lo primero que se ha tenido que decidir era si la empresa iba hacia una solución Opensource o de pago. Teniendo en cuenta las funciones que necesita desempeñar la solución NAC en el entorno de IEAISA, las tres opciones son válidas para llegar a la infraestructura final del proyecto. Viendo esto, IEAISA se decanta por una solución Opensource, aunque se arriesgue a que si hay cualquier tipo de incidencia no se ofrezca un servicio de soporte con gente especializada que pueda proporcionar una solución al problema. Al elegir la gratuita, cualquier tipo de inconveniente en el momento de la instalación o configuración recaerá sobre los ingenieros internos de la propia empresa. Aún y así, mirando al futuro y viendo el abanico de clientes de los que se dispone, IEAISA veía una explotación mucho mayor si únicamente se le facturará al cliente el coste del ingeniero por la instalación y no un precio tan elevado como tienen la gran mayoría de soluciones de pago de este tipo.

Una vez descartada la solución FortiNAC, queda elegir entre Packetfence y OpenNAC. Cualquiera de las dos es una solución clara que podría funcionar en la propia infraestructura de IEAISA y en cualquier otra. Por ello lo que se hace es buscar todavía más información sobre aspectos que podrían interesar o facilitar la instalación.

El primero de ellos es el tema del soporte de la comunidad. Tras la búsqueda, vemos que OpenNac tiene un foro bastante activo, pero con una documentación bastante limitada y de difícil acceso. En cambio, Packetfence resulta ser todo lo contrario, cuenta también con una comunidad online que participa mucho más activamente que en el anterior caso, además, se pueden encontrar todas las preguntas de los usuarios con las soluciones a las incidencias comentadas. Para finalizar, también cuenta con un soporte de guías de administración e instalación muy detalladas.

Otro factor importante que ayuda con la localización de problemas una vez la herramienta está en funcionamiento son los reports que ofrece la solución. Otra vez más Packetfence dispone de un sistema de reporting mucho más completo

que la otra solución. Reporta información de la IP y MAC relacionada con cada usuario conectado, los sistemas operativos que se utilizan, las conexiones que se realizan al momento, el uso de ancho de banda por dispositivo… Es decir, un abanico de posibilidades que hacen más atractivo su uso.

Por último, con vistas a la futura aplicación de esta solución en otras empresas, está el tema de la compatibilidad e integración con dispositivos de diferentes fabricantes. En este aspecto, Packetfence también logra una mayor integración respecto a la solución OpenNAC. Esto permite que en futuros proyectos no se tenga que estar mirando detenidamente si se podrá aplicar o no dependiendo de los fabricantes que use una empresa.

Por estas razones, se ha decidido que la solución que se implementará será Packetfence, ya que consigue adaptarse mucho mejor a las necesidades que pide IEAISA, lo cual no quiere decir que sea mejor, sino que en este caso y para las características requeridas en este proyecto es la mejor solución encontrada.

CAPÍTULO 4. ESCENARIO ACTUAL

En primer lugar, en la sección 4.1 se va a detallar la situación actual de la red de la empresa IEAISA. Primero se verá cómo está hecho el direccionamiento de los equipos y el esquema de la red (4.1.1); a continuación, veremos cómo funciona (4.1.2). En la sección 4.2 se verá la propuesta de mejoras a implementar, detallando cómo se encuentran actualmente los equipos configurados y qué mejoras habrá que aplicar. Dentro de esta sección primero estará como quedará la asignación de VLANs final (4.2.1), acto seguido se verán los firewalls de IEAISA, el Firewall Cisco ASA (4.2.2) y el Firewall Sonicwall (4.2.3). Para la conexión wifi se analizará el Cloud Meraki (4.2.4) y, para finalizar, se verá la solución Packetfence (4.2.5).

4.1 SITUACIÓN HOY EN DIA

En la Figura 4.1 se puede observar cómo está montada y segmentada la red actual de IEAISA. Puede verse que en la oficina se disponen de los tres elementos antes nombrados (dos switches Cisco y el Firewall ASA Cisco) y además dos APs Meraki (uno para cada planta de la oficina) que tienen la gestión en su propio Cloud.

Para dar la salida hacía la WAN se dispone del Firewall ASA conectado al router del operador funcionando en modo bridge, es decir, la IP pública deja de tenerla el router y la tiene el propio Firewall, el router deja de tener las funciones de routing para traspasarlas a otro dispositivo, el Firewall.

Siguiendo con la Figura 4.1, para que los equipos de la oficina y los del Cloud puedan acceder entre ellos existe una VPN site-to-site por donde se pasa la red plana local de IEAISA y las redes pertinentes del Cloud.

En el Cloud se dispone de una VLAN local para los usuarios que se conectan a través de Citrix. Esta VLAN sale a internet por un router de un operador conectado también en modo bridge al Sonicwall. En éste hay varios servidores con diversas funciones, en el caso de este proyecto, únicamente se centrará la atención en el Active Directory, ya que será el más importante que se deberá modificar para llegar al objetivo final.

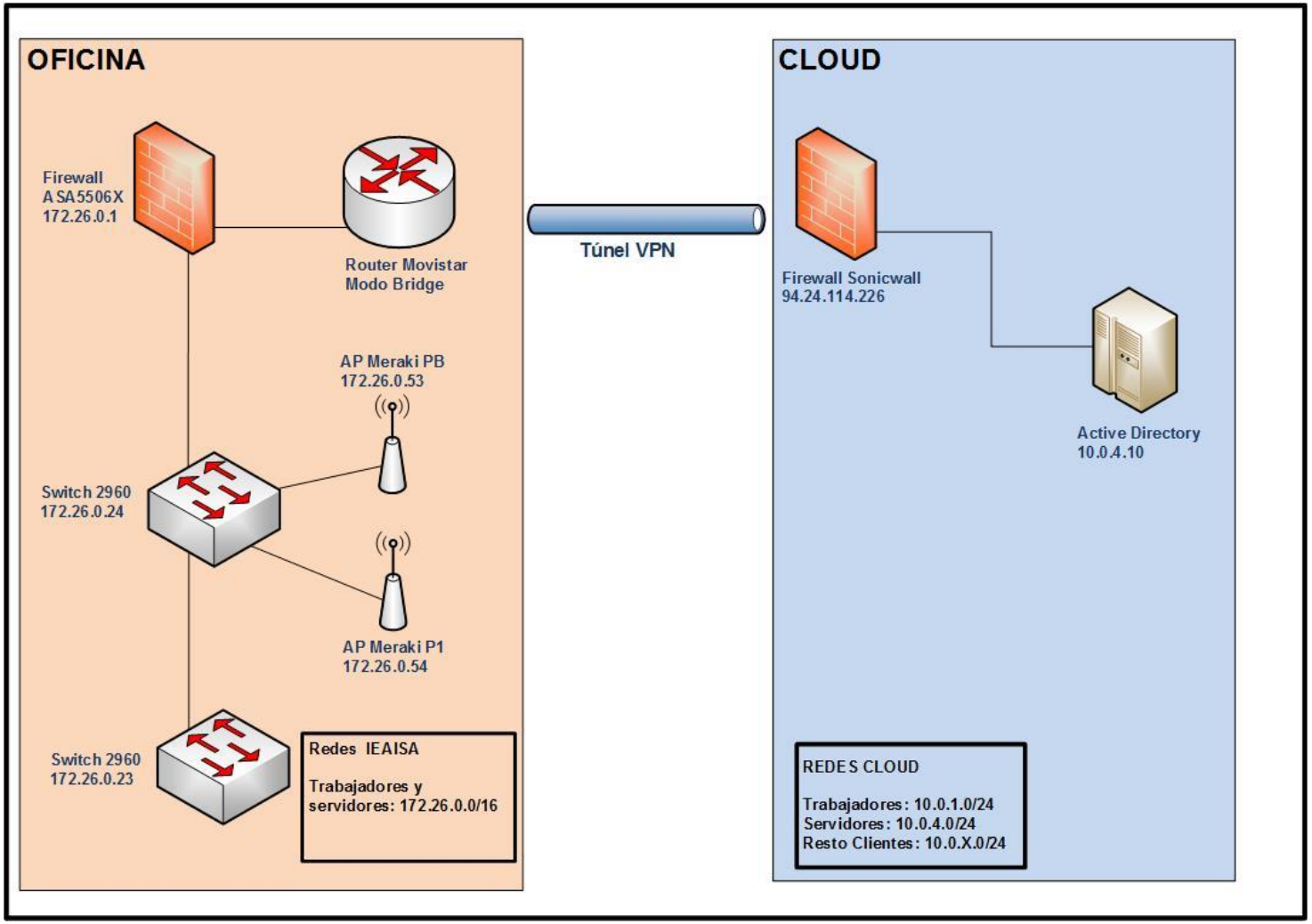


Figura 4.1 Esquema de red principal de IEAISA

Si se mira la organización de la red se ha de decir que IEAISA divide su red en dos partes:

- Red local de la empresa → Donde se conectan todos los trabajadores tanto por cableado como por wifi.
- Red del Cloud → Donde se encuentran la mayoría de servidores y se da acceso a los clientes para que realicen conexiones mediante Citrix.

Estas dos redes se diferencian por tener dos rangos IP distintos, uno de ellos asignado para la red local de la oficina y otro para las conexiones al Cloud. Además, en la Tabla 4.1 se recogen los elementos más importantes a los que se irá refiriendo a lo largo del proyecto:

Direccionamiento	IP de los equipos	Tipo de Dispositivo
172.26.0.0/16	172.26.0.1	Firewall ASA
	172.26.0.23	Switch-Oficina1
	172.26.0.24	Switch-Oficina2
10.0.0.8/8	10.0.4.10	Active Directory
	10.0.1.0/24	Equipos de IEAISA

Tabla 4.1 Elementos y direccionamiento de la red de IEAISA

Como podemos ver en la Tabla 4.1, actualmente en las oficinas se funciona con una red plana con un solo direccionamiento IP 172.26.0.0/24. Esta red incluye todos los accesos vía cable de la empresa, dando así acceso a todos los recursos compartidos y a los servidores locales como los que tiene la empresa en el Cloud.

Dentro de esta red se encuentran tres equipos importantes a los que se harán referencia:

- Firewall ASA → Con direccionamiento 172.26.0.1 para la red local, es un modelo Cisco ASA 5506 al que se le ha subido la versión para que trabaje con la consola Firepower.
- Switch 1 y 2 → Estos switches Cisco 2960-24P son los encargados de proporcionar los puertos necesarios para que se conecten usuarios y servidores a la red, su Default Gateway es el Firewall ASA que es el encargado de realizar el routing necesario para que lleguen a las redes del Cloud y a la vez tengan salida a internet.

Además de éstos, encontramos dos APs Cisco Meraki con IPs 172.26.0.53 y 172.26.0.54 que son los encargados de proporcionar conexión Wireless en toda la empresa. Que los APs tengan un direccionamiento interno no quiere decir que la red Wireless también lo entregue, será el Cloud Meraki quien dará las IPs en esta parte (se verá más detalladamente en la sección 4.1.2.2)

En el Cloud sí que tenemos la red segmentada para los diferentes clientes.

Los elementos importantes del Cloud a los que se hará referencia serán los siguientes:

- AD (Active Directory) → Contiene los grupos de usuarios y permite la autenticación. Actualmente solo tiene un grupo de Técnicos donde están todos los trabajadores.
- Equipos de IEAISA → Este rango de red se les da a los trabajadores de IEAISA cuando nos conectamos al Cloud, se tendrá que dar los permisos necesarios para poder conectarse al Packetfence y modificar sus configuraciones.

Otro elemento importante que no sale en la tabla debido a que no está situado en ninguno de los direccionamientos, es el Firewall que tenemos en el Cloud. Este Firewall es el modelo NSA2650 de Sonicwall y se accede mediante su IP pública con gestión HTTPS, no tiene gestión interna debido a que actualmente tiene cerrada su gestión por la propia LAN. Este elemento es el encargado de proporcionar la comunicación entre VLANs del Cloud y dar salida hacia internet.

4.1.1 Acceso a la red hoy en día

Como se ve a continuación, para acceder a la red actual de IEAISA y a los recursos compartidos de la misma existen dos maneras posibles. Una a través de la red cableada y otra a través de la red Wireless.

4.1.1.1 Red cableada

La Figura 4.2 muestra el esquema básico que sigue la conexión cableada en la empresa.

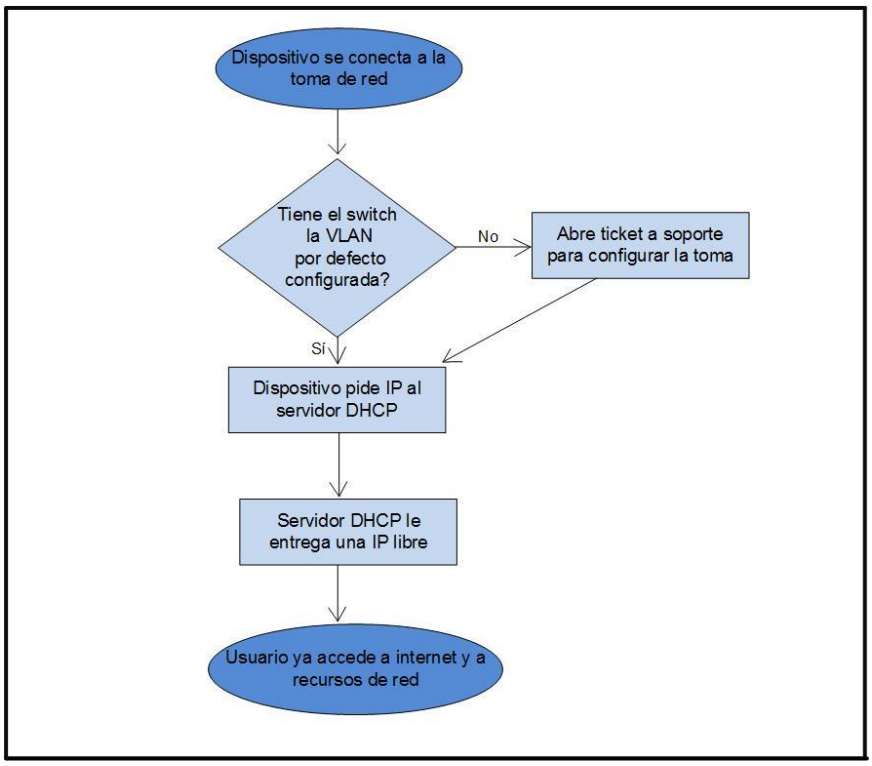


Figura 4.2 Funcionamiento actual de la red cableada de IEAISA

La red cableada en IEAISA sigue un esquema muy sencillo. Como se puede apreciar, el proceso que sigue un usuario sea externo o interno es conectarse a la toma de red, si no dispone de salida a internet porque no tiene la VLAN por defecto configurada abre una petición a soporte. Cuando el equipo técnico ve esa petición configura la toma para que tenga la VLAN por defecto. Con ésta configurada, cuando el dispositivo se conecta a la toma de red el switch le envía una petición DHCP al servidor situado en la misma red con IP 172.26.0.253, este servidor le otorga una IP libre del rango 172.26.0.0/24 y con esto ya tiene acceso a todos los recursos internos y salida hacia internet.

4.1.1.2 Red Wireless

La red Wireless de IEAISA funciona tal y como se puede apreciar en la Figura 4.3. Hay un único SSID con nombre “IEAISA_COORP”. Cuando un dispositivo quiere obtener conexión WIFI, se conecta a esta red poniendo una contraseña con seguridad WPA2, si es correcta, Meraki le entregará un direccionamiento propio ajeno a la red de IEAISA con el que podrá acceder a recursos internos y del Cloud por igual.

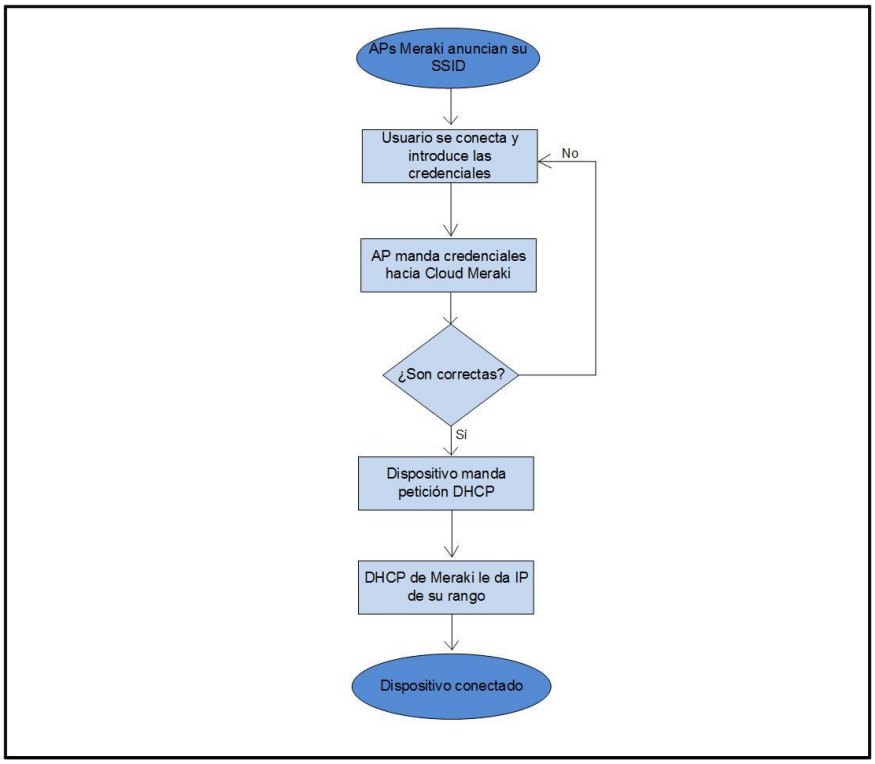


Figura 4.3 Funcionamiento actual de la red Wireless de IEAISA

Esta manera de funcionar es muy insegura ya que desde un direccionamiento que no da ni la propia red interna cualquier usuario tiene acceso a todos los recursos de la red de IEAISA; cualquier persona externa que viene a la empresa y se le facilita acceso a la wifi puede entrar a cualquier servidor o ver el tráfico que hay en cualquier direccionamiento.

4.1.2 Problemas de la red actual

A lo largo del proyecto se pueden haber ido comentando diversos problemas que tiene la red de IEAISA. En este punto se englobarán todos ellos para poder dar una visión más general de la problemática situación actual y porque se debe mejorar.

- Disponer de una red plana sin segmentar provoca un tráfico de broadcast mucho mayor que si se utilizaran las VLANs.
- Como se verá en la sección 4.2.4, Meraki da un DHCP propio de la nube con máscara 255.0.0.0, es decir, puede dar IPs a 16777214 hosts diferentes. Está claro que no existe tal número de trabajadores en la empresa, pero pensando en el crecimiento futuro no se puede dejar una red de estas características en funcionamiento.
- Cualquier persona que se conecta a una toma de red de la empresa tiene acceso a todos los recursos internos de IEAISA, servidores, switches, firewalls…

- Se necesita un técnico cada vez que se requiere la configuración de una toma nueva o habilitar la VLAN por defecto a cualquier usuario.
- Cualquier cliente que visita las instalaciones de IEAISA muchas veces pide ver o se le muestra cómo funciona la red en la empresa. Tener una red con los problemas nombrados anteriormente no da la mejor impresión a quien visita las instalaciones.

4.2 MEJORAS A IMPLEMENTAR

Para poder solventar los problemas que se muestran en la sección 4.1.2, se tendrán que aplicar diferentes cambios en los dispositivos de red que se nombrarán a lo largo de esta sección.

4.2.1 VLANs

La segmentación de la red es uno de los elementos más importantes a realizar, por ello antes de empezar a configurar cualquier dispositivo se deben organizar las futuras redes de la empresa.

VLANS	DIRECCIONAMIENTO	NOMBRE
1	172.26.0.0/24	Inside_Data
50	172.26.50.0/24	Inside_Wifi
51	172.26.51.0/24	Wifi_Invitados
100	172.26.100.0/24	Seguridad
200	172.26.200.0/24	Lan_Tecnicos
201	172.26.201.0/24	Lan_Comerciales

Tabla 4.2 Segmentación de la nueva red de IEAISA

Como se ve en la tabla 4.2, la red plana que se tenía antes de este proyecto pasaría a ser segmentada en 6 VLANs diferentes cada una con su función específica.

- Inside_Data → VLAN utilizada para los servidores que se encuentran en la oficina. Está estaría aislada del resto y no se configuraría en el Packetfence ya que todo su rango de red sería especificado por IPs estáticas y una configuración predeterminada en los switches para dar mayor seguridad. Es decir, se vincularía la dirección MAC de cada dispositivo a una dirección IP, con lo cual ya no sería necesario que Packetfence gestionará esta VLAN.
- Inside_Wifi → VLAN utilizada para la red wifi-corporativa, la cual tendría acceso a todos los recursos de red de la empresa y del Cloud. Se gestionaría mediante Packetfence y el Cloud de Meraki a través de autenticación LDAP.

- Wifi_Invitados → VLAN utilizada para que se conecten las personas externas a IEAISA. Con esta Wifi solo se tendría acceso a la salida a internet. Se gestionaría por un SSID específico configurado en el Cloud de Meraki.
- Seguridad → VLAN utilizada para todos los elementos de seguridad de la empresa, abarca desde cámaras de seguridad hasta controles de acceso por huella dactilar. Esta red no sería gestionada por Packetfence ya que funciona como en el caso de la VLAN Inside_Data, todos los dispositivos estarían fijados con una IP estática.
- Lan_Tecnicos → VLAN utilizada por los trabajadores de IT de la empresa, tanto del sector de Sistemas como el de Networking. Este direccionamiento estaría gestionado por Packetfence y tendría acceso a todos los recursos de la red local como del Cloud.
- Lan_Comerciales → VLAN utilizada por los comerciales de la empresa. Este direccionamiento estaría gestionado por Packetfence y se les daría acceso únicamente a los recursos compartidos que necesitan, es decir, algunos de los servidores que tenemos en el Cloud. Esta red no accedería ni a equipos de Networking tales como Firewall, switches, APs… ni a servidores como el Active Directory, Backups…

Estas VLANs tendrán que crearse en diversos dispositivos para que la red pueda funcionar, entre ellos los switches 2960 (ver Anexo A.1), el firewall ASA, el servidor DHCP y el Firewall Sonicwall entre otros.

4.2.2 Firewall Cisco ASA

Este Firewall actualmente solo tiene una VLAN interna creada a nivel 3.

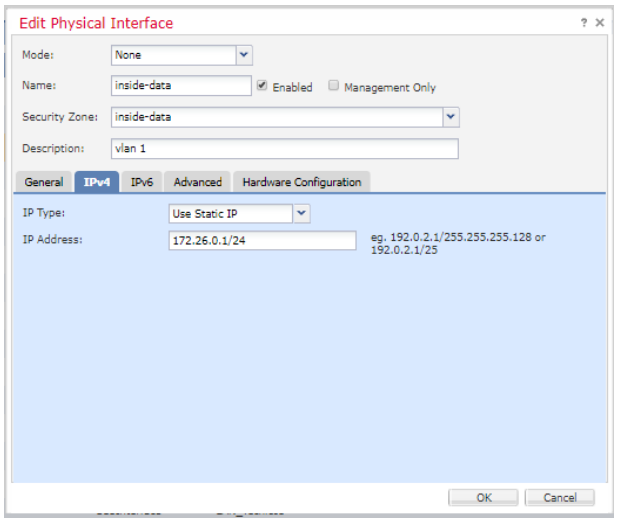


Figura 4.4 VLAN creada a nivel 3 en el Firewall Cisco ASA

La IP estática que tiene dentro de esta VLAN es la 172.26.0.1, la cual hace de Default Gateway de esa red. Es decir, es el encargado de enrutar el tráfico de esa VLAN hacía los diferentes direccionamientos.

Además, esta red consta de una única regla de acceso de salida sin ningún tipo de limitación.

Figura 4.5 Regla de acceso del Firewall para dar salida a internet

En el nuevo escenario que se plantea en el capítulo 5, en este dispositivo se tendrán que realizar las siguientes configuraciones:

- Creación de nuevas zonas → Cada interfaz que se crea en este firewall necesita vincularse a una zona. Éstas pueden ser por defecto como LAN, WAN, DMZ… o creadas por el propio usuario para tener más visibilidad y orden. En el caso de este proyecto, crearemos una zona para cada interfaz VLAN nueva.
- Creación de las nuevas VLANs → 4.2.1.
- Creación de nuevas reglas de acceso → Se deberán crear nuevas reglas que permitan o denieguen el tráfico de las nuevas redes hacía cualquier direccionamiento existente, tanto local como en el Cloud. Se seguirán las pautas también nombradas en el 4.2.1, es decir, la wifi de invitados únicamente tendrá salida hacía la WAN, pero no tendrá acceso por ejemplo a la VLAN de servidores.
- Modificación VPN (Virtual Private Network) → Al tener la VPN ya creada de antemano como se explica en la sección 4.1, no será necesario crearla de nuevo, solamente se tendrá que modificar el grupo de objetos que pasa por ésta para permitir las redes que se necesiten.

4.2.3 Firewall Sonicwall

El firewall Sonicwall NSA 2650 del que dispone IEAISA en el Cloud tiene una configuración más compleja que el de la oficina ya que es el encargado de permitir y denegar según convenga las conexiones que recibimos por parte de los clientes.

En la red actual en todas las reglas de este firewall existe el objeto IEAISA_Interna con la red 172.26.0.0/24. Este objeto es el que se usa en el momento de crear las reglas.

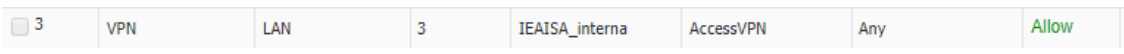


Figura 4.6 Regla de acceso para permitir tráfico desde la oficina de IEAISA

Esto se puede ver mejor con la Figura 4.6, esta es una regla básica donde explica que desde la zona VPN, donde se encuentra la red de IEAISA, hacia la zona LAN, donde se encuentran todas las VLANs del Cloud, con origen el objeto IEAISA_interna (haciendo referencia a la red 172.26.0.0/24) hacía el objeto AccessVPN (haciendo referencia a las redes 10.0.1.0/24 y 10.0.4.0/24), permita todo el tráfico.

Como veremos en el capítulo 5, en este dispositivo se tendrán que modificar y añadir configuraciones como:

- Modificación VPN → De igual manera que en el ASA, se tendrán que crear las nuevas redes, pero esta vez solo a nivel de objeto, no de interfaz. Una vez hecho esto se tendrán que pasar por la VPN hacía la red local.
- Creación Access rules → Se tendrán que crear nuevas reglas que marquen qué redes pueden acceder a cada direccionamiento o IP de máquina del Cloud. De igual manera se tendrá que crear otra regla para permitir el tráfico de la WAN hacia el Packetfence.
- Creación de NAT → Para que la nueva Wireless funcione tal y como se verá en la sección 5.2, se deberá crear un nuevo NAT para que el Cloud de Meraki pueda comunicarse con el Packetfence.

4.2.4 Meraki

Como se ha explicado resumidamente en el apartado 4.1, en IEAISA se obtiene conexión Wireless mediante dos dispositivos Cisco Meraki. Estos APs no necesitan de una controladora Wifi para trabajar o configurar conjuntamente si no que utilizan la nube de Meraki para todo tipo de gestión.

La configuración actual del SSID “IEAISA_COORP” es la siguiente:

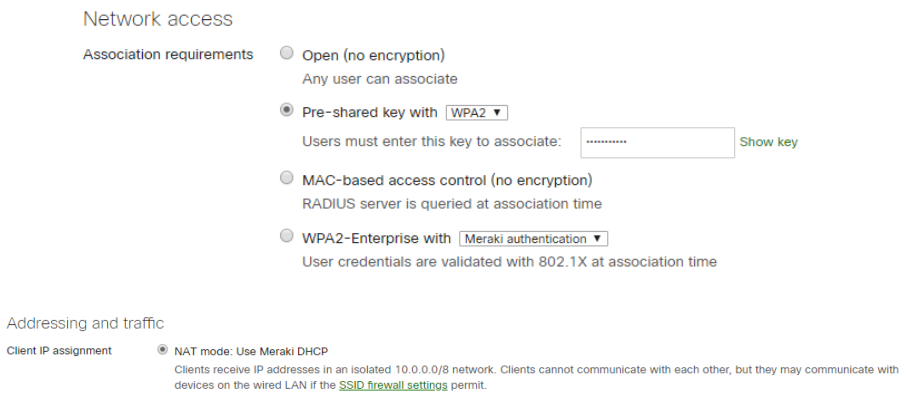


Figura 4.7 Configuración del SSID IEAISA_COORP

Como vemos en la Figura 4.7, se dispone de una clave WPA2 como clave de acceso compartida y para el DHCP está marcada la opción que es el propio Meraki el que entrega una IP del rango 10.0.0.0/8.

Las mejoras que se realizarán y veremos en el capítulo 5 serán:

- Creación SSID IEAISA → Esta dará acceso únicamente a los trabajadores internos de IEAISA, se accederá mediante autenticación por RADIUS, siendo el RADIUS Packetfence.
- Creación SSID IEAISA_GUEST → Este SSID dará salida a internet a la gente externa a IEAISA, se le dará el direccionamiento de la wifi de invitados.

4.2.5 Packetfence

Este dispositivo será el único elemento completamente nuevo que existirá en la red, por ello, no se explicará nada del funcionamiento que tiene actualmente, sino que se introducirá más detalladamente cuál será su funcionamiento.

En el capítulo 3 se han visto por encima sus características principales y su funcionamiento, en este apartado se analizará un nivel más bajo viendo cómo funciona a nivel de recursos y cuál será su función en el escenario real.

La arquitectura interna con los elementos que se han utilizado en el momento de aplicarlo en el escenario real son los que se ven en la Figura 4.8.

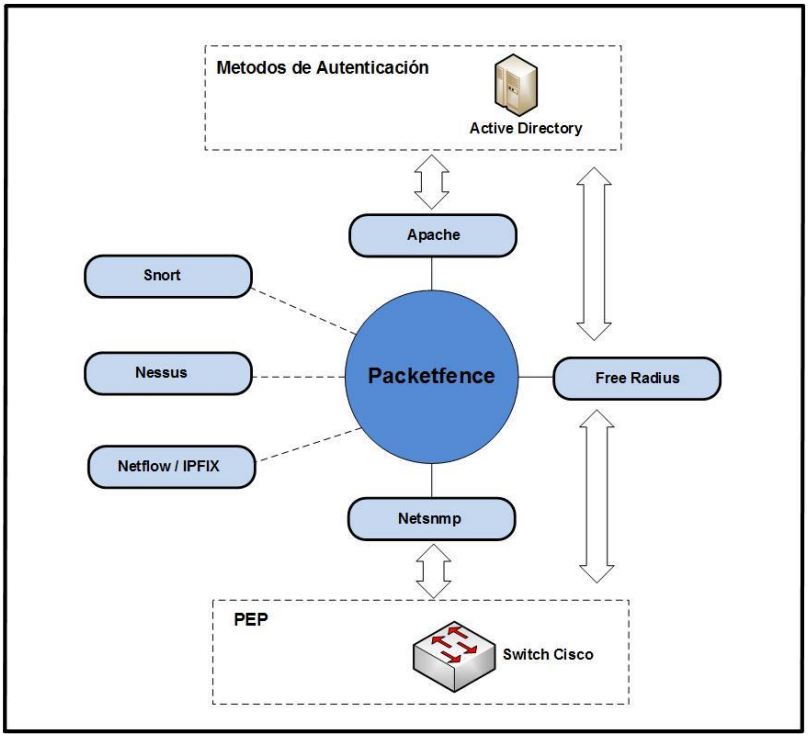


Figura 4.8 Arquitectura interna de Packetfence

Como se puede ver en la figura 4.8, Packetfence utiliza un servidor Radius para la comunicación entre el Active Directory y el switch Cisco de la oficina. Además, para poder vincularse con el switch utiliza snmp y para la comunicación con el AD utiliza Apache. Internamente utiliza Nessus para el escaneo de vulnerabilidades de los equipos, Snort para esnifar el tráfico de la red y Netflow/IPFIX para administrar y dar seguridad a la red.

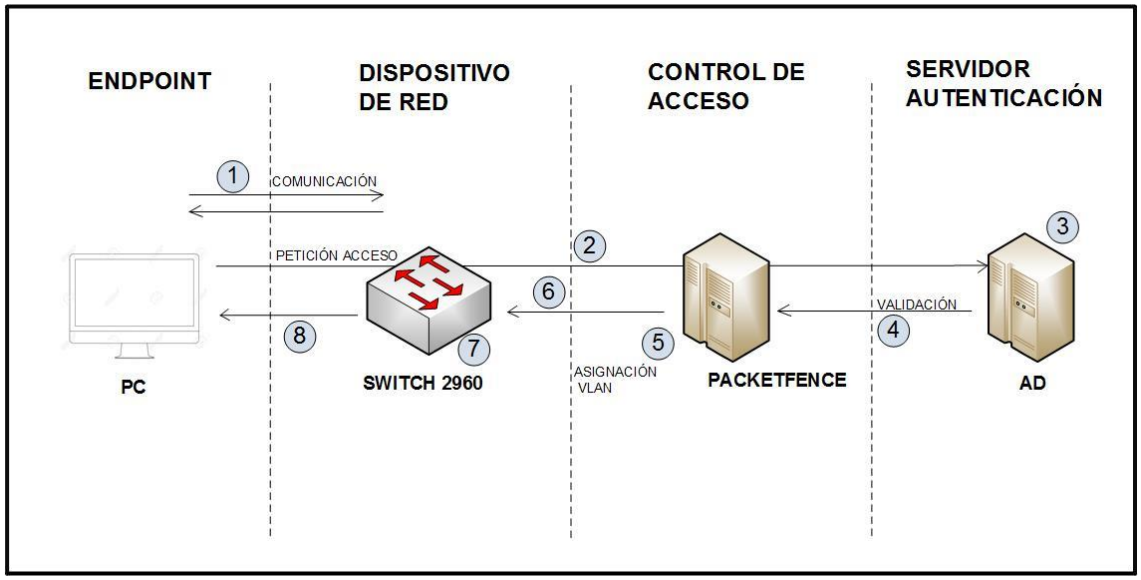


Figura 4.9 Esquema de funcionamiento de la solución Packetfence en la red de IEAISA

Aunque en apartados anteriores se ha visto el funcionamiento que tiene NAC o la tecnología 802.1x, con la Figura 4.9 se puede ver ya en el escenario final cuál sería el objetivo de esta solución. Explicado sin entrar en detalle a niveles más bajos y suponiendo que el PC utiliza la tecnología 802.1x, el proceso sería el siguiente:

1. Se establece comunicación entre el PC y el switch Cisco 2960
2. Se realiza la petición de acceso que pasa por el switch 2960, que lo reenvía a Packetfence y éste al Active Directory.
3. Active Directory valida el usuario que ha proporcionado el dispositivo.
4. Active Directory pasa a Packetfence en qué grupo se sitúa el usuario que se ha autenticado.
5. Packetfence aplica las políticas necesarias y decide en qué VLAN se situará el dispositivo.
6. Packetfence pasa al switch en que VLAN ha de colocar al usuario.
7. Switch configura el puerto con la VLAN que le han pasado.
8. Dispositivo ya tiene acceso a la red.

Para poder llegar a realizar las funciones vistas hasta ahora, se tendrán que realizar los siguientes pasos.

- Instalación de la solución NAC Packetfence
- Configuración inicial

- Vinculación con Active Directory
- Creación de políticas
- Creación de dispositivos de red
- Otras configuraciones como Fingerprint, Monitorización de dispositivos…

4.3 RESUMEN ACCIONES DE MEJORAS

A continuación, se muestra en la Tabla 4.3 el resumen de mejoras que se aplicarán en el capítulo 5.

Como podemos observar, aparece un elemento que no se ha nombrado antes en este capítulo, el Active Directory. Además de este último, hay otros dispositivos y/o configuraciones que se verán en la parte de Anexos.

- Configuración de los switches 2960 (Anexo A.1)
- Configuración 802.1x en SO Windows y Linux (Anexo A.4)
- Configuración del Fingerprint de Packetfence (Anexo A.2)
- Configuración DHCP relay en Cisco ASA (Anexo A.3)

EQUIPO	ACCIÓN	OBJETIVO
FW Cisco ASA	Creación zonas nuevas	Aislar las VLANs que se crearan
	Creación de nuevas VLANs	Segmentar la red
	Creación nuevas reglas de acceso	Permitir accesos de las nuevas redes
	Modificación VPN	Dar acceso a las nuevas redes hacia Cloud
FW Sonicwall	Modificación VPN	Dar acceso a las nuevas redes hacia Cloud
	Creación nuevas reglas de acceso	Permitir o denegar accesos de nuevas redes
	Creación de NAT	Permitir la redirección de entrada hacia Packetfence
Meraki	Creación SSID IEAISA	Limitar acceso a los usuarios externos a IEASA
	Creación SSID IEAISA_GUEST	Crear SSID para usuarios externos o sin permisos
Active Directory	Creación de nuevos grupos	Permitir la separación de usuarios en diferentes sectores
Packetfence	Instalación de la solución	Instalación de la OVA
	Configuración inicial	Adaptar configuración a IEAISA
	Creación de políticas	Controlar el acceso a la red
	Creación de dispositivos de red	Vincularse con los diferentes equipos de red

Tabla 4.3 Resumen de mejoras que se aplicarán en los dispositivos de IEAISA

CAPÍTULO 5. ESCENARIO FINAL

Una vez vistos los problemas de la red actual de IEAISA en la sección 4.1.2 y los dispositivos de red que se tendrán que configurar en la sección 4.3, se enseñará el funcionamiento que tendrá el nuevo acceso a la red (sección 5.1), y después de esto ya se pasará a las configuraciones propias que se ha realizado en cada equipo.

5.1 ACCESO A LA NUEVA RED

En este apartado podremos ver el nuevo funcionamiento que tendrá la red tanto en la parte cableada (Sección 5.1.1) como en la parte Wireless (Sección 5.1.2). A modo de resumen, un usuario que se conecte hará:

- Autenticación por 802.1x o MAC que conlleva a la asignación de VLAN
- Obtención de IP por DHCP en función de la VLAN asignada

5.1.1 Red cableada

Con todo lo hablado en apartados anteriores, la red de IEAISA deberá seguir el proceso que se ve a continuación.

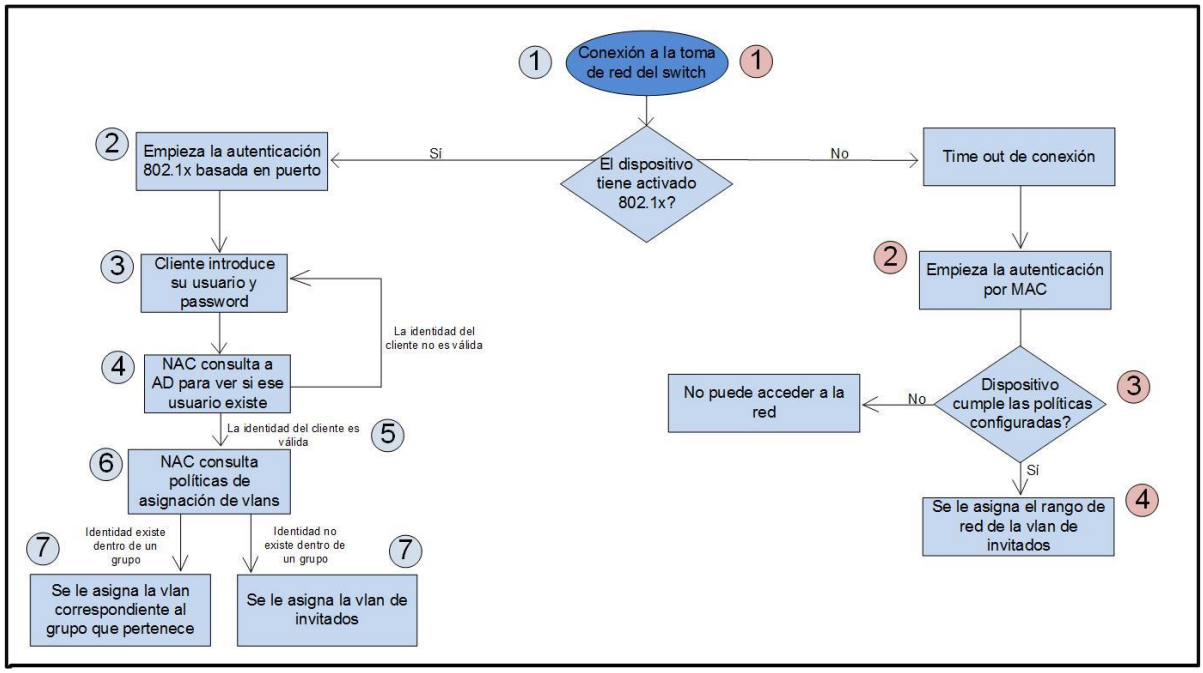


Figura 5.1 Esquema del nuevo funcionamiento de la red cableada de IEASA (1)

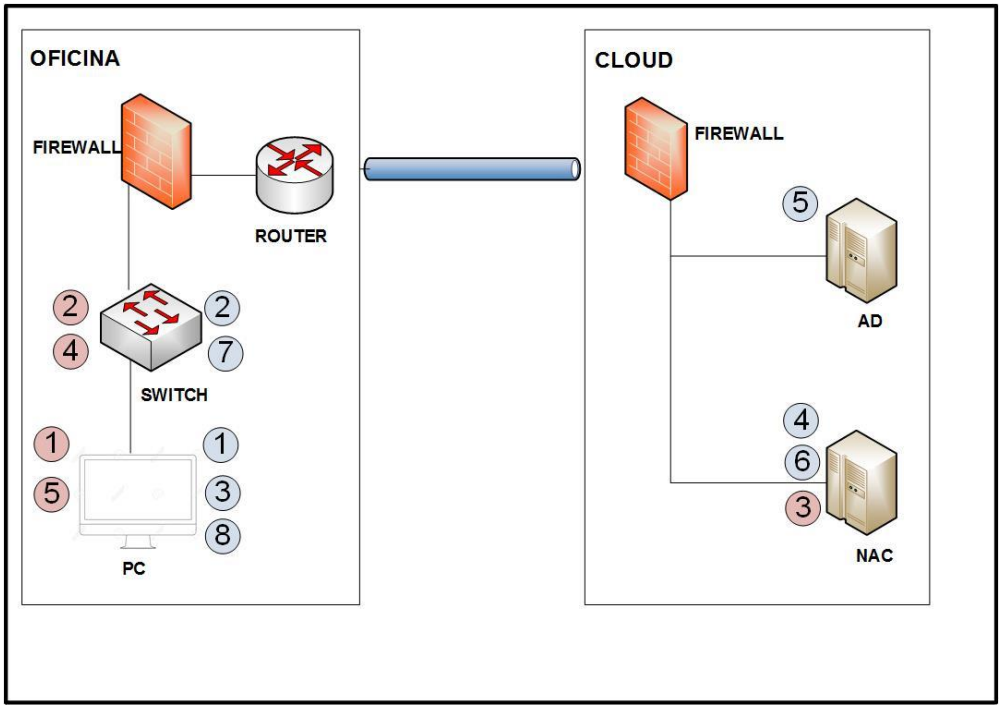


Figura 5.2 Esquema del nuevo funcionamiento de la red cableada de IEASA (2)

Tal y como se puede apreciar en las Figuras 5.1 y 5.2, este proceso se dividiría en dos casos muy diferenciados. El primero de ellos se dará cuando el dispositivo se conecte a un puerto del switch y no tenga el 802.1x configurado; el segundo se dará cuando es usuario se conecte y sí que tenga el 802.1x activado.

En el primer caso, la conexión dará un timeout configurado previamente en el switch y empezará la autenticación MAC; si llega a este punto, significa que el endpoint es un dispositivo externo a la empresa o sin acceso a los recursos compartidos que se ofrecen. En esta autenticación, Packetfence registrará el nuevo usuario en su base de datos y mirará si este pasa las políticas que se le hayan configurado, si no las pasa, directamente no se le dará la salida a internet a este dispositivo, si por el contrario sí que las pasa, se le asignará la VLAN de invitados para que de esta manera únicamente tenga salida a internet.

En cambio, si dicho dispositivo tiene la autenticación 802.1x activada, se le pedirá al usuario que introduzca un usuario y password, cuando lo haga, NAC consultará al Active Directory si existe, si fuera así, Packetfence consultará sus políticas para ver en qué grupo está colocado ese usuario y qué VLAN se le asigna. Cuando encuentre el grupo de ese usuario le asignará directamente la VLAN que le toque. Si por el contrario no lo encuentra, entrará en la regla por defecto donde se le asignará la VLAN de invitados. Si se diera la casuística de que el usuario no existe en el Active Directory, se volvería a preguntar al usuario por el usuario y password hasta que acertará.

Este proceso se realizará de esta manera ya que la empresa entiende que si cualquier trabajador tiene el 802.1x activado, es porque quiere acceder a los recursos compartidos de IEAISA; si no fuera así, se conectaría por MAC o simplemente en la Wifi de invitados. Por ello, el sistema vuelve a pedir la autenticación ya que se llega a la conclusión que es porque se ha fallado al escribirlo.

Al finalizar el proceso de asignación de VLAN, como ya se ha explicado en el capítulo 4, continuará con la obtención de IP mediante DHCP.

5.1.2 Red Wireless corporativa

Para el funcionamiento de la red Wireless corporativa se tendrán que combinar tres elementos: Packetfence, Active Directory y Meraki.

No se especificará el funcionamiento de la nueva red para invitados ya que el funcionamiento de ésta será el mismo que vemos en las Figura 4.3 de la sección 4.1.1.2. Solo cambiará el nombre del SSID que pasará a ser IEAISA_GUEST y el direccionamiento que otorgará, por lo tanto, al ser el mismo proceso de conexión, no se ha considerado oportuno añadir ninguna figura de su funcionamiento.

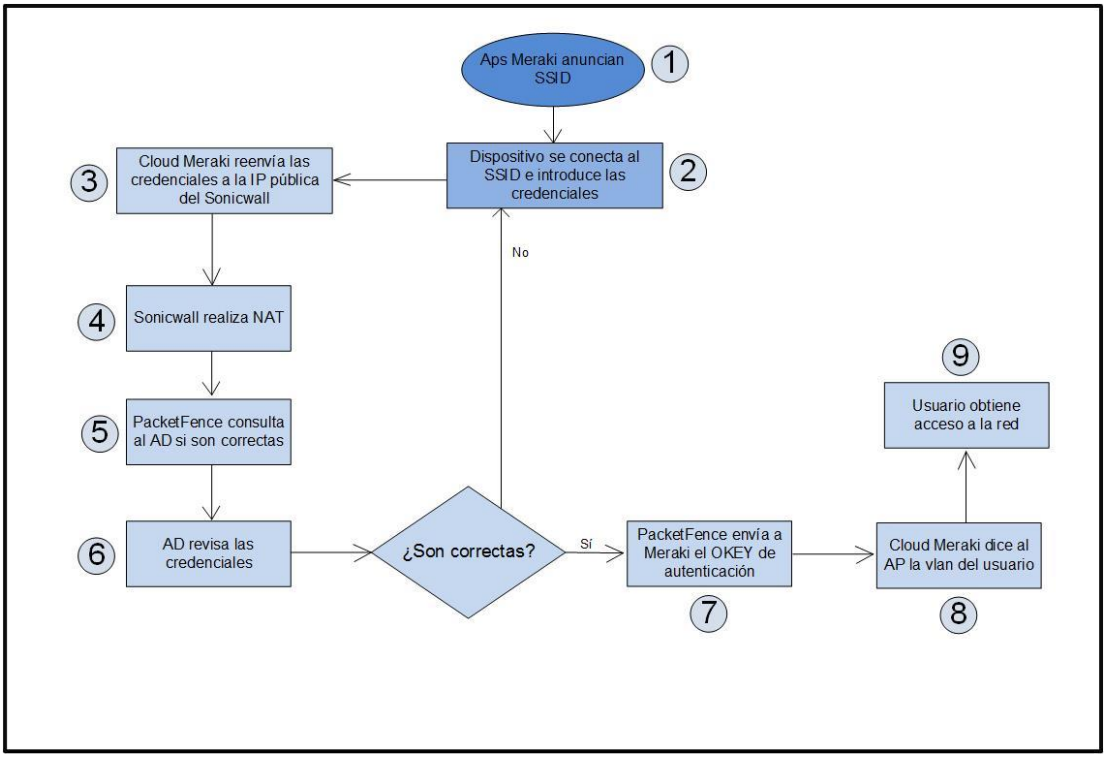


Figura 5.3 Esquema del nuevo funcionamiento de la red Wireless de IEAISA (1)

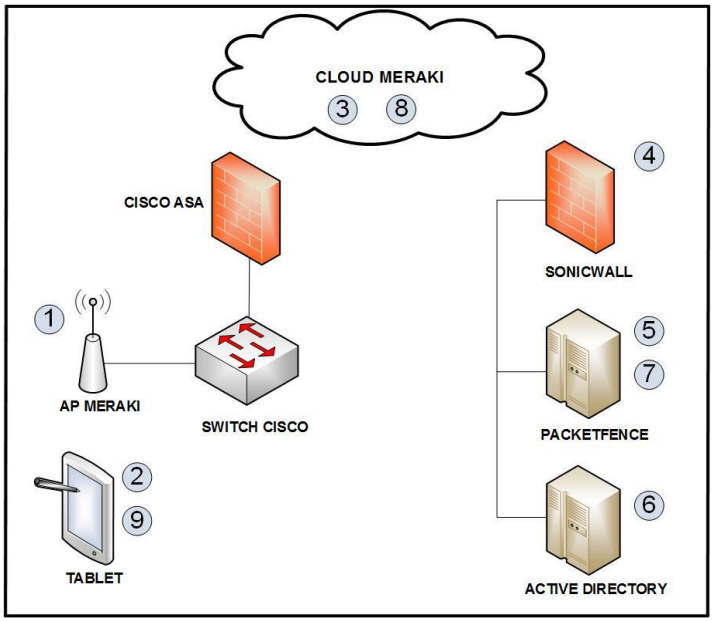


Figura 5.4 Esquema del nuevo funcionamiento de la red Wireless de IEAISA (2)

Como se ve en las Figuras 5.3 y 5.4, el proceso que seguirán los dispositivos que se quieran conectar a la wifi corporativa, seguirá el esquema que puede observarse. Es decir, cuando un usuario quiera conectarse a la wifi corporativa, se le pedirán las credenciales de acceso por LDAP, cuando las introduzca, el Cloud de Meraki pasará la información a Packetfence (se explica como hace este proceso en la sección 5.5) y éste hacia el Active Directory. Si las credenciales son correctas se le asignará la VLAN 50 (Wifi_Corporativo) y el usuario ya podrá acceder a internet y a los recursos compartidos de IEAISA.

Este proceso únicamente se realizará cuando el usuario quiera entrar en el SSID corporativo; para el guest, simplemente se le asignará la VLAN de wifi guest sin pasar por el Packetfence ni el Active Directory.

5.2 FIREWALL ASA

5.2.1 Configuración de nuevas VLANs

Como se ha explicado en el punto 4.2.1, para segmentar la red era necesario crear nuevos direccionamientos para las nuevas políticas que se iban a aplicar.

Para hacerlo se sigue el siguiente procedimiento.

1. Acceder al firewall por la IP de gestión https://172.26.0.2 y poner las credenciales correctas.
2. En Devices>DeviceManagement se selecciona el firewall de la oficina.

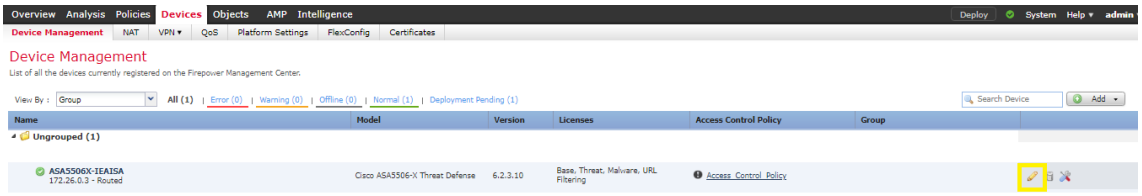


Figura 5.5 Selección del Firewall de la oficina en Cisco ASA Firepower

3. En el menú de Interfaces, se selecciona Add Interface>SubInterface, de esta manera se estará creando una VLAN dentro de la interfaz que se elija, en este caso, la eth1/1.

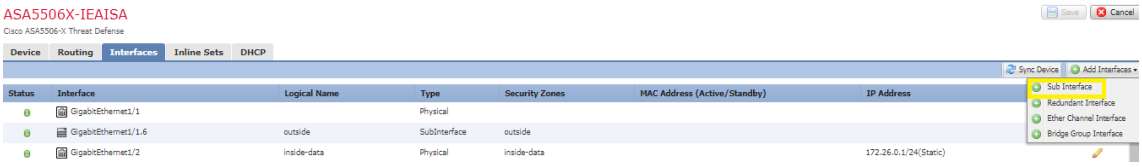


Figura 5.6 Creación de Subinterfaz VLAN

4. Se añaden los datos que se piden como la zona, descripción, dirección IP…

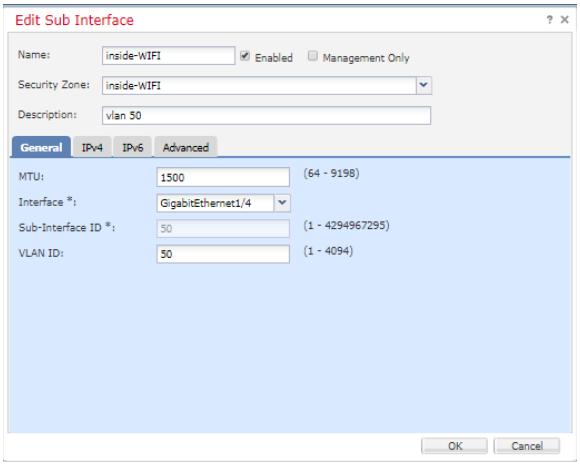
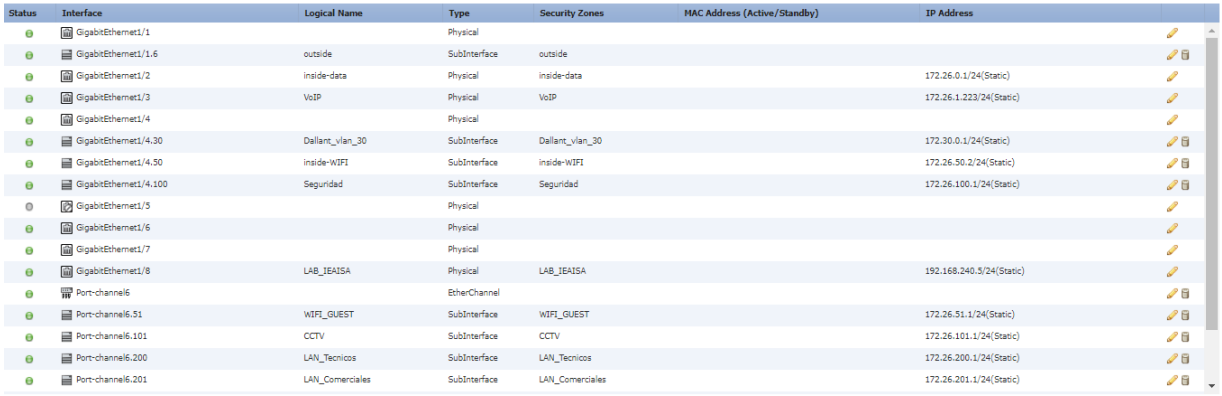


Figura 5.7 Datos necesarios para la creación de la VLAN

5. Se crean todas las nuevas VLANs que se habían especificado en los puntos anteriores



Status	Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
	GigabitEthernet1/1		Physical			
	GigabitEthernet1/1.6	outside	SubInterface	outside		
	GigabitEthernet1/2	inside-data	Physical	inside-data		172.26.0.1/24(Static)
	GigabitEthernet1/3	VoIP	Physical	VoIP		172.26.1.223/24(Static)
	GigabitEthernet1/4		Physical			
	GigabitEthernet1/4.30	Dallant_vlan_30	SubInterface	Dallant_vlan_30		172.30.0.1/24(Static)
	GigabitEthernet1/4.50	inside-WIFI	SubInterface	inside-WIFI		172.26.50.2/24(Static)
	GigabitEthernet1/4.100	Seguridad	SubInterface	Seguridad		172.26.100.1/24(Static)
	GigabitEthernet1/5		Physical			
	GigabitEthernet1/6		Physical			
	GigabitEthernet1/7		Physical			
	GigabitEthernet1/8	LAB_IEAISA	Physical	LAB_IEAISA		192.168.240.5/24(Static)
	Port-channel6		EtherChannel			
	Port-channel6.51	WIFI_GUEST	SubInterface	WIFI_GUEST		172.26.51.1/24(Static)
	Port-channel6.101	CCTV	SubInterface	CCTV		172.26.101.1/24(Static)
	Port-channel6.200	LAN_Tecnicos	SubInterface	LAN_Tecnicos		172.26.200.1/24(Static)
	Port-channel6.201	LAN_Comerciales	SubInterface	LAN_Comerciales		172.26.201.1/24(Static)

Figura 5.8 VLANs creadas para la nueva red de IEAISA

5.2.2 Configuración de VPN

Una vez creadas las nuevas VLANs, se necesitará que tanto la wifi-corporativa, LAN técnicos, Seguridad y LAN comerciales pasen por la VPN que nos une con el Cloud, ya que todos estos direccionamientos necesitarán acceder a algún recurso del Cloud. En este caso resulta más sencillo ya que se dispone de la VPN levantada previamente. Por ello, la realización de esta configuración se verá reducida considerablemente.

1. Se entra en el menú Objects>Objects Management y se filtra la búsqueda por nets_VPN_L2L_IEAISA, este es el objeto que se pasa por la VPN con las redes locales.

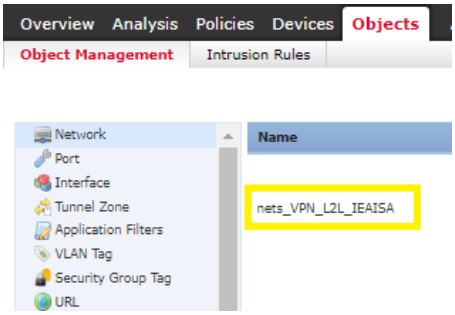


Figura 5.9 Objeto del Firewall ASA que contiene las redes internas de la oficina de IEAISA

2. Dentro del objeto, se añaden las nuevas interfaces creadas y se guarda, una vez hecho esto, solo faltará que el Sonicwall también conozca estas redes para que pueda enrutarlas debidamente.

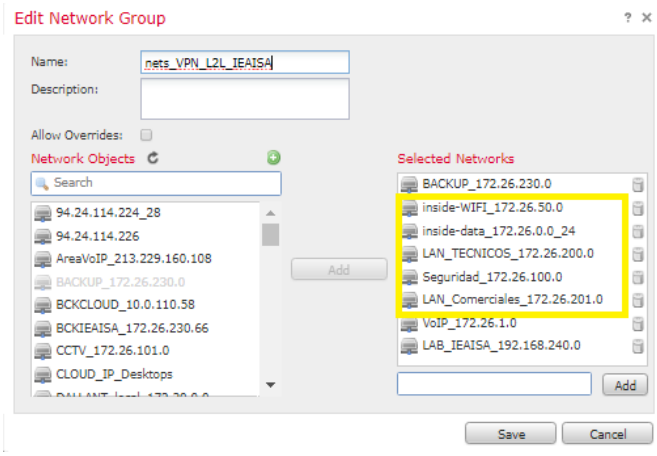


Figura 5.10 Asociación de objetos de las nuevas VLANs en el al grupo VPN

5.2.3 Creación de las reglas de acceso

Por último, se tendrán que configurar reglas de salida para que todas las nuevas VLANs puedan tener acceso a cualquier direccionamiento, en el caso de las que no pueden llegar a todos los recursos del Cloud, será desde el propio Sonicwall donde se limitaran estos permisos. Para la creación de nuevas reglas de acceso se sigue el siguiente procedimiento.

1. En el menú Policies>AccessControl seleccionamos para ver las reglas creadas, dentro del menú, se selecciona Add new rule y se rellenan los parámetros de la VLAN para que tenga acceso a todo.

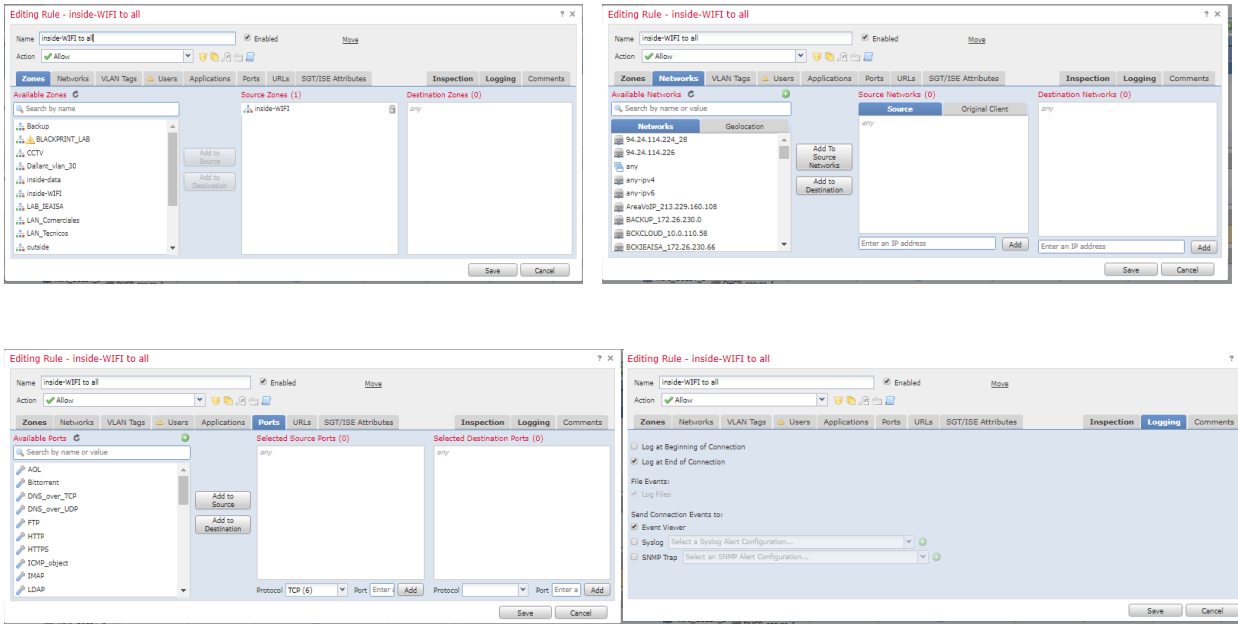


Figura 5.11Creación de regla de acceso para dar salida hacia internet a las nuevas VLANs

2. Se realiza lo mismo para el resto de nuevas VLANs creadas.

5.3 FIREWALL SONICWALL

Siguiendo los pasos de la sección 5.3.2, donde se ha creado el objeto con las nuevas VLANs para pasar por la VPN hacía el Cloud, lo primero que se ha de configurar en el Sonicwall son los objetos con las redes necesarias para poder enrutar el tráfico.

Otra configuración necesaria en este dispositivo es el NAT que se puede ver en la sección 5.1.2, necesario para la comunicación entre el Cloud Meraki y el Packetfence. Para realizar este NAT también se tendrá que crear las reglas de acceso pertinentes para que permitan el tráfico por los puertos especificados.

5.3.1 Nuevas redes por la VPN

Para realizarlo, se siguen los siguientes pasos.

1. Se accede al Sonicwall desde el Cloud por la IP 94.24.114.226 por HTTPS.
2. Se va al menú Network>Address Objects y se añade un nuevo objeto con una de las nuevas redes a crear.

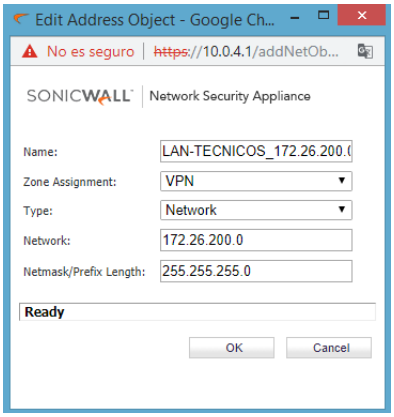


Figura 5.12 Creación de nuevo objeto en Sonicwall

3. Crear el resto de objetos necesarios.
4. Dentro del mismo menú, se va a la pestaña de Address Groups y se filtra por el nombre IEAISA_interna, este es el grupo de objetos que contiene todas las redes de la oficina que necesita conocer el Sonicwall y se pasan por la VPN. Dentro de este grupo, se añaden las mismas VLANs que se añadieron para el caso de ASA Firepower. Es importante que

sean las mismas ya que si por el túnel pasan redes diferentes entre un sitio y otro a veces los dispositivos no saben qué hacer y no levantan la VPN.

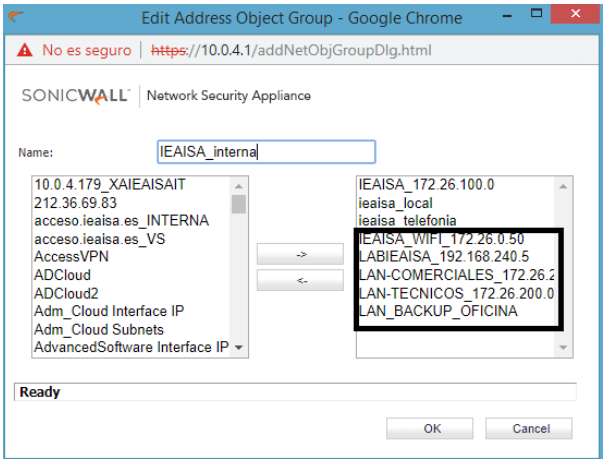


Figura 5.13 Asociación de nuevos objetos en el grupo de la VPN

5. Comprobar que el túnel sigue levantado correctamente dentro del menú VPN>Settings.

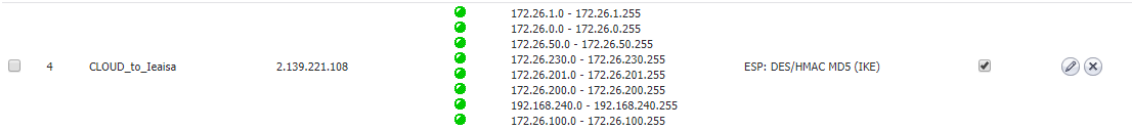


Figura 5.14 Túnel VPN levantado entre la oficina de IEAISA y el Cloud

Como puede verse en la captura, todas las redes se levantan correctamente después de la modificación del objeto.

5.3.2 NAT para Packetfence

Para realizar el NAT correspondiente siempre es importante saber IPs origen desde donde se atacará a la IP pública en este caso del Sonicwall, la IP pública del Sonicwall, la IP interna del dispositivo y porque puertos necesitará comunicarse. En este caso, mirando la documentación oficial de Meraki, vemos que su Cloud puede usar un rango diferente de IPs públicas para iniciar la comunicación. Este rango es el siguiente:

- 185.17.255.128/255.255.255.128
- 209.206.48.0/255.255.240.0

Conociendo estas IPs, se puede empezar la configuración del NAT siguiendo los siguientes pasos.

1. Se crean los objetos y seguidamente un grupo de objetos que contenga las IPs mencionadas anteriormente.

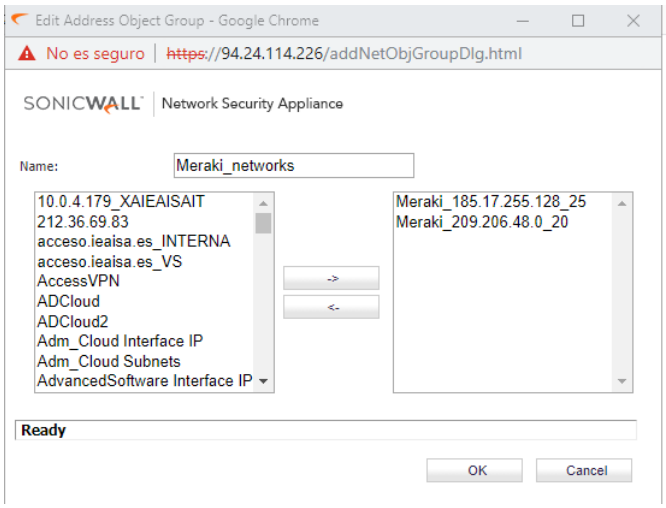


Figura 5.15 Creación del objeto con las IPs públicas de Meraki

2. En el menú Network>NAT Policies se crea el NAT pensado en las figuras vistas en la sección 5.1.2

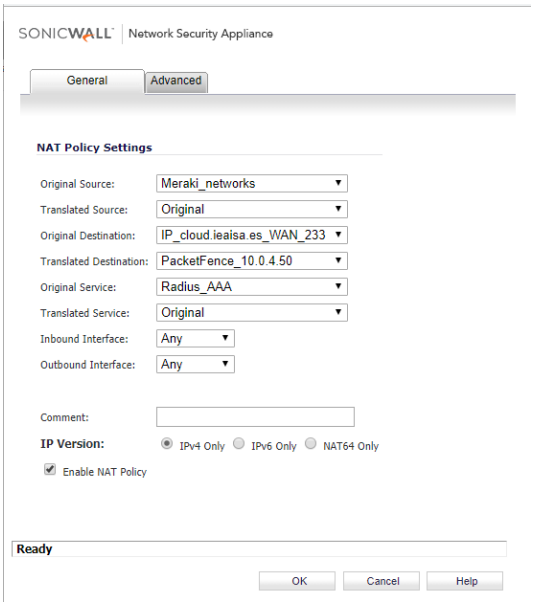


Figura 5.16 Creación del NAT para dar permitir la comunicación entre Meraki y el Sonicwall del Cloud

Como se puede ver, como Original Source se seleccionarían las IPs de Meraki y no se necesitaría traducción, como Original Destination se seleccionaría la IP pública donde atacaría la nube de Meraki (en este caso una IP pública del Sonicwall con dirección 94.24.114.223), y, como traducción, se tendría que redirigir ese tráfico hacia la IP interna del Packetfence (10.0.4.50). Por otro

lado, los puertos utilizados serían los que utiliza radius y radius accounting 1812 y 1813 UDP.

5.3.3 Access rules

Una vez realizado el NAT anterior se tendrá que habilitar la comunicación entre la IP pública a la cual se le realizará el NAT y las IPs públicas de Meraki, se ha de saber antes de ellos de que zona a que zona del firewall se producirá esta comunicación. Por lógica, las IPs de Meraki entrarán por la Zona WAN, pero todavía no se sabe en qué Zona está situado Packetfence, para realizar todo este proceso se siguen los siguientes pasos.

1. En el menú Network>Interfaces, se busca la red 10.0.4.0/24 para saber a qué Zona pertenece como se ve en la Figura 5.17.

Figura 5.17 VLAN 4 del Sonicwall en el Cloud

2. Una vez averiguado que la red se encuentra en la Zona IEAISA, en Firewall>Access Rules se tendrá que añadir una regla que permita el tráfico de la Zona WAN a IEAISA con origen las IPs públicas de Meraki y destino la IP pública de Sonicwall a la que aplicamos el NAT con los puertos nombrados anteriormente.

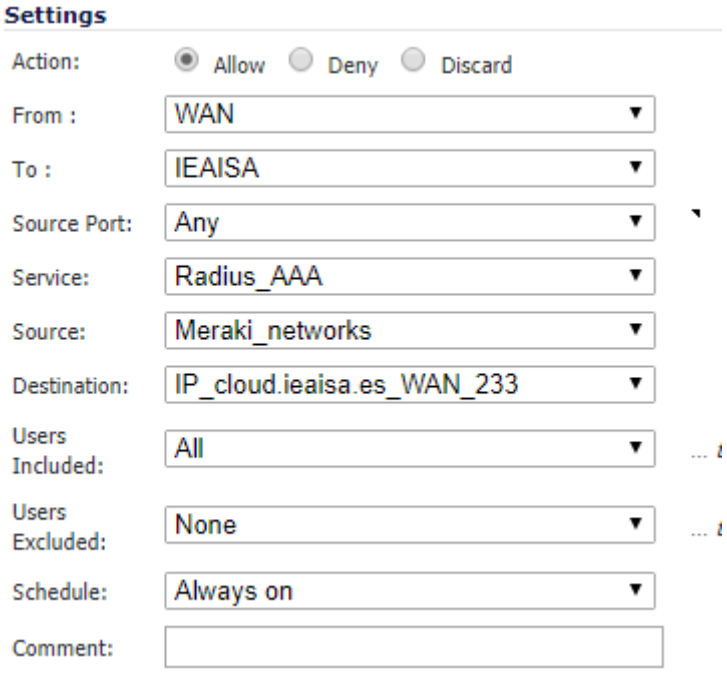


Figura 5.18 Regla de acceso que permite el tráfico entre Meraki y la IP pública

5.4 CLOUD MERAKI

Tal como se ha hablado en la sección 4.2.4, la red Wireless será cambiada por completo. Para ello, se tendrán que crear dos nuevos SSID cada uno con su configuración específica.

5.4.1 Creación SSID IEAISA_GEST

La configuración que se realiza en esta solución es muy diferente a otras que se ven para otros APs, esta se realiza toda a través de la gestión web por la nube, los pasos para poder dejar este SSID configurado son los siguientes.

1. Entrar en el Cloud Meraki a través de la web https://account.meraki.com y autenticarse con el usuario y contraseña
2. Ir al menú de Wireless y dentro de Configure entrar en SSID

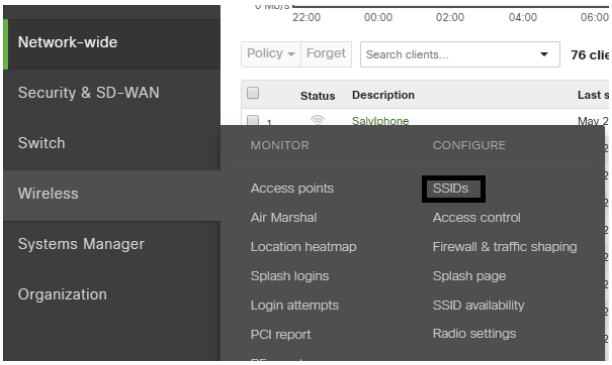


Figura 5.19 Menú SSID dentro del Cloud de Meraki

3. En esta pantalla se ven todas las SSID que están activas y todas las que se pueden configurar, se selecciona una vacía nombrándola en este caso con IEAISA_GUEST.

	IEAISA_COORP	IEAISA_GUEST
Enabled	disabled	enabled
Name	rename	IEAISA_GUEST
Access control	edit settings	edit settings
Encryption	WPA2-PSK	WPA2-PSK
Sign-on method	None	None
Bandwidth limit	unlimited	unlimited
Client IP assignment	Meraki DHCP	L3 roaming
Clients blocked from using LAN	no	yes
Wired clients are part of Wi-Fi network	no	no
VLAN tag	n/a	51
VPN	Disabled	Disabled
Splash page		
Splash page enabled	no	no
Splash theme	n/a	n/a
Custom splash URL	n/a	n/a

Figura 5.20 Configuración básica SSID IEAISA_GUEST

4. Una vez renombrado, dentro de edit settings, se configuran los diferentes parámetros como seguridad utilizada, clave de acceso, VLAN… Como se observa en la Figura 5.20, este SSID se ha configurado con Client assigment “L3 roaming”. Esta opción significa que el Cloud Meraki cederá el DHCP a la propia LAN. También se puede observar la VLAN asociada a este SSID (VLAN 51).

5.4.2 Creación SSID IEAISA

Este SSID para técnicos necesitará de una configuración más compleja para su correcto funcionamiento, se empezará desde el punto 4 de la sección 5.4.1 para no repetir los mismos pasos, es decir, se empezará una vez se entra en la propia configuración del SSID.

Dejar claro que estas configuraciones son específicas para la red de IEAISA y se configura acorde a las necesidades y recursos de la propia empresa, si nos encontráramos en otro entorno se tendrían que hacer de otra manera adaptándonos a las necesidades y equipos del escenario.

1. En la sección de Network Access, se selecciona la opción de Radius Server.

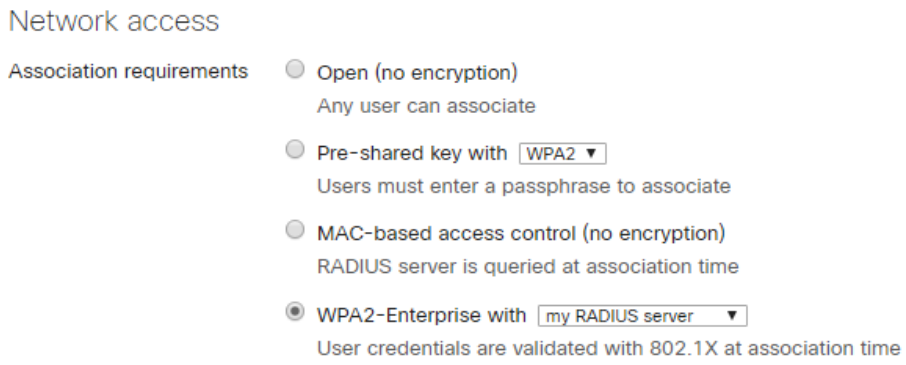


Figura 5.21 Selección de Radius Server para permitir la autenticación 802.1x

2. En Radius Setting, se introduce la IP pública del Cloud que redirige hacia Packetfence junto con la clave compartida que se configurará tanto aquí como en Packetfence (sección 5.6.5).

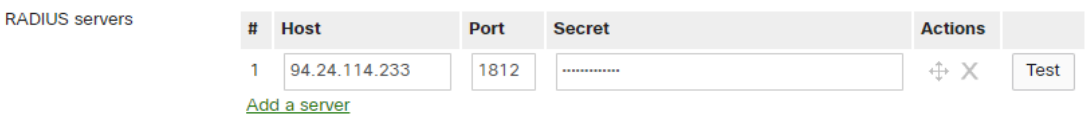


Figura 5.22 Configuración del Radius server

3. En Test, se comprueba que la conexión funciona correctamente probando cualquier usuario que exista en el AD.

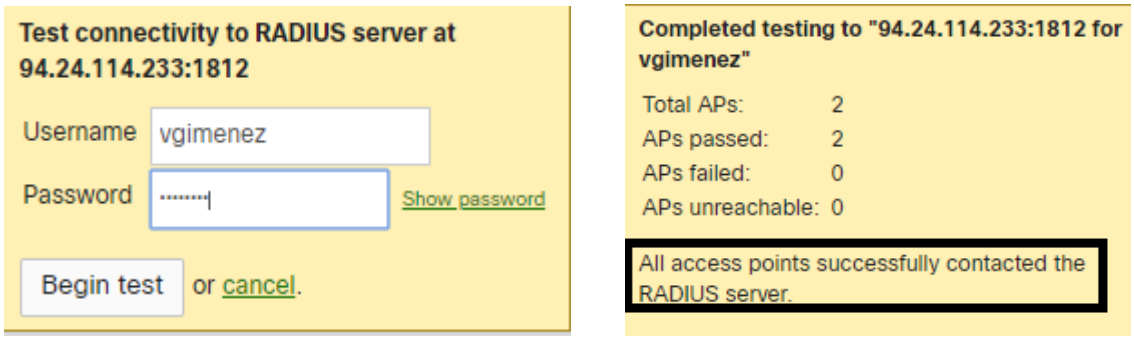


Figura 5.23 Comprobación de la correcta vinculación de Meraki con Packetfence y Active Directory

4. Se realiza la misma configuración en el apartado de Radius Accounting.
5. Se selecciona la opción Layer3 Roaming para que el DHCP lo haga un elemento de la red y no el propio Meraki.

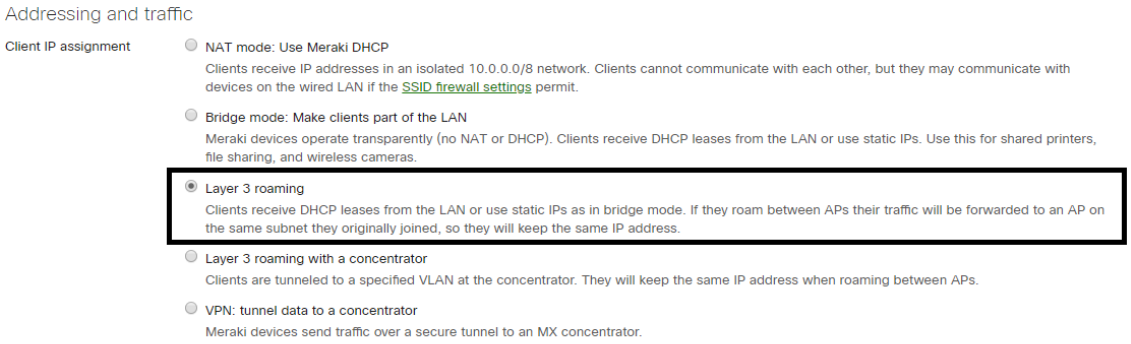


Figura 5.24 Configuración del DHCP para que lo realice el propio servidor interno de IEIASA y no el Cloud de Meraki

6. En el apartado de VLANs, se selecciona la VLAN 50, ya que ésta será la que se utilizará para la wifi de técnicos.

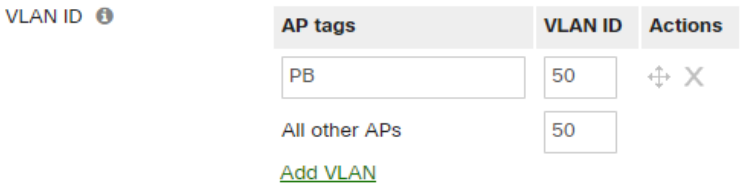


Figura 5.25 Selección de VLAN para el SSID IEAISA

5.5 ACTIVE DIRECTORY

El Active Directory no ha sido lo más nombrado a lo largo del proyecto, pero sin su configuración Packetfence solo reconocería un grupo de usuarios que es lo que tenía previamente a la realización del proyecto. Para crear un nuevo grupo y poder asignarle usuarios ya creados el procedimiento es el que vemos a continuación.

1. Lo primero será entrar en la unidad organizativa donde se quiere crear el nuevo grupo, se le da click derecho y se selecciona la opción crear nuevo grupo.

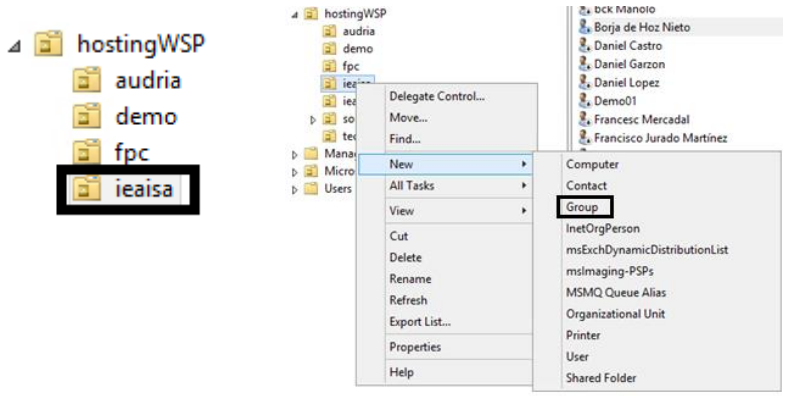


Figura 5.26 Menú principal de Active Directory donde se crearán los nuevos grupos

2. Utilizando el asistente de creación de grupos, se ponen todos los datos que se piden en la Figura 5.27.

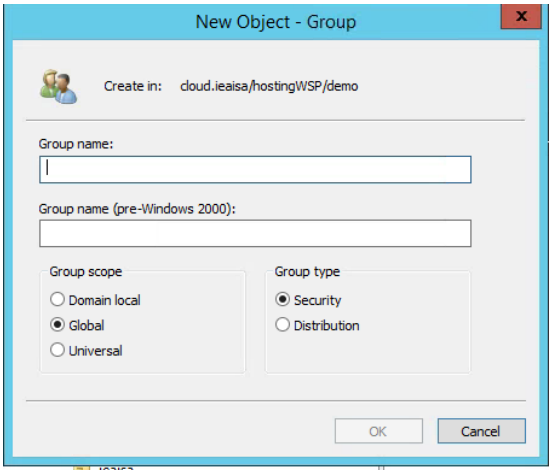


Figura 5.27 Datos requeridos para la creación de nuevo grupo en el Active Directory

3. Una vez que está creado el grupo, con el click derecho y en Properties se podrán añadir los usuarios que ya estaban creados a este nuevo grupo.

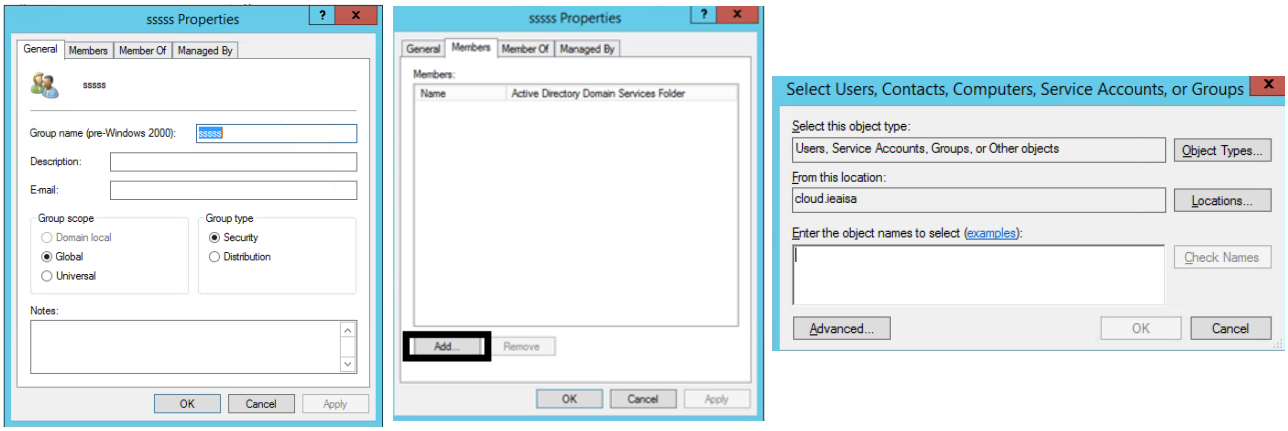


Figura 5.28 Asociación de usuarios con nuevos grupos en el Active Directory

Como se puede ver en la figura 5.28, para asociar un usuario al nuevo grupo creado únicamente se debería añadir el nombre en la última parte donde pide que se añada el nombre del objeto.

5.6 PACKETFENCE

Tal y como se ha explicado en el apartado 4.2.5, para llegar al funcionamiento correcto de esta solución se tendrán que seguir una serie de pasos.

5.6.1 Instalación de la OVA

Lo primero por razones más que obvias será proceder a la instalación de la OVA que se encuentra en la página "https://packetfence.org/download.html", una vez en ella, se descarga la OVA para RHEL 7.

Figura 5.29 Descarga de la OVA de Packetfence

Cuando está descargada, creamos la nueva máquina virtual en el Cloud en la Zona que se ha nombrado en la sección 5.3.3 y con la IP 10.0.4.50. Una vez

instalada, ya se podrá acceder a ella por ssh con user: root y password: p@ck3tf3nc3.

5.6.2 Configuración inicial

Una vez que se ha creado la máquina, ya se puede acceder a ella a través de la web http://10.0.4.50:1443/configurator para poder llevar a cabo la configuración inicial.

1. En el paso 1 se selecciona la opción de VLAN Enforcement, lo que hace esta es que Packetfence sea el encargado de asignar las VLANs a los usuarios, y, como se lleva explicando a lo largo del proyecto, esta es la opción que se necesita para el escenario al que se quiere llegar.

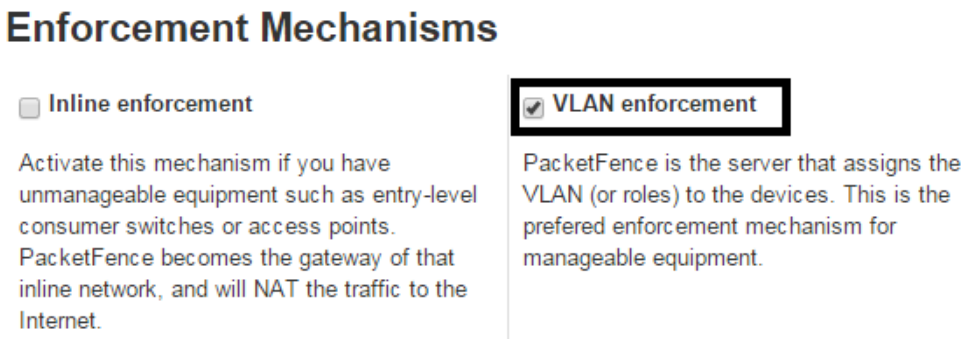


Figura 5.30 Paso 1 de la instalación de Packetfence, selección de opción para que Packetfence realice la asignación de VLANs

2. Se configuran las interfaces de red necesarias, para la infraestructura de IEAISA se configurará la interfaz eth0 con la IP 10.0.4.50/32 como la IP de Management de Packetfence.

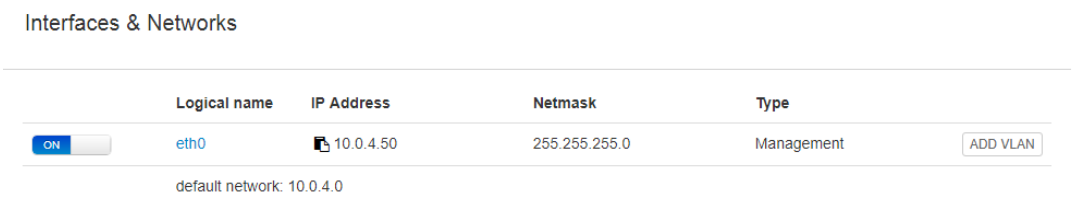


Figura 5.31 Asignación de IP de gestión para la solución Packetfence

3. Se crea la base de datos con un usuario y contraseña consultado previamente.

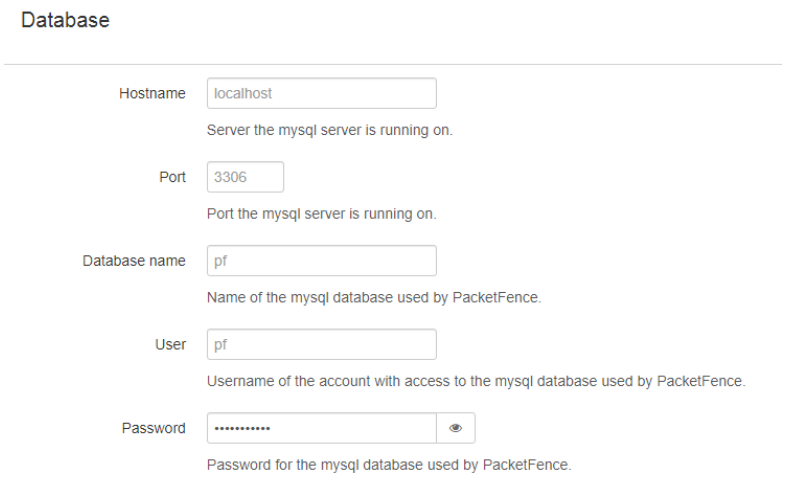


Figura 5.32 Creación de la base de datos de Packetfence

4. Se llega al punto de la configuración principal de Packetfence, en esta se elige un dominio, un nombre para la máquina que en este caso será la IP de gestión 10.0.4.50, los DHCP a los que preguntará, que son él mismo y el que se tiene internamente en el Cloud y el timezone.

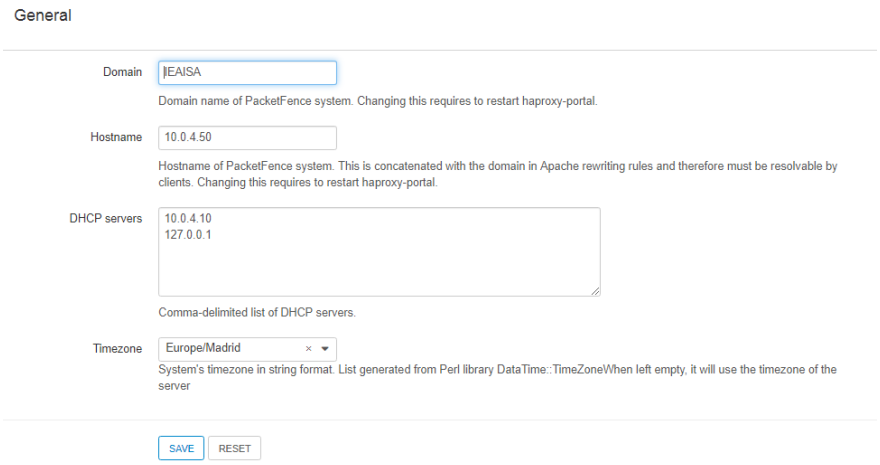


Figura 5.33 Último paso de configuración de Packetfence

5. Como se puede ver en la Figura 5.34, se inician todos los servicios que se necesitan en Packetfence.

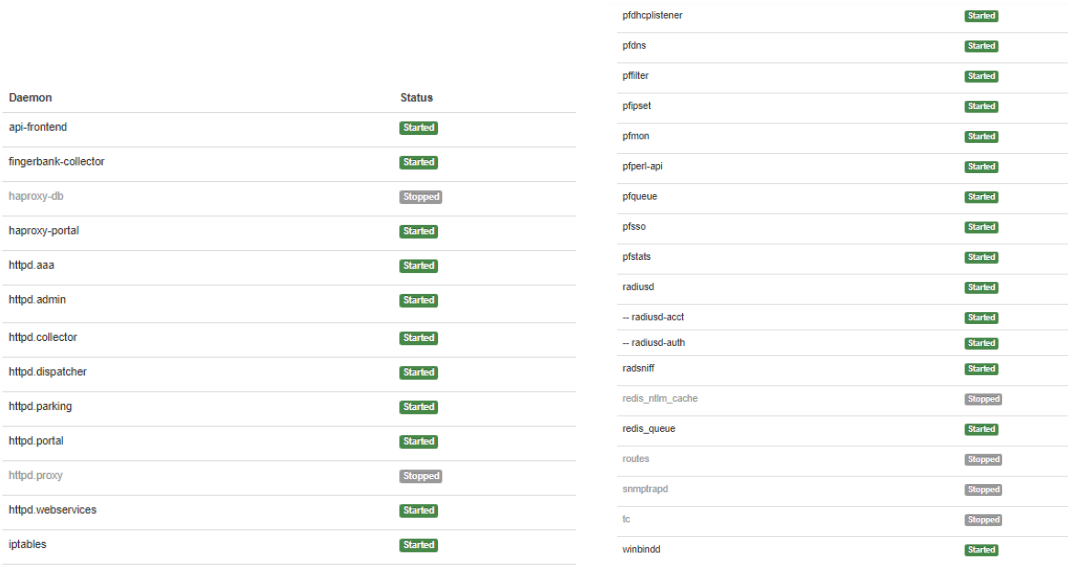
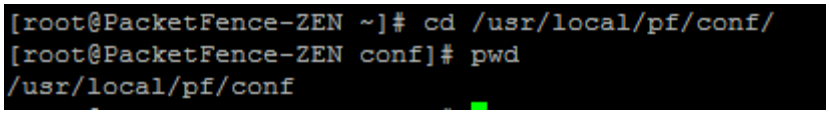


Figura 5.34 Servicios iniciados en Packetfence

Si hubiera algún problema en la configuración realizada en este último punto sería cuando la propia aplicación avisaría de ello. En el caso de esta instalación, no se sabe el motivo, pero el timezone no se acaba de configurar correctamente. Para solucionarlo, se entra por ssh a la máquina y se abre el archivo */usr/local/of/conf/pf.conf,* dentro de éste se modifica el timezone que no se ha configurado y se pone Europe/Madrid.



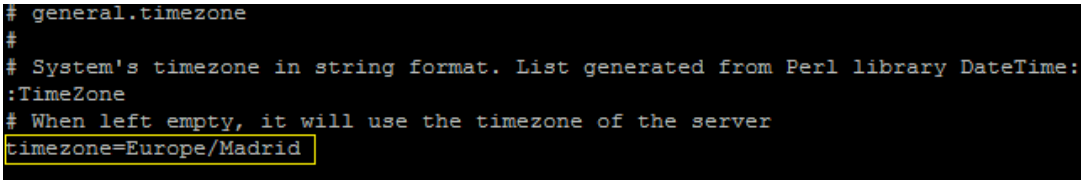


Figura 5.35 Configuración del timezone para que Packetfence lo coja correctamente

5.7.3 Vinculación con AD

Una vez hecha toda la instalación inicial, ya se podrá acceder por web a la administración principal a través de la url https://10.0.4.50:1443/admin, lo primero que se hará al acceder es cambiar el password por temas obvios de seguridad. Una vez hecho esto, para llevar a cabo la vinculación se realiza lo siguiente.

Dentro del Menú Configuration>Policy, en Domain se crea un nuevo dominio con nombre IEAISA.

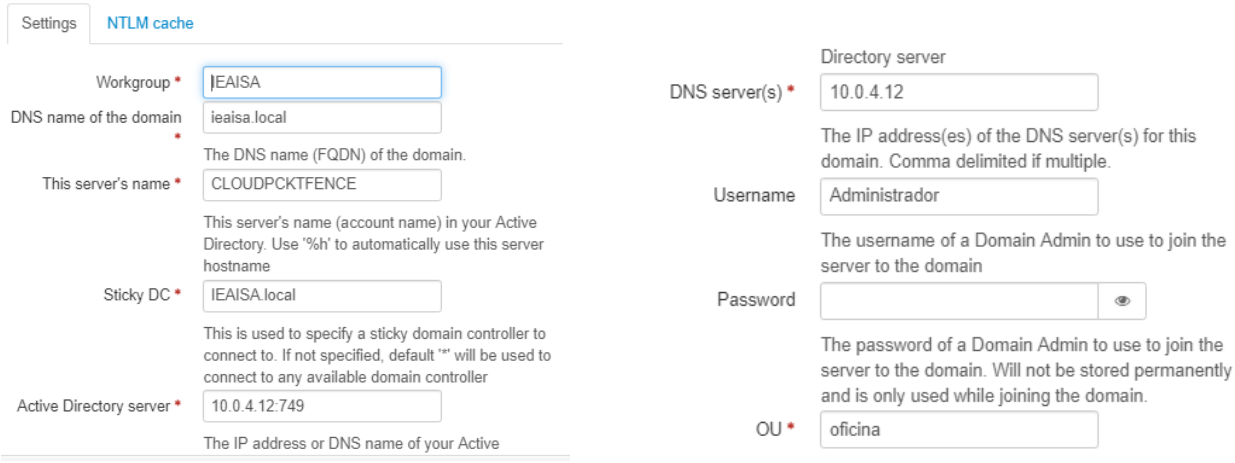


Figura 5.36 Asociación de Packetfence con el Active Directory de IEAISA

Los datos que se introducen como vemos en la Figura 5.36 serían el nombre que tendrá esta asociación dentro de Packetfence (IEAISA), en nombre del dominio DNS donde se querrá vincular, el nombre que tendrá la máquina dentro del AD, en este caso se pone CLOUDPCKTFENCE, la IP del AD donde vincularlo, y un username y password con permisos para poder realizar la vinculación entre estas dos máquinas.

Una vez rellenados todos los datos, se guarda y si consigue vincularse correctamente saldrá el mensaje que vemos en la Figura 5.37.

Figura 5.37 Vinculación entre Packetfence y Active Directory realizada con éxito

5.6.3 Creación de políticas

Una vez se ha vinculado el AD, se necesitarán hacer las políticas con las que se colocarán a los usuarios en una VLAN u otra dependiendo de en qué grupo del AD se encuentren.

Lo primero que se ha de saber es que para configurar las políticas que se quieren llevar a cabo en este proyecto en Packetfence se tendrán que configurar dos parámetros, uno de ellos es “Connection Profiles”, y el otro Authentication Sources.

El funcionamiento que seguirán será el siguiente. Cuando un endpoint se conecta consultará los Connection Profiles existentes y cogerá los parámetros del que concuerde con sus características, este proceso funciona como un firewall, las reglas se analizan de arriba hacia abajo, si se hace match en la primera regla de todas no seguirá analizando las siguientes. Una vez en un Connection Profile este lo redirigirá hacia el Authentication Source que tenga configurado, éste será el encargado de decidir qué VLAN se le asigna dependiendo de los parámetros que se necesiten. A continuación, veremos el ejemplo de configuración de los dos elementos nombrados que se ha realizado para la red cableada.

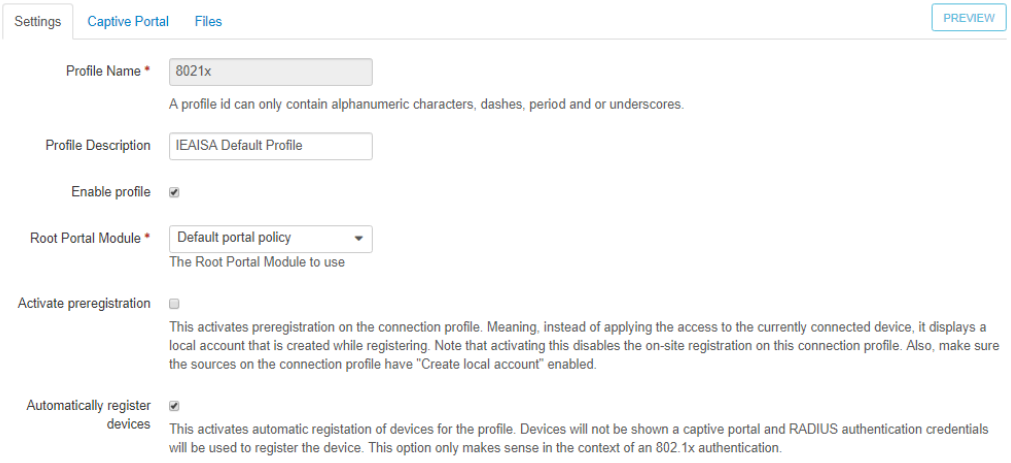


Figura 5.38 Configuración principal del Connection Profile para la red cableada

Para la configuración del Connection Profile lo primero que se hace es asignarle un nombre y una descripción. Acto seguido se marcará la opción “Automatically register devices”, que es la usada para la conexión 802.1X.

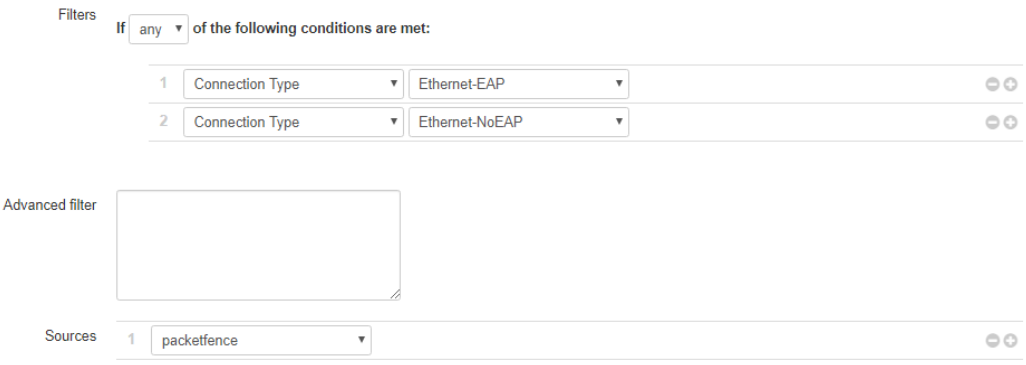


Figura 5.39 Condiciones para seleccionar este Connection Profile

Tal y como vemos en la Figura 5.39, en esta segunda parte se configura para que condiciones hará match en él, en este caso se configura que si la conexión

es Ethernet-EAP o Ethernet-NoEAP se quede en este perfil y lo mande al Authentication Source packetfence, tal y como se muestra en la Figura 5.40.

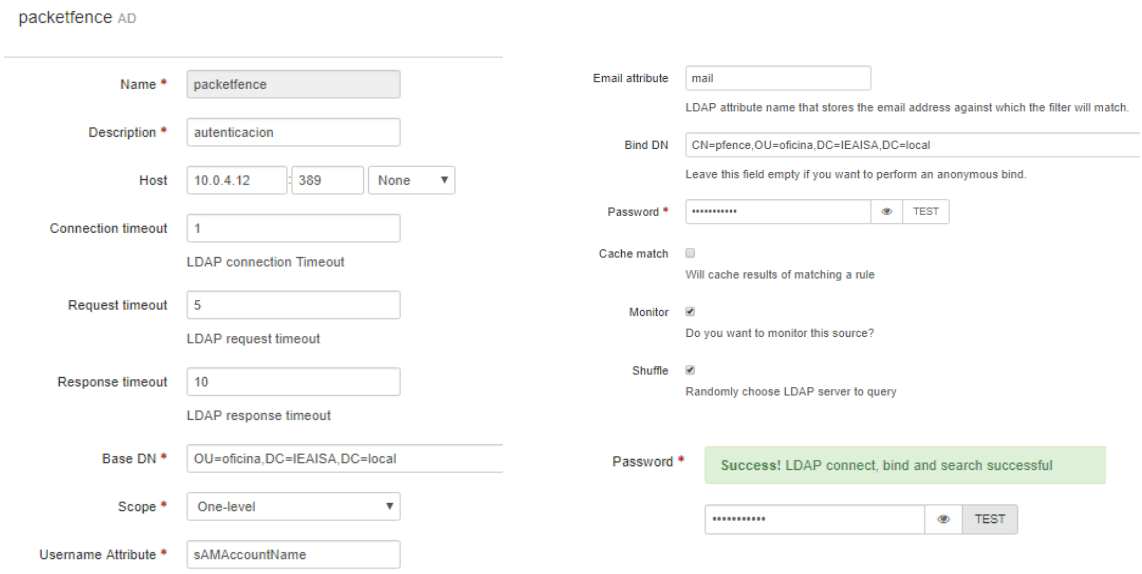


Figura 5.40 Configuración de Authentication Source packetfence

En esta parte del Authentication Source packetfence es donde se configuran los aspectos relacionados con la conexión al AD, como podemos ver, en la parte de BaseDN se le estará diciendo en que parte del AD tendrá que buscar los usuarios que se conecten, por otro lado, en la parte de Bind DN se pondrá el usuario con permisos que realizará la consulta a ese grupo del AD, para comprobar si el funcionamiento es correcto, dándole a TEST se verá si es capaz de comunicarse correctamente.

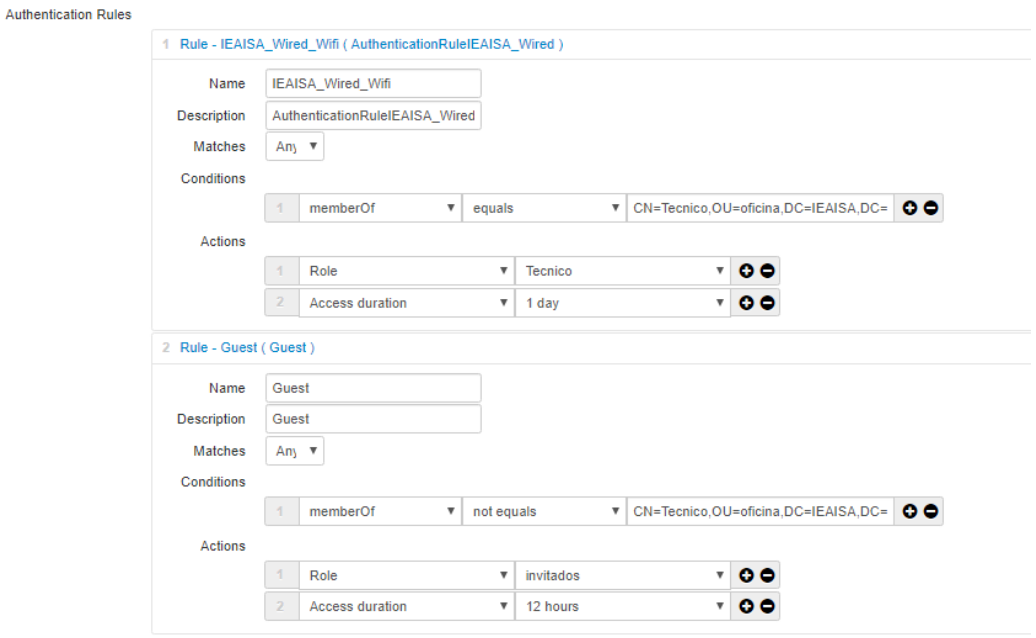


Figura 5.41 Configuración de las reglas dentro del Authentication Source

La última parte sería la configuración de las reglas. Como se puede ver en la Figura 5.41, la primera de ellas sería para el caso que la conexión fuera 802.1x y el usuario formará parte del grupo Técnicos. En este caso, si el usuario que introduce las credenciales está dentro del grupo Técnicos se le dará ese mismo rol y acceso durante un día. Si se da otro caso donde el usuario no introduzca ningún usuario se le dará el rol de invitados durante 12 horas. Con este procedimiento se conseguirá que cada usuario que introduzca credenciales tenga un rol en concreto dependiendo del grupo al que pertenezca.

5.6.4 Vinculación de dispositivos de red

Una vez el usuario que se ha conectado tiene un rol asignado, los encargados de asignarle un VLAN u otra serán los switches Cisco 2960 (Anexo A.1), por ello, será necesario establecer una conexión entre Packetfence y estos dispositivos.

Para hacerlo dentro del apartado de Configuration>Network Devices>Switches se tendrán que crear 2 tipos de dispositivos. Uno será los switches 2960, y el otro serán las IPs públicas del Cloud de Meraki.

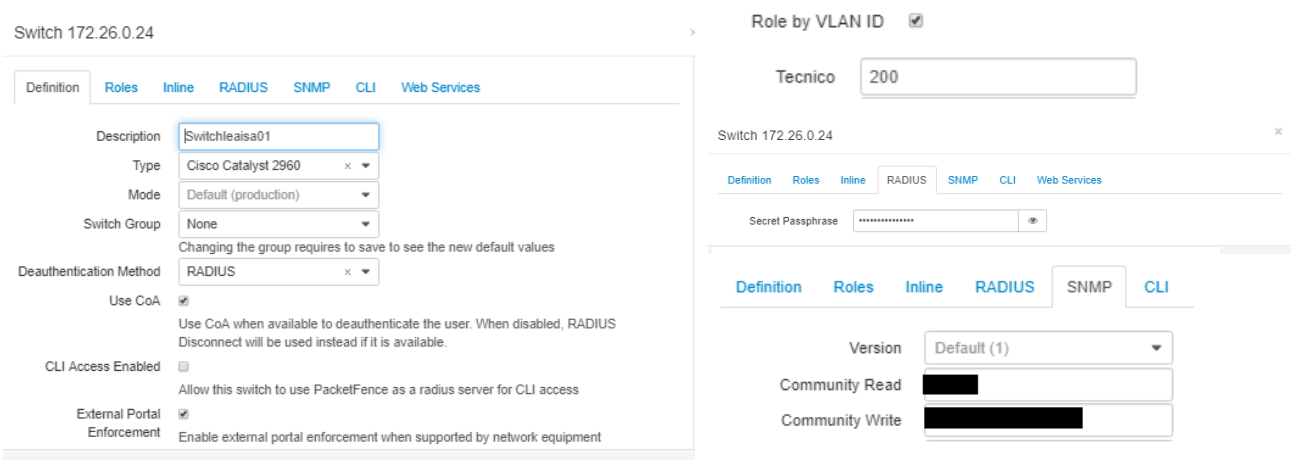


Figura 5.42 Vinculación de Packetfence con los switches 2960 de la oficina de IEAISA

Para el caso de los switches 2960 se introducirá primero la información general como IP, descripción… En la parte de Roles será donde se relacione cada rol que se ha asignado con una VLAN (en este caso se puede ver como en el rol Técnico del ejemplo anterior se le asignaría la VLAN 200). Por último, para establecer el vínculo se configura una clave Radius igual en los dos dispositivos y una comunidad snmp.

En el caso de los APs se realizará lo mismo, pero sin comunidad snmp y en la clave Radius se pondrá la que se configura en el apartado 5.4.2 cuando se realiza la configuración del SSID IEAISA.

CAPÍTULO 6. CONCLUSIONES Y TRABAJO FUTURO

6.1 CONCLUSIONES

La motivación de este proyecto nace de la necesidad de mejorar la infraestructura de red de IEAISA y protegerla frente ataques que se producen desde la misma red LAN de la empresa. El objetivo del proyecto de mejorar dicha seguridad y mejorar la infraestructura general se ha cumplido a través de la segmentación de la red y de la consecuente reconfiguración de muchos de los equipos. Además, se han tenido que estudiar diferentes opciones de mercado de la solución NAC para ver cual se adaptaba mejor a las necesidades de la empresa, llegando a la conclusión que Packetfence era la mejor opción posible.

Haciendo un estudio de la situación de la red actual y las mejoras que se querían llevar a cabo se ha pasado a la aplicación en el escenario real. Es decir, se han hecho todos los cambios que eran necesarios en todos los dispositivos para poder cumplir los objetivos. Con todo esto y la instalación y configuración de Packetfence se ha conseguido sacar mucho más partido a todos los elementos de la empresa. Se ha pasado de una red plana donde no había ningún tipo de distinción de tráfico (era lo mismo el tráfico de un servidor que de un usuario externo a la empresa que se había conectado a cualquier punto para navegar mientras realizaba una presentación), a una red segmentada donde se consigue que ese tráfico ya no vaya por la misma VLAN y sea la propia empresa y el equipo de ingenieros los que decidan que direccionamientos tienen acceso a unos recursos u otros.

Con la configuración también de los switches se ha conseguido que la red se autogestione de una manera eficiente. Con la nueva estructura de red, por lo tanto, el IT se encargará de configurar un usuario y contraseña para los trabajadores autorizados a conectarse a la red de la empresa y asignando su pertenencia a uno de los grupos VLAN. Hay que decir que en el caso de que un usuario en concreto necesitara más permisos dentro de su VLAN, la solución sería realizar una regla específica para su dispositivo en los Firewalls para que obtuviera el acceso que necesita.

Por último, al conseguir esta mejora en la parte LAN junto con otras mejoras a parte de este proyecto, la empresa IEAISA ha podido obtener los certificados ISO 27001 y 27017, los cuales entregan a la empresa un prestigio a nivel de seguridad de la información muy alto y permiten acceder a un abanico de clientes a los que no accedían antes.

Para concluir, la tecnología NAC ofrece el empujón necesario para que muchas empresas den el paso para remodelar y dar un salto en la seguridad de su red. Aunque exista desde hace años la tecnología NAC empieza a implantarse ahora en muchas empresas y por eso es actualmente cuando se le está sacando el máximo partido a esta solución.

6.2 TRABAJO FUTURO

Como se ha nombrado en la sección 6.1, la solución NAC actualmente está consiguiendo un aumento de su utilización en muchas empresas. Es por ello por lo que este proyecto ha servido a IEAISA para poder introducirse en este sector del mercado. Es por ello que tras acabarlo han salido diferentes proyectos complementarios que se comentarán a continuación.

- Conseguir filtrar acceso en IEAISA por Sistema Operativo a través de Packetfence.
- Denegar el acceso a la red a los usuarios que tengan componentes de su dispositivo desactualizado a través de Packetfence.
- Instalación de Packetfence para un nuevo cliente de índole mediana de IEAISA. Este proyecto surgió mientras se realizaba la configuración de esta solución en IEAISA y se evaluó si era posible realizarlo en su red. Actualmente está en proceso la propuesta de proyecto y se prevé empezarlo antes de final de este año 2019.
- Instalación de una solución NAC de pago, más concretamente, Cisco ISE para una empresa de gran tamaño. En este caso, las soluciones gratuitas no podían aportar lo que el cliente solicitaba.

Como se puede apreciar, la realización de este proyecto ha permitido abrir ofertas de trabajo y de investigación a corto plazo. En un futuro más largo se espera que vaya creciendo la demanda de esta solución y que, como en el caso de este proyecto, eso incluya una remodelación de las redes de las diferentes empresas.

BIBLIOGRAFIA

[1] Ciberataques en España: un tercio de usuarios fue víctima en 2018 - enero de 2019.
https://www.tuyu.es/ciberataques-mas-comunes-en-espana-2018/.

[2] Top 5 cybercrimes in the U.S, from the Norton Cyber Security Insights Report - Último acceso junio de 2019.
https://us.norton.com/cyber-security-insights-2018--

[3] Seguridad industrial 2018 cifras - enero de 2019.
ttps://www.incibe-cert.es/blog/seguridad-industrial-2018-cifras

[4] ¿Qué es BYOD? Ventajas e inconvenientes - diciembre del 2013.
https://computerhoy.com/noticias/moviles/que-es-byod-ventajas-e-inconvenientes-7250

[5] Nuuno Mensah, Henry, etal. A review of Opensource Network Acces Control Tools for Enterprise Educational Networks. International Journal of Computer Applications 106(6) - diciembre de 2014

[6] Seguridad en la información. Modelo 802.1x - Último acceso junio de 2019
https://www.youtube.com/watch?v=Wv16F1LXcxc

[7] Network Access Control - Último acceso junio de 2019
https://en.wikipedia.org/wiki/Network_Access_Control

[8] Fortinet - Último acceso junio de 2019
https://www.fortinet.com/

[9] OpenNac - Último acceso junio de 2019
http://www.opennac.org/opennac/en.html

[10] Packetfence - Último acceso junio de 2019
https://packetfence.org/

[11] Bonete, Samuel. NAC, una solución real. Boletín de RedIRIS, número 82-83 - abril de 2008.
https://www.rediris.es/difusion/publicaciones/boletin/82-83/ponencia1.3D.pdf

[12] Configuración Cisco ASA - Último acceso junio de 2019
https://www.w0lff4ng.org/configuracion-basica-cisco-asa/

[13] Configuración NAT policies Sonicwall - Último acceso junio de 2019
https://www.sonicwall.com/support/knowledge-base/?sol_id=170505782921100

[14] Cisco Meraki suport - Último acceso junio de 2019
https://meraki.cisco.com/support/

[15] Packetfence error timezone - Último acceso junio de 2019
https://sourceforge.net/p/packetfence/mailman/message/20231661/

[16] Cisco ISE - Último acceso junio de 2019
https://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/datasheet-c78-738846.html

ANEXOS

REMODELACIÓN DE LA RED LAN DE IEAISA A TRAVÉS DE SOLUCIÓN NAC

TITULACIÓN: Grado en Ingeniería de Sistemas de Telecomunicación

AUTOR: Víctor Giménez Porcell

DIRECTOR: Héctor Rodríguez Carro

FECHA: 17 de junio de 2019

ANEXO A. CONFIGURACIONES ADICIONALES

A.1 Configuración en Switch 2960

Para poder vincular el switch 2960 y Packetfence se tuvieron que llevar a cabo una serie de configuraciones adicionales.

Además, la configuración de los puertos de usuarios cambió para adaptarse a la nueva función que requería la red.

A.1.1 Backup antiguo de la configuración

La configuración básica que tenía previamente a la realización de este proyecto el switch era la siguiente.

```
version 15.0
no service pad
service timestamps debug datetime localtime
service timestamps log datetime localtime
no service password-encryption
hostname IEAISA_SW01
boot-start-marker
boot-end-marker
enable secret 5 $1$G7S.$RO.6v7kFK20z6sEF1Py.N/
username ieaisa password 0 sw1tch0f1c1n@.%#$
aaa new-model
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 1 priority 4096
vlan 1
  name Tecnicos
interface Port-channel1
 description Portchannel con Cisco_ASA
 switchport mode trunk
interface GigabitEthernet1/0/5
 switchport mode Access
swtichport Access voice vlan 10
 ip arp inspection trust
 ip dhcp snooping trust
interface GigabitEthernet1/0/43
 description to_ASA5506X
 switchport mode trunk
 channel-group 1 mode on
interface GigabitEthernet1/0/44
 description to_ASA5506X
 switchport mode trunk
 channel-group 1 mode on
```

Como se puede ver está configurado el username y password, el spanning tree y después se define la VLAN 1 como la principal de la red. La interfaz G1/0/5 es un ejemplo de cómo sería cualquier puerto de usuario donde se configura la VLAN por defecto y, a parte, la VLAN que usará la telefonía IP. Por último, se puede ver el portchannel 1 configurado en modo trunk que será el encargado de unir el switch con el firewall ASA por los puertos g1/0/43 y g1/0/44.

A.1.2 Configuración añadida una vez instalado Packetfence

Una vez se llevó a cabo la instalación de la solución NAC Packetfence se tuvieron que modificar diversos aspectos en la configuración del switch.

- Añadir nuevas VLANs que se han creado en el ASA. Es necesario que si ha de existir una comunicación entre esas VLANs por toda la red estén creadas también a nivel 2 en el switch.

Figura Anexo 1. Configuración a nivel 2 de las nuevas VLANs

- Creación de comunidad snmp para comunicarse con el Packetfence. Como se ha explicado en la sección del proyecto 5.6.4, Packetfence necesitará comunicarse con el switch para poder pasarle la información necesaria de los usuarios que se conecten a la red.

Figura Anexo 2. Configuración de la comunidad snmp

- Configuración del radius-server para establecer conexión también con Packetfence.

```
radius-server host 10.0.4.50 auth-port 1812 acct-port 1813 timeout 2 key Packetfence2018
radius-server vsa send authentication
```

Figura Anexo 3. Configuración del servidor Radius

- Configuración de los puertos.

```
switchport mode access
switchport voice vlan 10
shutdown
authentication order dot1x mab
authentication priority dot1x mab
authentication port-control auto
authentication periodic
authentication timer restart 10800
authentication timer reauthenticate 10800
mab
no snmp trap link-status
dot1x pae authenticator
spanning-tree portfast
end
```

Figura Anexo 4. Nueva configuración de los puertos de usuario

Como se ve en la Figura Anexo 4, esta sería la configuración básica que tendría un puerto una vez en funcionamiento la solución Packetfence. Tiene varios más parámetros que la configuración antigua y las funciones más importantes que tiene son las siguientes.

- Authentication order dot1x mab → habilita la autenticación dot1x y mab
- Authentication priority dot1x mab → primero intentará realizar la conexión mediante 802.1x y si no lo consigue intentará la conexión mab
- Authentication port-control auto → port-control puede configurarse de tres maneras diferentes.

A.2 Configuración Fingerprint en Packetfence

Fingerprint es un proceso de recopilación de información que permite identificar el SO del dispositivo que se conecta a la red. Es capaz de ello examinado el tráfico que se genera, en el caso de este proyecto, haciendo un DHCP relay donde se reenvié el paquete además de al servidor DHCP a Packetfence, Fingerprint será capaz examinando este paquete de extraer el SO además de otras características del dispositivo que está estableciendo la conexión.

Para su configuración, dentro de la web de Packetfence se entra al menú Configuration>Compliance.

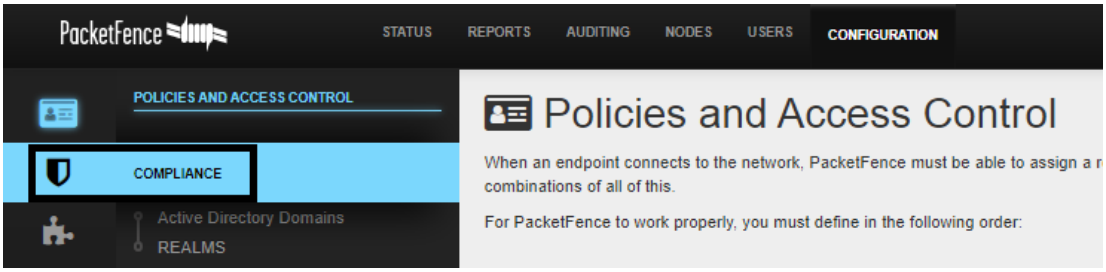


Figura Anexo 5. Menú para la configuración de Packetfence

Dentro de General Setting, se tendrá que crear una cuenta en GitHub para poder acceder a este recurso. En el caso de este proyecto, se crea una de “networkingieaisa”.

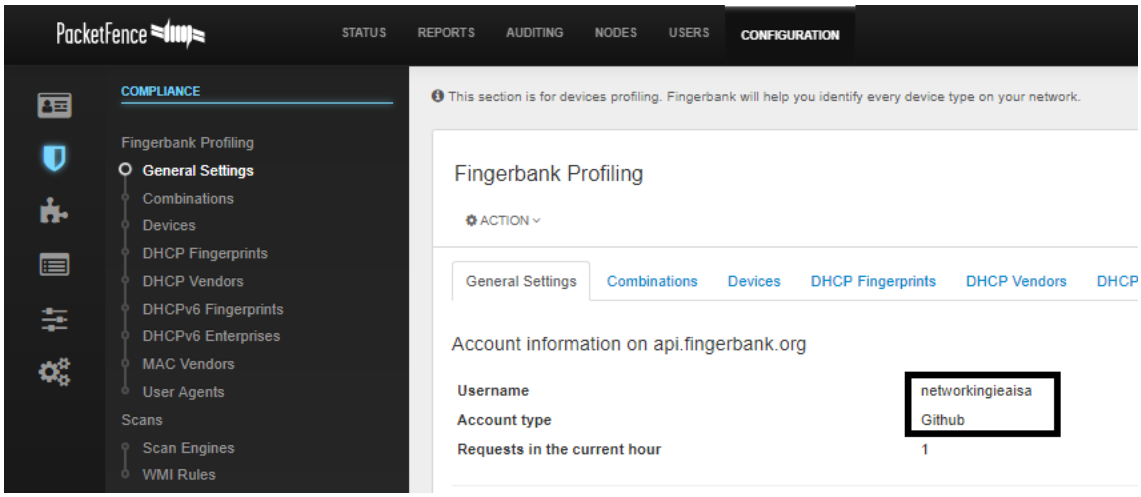


Figura Anexo 6. Vinculación de cuenta de Github con Packetfence Fingerprint

Una vez hecho esto se nos dará una API key y podremos configurar los aspectos básicos como puertos de escucha, colector HTTPS y otros aspectos que podemos ver en la Figura Anexo 7.

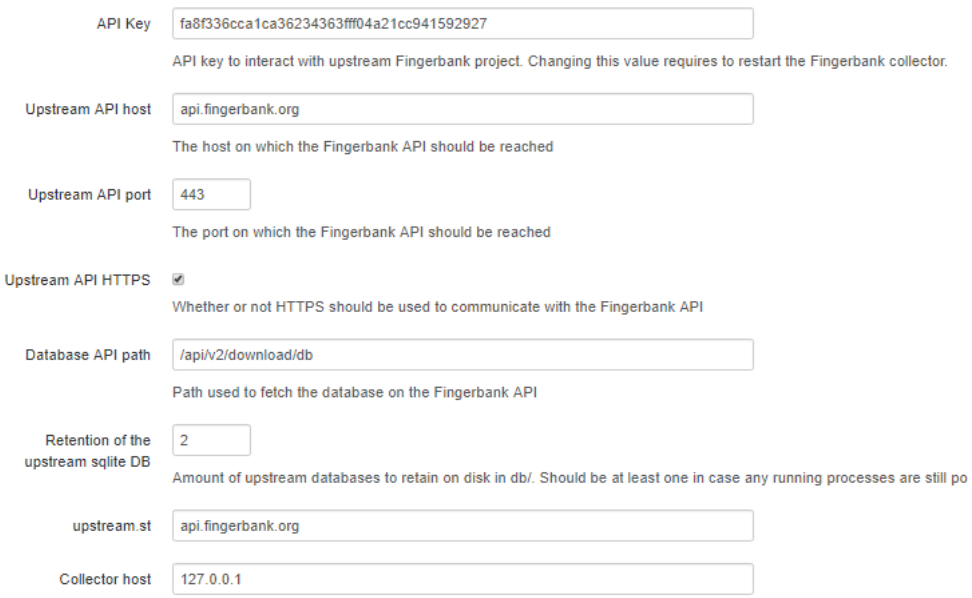


Figura Anexo 7. Configuración de parámetros de Fingerprint

Si la API key no la coge correctamente como paso en el caso de este proyecto se tendrá que ir a */usr/local/fingerbank/conf* y modificar el archivo *fingerbank.conf* de la manera que vemos en la Figura Anexo 8.

```
[upstream]
api_key=fa8f336cca1ca36234363fff04a21cc941592927
st=api.fingerbank.org
port=443
use_https=enabled
db_path = /api/v2/download/db
sqlite_db_retention = 2


[query]
record_unmatched=enabled

[collector]
host=127.0.0.1
port=4723
use_https=enabled
inactive_endpoints_expiration=168
arp_lookup=disabled
query_cache_time=1440
db_persistence_interval=60
cluster_resync_interval=120
```

Figura Anexo 8. Configuración de fingerbank.conf

Una vez configurado hecha toda esta configuración, tendrá que hacerse el DHCP relay en el ASA (se ve en la sección de anexos A.3). Si todo funciona correctamente en los logs ya aparecerá como se extraen datos de los dispositivos que se conectan.

```
PacketFence-ZEN fingerbank-collector: [GIN] 2019/06/10 - 17:17:03 | 200 |     136.634µs | 127.0.0.1 |   GET     /endpoint_data/00:50:56:aa:59:f3
PacketFence-ZEN fingerbank-collector: [GIN] 2019/06/10 - 17:17:03 | 200 |      92.797µs | 127.0.0.1 |   GET     /endpoint_data/00:50:56:aa:59:f3
PacketFence-ZEN fingerbank-collector: [GIN] 2019/06/10 - 17:17:04 | 200 |     126.839µs | 127.0.0.1 |   GET     /endpoint_data/00:50:56:aa:59:f3
PacketFence-ZEN fingerbank-collector: [GIN] 2019/06/10 - 17:17:04 | 200 |     139.985µs | 127.0.0.1 |   GET     /endpoint_data/00:50:56:aa:59:f3
PacketFence-ZEN fingerbank-collector: [GIN] 2019/06/10 - 17:17:06 | 200 |       148.3µs | 127.0.0.1 |   GET     /endpoint_data/00:50:56:aa:59:f3
```

Figura Anexo 9. Logs de Fingerpint mostrando como saca información de los dispositivos

Para ver realmente que se están cogiendo datos de los dispositivos conectados, en la web de Packetfence en la parte de Auditing si se hace click en cualquier dispositivo conectado en la parte de Fingerprint nos aparecerá la MAC del dispositivo y el tipo de SO que es junto con otros detalles.

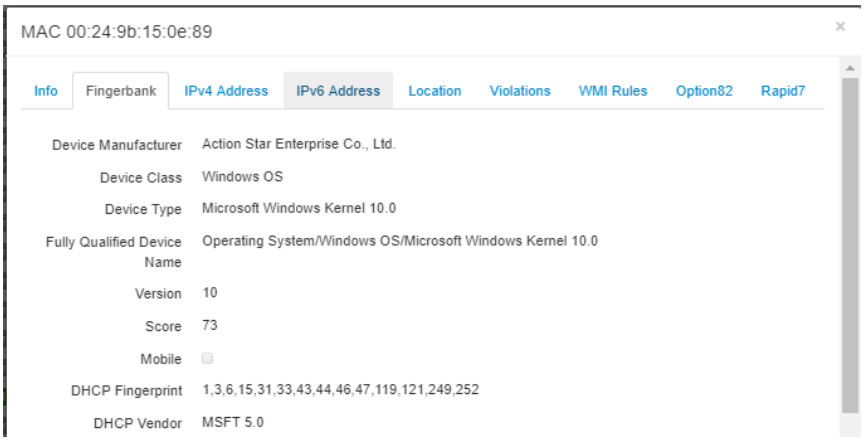


Figura Anexo 10. Comprobación de los datos que extrae Fingerprint de un dispositivo cualquiera

A.3 Configuración DHCP Relay en Cisco ASA

Como se ha dicho en el apartado anterior, para poder llegar a obtener la información de los dispositivos Packetfence necesita que le llegue una copia del paquete DHCP. Para hacer esto posible se ha de ir al Firewall ASA y realizar la siguiente configuración.

Dentro del apartado Devices>Devices Management se tendrá que seleccionar el firewall de la oficina.

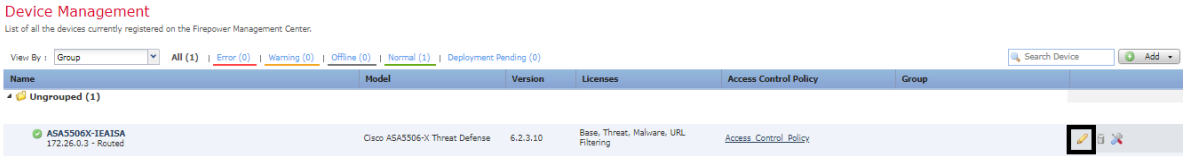


Figura Anexo 11. Menú para entrar al Firewall Cisco ASA

Dentro de este se tendrá que ir a la sección DHCP>DHCP Relay>DHCP Servers y añadir Packetfence además del servidor DHCP de la oficina para que también se le envié el paquete.

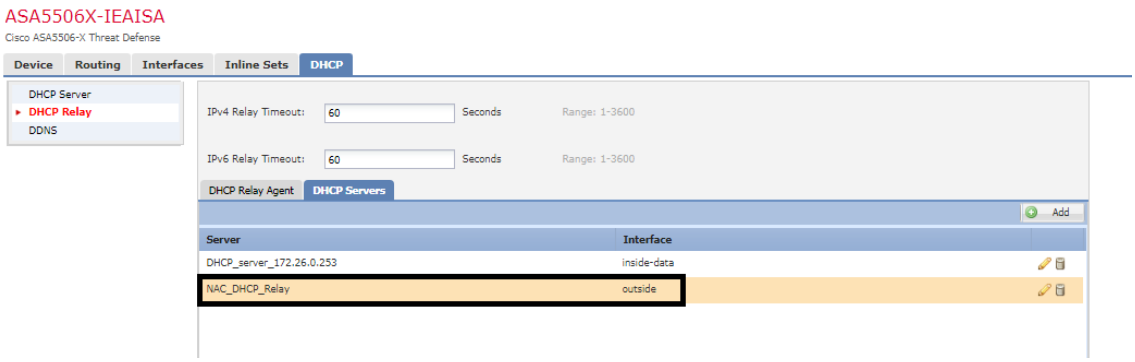


Figura Anexo 12. Packetfence forma parte del DHCP Relay además del servidor

Como vemos en la Figura Anexo 12, en la parte de Interface se selecciona la outside debido a que se encuentra en el Cloud.

A.4 Configuración 802.1X en PC

A.4.1 Configuración en Windows

Para el escenario de este proyecto, la configuración en el SO Windows para que acepte la autenticación 802.1x es la siguiente.

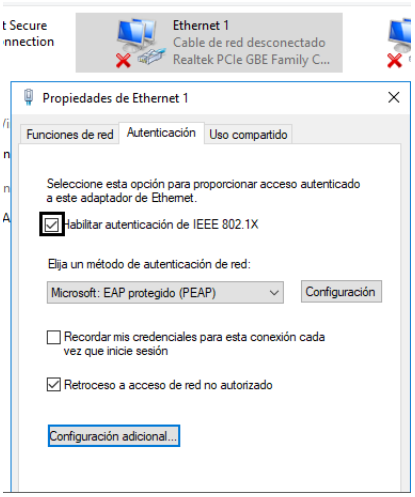


Figura Anexo 13. Habilitar configuración 802.1x

Como se ve en Figura Anexo 13, lo primero es dentro de configuraciones del adaptador de red, se marca la opción de Habilitar la autenticación de IEEE 802.1x.

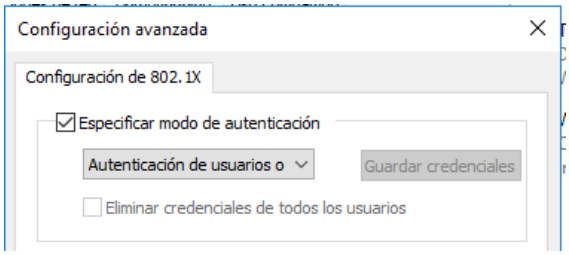


Figura Anexo 14. Configuración addicional

Dentro de configuración adicional, nos aparecerá un menú como se ve en la Figura Anexo 14. Dentro se selecciona especificar modo de autenticación y la opción de Autenticación de usuarios o equipos.

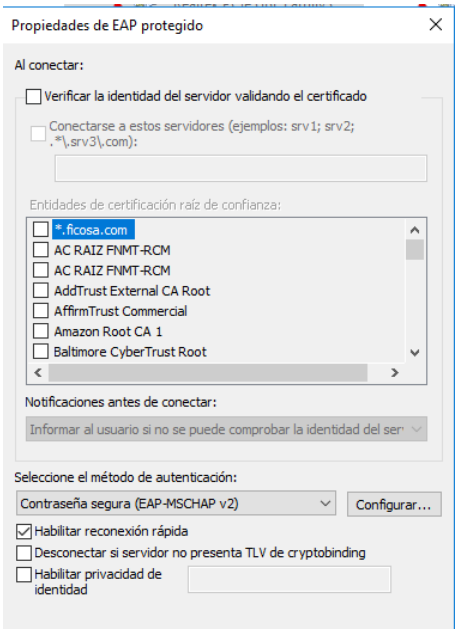


Figura Anexo 15. Menú configuración de las opciones 802.1x

Dentro del menú Configuración, se desmarca la opción de Verificar la identidad del servidor y se deja el método de autenticación por defecto.

Antes de finalizar, al no tener los PCs en dominio dentro del método de autenticación>Configurar, se quita la opción de utilizar automáticamente el nombre de inicio de sesión. Si en un futuro se ponen todos los PCs en dominio, esta opción se tendría que marcar para que no se pidiera usuario y password.

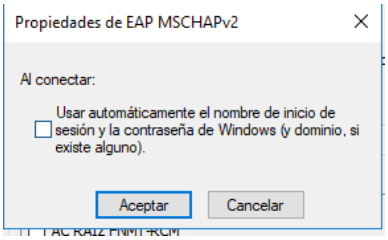


Figura Anexo 16. Configuración para que se pida autenticación al conectarse por cable

A.4.2 Configuración en Linux

Para la configuración de 802.1x en Linux, el procedimiento será más sencillo que para el anterior caso.

Únicamente se tendrá que crear una nueva conexión con los valores que se detallan en la Figura Anexo 17.

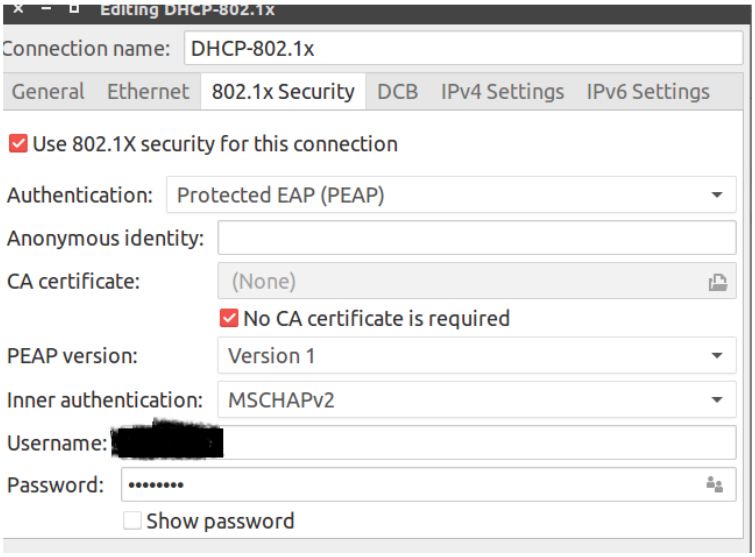


Figura Anexo 17. Valores para conectarse por cable a la red de IEAISA

ANEXO B. EJEMPLO DE FUNCIONAMIENTO

Para ver el comportamiento final de la red se pondrá un ejemplo de conexión de un técnico de redes en un puerto cualquiera de la oficina.

No se explicará todo el proceso que sigue la conexión una vez un usuario se conecta a la toma de red debido a que se ha ido explicando a lo largo de todo el proyecto, simplemente se mostrarán las capturas que se obtienen tanto del switch como del Packetfence en este proceso de conexión.

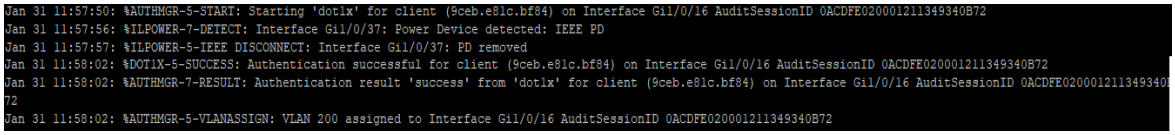


Figura Anexo 18. Logs del switch Cisco 2960 al recibir una conexión por cable con 802.1x activado

En la Figura Anexo 18. se puede ver como realiza la conexión el switch cuando se conecta un usuario a una toma. Como se puede ver, lo primero que hace es iniciar la autenticación dot1x, para iniciar esta autenticación con éxito es necesario haber realizado el procedimiento de la sección A.4. Una vez el usuario introduce el usuario y contraseña el switch enseña que la autenticación ha sido correcta para el cliente con la dirección MAC mostrada. Para finalizar, se ve como se le asigna la VLAN 200 a este puerto y el usuario ya podrá navegar con el direccionamiento de dicha VLAN.

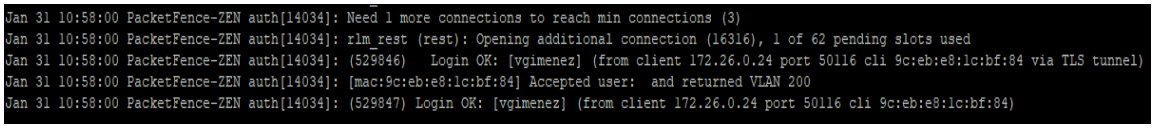


Figura Anexo 19. Logs de Packetfence al recibir notificación de autenticación por parte del switch

En el caso de la Figura Anexo 20. se puede ver la autenticación que se lleva a cabo paralelamente en Packetfence. Aquí se ve como el usuario vgimenez se autentica correctamente y se le asigna la VLAN 200 de Técnicos.

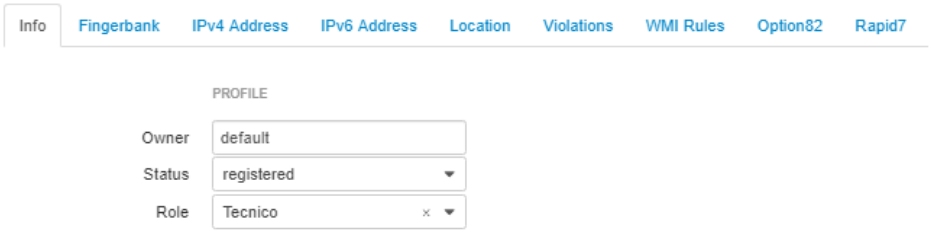


Figura Anexo 20. Conexión a través de 802.1x del usuario vgimenez

En la web de Packetfence en información puede verse si tiene el estado de registrado y en que rol lo ha colocado, en este caso se ve que sí que está registrado y está situado en el rol de Técnico.

ANEXO C. EJEMPLOS REPORTS PACKETFENCE

Tal y como se ha dicho en la sección 3.3 donde se comparaban las soluciones NAC que se habían seleccionado, Packetfence ofrece una serie de reports atractivos para el usuario final. En este apartado se verán unos pocos que se han seleccionado para demostrarlo.

C.1 INFORMACIÓN INTERNA DE PACKETFENCE

Para poder saber como está el estado de la máquina, packetfence ofrece una serie de reports que se pueden ver en la Figura Anexo 21. Entre ellos hay la carga del sistema, el espacio en disco y la RAM utilizada entre otros.

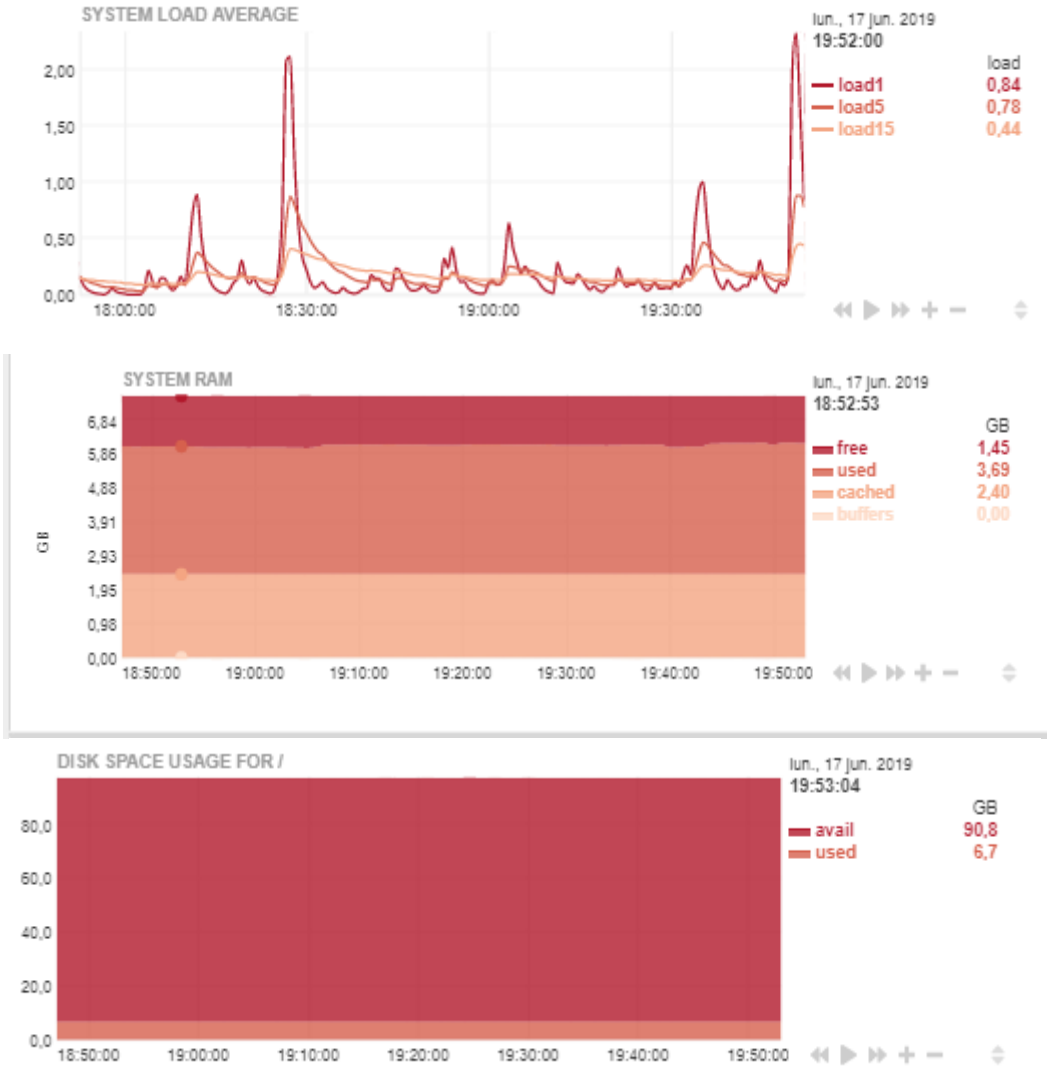


Figura Anexo 21. Reports de Packetfence internos

C.1.1 INFORMACIÓN SOBRE LA BASE DE DATOS

Packetfence también proporciona datos sobre su base de datos interna donde se ven las peticiones que se realizan en tiempo real.

Figura Anexo 22. Información sobre la base de datos de Packetfence

C.2 INFORMACIÓN SOBRE DISPOSITIVOS DE LA RED

Además de la parte de Auditing que hemos visto en otras partes del proyecto como en la de Anexo A.2, Packetfence ofrece unos reports sobre los dispositivos que se conectan a la red.

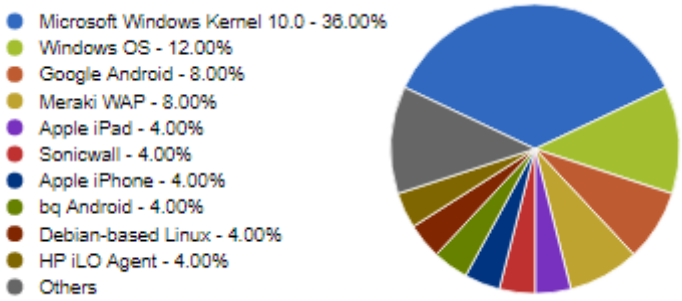
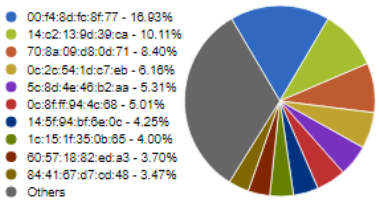
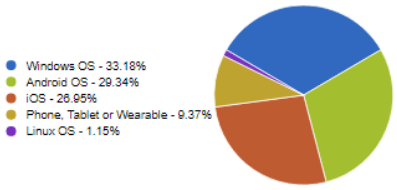


Figura Anexo 23. Sistemas operatives conectados a la red



MAC Address	Total
00:f4:8d:fc:8f:77	5.63 GB
14:c2:13:9d:39:ca	3.36 GB
70:8a:09:d8:0d:71	2.80 GB
0c:2c:54:1d:c7:eb	2.05 GB
5c:8d:4e:46:b2:aa	1.77 GB
0c:8f:ff:94:4c:68	1.67 GB
14:5f:94:bf:6e:0c	1.41 GB
1c:15:1f:35:0b:65	1.33 GB
60:57:18:82:ed:a3	1.23 GB
84:41:67:d7:cd:48	1.15 GB

Figura Anexo 24. Ancho de banda consumido por MAC



DHCP Fingerprint	Total
Windows OS	11.56 GB
Android OS	10.22 GB
iOS	9.39 GB
Phone, Tablet or Wearable	3.27 GB
Linux OS	410.45 MB

Figura Anexo 25. Ancho de banda consumido por Sistema Operativo

Además de estos y muchos otros, Packetfence permite realizar algunos reports personalizados que se adapten a las necesidades de cada usuario.